Politics and Governance
2026 • Volume 14 • Article 12300
https://doi.org/10.17645/pag.12300

cogitatio

ARTICLE

Open Access Journal

Security–Resilience (Con)Fusion: Governance and Legal Risks in Baltic Sea Energy Infrastructure

Eneken Ellinor Tikk [1,2]

[1] Faculty of Management and Business, Tampere University, Finland
[2] Institute of Computer Science, University of Tartu, Estonia

Correspondence: Eneken Ellinor Tikk (eneken.tikk@ut.ee)

Submitted: 28 February 2026 **Accepted:** 6 July 2026 **Published:** 6 November 2026

Issue: This article is part of the issue "The Politics of Resilient and Just Energy Transitions: Institutions and Critical Infrastructure" edited by Pami Aalto (Tampere University) and Marco Siddi (Finnish Institute of International Affairs / University of Cagliari), fully open access at https://doi.org/10.17645/pag.i489

Abstract

Resilience and security have become undeniable governance imperatives—sometimes attaining similar, near-synonymous, connotations in contemporary security strategies. Long-term investments in dual-use civilian and military infrastructure and functions, like drone walls or surveillance-equipped wind power parks, result in closer handshakes between resilience and security in democratic societies. However, how these two concepts interrelate in practice—i.e., which of them becomes the dog and which becomes the tail—is a matter of great importance to the ability of societies to govern their affairs in a sustainable, fair, and democratic manner. The fusion of resilience and hard security through the co-investment, co-location, and co-engagement of civilian and military investments, infrastructure, and functions carries significant political and legal risk for infrastructure operators, including the possibility of harm to the civilian population and objects. The obfuscation of civilian and military roles and capabilities entrenches a risk-averse security culture and erodes democratic measures and processes and may in that way build strategic advantage for authoritarian adversaries. Preoccupied with the blending of security and resilience in wind energy infrastructure in the Baltic Sea region, the article calls for scrutiny of relevant decisions and applicable legal frameworks. It bridges the literature on Polish and Swedish policy approaches to civil–military collaboration in the energy sector with the international legal literature on dual-use objects and civil–military accountability to reveal unresolved legal challenges acute in the Baltic Sea region.

Keywords

civil–military nexus; critical infrastructure; dual use; resilience; securitization; security

© 2026 by the author(s), licensed under a Creative Commons Attribution 4.0 International License (CC BY).

1. Introduction

In a climate of hostilities, instability, and unrest, handshakes are frequent between civilian and military resources, mandates, and procedures. National guards on the streets, industry involvement in the mitigation of politico-military risks, politically motivated disruptions of civilian services and infrastructure, as well as the normalization of crisis-time governance and decision-making are all examples of a narrowing civilian space and the expansion of a military one—militarization, as some may express the tendency (Åhäll, 2016), or securitization, as framed by others (Buzan et al., 1998; Silva & Pereira, 2024; Wæver, 1995). Cyber-attacks, cable sabotage, GPS disruptions, and instrumentalized migration all feature a combination of politico-military objectives with the exploitation of civilians and/or civilian infrastructure in peacetime (Kapsokoli, 2025). The ad hoc availability of the Starlink communication platform in Russia's war against Ukraine, Microsoft's assistance to Ukraine's cyber defence, and the functioning of Ukraine's cyber army are examples of inserting novel and significant civilian components in armed conflict. Moreover, to bolster resilience, security, and defence through civil–military cooperation and co-investment, it is attractive to complement defence forces' needs and capabilities with industry solutions, for instance in the fields of imagery and AI capabilities (European Commission, 2025a).

This article looks at the growing civilian–military nexus and its legal and political implications in the Baltic Sea area. The Swedish and Polish approaches to wind energy infrastructure will serve as examples of diverging policy approaches. The emphasis here is that the trends of military and civilian co-location, co-investment, and co-engagement are as acute in Europe as they are in other parts of the world. Political tensions invoke new civilian–military calculus in countries at the receiving end of provocation and influence operations. European policies and strategies are revisiting the concept of civil and defence interaction to address the deteriorating security environment following Russia's aggression against Ukraine and to boost the EU's capacity to protect its citizens and infrastructure, notably by enhancing the resilience and cyber protection of strategic dual-use infrastructure such as ports, airports, bridges, tunnels, and transport-relevant energy infrastructure (European Commission, 2025b). There appears to be preparedness and willingness in private companies to join forces with governments beyond the traditional client–provider relationship in addressing security issues and politico-military risk, as earlier observed by Cohen and Cohen (2022), Coveri et al. (2025), Bitzinger (2021), and Cusumano (2023).

Despite attention to the theme in the past decades, the contours of the feasibility and sustainability of increased civil–military cooperation remain to be clarified (Has, 2025; Huskey, 2012; Minow, 2005; Ulrich, 2021). However, for liberal democracies, the tendencies of mixing military and civilian interests and assets come with several challenges: the potential domination of military and defence interests over private investment prospects; the competition between civilian and security roles and mandates; the expectation that political risk is at least partially absorbed by industry and private companies; and, overwhelmingly, the necessity of making decisions about co-location and co-engagement of civilian and military resources (Brooks, 2025; Coveri et al., 2025).

Hard security, as understood here, refers to state-centric measures designed to deter or counter existential threats and is typically the preserve of governmental security and defence authorities. Resilience, by contrast, extends these concerns outward to encompass the adaptability and continuity of companies, civil society, and the broader population. The fusion of resilience and security concerns unsettles common understandings,

as well as legal and political conventions, of what is military and what is civilian—hence the confusion. This article revisits the civil–military nexus with a focus on the blurring line between the concepts of security and resilience in global governance processes, and on relevant political challenges in Europe. It does so with the example of the emerging practices around energy infrastructure in countries surrounding the "Lake NATO"—an informal designation reflecting the Baltic Sea's status as an effectively NATO-controlled maritime space following Sweden and Finland's accession to the Alliance in 2023–2024. The diverging views of Poland and Sweden on the balance between military and civilian interests in the context of wind energy infrastructure location and investments present a challenge for other countries in the region: which practice should be followed, or do the differing views on the subject need to be reconciled?

Framing the question as one of security and resilience governance, this article makes two contributions to the discussion. First, it shows that international policy processes and agendas are shifting away from conceptual clarity regarding security and resilience. Second, it examines the legal risks associated with these trends and highlights the fragmentation of the relevant remedies and solutions. In sum, the article seeks to inform further debate on the now-normalizing civil–military collaboration: What can governments and industry do together to address threats and violence, and what are the risks associated with new forms of cooperation? What guarantees should be offered regarding the functionality and durability of strategic security solutions from the private sector? How to avoid extra hazards to the population and allocate costs and risks associated with civil–military co-engagement?

2. Resilience and Security (Con)Fusion in Global and Political Discourses

Conceptually, security and resilience can be explained as interlinked, parallel notions, of which the first focuses on mitigating threats to survival as understood in terms of statehood and sovereignty (Adhikari, 2024; Baldwin, 1997; Nye & Lynn-Jones, 1988; Raza, 2023; Walt, 1991; Wolfers, 1952), while the other addresses threats and hazards of societal dimensions. Both concepts have been broadened due to increased international tensions surrounding new technologies, competition for resources, deteriorating living conditions, and natural disasters (e.g., Dunn Cavelty & Egloff, 2021).

Current global and regional resilience policy discourses do not provide a clear conceptual taxonomy of the two notions. In the early discourses, resilience was framed as a strategic and systematic approach to reducing vulnerabilities and risks to hazards (UN/ISDR, 2004). In this discussion, vulnerabilities were seen as conditions determined by physical, social, economic, and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards (UNDRR, 2017). Hazards refer to a potentially damaging physical event, phenomenon, or human activity that may cause the loss of life or injury, property damage, social and economic disruption, or environmental degradation (UN/ISDR, 2004).

Amidst the world food crisis, the special rapporteur on the right to food, Olivier De Schutter, associated resilience with food, nutrition, and human rights, thus linking nutrition security and resilience (De Schutter, 2008). The year 2009 saw the emergence of talks about resilience and climate change (UNFCCC, 2009). By 2013, disaster risk reduction began to be mainstreamed into development strategies in Asia and the Pacific. Since 2014, the UN has hosted discussions on resilience across an expanding range of contexts—from disaster risk reduction, economic crises, and climate change to energy, transport, and urbanization—through ECOSOC, the Conference on Trade and Development, the Environment Programme, and the General Assembly.

A struggle to clearly define risks, hazards, and threats as those of resilience or security is evident in the reading of global and regional security and resilience policy discourses. Security policy has undergone a similar expansion in the past decades. The UN World Food Programme frames food security as a condition in which people have access to enough safe and nutritious food for normal growth and development, and an active and healthy life (Anthem, 2025). The IEA (2022) frames energy security as not just uninterrupted access to energy but also the securing of energy supplies at an affordable price. Climate security is defined as the direct and indirect impacts of the climate crisis on peace and security, with climate change acting as a threat multiplier (IOM, n.d.). NATO has developed a role in energy security (NATO, 2008) as well as climate security (NATO, 2021, 2022).

One can discern a more welfare-centric evolution of resilience discourses in the years preceding Russia's war in Ukraine. The seminal 2012 report of the UN Secretary-General's high-level panel on global sustainability linked resilience to sustainability, positing that global sustainability produces both a resilient people and a resilient planet (UN, 2012). It defined resilience as the ability to cope with climate change and natural disasters, particularly those associated with droughts, sea-level rise, increased temperatures, and extreme weather events (UN, 2012). A trend towards associating resilience with the way of life and societal welfare can be read from both the UN and regional discourses. Some documents have adopted the definition from the UN Economic and Social Commission for Asia and the Pacific (ESCAP): all measures required by governments to build the capacity of their countries to withstand, adapt to, and recover from natural disasters and major economic crises, so that their people can continue to lead the kind of life they value (UN ESCAP, 2013). The EU's 2020 *Strategic Foresight Report* regards resilience as the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner (European Commission, 2020).

However, more recently, the European Union has regarded resilience and security as equally fundamental pillars of its path to the digital transformation of the economy and society. Conceptually, resilience and security have been given similar weight as the notions of sustainability, sovereignty, or democracy (Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022, 2022).

Further adding to the intertwinement of the two concepts in policy and governance discourses, especially in the context of energy systems, the interaction of resilience and security is a given. A resilient system has been referred to as one where energy makes an optimal contribution to a country's social, economic, and environmental development and is able to withstand and recover quickly from any shock (UNECE, 2023). A resilient energy system is thus based on three pillars: (a) energy security that strengthens energy independence through decentralization, interconnectivity, and trade; (b) affordability that reduces the costs and improves the accessibility of electricity, heating, cooling, and transport services; and (c) environmental sustainability that lowers pollutant emissions and the overall environmental footprint and enhances efficiency across the energy supply chain (UNECE, 2023).

In sum, the relationship between resilience and security remains conceptually unclear, adding to the difficulty of delineating relevant mandates and accountability. The two notions can attain near-synonymous as well as diametrically different connotations in political and strategic discourses. Resilience has connotations that emphasize opportunities and sustainability, but also near-synonymous uses with means and measures to provide security and safety. The UN approach to resilience, for instance, presupposes systemic disruption—whether from natural disaster or politically motivated violence—as the baseline

condition requiring remedy, rather than a proactive governance orientation. The relative lack of conceptual clarity leaves decisions about the exact meaning and functions of security and resilience to domestic authorities and makes it possible for states to develop rather different approaches to the mechanisms and capabilities providing security and resilience.

3. The Shifting Civil–Military Nexus Around "Lake NATO"

In November 2024, the Swedish government refused 13 applications to build offshore wind farms in the Baltic Sea on the grounds that the projects would have unacceptable consequences for Sweden's military defence. Sweden's decision is an illustration of civil–military interests and assets interacting in Europe's current security context, and of security considerations bearing on the siting of energy infrastructure rather than on its construction as such. Commenting on the decision to reject the investment applications seeking to build wind farms in the Baltic Sea, Defence Minister Pål Jonson stressed that building such farms would pose defence risks, not least by making it harder to detect and shoot down missiles using Sweden's Patriot batteries in case of a conflict. He explained that Baltic wind farms could halve the time Sweden had to react to a missile attack to just one minute. Sweden's capital is barely 500 kilometres from the Russian exclave of Kaliningrad: "In the current, very serious international security climate with Sweden where it is and with Kaliningrad where it is…the Swedish armed forces judge it would bring unacceptable risks and the government also has that view," Jonson told reporters ("Sweden rejects Baltic Sea," 2024).

More assertive tendencies of civil–military collaboration are emerging in other European countries. In Poland, the Baltic Power wind farm is outfitting its turbine towers with surveillance radars and sensors in collaboration with Poland's Ministry of Defence ("Poland transforms wind energy project," 2025). As a result, the towers will double as surveillance platforms in a wind farm expected to supply more than 1.5 million households and to cover 3% of Poland's current electricity demand (Baltic Power, 2026). Significantly strengthening networking and cooperation between national security authorities and energy companies, through both co-investment and co-location of infrastructure and functions, is increasingly seen as one of the counter-strategies to the conventional and hybrid threats posed by the Russian navy, and the so-called shadow fleet supporting Russian trade endeavours. The employment of energy infrastructure sensors to enhance security in the Baltic Sea is seen as a possible modality (DENA, 2025). As stated by the Polish state secretary for EU affairs, Ignacy Niemczycki: "We are looking at infrastructure differently than we were one year ago" ("Poland transforms wind energy project," 2025).

Equipping turbine towers with radars and sensors, following a security checklist drafted by Poland's defence ministry, is seen as a milestone towards Poland's energy independence and for building security and stability in the region. However, Poland's approach to infrastructure can also be read as consistent with its ambition to become a leading military power in Europe (Polish Government, 2025a, 2025b). Sweden and Poland thus represent opposite ends of the civil–military spectrum in the Baltic Sea: one trading energy capacity for operational security certainty, the other treating energy infrastructure as an active security asset. Both choices carry governance and legal consequences that existing frameworks are not equipped to manage.

The expectation and, indeed, imperative, of intensified civil–military collaboration are not limited to energy infrastructure. At the end of February 2025, Władysław Kosiniak-Kamysz, Minister of National Defence of Poland, requested military co-investment by demanding that all civilian airports in Poland modernize and adapt

for potential cooperation with the military (Kushnikov, 2025). This militarization of civilian airports would happen in coordination between defence and infrastructure authorities. Maciej Lasek, Deputy Minister of Infrastructure and Government Commissioner for the Construction of the Central Communication Port, said that negotiations are underway with the Ministry of National Defence on "the dual use of Polish airports for both civilian and military purposes" (Kushnikov, 2025). Similarly, several civilian airports, like Kuopio/Rissala or Tampere/Pirkkala, are also homes for the Finnish Air Force's Air Wings and Air Combat Centres.

More broadly, the exact contours and modalities of civil–military co-engagement remain open in most countries. While rejecting the co-location of civilian and military infrastructure offshore, the Swedish government overall seems to be increasing intertwinement of civil and military defence resources and capabilities. In October 2024, when reforming the Swedish Civil Defence and Resilience Agency, it was argued that Sweden was facing its most serious security situation since the Second World War and that, to deter war, an urgent increase in capacity was needed, especially in the area of civil defence (MCF, 2026). The Swedish Government's latest total defence bill (Swedish Government, 2024) seeks to strengthen the civilian element in the concept and doctrine of total defence. The bill frames civilian support to military operations within NATO endeavours to enhance societal resilience and the crisis preparedness of civilian actors. As NATO notes, military forces deployed during crises and conflict depend heavily on the civilian and commercial sectors for transport, communications, energy and basic supplies, and that effective civil preparedness ensures those sectors can continue to support them (NATO, 2024). Civilian support is considered a precondition of NATO's collective defence of the Nordic states, the Baltic Sea region, and the Alliance as a whole (Swedish Government, 2024, Section 7.2.4). As given by the Swedish Armed Forces, and in accordance with NATO's outline, the bill exemplifies health care, energy supply, transportation, electronic communications, and food and water supply as potential areas of civilian support to military operations (Swedish Government, 2024, Section 7). Similarly, the Finnish mobilization system is to use dispersed and local civilian facilities, such as sports halls, warehouses, and school buildings, to gather, equip, and organize reserve units. Moreover, as allowed by the law, private assets such as buildings, vehicles, and materiel can be obtained and used by military units (Valmiuslaki, 2011).

While civil–military collaboration is hardly a new phenomenon, several factors of it require attention from a governance and political administration perspective. The question of civil–military collaboration in the context of energy infrastructure remains a pressing political debate between NATO member states. In and around "Lake NATO," the imperative of defending and controlling strategically important waters engages members of the military alliance in search of ways to detect and control drones, spy ships, aerial stand-offs, and blatant sabotage of power and communication cables and energy infrastructure. Especially after the 2022 sabotage of the Nord Stream pipelines and the damage to cables on the Baltic Sea floor in 2024, NATO began considering the integration of offshore wind farms into its surveillance systems. As turning oil rigs into military bases has proven unfeasible for cost, security, and engineering reasons, wind turbines offer a attractive alternative approach. Offshore wind turbines already carry sensors and navigation aids for shipping and aviation, which sets a baseline for further functionality and uses. Moreover, offshore wind farms can be networked together, thereby improving the surveillance data. In parallel, efforts have been made to accelerate innovation in "sensing and surveillance" for subsea offshore zones, including undersea infrastructure monitoring for infrastructure such as offshore wind farms (WindEurope, 2024). Therefore, infrastructure owners and operators are faced with increasing pressure and expectations, which can result in diverging practices that are still to be assessed as to their legality and sustainability.

A certain gradation between the levels and intensity of civil–military relations may help to grasp the forms of nowadays possible combinations of resilience and security measures. The civil–military nexus can be characterized through the simple burden-sharing of investments needed to prevent and mitigate security risk (i.e., co-investment). Here, the main factor to mitigate the recently aggravated political tensions and additional political risk is the burden-sharing between private and public sector resources. For instance, the energy sector, among other critical infrastructure providers, has faced increasing demands for investment in cybersecurity and data protection preparedness and capabilities. Co-location of civilian and military infrastructure is a growing trend where new infrastructure is built with security needs in mind or where existing civilian infrastructure is being expected to support some security and military needs and requirements. An increasing perspective, however, is that of co-engagement of originally civilian resources and skills to security and military needs and the turning of inherently civilian infrastructure into a direct military asset. Co-engagement—termed co-application by some authors, where originally civilian resources are directly applied to security ends—is the most severe form of civil–military fusion that could result in active contribution to defence and, as applicable, warfare, of not just the infrastructure in question but also its owners and operators. This has been problematized by the International Committee of the Red Cross (Pollard et al., 2024).

4. Governance Risks of the Security and Resilience Fusion

(Hyper-)securitization, normalization of crisis-time governance models, and cementing civil–military co-engagement modalities incur political and legal risks to democracy and, as the discussion in this section suggests, may serve the ultimate strategic objective of authoritarian adversaries. The very evolution of the concepts of resilience and security is a testament to the difficulty of managing risks and crises in a highly interconnected, polycentric, and volatile international environment. In the current geopolitical outlook, dubbed permacrisis (Sik, 2025), polycrisis (Cant, 2025; Lawrence et al., 2024; Morin & Kern, 1999), unpeace (Kello, 2017; Leonard, 2021), and international disorder and unrest (Haass, 2017; Ikenberry, 2018; McKeil, 2021), the balance between civilian and military co-investment, co-location, and co-engagement becomes thornier than ever—crisis-time governance has its appeal and can start eroding democratic principles and processes. In liberal democracies, separation of powers, the rule of law, and transparency and accountability have been presumed as the normal state of affairs. Accordingly, any expansion of the military space and powers in peacetime as well as in times of conflict remains exceptional and limited in time, space, and scope. Any such move, if legally permitted at all, requires specific justifications, decision-making procedures, and control mechanisms.

In practice, critical infrastructure is a frequent target of politically motivated cyber and hybrid attacks and operations in peacetime (EUREPOC, 2026; OHCHR, 2025). The co-location of civilian–military capabilities will effectively lower the threshold of such attacks. Also, data sharing with the military, hosting military hardware, co-investment in national security, as well as co-contribution to threat mitigation open the participating communities and entities to new challenges and potentially unwanted consequences. Poland's "looking at infrastructure differently" is an interpretative, constructive, and transitional move which by default is highly political. The problem is that combining the transformed modes of energy production and distribution—broadly characterized as cleaner and more diversified, though both labels remain contested in energy policy discourse—with national security and military intelligence capabilities necessitates rearrangements also in the modes and distribution of security awareness, military intelligence, and violence.

The new views and integrating rearrangements, as discussed and evidenced in Section 3, will entail governmental and corporate risk-taking beyond the common understanding of energy security as having uninterrupted access to energy at an affordable price. At the local and material level, the co-location of civilian and military intelligence capabilities in, for example, turbine towers could turn the original civilian property and functions protected by international humanitarian law into potentially legitimate military targets during an armed conflict.

As what is at stake in practice is civilian property, societal functions, and military installations, the question of who is responsible for protecting them becomes one of agency, that is, of mandates and competences. It is common that major energy facilities, such as dams and nuclear power plants, are protected by armed guards, and that the protection is often contracted to private security companies. For inland or offshore wind parks, the zone of protection is wider and the potential threat far more complicated than rather simple facility or perimeter patrolling against protesters and saboteurs. If the task to protect nationally significant but primarily civilian energy installations against, e.g., aerial, maritime, or cyber-attacks is given to military forces, one may ask whether that constitutes a politically correct expenditure of taxpayers' money and an appropriate, even feasible, employment of trained and exercised, by default lethal, military power. However, if a civilian energy or security company is responsible for such multi-domain protection, one can ask of the competence and sustainability of such civilian activities. Importantly, significant national political risk of unintended escalation arises with local, civilian, and non-governmental response, hack-backs or shoot-backs. In short, the question is whether and to what extent the monopoly of violence remains in the public sphere (Diaz et al., 2021; Huntington, 1957; Janowitz, 1960; Smith, 2008).

The newly created or strengthened government-corporate zones of interest and exclusion tend to reduce public debate and parliamentary oversight in the name of national and military security. Civilian issues (here, energy infrastructure) become securitized and militarized, while military issues (here, the deployment and employment of military capabilities) become corporate matters. Ultimately, roles, responsibilities, and risk-taking become functions of opaque decision-making and extraordinary powers (Buzan et al., 1998; Dunn Cavelty, 2008; Wæver, 1995). In 2025, the Estonian Secretary of State argued in an interview with Estonian Public Broadcasting (ERR) that Estonia should abstain from the already normalized crisis-time governance model, where decisions are made fast and with limited information (Krjukov, 2025). Acknowledging the need to deal with emergencies in the era of permacrisis and polycrisis, Taimar Peterkop pointed to the rise of autocracy and emphasized the dangers of resorting to crisis-time governance as a routine. As Peterkop stressed, crisis management decisions tend to be made fast and without comprehensive calculation of the pros and cons.

Seen from a national governance perspective, the risk is one of creating unsustainable dual practices and double standards. The co-location of civilian energy infrastructure and military capabilities may accelerate the already witnessed decline of democracy. Once bypassed or rooted out, the hard-earned fundamental political rights and freedoms, such as transparency, accountability, and the freedom of the press, are difficult to re-establish (Freedom House, 2025). Similarly, security–resilience, acknowledged as a major political parameter, may disturb the functioning markets that a cost-effective energy transition will need (IEA, 2022). The manoeuvres to provide micro-level security and resilience may at the same time provide unforeseen advantages to belligerent actors and erode macro-level political and societal cohesion and sustainability. As demonstrated by litigation—including insurance disputes brought by aviation lessors over aircraft

stranded by sanctions, as in the 2025 Russian Aircraft Lessor Policy Claims ([2025] EWHC 1430 (Comm))—blurring the civilian–military boundary also triggers insurance and investment protection problems.

5. Clarity Through Law?

Novel ways of collaboration and contributions may incur additional political risks for both industry and the civilian population and therefore require further principles and rules for burden-sharing and risk mitigation. The normalizing of the security–resilience fusion raises several legal questions. While legal problems on the matter have been clearly identified, their discussions span different jurisdictions and remain scattered across distinct legal sub-fields. The distinction between co-investment, co-location, and co-engagement is used here to structure the discussion. In the context of co-investment, authors have stressed the challenges of intellectual property, technology transfer, export controls, and foreign investment screening. With co-location, issues of dual-use objects and spaces emerge, mainly with emphasis on the law of targeting. Co-engagement triggers additional considerations of rules of engagement and the protections afforded to civilians. Authors also emphasize that defence funding reshapes what can be published, who can be hired, and how international collaborations work (Simmons-Edler et al., 2025).

The US-based Institute for Defense Analyses notes that the legal frameworks designed for civilian academic commercialization are too ambiguous when applied to dual-use technologies (Howieson et al., 2013). Legal practitioners have also pointed out that export controls and foreign actors' co-investment in dual-use regimes may create overlapping, sometimes contradictory obligations (Beahn & LaRussa, 2021). No academic framework yet reconciles them. Coveri et al. (2025) point out legal and regulatory gaps surrounding Big Tech corporations assuming de facto military infrastructure roles without being subject to public accountability norms. Bhaskar et al. (2025) observe a relative absence of the legal interface between export control regimes and international humanitarian law (IHL) when civilian technology is transferred into military use in conflict environments, while Jones et al. (2026) posit that dual-use classification operates as a legal and political device that deliberately blurs investment boundaries.

Co-location adds the dimension of the legal status of shared physical spaces and infrastructure. Hathaway et al. (2025) note the danger of the rise of dual-use objects, explaining how co-located civilian–military infrastructure erodes IHL targeting protections. It is widely acknowledged that from the point of view of targeting law, infrastructure that is simultaneously civilian and military—power grids, water systems, communications networks, and ports—falls into a legal grey zone. This complicates the application of IHL, whereby an object is either a military objective or it is not, leading scholars to argue that this binary approach is unfit for modern co-location realities (Capone, 2025). Authors conclude that existing IHL targeting rules for co-located civilian–military structures need reinterpretation, not just application (Schmitt, 2021), as the current doctrine fails to adequately protect civilians in co-located environments (Chakrabarty, 2020). Others emphasize issues related to involuntary civilian presence near military assets—including service, maintenance, and operational personnel present at offshore wind parks—criticizing IHL's human shields framework as under-specified and risking "excessive legalization" that could actually weaken civilian protection (Lafazani, 2021). Operational frameworks for civil–military co-location in airspace and airport facilities have been addressed at the domestic regulatory level. However, sovereignty and liability questions when incidents occur in shared civil–military airspace—flight information regions or corridors where civil aviation and military aircraft operate under separate but coordinated regulatory frameworks—remain legally unresolved between states.

In the context of co-engagement, a look at the UN, NATO, and ASEAN frameworks of civil–military cooperation finds them inconsistent and insufficiently binding. Importantly, military doctrine on civil–military cooperation (CIMIC) and humanitarian law's principles of neutrality, impartiality, and distinction remain structurally in conflict in situations where the same actors simultaneously provide aid and conduct operations. The EEAS has published best-practice analysis on IHL compliance in CSDP civil–military coordination missions, acknowledging that legal obligations for civilian EU actors and military contingents in the same theatre are governed by different instruments, creating accountability gaps when things go wrong. Boddens Hosang (2020) adds that rules of engagement governing military co-engagement with civilian actors fall between domestic law, IHL, and operational command authority and concludes that the three-way tension remains structurally unresolved. Ghenai (2026) and Mako (2026) raise the issue of private technology companies co-engaging in military operations through AI systems and cloud infrastructure. They maintain that the existing IHL's chain-of-command accountability model breaks down entirely, which means no clear responsibility can be assigned for autonomous targeting errors in a co-engaged civil–military AI system.

Across all three modalities of civil–military nexus, the common scholarly finding is that legal frameworks built for separate spheres are yet to be redesigned for fusion. Co-investment law is a patchwork of rules with different purposes and directions. Co-location law is binary where reality is gradient. Co-engagement law assigns accountability through chains of command that dissolve when civilian and military actors are intertwined. Importantly, no integrated legal framework addressing all three simultaneously yet exists. Cooperation between the private and the public sector, consequently, may be interpreted, even deliberately misconstrued, as offensive and hostile and used as triggers or justifications for escalation ("Putin says services like Microsoft," 2025). Companies and individuals may inadvertently become targets of politically motivated attacks and operations. Critical infrastructure, including energy and finance sectors, has frequently been subjected to politically motivated cyberattacks and influence operations. Moreover, industry and volunteer engagement in the context of armed conflict may be regarded as direct participation in hostilities and incur an additional likelihood of becoming a legitimate target of a military operation (Pollard et al., 2024). Industrial infrastructure and assets, in turn, risk becoming legitimate military objectives due to their nexus with defence organization and capabilities.

In the EU context, further parallels can be drawn with the legal landscape of the civil–military nexus. Significantly heightened corporate cybersecurity requirements under the EU Network and Information Security Directive (NIS/NIS2) are an example of how politically motivated offensiveness needs to be mitigated through additional private investment and industry-government information and practices sharing. One of the nine principles of the Paris Call for trust and security in cyberspace (2018) calls on actors to take steps to prevent non-state actors, including the private sector, from hacking back (Paris Call, 2018). A separate but related instrument, the EU dual-use regulation (Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, 2021), addresses the co-investment and technology transfer dimension. In the EU, "dual-use items" refer to items, including software and technology, which can be used for both civil and military purposes (Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, 2021). The regulation provides a legal basis for requiring export authorization before civilian-developed dual-use technology can be transferred to foreign military actors, closing some of the regulatory gap Bhaskar et al. (2025) identified regarding technology transfer in conflict environments. Its Article 5 on cyber-surveillance begins to address Coveri et al.'s (2025) concern about Big Tech co-investment with military actors producing infrastructure with surveillance and targeting utility. However,

scholars consider these gains limited (Maciata, 2026; Stalenhoef et al., 2022). They find that the regulation creates serious legal uncertainty for universities co-investing with defence actors—the definitions are vague, guidance is absent, and there is no mechanism to reconcile the regulation's compliance demands with academic freedom and institutional autonomy. Read in the spirit of Manca et al. (2017), for whom societal resilience rests on the capacity to absorb, adapt and transform, this gap weakens the resilience the regulation is meant to serve. Importantly, the regulation imposes obligations without providing governance structures for the civil–military co-investment relationship. The regulation's conceptual foundation, the binary civilian/military classification, is increasingly recognized as obsolete in an environment where AI, semiconductors, and satellite communications are simultaneously civilian, commercial, and military—rigid dual-use listings systematically lag reality and leave large swathes of co-investment activity uncontrolled.

6. Conclusion

Modern wars are fought in the same environments in which civilian and societal actors and functions operate. As contemporary warfare is dependent on advanced systems, services, and technologies, standing and professional forces become increasingly dependent on civilian support. It can therefore be expected that defence organizations will continue drawing on civilian extensions of their capabilities. By the same token, armed forces are increasingly expected to utilize civilian assets for military purposes and be supported by civilian agencies and authorities. The legal challenge is not simply one of catching up: existing law was built on the premise of separability between military and civilian spheres that current practice is systematically dismantling.

Decisions about co-investment, co-location, and co-engagement can vary significantly as illustrated by the Swedish and Polish approaches. Politically, both choices are open to EU and NATO countries. Legally, both paths merit scrutiny as to their sustainability as means of providing security and resilience in democratic, rule-of-law societies. The terminological diffusion in both the UN and EU discourses promises little recourse from international and regional policy processes. This leaves states to tackle the political, administrative, and legal consequences of their decisions and actions.

Importantly, the legal premises of the feasibility and sustainability of civil–military cooperation remain to be clarified. Political risk burden-sharing depends on the goodwill of parties involved. Legal bases and guarantees of co-investment, co-location, and co-engagement are, at best, fragmented and overlapping, absent, or obsolete. Differences might stem from domestic legislation, EU and international law, as well as non-legal factors such as organizational mandates, differences in resources, and preparedness. The domestic literature on Poland's and Sweden's approaches adds limited insight to the legal accountability dimension of civil–military energy security collaboration. Thus, the legal issues identified in the wider scholarship remain unresolved. The most pressing for the Baltic Sea area, given the acute security concerns, is the IHL targeting question: what happens to co-located wind turbines equipped with military sensors under the law of armed conflict? Second is the co-investment liability question: who bears legal responsibility when private energy operators co-invest in national security capabilities and assets are damaged or operations disrupted? Third is the democratic accountability question: what obligations flow from civil–military fusion?

These challenges are further compounded in contexts where civilian populations live or work in proximity to co-located assets—there, the co-engagement problem is not merely legal or abstract but immediate and

human. What is needed, at minimum, is a unified accountability standard covering the full spectrum from co-investment governance to IHL compliance, and a coherent due diligence obligation for both governments and operators that matches the reality of fusion rather than the fiction of separation.

Funding

Publication of this article in open access was made possible through the institutional membership agreement between Tampere University and Cogitatio Press.

Conflict of Interests

The author declares no conflict of interests.

LLMs Disclosure

A large language model (Claude, claude-opus-5-5) was used to consolidate the final manuscript versions, to check citation–reference correspondence, and to verify source locators.

References

Adhikari, A. S. (2024). The concept of international security. *Hasanuddin Journal of International Affairs*, *4*(2), 78–89.

Åhäll, L. (2016). The dance of militarisation: A feminist security studies take on 'the political.' *Critical Studies on Security*, *4*(2), 154–168.

Anthem, P. (2025). *Food security—What it means and why it matters*. World Food Programme. https://www.wfp.org/stories/food-security-what-it-means-and-why-it-matters

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5–26.

Baltic Power. (2026, July 10). *Baltic Power offshore wind farm produces and delivers electricity to Polish energy grid for the first time* [Press Release]. https://balticpower.pl/news/baltic-power-offshore-wind-farm-produces-and-delivers-electricity-to-polish-energy-grid-for-the-first-time

Beahn, J., & LaRussa, R. (2021, June 3). *Beyond CFIUS: The growing use of US export controls to control foreign direct investment*. Mondaq. https://www.legal500.com/intelligence/united-states/international-law/beyond-cfius-the-growing-use-of-us-export-controls-to-control-foreign-direct-investment

Bhaskar, N., Magoge, J. S., & Hashimy, S. Q. (2025). Technology transfer in the era of military conflict: Legal challenges for international trade and international humanitarian law. *Journal of Digital Technologies and Law*, *3*(2), 222–258. https://doi.org/10.21202/jdtl.2025.10

Bitzinger, R. A. (2021). China's shift from civil-military integration to military-civil fusion. *Asia Policy*, *16*(1), 5–24.

Boddens Hosang, J. F. R. (2020). *Rules of engagement and the international law of military operations*. Oxford University Press.

Brooks, R. (2025). Understanding current threats to democracy: The limits of the civil-military relations paradigm. *Daedalus*, *154*(4), 231–257. https://doi.org/10.1162/DAED.a.959

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.

Cant, C. (2025). The mirage of polycrisis: A symptomatic reading of Tooze. *Capital & Class*, *49*(4). https://doi.org/10.1177/03098168251342949

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

Chakrabarty, I. (2020). Reformulating rules on dual object targeting. *New York University Journal of International*

Law and Politics Online Forum, *52*(Winter–Spring), 24–38. https://nyujilp.org/wp-content/uploads/2020/03/Chakrabarty-Note_EIC-Edits_Final.pdf

Cohen, A., & Cohen, S. A. (2022). Beyond the conventional civil–military "gap": Cleavages and convergences in Israel. *Armed Forces & Society*, *48*(1), 164–184.

Coveri, A., Cozza, C., & Guarascio, D. (2025). Blurring boundaries: An analysis of the digital platforms-military nexus. Review of Political Economy, *37*(4), 1632–1663.

Cusumano, E. (2023). *Mobilization constraints and military privatization: The political cost-effectiveness of outsourcing security*. Palgrave Macmillan.

De Schutter, O. (2008). *Building resilience: A human rights framework for world food and nutrition security* (UN Document A/HRC/9/23). UN. https://docs.un.org/en/A/HRC/9/23

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. (2022). *Official Journal of the European Union*, L 323. http://data.europa.eu/eli/dec/2022/2481/oj

DENA. (2025). *Baltic energy and cyber security forum*. https://www.dena.de/en/german-polish-energy-platform/infocenter/news/baltic-energy-and-cyber-security-forum

Diaz, C., Zepnova, E., Daza, F., Gampisi, G., & Miralles, N. (2021). *Blurring the monopoly on violence: Private military and security companies and coercive state power*. Transnational Institute. https://www.tni.org/en/article/blurring-the-monopoly-on-violence

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Dunn Cavelty, M., & Egloff, F. (2021). Hyper-securitization, everyday security practice and technification: Cyber-security logics in Switzerland. *Swiss Political Science Review*, *27*(1), 139–149.

EUREPOC. (2026). *Critical infrastructure tracker*. https://cit.eurepoc.eu

European Commission. (2020). *2020 strategic foresight report: Charting the course towards a more resilient Europe* (COM(2020) 493 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0493

European Commission. (2025a). *EU defence industry transformation roadmap: Unleashing disruptive innovation for defence readiness* (COM(2025) 845 final). https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en

European Commission. (2025b, November 19). *Military mobility*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/military-mobility_en

Freedom House. (2025). *Democracies in decline*. https://freedomhouse.org/issues/democracies-decline

Ghenai, R. (2026, March 25). The big tech–military nexus: AI, warfare, and the future of international law [Paper presentation]. JSDA Conference 2025, New York, USA. https://publications.lawschool.cornell.edu/cilj/2026/03/25/the-big-tech-military-nexus-ai-warfare-and-the-future-of-international-law

Haass, R. (2017). *A world in disarray: American foreign policy and the crisis of the old order*. Penguin.

Has, Ö. (2025). Regulating private military companies: A comparative study of national approaches in the United States, Turkey, and Russia. *Journal of Conflict and Security Law*, *30*(3), 359–375.

Hathaway, O. A., Khan, A., & Revkin, M. R. (2025). The dangerous rise of "dual-use" objects in war. *Yale Law Journal*, *134*(8), 2645–2750.

Howieson, S. V., Shipp, S. S., Walejko, G. K., Rambow, P. B., Peña, V., Holloman, S. S., & Miller, P. N. (2013). *Policy issues for Department of Defense technology transfer*. Institute for Defense Analyses. https://apps.dtic.mil/sti/trecms/pdf/AD1123849.pdf

Huntington, S. P. (1957). *The soldier and the state: The theory and politics of civil–military relations*. Belknap Press of Harvard University Press.

Huskey, K. A. (2012). Accountability for private military and security contractors in the international legal regime. *Criminal Justice Ethics*, *31*(3), 193–212.

IEA. (2022). *World energy outlook 2022: Energy security in energy transitions*. https://www.iea.org/reports/world-energy-outlook-2022/energy-security-in-energy-transitions

Ikenberry, G. J. (2018). The end of liberal international order? *International Affairs*, *94*(1), 7–23.

IOM. (n.d.). *Climate security*. Environmental Migration Portal. https://environmentalmigration.iom.int/climate-and-security

Janowitz, M. (1960). *The professional soldier: A social and political portrait*. Free Press.

Jones, C., Mousamputri, I., & Griffiths, M. (2026). Dual use as a political technology of contemporary military violence. *Political Geography*, *127*, Article 103525. https://doi.org/10.1016/j.polgeo.2026.103525

Kapsokoli, E. (2025). Weaponizing cyberspace: The Russia–Ukrainian war. *Security Science Journal*, *6*(2), 71–97.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Krjukov, A. (2025, January 15). Peterkop: Peaksime hoiduma juba normiks saanud kriisiaja valitsemismudelist. *ERR*. https://www.err.ee/1609575631/peterkop-peaksime-hoiduma-juba-normiks-saanud-kriisiaja-valitsemismudelist

Kushnikov, V. (2025, February 26). Poland to use civilian airports for military purposes. *Militarnyi*. https://militarnyi.com/en/news/poland-to-use-civilian-airports-for-military-purposes

Lafazani, Z. (2021, November 16). Human shields under IHL: A path towards excessive legalization. *Humanitarian Law & Policy Blog*. https://blogs.icrc.org/law-and-policy/2021/11/16/human-shields-ihl

Lawrence, M., Homer-Dixon, T., Janzwood, S., Rockström, J., Renn, O., & Donges, J. F. (2024). Global polycrisis: The causal mechanisms of crisis entanglement. *Global Sustainability*, *7*, Article e6.

Leonard, M. (2021). *The age of unpeace: How connectivity causes conflict*. Transworld.

Maciata, K. (2026). Securing offshore wind farms in Poland: Legal responsibilities, institutional gaps, and hybrid threat resilience in the Baltic Sea: Towards an integrated model of protection and resilience. *Journal on Baltic Security*, *12*(1), 28–60.

Mako, G. (2026, March 9). Legal accountability for AI-driven autonomous weapons. *Articles of War*. https://lieber.westpoint.edu/legal-accountability-ai-driven-autonomous-weapons

Manca, A., Benczur, P., & Giovannini, E. (2017). *Building a scientific narrative towards a more resilient EU society*. Publications Office of the European Union.

MCF. (2026). *MSB is Swedish Civil Defence and Resilience Agency*. https://www.mcf.se/en/about-us/swedish-civil-defence-and-resilience-agency

McKeil, A. (2021). On the concept of international disorder. *International Relations*, *35*(2), 197–215.

Minow, M. (2005). Outsourcing power: How privatizing military efforts challenges accountability, professionalism, and democracy. *Boston College Law Review*, *46*(5), 989–1026.

Morin, E., & Kern, A. (1999). *Homeland Earth: A manifesto for the new millennium*. Hampton Press.

NATO. (2008). *Bucharest Summit Declaration*. https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2021). *Climate change and security action plan*. https://www.nato.int/cps/en/natohq/official_texts_185174.htm

NATO. (2022). *Strategic concept*. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

NATO. (2024). *Resilience, civil preparedness and Article 3*. https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

Nye, J. S., Jr., & Lynn-Jones, S. M. (1988). International security studies: A report of a conference on the state of the field. *International Security*, *12*(4), 5–27.

OHCHR. (2025). *Increasing attacks on Ukraine's energy infrastructure place civilians at risk, UN human rights monitors warn*. UN. https://ukraine.ohchr.org/en/Increasing-attacks-on-Ukraine-s-energy-infrastructure-place-civilians-at-risk-UN-human-rights-monitors-warn

Paris Call. (2018). *Paris call for trust and security in cyberspace*. https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace

Poland transforms wind energy project into strategic surveillance platform for NATO. (2025, August 12). *Business Today Poland*. https://businesstodaypoland.com/article/839156875-poland-transforms-wind-energy-project-into-strategic-surveillance-platform-for-nato

Polish Government. (2025a). *Poland's security strategy: A stronger Europe and transatlantic unity*. https://www.gov.pl/web/primeminister/polands-security-strategy-a-stronger-europe-and-transatlantic-unity

Polish Government. (2025b). *Programme of the Polish presidency of the Council of the European Union*. https://polish-presidency.consilium.europa.eu/media/zkcno325/programme-of-the-polish-presidency-of-the-council-of-the-european-union.pdf

Pollard, M., Kurnadi, F., & Beytout-Lamarque, C. (2024). *What private businesses need to know about international humanitarian law*. International Committee of the Red Cross. https://blogs.icrc.org/law-and-policy/2024/11/26/what-private-businesses-need-to-know-about-international-humanitarian-law

Putin says services like Microsoft, Zoom should be "throttled" in Russia. (2025, May 26). *Reuters*. https://www.reuters.com/technology/putin-says-services-like-microsoft-zoom-should-be-throttled-russia-2025-05-26

Raza, A. (2023). *Core concepts of international security within the realm of international relations*. SSRN. https://doi.org/10.2139/ssrn.4504853

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. (2021). *Official Journal of the European Union*, L 206. http://data.europa.eu/eli/reg/2021/821/oj

Schmitt, M. N. (2021, June 28). Targeting dual-use structures: An alternative interpretation. *Articles of War*. https://lieber.westpoint.edu/targeting-dual-use-structures-alternative

Sik, D. (2025). Introduction: A critical theory for the age of permacrisis. In D. Sik (Ed.), *Salvaging modernity: A social contract for the age of permacrisis* (pp. 1–17). Brill. https://doi.org/10.1163/9789004736177_002

Silva, C. C. V., & Pereira, A. E. (2024). Securitization theory and its empirical application: A literature review. *Revista de Sociologia e Política*, *32*, Article e019.

Simmons-Edler, R., Dong, J., Lushenko, P., Rajan, K., & Badman, R. P. (2025). *Military AI needs technically-informed regulation to safeguard AI research and its applications*. arXiv. https://arxiv.org/abs/2505.18371

Smith, R. (2008). *The utility of force: The art of war in the modern world*. Random House.

Stalenhoef, C., Kanetake, M., & van der Wende, M. (2022). *The implications of the EU's dual-use export control Regulation 2021/821 for universities and academics*. SSRN. https://doi.org/10.2139/ssrn.4248860

Sweden rejects Baltic Sea wind farms, citing defence concerns. (2024, November 4). *Reuters*. https://www.reuters.com/business/energy/sweden-rejects-baltic-sea-wind-farms-citing-defence-concerns-2024-11-04

Swedish Government. (2024). *Totalförsvaret 2025–2030* (Proposition 2024/25:34). https://www.regeringen.se/rattsliga-dokument/proposition/2024/10/prop.-20242534

Ulrich, M. P. (2021). The U.S. civil–military relations gap and the erosion of historical democratic norms. In W. R. Thompson (Ed.), *Oxford research encyclopedia of politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1932

UN. (2012). *Resilient people, resilient planet: A future worth choosing* (A/66/700). https://docs.un.org/en/A/66/700

UN ESCAP. (2013). *Building resilience to natural disasters and major economic crises*. UN. https://hdl.handle.net/20.500.12870/1594

UN/ISDR. (2004). *Living with risk: A global review of disaster reduction initiatives*. UN. https://www.undrr.org/publication/living-risk-global-review-disaster-reduction-initiatives

UNDRR. (2017). *Sendai Framework terminology on disaster risk reduction* (A/71/644, endorsed by General Assembly resolution A/RES/71/276). UN. https://docs.un.org/en/A/71/644

UNECE. (2023). *Energy system resilience: The future of gas supply in Europe* (ECE/ENERGY/GE.8/2023/3). https://unece.org/documents/2023/03/working-documents/energy-system-resilience-future-gas-supply-europe

UNFCCC. (2009). *Measures, methodologies and tools for increasing economic resilience to climate change and reducing reliance on vulnerable economic sectors: Submissions from Parties and relevant organizations* (FCCC/SBSTA/2009/MISC.6). UN. https://unfccc.int/resource/docs/2009/sbsta/eng/misc06.pdf

Valmiuslaki, 2011, Emergency powers act 1552/2011. https://www.finlex.fi/fi/laki/ajantasa/2011/20111552

Wæver, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On security* (pp. 46–87). Columbia University Press.

Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly*, *35*(2), 211–239.

WindEurope. (2024, May 19). *NATO determined to protect critical undersea energy infrastructure*. https://windeurope.org/news/nato-determined-to-protect-critical-undersea-energy-infrastructure

Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political Science Quarterly*, *67*(4), 481–502.

About the Authors



Eneken Ellinor Tikk is a lawyer and an international relations scholar specialising in cyber and digital policy. Her research interests focus on peaceful settlement of international disputes, and the emergence and durability of international understanding and agreements.