Review

Critical Infrastructure Resilience and Civil Preparedness: EU and NATO approaches

Cotroneo, C.[1], Georgescu, A.[2]

[1]Global Governance Institute, Brussels, Belgium,
c.cotroneo@globalgovernance.eu

[2]National Institute for Research and Development in Informatics, ICI, Bucharest, Romania,
alexandru.georgescu@ici.ro

Abstract: *Following three subsequent attacks against EU Member States' critical infrastructures (CIs) in the Baltic Sea in late 2024, NATO urged its member countries to think about conflict preparedness. In early 2025, while debating the risks and consequences of attacks against EU CIs, the European Parliament urged Member States to consider how to prepare for the worst-case scenario, considering the rising geopolitical tensions and Russia's hybrid attacks against EU CIs. In absence of its own defence capabilities, the EU depends heavily on NATO for military defence. While the military Alliance considers civil preparedness a central pillar of its members' resilience in the face of conflict and an enabler for collective defence, EU Member States' degree of civil preparedness has been evaluated as inadequate. Yet, former Finnish President considers civil preparedness as a citizens' right and Sweden has already distributed booklets, across the country's households, on what to do in case of war. This paper compares the civil preparedness policy frameworks and capabilities of the EU and NATO, in case of CI failure during conflict. It identifies points of convergence, divergence, complementarities and synergies to assess the degree to which the EU is adequately equipped to respond and recover from cyber-attacks against CIs and mitigate their impacts on the civilian population. The discussion focuses on the current weaknesses of the EU's framework and capacities and provides guidance on how to integrate the governance of CI resilience within civil preparedness and crisis management frameworks.*

Keywords: *crisis preparedness, civilian preparedness, critical infrastructure, cyber-attack, resilience*

1. INTRODUCTION

Russia's full-scale invasion of Ukraine and the ensuing rising tensions between Russia and NATO countries has forced the European Union (EU) to re-assess its defence and civil preparedness strategies. Within this new security context, the EU is re-prioritising civil preparedness, for the first time since the Cold War period. A core objective of civil preparedness is to ensure that the civilian population can better withstand military attacks. This requires that essential goods and services, such as food, health, energy can still be provided in case of crises. Critical infrastructures (CIs) are systems and assets that underpin key

governmental and societal functions and ensure that essential goods and services can be delivered to civilians. Damages to CIs arising from deliberate, environmental or system malfunctions cause disruptions to the provision of essential goods and services, with potentially dire impact on the civilian population. Recent years have shown the dangers related to cyber-attacks against critical infrastructures (CIs), in peacetime and conflict. The objective of this paper is to critically assess the current state of civil preparedness in case of cyber-attacks against CIs in NATO EU countries. As EU member states (MS) are also NATO countries, the civilian sector can benefit from civil preparedness strategies put in place by both organisations. However, for civil preparedness in the EU to be maximised, EU and NATO strategies need to be comprehensive, complementary and equally implemented across countries. This introductory section provides a broad overview of the risks and impacts arising from cyber-attacks against CIs on civilians. The next section examines and compares EU and NATO approaches. Finally, the concluding section provides some policy recommendations. One of the 30 action points of the EU's Preparedness Union Strategy (2025) is to integrate preparedness and resilience into the cooperation with NATO. The recommendations of this paper will help in setting up the baseline and benchmark against which to assess EU progress and in identifying the remaining gaps.

The work presented engages with ongoing discussions in EU and NATO countries on how to enhance defence and civilian preparedness in case of military attacks. While military attacks carry significant consequences for the civilian populations through the destructive and disruptive impact of kinetic strikes, cyber-operations against CIs also have actual and potential impacts that severely endanger civilian lives and pose a challenge to survival itself in crisis contexts. In crises arising from military conflicts, cyber-attacks against CIs can be used to exploit and increase the vulnerability of a nation and hit the civilian population indirectly. These attacks increase a nation's vulnerability by amplifying the effects of military attacks (Stephane and Pavlova, 2023), as the recent uses of Russia's cyber-attacks against Ukraine have shown. Crucially, cyber-attacks against CIs impact the civilian population by disrupting access to food, water, sanitation, health and energy, all essential services for survival. Finally, they also impact morale and can be used as a coercive tool.

However, cyber-attacks against CIs also impact civilians in peacetime or in periods of geopolitical tensions. In December 2015, the BlackEnergy malware attack on Ukraine's power grid led to power outages affecting about 225,000 people. This cyber-attack, which marked the first known cyber-induced power outage, left civilians without electricity, affecting homes and essential services. In December 2016, the Industroyer attack targeted Ukraine's power grid, causing a temporary blackout in parts of Kyiv. The attack on industrial control systems led to power outages and disruptions of heating systems during winter, adding to the hardships faced by civilians. In June 2017, Ukraine experienced the NotPetya attack, which spread via Ukrainian accounting software and quickly propagated globally, causing severe disruption. The attack targeted sectors including banking, energy, and transportation, leading to significant

economic losses. Civilians faced power outages, disruptions to public services, and interruptions at the Chernobyl nuclear power plant. In May 2017, the WannaCry ransomware attack affected numerous organizations across Europe, including critical infrastructure sectors like healthcare and transportation. The UK's National Health Service (NHS) was severely impacted, leading to cancelled medical appointments and surgeries, causing disruptions to healthcare services and affecting civilian access to medical care. Cyber-attacks can also disrupt the delivery of humanitarian aid, thus making the population more vulnerable to a range of physical and psychological risks. These examples illustrate the severe consequences of cyber-attacks on critical infrastructure, emphasizing the need for civil preparedness to these events in crisis contexts. Moreover, by promoting civil preparedness to the consequences of these events in crisis contexts, civilians would be able to better withstand the impact of attacks also during peacetime.

The urgency of enhancing EU civil preparedness has been emphasised across institutions and policy documents. A 2024 European Commission's report (i.e., the Niinistö report) concluded that currently the EU lacks a clear plan on what to do in case of military attacks or other threats and that there is an urgent need to enhance preparedness for all hazard in the EU. Key findings suggested that citizens need to be at the centre of preparedness strategy, that civilian-military cooperation needs to be part of a comprehensive preparedness strategy, including strengthening dual-use infrastructure and technology and, that EU-NATO partnership was essential (pp 13-14). It is also important to note that given disputes over EU strategic autonomy and the advisability of an "EU Army", with concerns that it may lead to a doubling of efforts and with the functionality of NATO, resilience, civil protection and crisis preparedness have emerged as a preferred topic for constructive engagement between the EU and NATO and within the transatlantic partnership and an area where efforts on both sides of the overlapping organizations can enhance rather than detract from security outcomes

With regards to civil preparedness, both organisations align in two important elements: first, in considering civil preparedness as a necessary pillar of resilience and second, in framing CI protection as a key element for civil preparedness and resilience. NATO's 2022 Strategic Concept emphasises the importance of civil preparedness as a cornerstone of resilience, urging member states to enhance their crisis response mechanisms and infrastructure protection (NATO, 2022). Additionally, NATO's Strategic Concept (NATO, 2022) points out the critical role of civil preparedness in ensuring member states' resilience, urging them to enhance their infrastructure protection and crisis management frameworks. The recent European Commission's *Preserving Peace – Defence Readiness Roadmap 2030* puts forward a key initiatives to improve European civilian protection, including the European Drone Defence Initiative, the implementation of which should improve situational awareness and critical infrastructure security jointly with NATO. Furthermore, a 2025 European Parliament's briefing cascades Jamie Shea (Nato Deputy Assistant Secretary General)'s message to Europe to systematically invest in civil-military resilience.

Notwithstanding these policy objectives, recent policy and governmental reports have revealed significant deficiencies in the EU's civil preparedness capacities and capabilities. A European Parliament's briefing on EU preparedness stresses that the current geopolitical and international security environments demand a new defence and preparedness posture for the EU (European Parliament, 2025). However, the briefing concludes that the current EU strategy for preparedness has key shortfalls. These include: reactive, rather than proactive crisis management mechanisms; fragmented toolboxes across institutions, agencies and sectors across borders; a deficit in civil-military coordination; limited resources for EU structures and mechanisms (European Parliament, 2025).

2. EU and NATO approaches to civil preparedness in case of CI failure

This section of the paper examines the EU and NATO's approaches to civilian preparedness to disruptions arising from cyber-attacks against CIs. The analysis is based on a comparative approach which examines the complementarity, synergies, gaps and progress status by looking at the following dimensions. First, the coherence between NATO's baseline requirements and the corresponding EU objectives. Second, the status of implementation of EU initiatives relevant to achieving NATO's baseline requirements for civil preparedness and corresponding EU objectives.

Historically, civil preparedness – formerly known as civil emergency planning – has been one of the key areas for of NATO's strategy and operations. NATO's organisational structures and resources for civil preparedness, however, have significantly changed through the years, in response to geopolitical shifts, changing threats and security contexts (Roepke and Thankey, 2019). For example, civil preparedness resources and capabilities in NATO countries were higher during the Cold War period, compared tow during the 1990s, when efforts and budget allocated were reduced in line with lower alert levels. On the opposite, as of 2014, following Russia's illegal annexation of Crimea and concerns about terrorist threats, such as the rise of ISIS, the alliance has re-focused its civil preparedness efforts to face terrorist, cyber and hybrid threats (Andrzej, 2020). It is in this context that NATO started prioritising cyber-attacks against CIs in its defence and civil preparedness frameworks. This re-focusing of efforts arose from the rising number of cyber-attacks against CIs by multiple actors, including state and non-state actors.

NATO embeds civil preparedness into its framework for overall *resilience*, understood as the capacity of individual nations as well as of the Alliance overall to resist and withstand military attacks. The Alliance sees civil preparedness as complementary to military efforts in reducing populations' vulnerabilities in peacetime, conflict, and during crises. Moreover, from NATO's perspective, member nations need to be prepared for a range of crises, including military attacks, cyber-attacks, hybrid, and environmental crises. Crucially, the core functions of civil preparedness for NATO are to ensure continuity of government, essential services to civilians

and support for the military. In the context of civil preparedness, the protection of civilian CIs, therefore, has a twofold value for the Alliance: first, to support continued governmental function and the provision of services to civilians; second, to support military operations, in that these depend on civilian and CIs (dual use infrastructures), including communication, transport, energy, food and water.

With regards to the EU, In March 2025, the EU has launched its EU Preparedness Union Strategy to prevent and react to emerging threats and crises. The Strategy gives a place of relevance to preparedness in case of cyber-attacks against the CIs, by urging EU MS to transpose and implement the Critical Resilience Directive (CER) and the NIS2 Directive, whereby the former focuses on the protection and resilience of critical entities in an expanded list of sectors with cross-border impact, and the latter provides for cyber-security and resilience to cyber-attacks for essential entities specifically in the same sector list. The Strategy is intended to also address disruptions arising from state-sponsored hybrid and cyber-attacks, including targeting and sabotaging critical assets. The document builds on the Disaster Resilience Goals and sets up 30 action points across seven areas, including population preparedness and related ones, such as foresight and anticipation, resilience of vital societal functions, public-private cooperation, civil-military cooperation, crisis response coordination and resilience through partnership.

In terms of comprehensiveness, the EU strategy is significantly more far-reaching than NATO's policies on the same matter. However, the NATO and EU strategies are aligned, complementary with one another, and their implementation reinforces the achievement of each strategy's specific objectives. The Alliance has set seven baseline requirements for national resilience against which each nation assesses its level of preparedness. The EU Disaster Resilience Goals are in coherent with NATO's resilience baseline requirements and EU objectives and actions for civilian preparedness reinforce and contribute to NATO's baseline requirements, as synthesised in Table 1.

Table 1: NATO and EU areas for civil preparedness[1]

NATO baseline requirement	Corresponding EU objective	Indicative timeline	Implementation status (EU)	Reference measure
Assured continuity of government and critical government services				
	Put in place a framework to maintain vital societal functions, including governmental continuity and decision-making	Not yet defined	The framework still needs to be drafted	European Preparedness Union Strategy
Resilient energy supplies				

[1] In the table, the EU objectives included in the EU Preparedness Union Strategy are made to correspond to the NATO's baseline requirements for resilience. For each EU preparedness objective is then indicated the proposed timeline for implementation, where available, the current status and other key relevant EU policy documents.

	Propose a stockpiling strategy for energy equipment and raw materials	2025	Registration for the raw materials mechanisms under the EU Energy and Raw Materials Platform has opened on 18 November 2025	European Preparedness Union Strategy
	Scale-up on response capabilities for energy	Not defined	Same as above	European Preparedness Union Strategy rescEU
	Build energy resilience with external partners	Not defined	Planning phase and some implementation via risk assessments, mapping of mutual resilience interests and diplomatic efforts	European Preparedness Union Strategy European Defence Readiness 2030
	Review the energy security of supply framework	2026	Ongoing	European Preparedness Union Strategy European Defence Readiness 2030
Ability to deal effectively with uncontrolled movement of people				
	Not incorporated in civilian preparedness plan	N/A	N/A	N/A
Resilient food and water resources				
	Ensure supply of water; Secure critical supplies;	2025	Some good practices have been identified There are three sets of recommendations under the European Food Security Crisis preparedness and response Mechanism (EFSCM)	EU preparedness strategy Prepar-EU

	Develop guidelines to reach a population self-sufficiency of minimum 72 hours, including storage of essential supplies	2025	The guidelines are not yet developed	EU preparedness strategy Prepar-EU
	Propose a stockpiling strategy for agri-food products and water	2025	EU stockpiling strategy proposed on 9 July 2025	EU preparedness strategy Prepar-EU
Ability to deal with mass casualties				
	Set up a European field hospital	Not defined	Conceptualisation phase	EU preparedness strategy
Resilient civil communications systems				
	Establish a public-private Preparedness Task Force which supports crisis communication efforts	2025	Established	Preparedness Strategy
	Establish a European Critical Communication System	2026	In progress, the European Commission has launched a feasibility study. In the meantime, some initiatives exist at the national level for communication between member States	Preparedness Strategy rescEU
	Establish an EU Earth Observation Governmental Service (EOGS)	2027	Operational implementation still under definition	Preparedness Strategy
Resilient transportation systems				
	Develop a EU Contingency Plan for Transport		Planning phase	EU stockpiling strategy
	Promote dual-use infrastructure	Not defined	Strategy design phase	Preparedness Union Strategy

Both NATO and EU strategies emphasise the interdependence between civilian and military sectors, stating that in case of cyber-attacks civilian authorities need military support and military operations need civilian structures. In its Strategy, the EU sets to identify dual-use

infrastructure and assets across MS to ensure that their design and operationalisation meet high cyber-security standards. With regards to infrastructures for transport crossing different MS, the Commission and High Representative require that MS invest, where possible and relevant, on building or upgrading civilian infrastructures so that these can serve to the transport of troops or military materials. Crucially, the EU strategy reinforces NATO's civil and military preparedness in two ways. First, by requiring MS to construct or upgrade transport infrastructure so that these can accommodate troops and materials 'in accordance with NATO military requirements'. Second, by developing technical standards for dual-use infrastructures and assets that align with NATO's standards. Similarly, in the field of energy, promoting the resilience of energy infrastructures, which are necessary also to military efforts, is a priority for both NATO and the UE, under the rescEU programme.

With regards to EU-NATO cooperation in case of crisis, the EU strategy integrates preparedness and resilience into the cooperation with NATO, through exchanges via dialogues and briefings and through training. Core mechanisms for EU-NATO coordination in case of crisis, however, are in a conceptualisation state, rather than ready to be fully operationalised. In case of crisis, the EU intends to encourage operational cooperation amongst EU and NATO staff, though the exact mechanisms and actors involved are still unclear. Moreover, the EU intends to organise regular exercises, but these are also still in the planning stage. Given the status of current efforts, this paper proposes a tailored set of recommendations in the upcoming sections.

3. Conclusions and recommendations

Having examined the EU and NATO approaches to civil preparedness in case of CI failure, due to cyber-attacks, the paper concludes that the EU approach is more comprehensive and far-reaching that the NATO's one. This is also due to the nature of NATO's focus, which sees civil preparedness as objective of military action and instrumental to military actions, whereby the resilience of civilian infrastructures is a key enabler for the sustainability of military operations. However, the two approaches are coherent with one another and can be seen in continuity, in that the implementation of EU objectives and actions towards civilian preparedness strengthen NATO's requirements for civil preparedness, and vice versa.

Looking forward, civil preparedness in case of cyber-attacks against CIs need to be improved via targeted actions, coordination and integration of efforts between EU and NATO and between EU MS. Plans and guidelines developed can benefit from lessons learned from different types of crises and can be applied also to improve civilian resilience during CI disruptions in peace-time. This section presents a non-exhaustive list of recommendations where EU-NATO cooperation is both possible and advisable in order to enhance CI resilience to cyber-attacks and, in turn, civil and military preparedness. The recommendations are based on a phase approach to crisis analysis, which sees crisis events divided into pre-crisis measures which enhance the baseline resilience and capacity, measures during crises which reduce the

duration and severity of disruptions, and measures for the recovery phase after crises with rapid resumption of acceptable levels of functioning and the extraction and implementation of lessons learned.

With this in mind, we advance the following recommendation of areas of EU-NATO cooperation on crisis preparedness to cyber-attacks:

- The development of a regulatory and policy debate format that can close systemic gaps preventing greater preparedness for disruptions. For instance, many MoDs in the EU (and consequently also NATO) are developing their own energy production and storage facilities to lower dependence on the civilian sectors and to free resources for civilians in case of crisis. Many of these are in the renewables sectors, making Ministers of Defence (MoDs) capable of acting as prosumers. However, there is a lack of national and EU legislation allowing them to act as prosumers, which cuts off one avenue for increased resilience to CI disruption;
- Investment in CI security and in new CI development, especially in dual-use sectors, is very important and yet constrained by the availability of resources and higher requirements. Formulas such as defence-oriented banks and infrastructure funds have been advanced but not implemented in the EU, while there is limited experience in some NATO countries, such as Turkey. A 2024 Atlantic Council report recommended the establishment of a Defense, Security, and Resilience Bank (Murray, 2024). Even with the latest announcements from the Hague Summit regarding the allocation of 1.5% in defence adjacent spending such as cybersecurity, infrastructure and, presumably, resilience and preparedness, requirements will be quite higher overall, and the latest commitments are synergistic rather than in competition with such a proposal for a bank which could be implemented at EU level. Murray (2024) proposed it in the context of NATO, but the Trump Administration's turn against multilateralism makes such a bank more suited for the EU;
- EU efforts for civil-military cooperation that enable NATO goals can also be a valuable "force multiplier". For instance, the EU can facilitate a formula for a dialogue format for MoDs and operators of critical infrastructures to exchange views on the security environment and the potential contributions that MoDs can make to enhanced resilience of the CIs within the national territory, such as acting as redteams in exercises;
- An EU-NATO focus on secure supply chains for cyber-physical systems in critical infrastructures, aimed at enhancing resilience against supply chain attacks, which is emerging as a significant vulnerability and can be implemented through common standards, yearly reviews of supply chain security by sector, such as in energy and telecommunications, and an enhancement of the role of the US-EU Trade and Technology Cooperation Council;
- The development of an EU-NATO partnership on sustainable adoption of emerging digital technologies such as AI;

- A societal resilience initiative that aims to combat disinformation, fake news and radicalization, with the EU taking point on implementing methodologies and strategies to detect and counteract threats such as attacks on telecom infrastructure by people radicalized by online propaganda against 5G propaganda or by environmentally-motivated actors countering nuclear or fossil fuel energy sources;
- The establishment of a clearing house for information on cyber-attacks and the distribution of lessons learned through on-site analysis of cyber-attacks against CI, an area where the EU has an emerging framework;
- A joint EU-NATO approach towards enhancing resilience of North-South infrastructure through Three Seas Initiative projects that can then be expanded through partnerships in other areas such as on the security dimension of Macroregional Strategies in the Baltics, Black Sea, Adriatic etc.

REFERENCES

Jacuch, Andrzej. "Security and defense challenges–civil preparedness in NATO." *Scientific Journal of the Military University of Land Forces* 52, no. 2 (196 (2020): 270-280.

Duguin, Stéphane, and Pavlina Pavlova. "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict." *Policy Department for External Relations Directorate General for External Policies of the Union. https://www. europarl. europa. eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI (2023) 702594_EN. pdf* (2023).

European Commission (2024) "Safer together: Strengthening Europe's civilian and military preparedness and readiness", Report by Sauli Niinistö, former President of the Republic of Finland in its capacity as special adviser of the President of the European Commission.

European Commission (2025). Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions On The European Preparedness Union Strategy. Join/2025/130 Final

European Commission Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions Eu Stockpiling Strategy: Boosting The Eu's Material Preparedness For Crises

European Commission (2024) "Safer together: Strengthening Europe's civilian and military preparedness and readiness", Report by Sauli Niinistö, former President of the Republic of Finland in its capacity as special adviser of the President of the European Commission

European Commission: Secretariat-General, *EU Preparedness Union Strategy*, Publications Office of the European Union, 2025, **https://data.europa.eu/doi/10.2792/1964849**

European Disaster Resilience Goals - European Commission : https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/european-disaster-risk-management/european-disaster-resilience-goals_en

Joint White Paper For European Defence Readiness 2030

Murray, R. (2024). How a new global defense bank—the 'Defense, Security, and Resilience Bank'—can solve US and allied funding problems. Atlantic Council, 13 December 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/how-a-new-global-defense-bank-can-solve-us-and-allied-funding-problems/

NATO. (2022). Strategic Concept. Brussels.

Roepke, W.-D., & Thankey, H. (2019, February 27). Resilience is the first line of defense. NATO Review. https://www.nato.int/docu/review/uk/articles/2019/02/27/stjkst-persha-lnya-oboroni/index.html