ISSN 1831-9424

EUROPEAN DEFENCE AGENCY

European Commission

FORTIFYING DEFENCE

Strengthening Critical Energy Infrastructure against Hybrid Threats

EUR 31505 EN

This publication is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information
European Commission, Joint Research Centre (JRC)
Directorate E – Space, Security and Migration
JRC.E.2 – Technologies for Space, Security and Connectivity
E-mail: JRC-E2@ec.europa.eu

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC133083
EUR 31505 EN

Print	ISBN 978-92-68-03257-2	ISSN 1018-5593	doi: 10.2760/824475
PDF	ISBN 978-92-68-03246-6	ISSN 1831-9424	doi: 10.2760/58406

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: G. Giannopoulos, R. Jungwirth, C. Hadjisavvas (European Defence Agency) Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/58406, JRC133083.

Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats

Authors

Georgios Giannopoulos (European Commission Directorate-General Joint Research Centre)
Rainer Jungwirth (European Commission Directorate-General Joint Research Centre)
Constantinos Hadjisavvas (European Defence Agency)

Contributors

European Commission Directorate-General Joint Research Centre
Etienne Willkomm
Monica Cardarilli
Georgios Valsamos

European Defence Agency
Ioannis Chatzialexandris
Maja Kuzel
Alessandra Lazzari
Ruairi Talbot

ICI Bucharest
Alexandru Georgescu

FOREWORD

The alarming surge in hybrid threats on European soil has starkly exploited the vulnerabilities and interdependencies of the EU's critical infrastructure. Such threats include relentless waves of cyber-attacks on our critical entities and intensifying challenges arising from the cascading effects of climate change and the COVID-19 pandemic. State and non-state actors are employing hybrid threats to destabilise our societies for example through economic coercion, disinformation campaigns, interference in our political processes, and the abuse of migration flows. The Russian invasion of Ukraine has illustrated the potential intersection of energy security and hybrid threats, as malicious actors endeavour to exploit vulnerabilities in energy supplies to impair the functioning of our societies.

These challenges have demonstrated unequivocally the urgent need for the European Union to enhance its energy security and autonomy. This is not only vital for the Union's prosperity but also indispensable for the readiness and sustainability of the armed forces. Within the framework of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS III) the European Defence Agency and the European Commission Joint Research Centre embarked on an in-depth study on bolstering the resilience of defence-related critical energy infrastructure in the face of hybrid threats.

The ground-breaking study identifies potential hostile actors that could undermine the EU's interests and describes diverse hybrid tools they may employ to target our critical entities and exploit our weaknesses. It examines the far-reaching implications such activities may have on our societies. The study offers an invaluable resource for stakeholders seeking a deeper understanding of the evolving nature of hybrid threats.

The study's overarching goal is to fortify defence energy resilience by proposing a comprehensive suite of measures at the EU and national levels designed to assess and mitigate vulnerabilities, streamline policies and procedures, and to harness advanced technologies and capabilities to counter hybrid threats effectively and holistically. In doing so, the study provides the Ministries of Defence and other relevant stakeholders with recommendations for fostering civil-military collaboration, heightening awareness, sharing best practices and creating synergies for joint projects to ensure defence energy resilience. As EU Member States underscore in the EU's Strategic Compass for security and defence, all these efforts will strengthen our solidarity and mutual assistance.

Jiří Šedivý
Chief Executive
European Defence Agency

Salla Saastamoinen
Deputy Director-General
Joint Research Centre

CONTENT

ACKNOWLEDGEMENTS

The authors would like to thank the members of the third phase of the Consultation Forum for Sustainable Energy in the Defence and Security Sector, especially Working Group 3 on the Protection of Critical Energy Infrastructure, for their valuable feedback and contributions to this study. The authors also thank the colleagues of the European Commission Directorate-General for Energy and the European External Action Service who contributed to this study for their insightful comments, helpful discussions, and careful review.

ABSTRACT

The European security order is undergoing a fundamental transformation, where hybrid threats will likely increase. In this context, this study aims to respond to the evolving geopolitical landscape and provide the ministries of defence (MoDs) with a more comprehensive conceptual basis to facilitate the development of the necessary measures to counter hybrid threats. This will enhance the resilience of critical energy infrastructure (CEI) necessary for the functioning of the defence sector.

To ensure EU-wide coherence, this study follows the conceptual framework on hybrid threats and the comprehensive resilience ecosystem (CORE) model developed by JRC and the Centre of Excellence for Countering Hybrid Threats in Helsinki (HCoE). Thus, it focuses on (sub)domains for identifying defence-related CEI interdependencies and investigating the tools that adversaries could employ to undermine their performance.

In addition, this document provides MoDs and other stakeholders with recommendations for increasing the resilience of defence-related CEI against hybrid threats by promoting civil-military collaboration at the EU level, raising awareness, sharing best practices, stimulating discussion and triggering critical thinking on how to maintain the energy supply and thus safeguard military performance.

EXECUTIVE SUMMARY

In 2015 the European Commission and the European Defence Agency (EDA) established the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) with the primary scope to assist the European Union (EU) ministries of defence (MoDs) and relevant stakeholders in moving towards green, resilient, and efficient energy models. Since then, the Forum has grown and become the largest European defence energy community. It provides a unique platform for MoDs and relevant stakeholders to share knowledge and promote collaborative defence research and innovation on sustainable energy. In fulfilling its role, the Forum stimulates research to tackle energy security challenges and contributes to implementing the European Green Deal, a key initiative targeting climate neutrality by 2050.

One of the primary objectives of the Consultation Forum is identifying how the EU MoDs and relevant stakeholders could contribute to bolstering the resilience of critical energy infrastructure (CEI) on which the defence sector, including the armed forces, depends to preserve its sustainability and operational effectiveness. Within the Forum, the working group «Protection of Critical Energy Infrastructure» (PCEI WG-3) determines the role of defence in ensuring the uninterrupted provision of CEI services. The group recognises that if this infrastructure is not adequately protected and resilient, significant disruptions may occur as the result of physical or cyber-attacks, leading to substantial repercussions within the individual EU Member States and the entire EU.

In response to the evolving threat landscape, the EDA, the European Commission Directorate-General Joint Research Centre (JRC), and the CF SEDSS III PCEI WG-3 have jointly produced this study to provide the MoDs and relevant stakeholders with recommendations on how to increase the resilience of defence-related CEI against hybrid threats. These recommendations focus on promoting awareness, sharing best practices and appropriate counter-measures. Therefore, the study emphasises promoting civil-military collaboration at the EU and national levels to enhance the resilience of CEI further, stimulating discussion and triggering critical thinking among EU MoDs and institutions and bodies.

To ensure coherence at the European level, the study adheres to the conceptual framework on hybrid threats (Giannopoulos et al., 2021) and the comprehensive resilience ecosystem (CORE) model developed by JRC and the Centre of Excellence for Countering Hybrid Threats in Helsinki (HCoE). The CORE model provides an ecosystem-level analysis of the impact of hybrid threats, offering a comprehensive perspective to counter them. It adopts a whole-of-society approach, encapsulating three spaces (civic, governance, services) and three layers (international, national, local). This analytical framework is applied by the study to the impact of hybrid threats on defence-related CEI. The focus is placed on the infrastructure and military/defence domain, consistent with the rationale defined by the CORE Model. In this regard, the study explores various tools that could be employed to compromise the operational effectiveness of infrastructure and the military/defence domain, providing a solid basis for MoDs to develop necessary measures for ensuring their resilience.

Building on this framework, the study provides recommendations to fortify defence-related CEI against hybrid threats at the EU and MoD levels. These recommendations involve a comprehensive inter-dependency analysis, risk management development, technology investment, intelligence reporting, training and education and scenario-based exercises. At the EU level, the study proposes establishing an EU collaborative platform and communication channels to address hybrid threats and foster civil-military collaboration. At the MoD level, the recommendations focus on tracking CEI ownership, regular vulnerability assessments, post-event data collection and analysis, establishing communication channels, and investment in personnel training.

The study seeks to enrich the EU-wide efforts by assimilating lessons from past experiences, determining how the EU can better synergise with national initiatives and promoting a robust European comprehensive approach to maintain the resilience of defence-relate CEI against hybrid threats. This comprehensive approach will result in a more profound understanding of hybrid threats and encouraging collaboration and information sharing at the strategic level. Enhancing dialogue between the civil and military communities is a sine qua non for addressing hybrid threats against defence-related CEI. As the nature of hybrid threats continues to evolve, this study will adapt accordingly to reflect both European and national policy priorities, thus serving as a dynamic resource for decision-makers.

Understanding the evolving nature of hybrid threats is vital for fortifying defence-related infrastructure.

1. INTRODUCTION

1.1. Context and Project Phases

Building on the successful outcome of its first two phases (2015-2019) and to address emerging and future challenges in the field of energy, EDA and the European Commission launched on 1 October 2019 the third phase of the **Consultation Forum for Sustainable Energy in Defence and Security Sector** (CF SEDSS)[1]. Since 2015 the Consultation Forum has become the ***largest European defence energy community***, providing a unique platform for MoDs and relevant stakeholders to share knowledge and promote collaborative defence research and innovation on sustainable energy.

In Phase III (2019-2023), the project continues improving energy efficiency and buildings performance, utilising renewable energy sources in the defence sector and increasing the resilience of defence-related critical energy infrastructure. It also focuses on addressing the cross-cutting thematic areas on energy management and policy, energy innovative technologies and identifies applicable instruments for funding or financing defence energy-related topics. Furthermore, emphasis is given on bringing closer the defence and energy communities as well as gaining and sharing expertise from research technology organisations, academia and industry to address emerging and future challenges ranging from climate change and environmental issues to hybrid threats.

Overall, Phase III presents the defence and security sector with an economic, operational, and strategic opportunity to reduce reliance on fossil fuel and natural gas, progressively minimise energy costs and carbon footprint, and enhance operational effectiveness and energy resilience.

1.2. Study's Objectives, Structure and Limitations

Despite the high relevance of enhancing resilience of critical infrastructure, there is still a knowledge gap on this issue. Thus, this study is dedicated to closing such a gap, focusing on CEI, owned by the civil side of public or private sectors. Civil and military energy supplies are difficult to separate completely. The **defence sector relies, to a great extent, on civil energy infrastructure for its functioning and operations.** MoDs are aware of this reality and the associated dependencies which might hinder the defence sector from performing its duties and missions in case of major energy infrastructure disruptions.

Defence-related (civil) CEI can be described as the 'Achilles heel' of the military and its performance capabilities. Simply put, without the availability of those infrastructure, the operational capability of an army is severely hampered. A **key challenge** of **any military operation is therefore to maintain the energy supply and thus enable military performance** and combat power,

1 The phase III of the CF SEDSS project is funded by the EU's horizon 2020 research and innovation programme under the grant agreement No. 882171 and will cover a period of four years until 30 September 2023. For more information about the CF SESS, visit the dedicated web-page: Consultation Forum Sustainable Energy (europa.eu)

focusing on the measures and procedures to ensure resilience.

In particular, the study elaborates upon the need to enhance resilience of defence-related CEI against hybrid threats. Countering hybrid threats requires a common understanding among policy-makers and practitioners, identifying at an early stage the occurrence of hybrid threat activities as well as identifying gaps and developing adequate actions in order to bolster resilience at local, national and European levels. Currently, the scientific community, as well as policy-makers and security practitioners, are providing different views on the topic which undoubtedly enriches the amount of knowledge in this area; however, they do not necessarily contribute towards a common understanding.

Against this background, this study builds on previous work done by the JRC and the HCoE (Giannopoulos et al., 2021), which has provided a basic framework for understanding hybrid threats and become the de facto standard for addressing hybrid threats in the EU. Thus, the scope of this work builds on this theoretical groundwork and applies it to the issue of hybrid threats targeting defence-related CEI.

Following the introduction of the analytical framework, this **study focuses on outlining and analysing specific threats facing defence-related CEI,** highlighting the elements that need to be considered to increase their resilience. Finally, it **provides the MoDs with recommendations on better contributing to increasing the resilience of defence-related CEI against hybrid threats** by raising awareness, sharing best practices and developing the appropriate measures to counter them.

1.3. EU Policy Landscape

The European security order is currently undergoing a fundamental transformation. One aspect of this change is the prevalence of hybrid threats over the last 10 to 15 years, which is expected to increase further. In particular, hostile actors increasingly employ hybrid methods to target the strategic interests of the EU and its Member States, posing growing threats to the security of the EU (Council of the European Union, 2022a). This is reflected in a number of policy actions and decisions, as well as in the engagement of both EU Member States and institutions in countering hybrid threats.

At the EU inter-institutional level, the **Joint Framework on countering hybrid threats** (European Commission, 2016) and **the Joint**

Hostile actors increasingly employ hybrid methods to target the strategic interests of the EU and its Member States, posing growing threats to the security of the EU.

Communication on increasing resilience and bolstering capabilities to address hybrid threats (European Commission, 2018) focus on the need to strengthen resilience. Furthermore, the **EU Security Union Strategy** (SUS) (European Commission, 2020a) underlines the need to build resilience to prevent and protect the EU against hybrid threats and the importance of systematically tracking and objectively measuring progress in this area.

In November 2020, the EU published its **first Climate Change and Defence Roadmap** (EEAS, 2020) to address the links between defence and climate change as part of the wider climate-security nexus. Significantly, the Roadmap acknowledges the need for further research on enhancing the resilience of defence-related CEI against hybrid and asymmetrical threats, and emphasises the role of the Consultation Forum (CF SEDSS) in generating new project ideas and facilitating their implementation. In response, the EDA and JRC conducted research within the CF SEDSS, and the initial findings were reported in the 2022 Joint Progress Report on Climate Change, Defence and Security (EEAS, 2022). The progress report emphasises the importance of EU and Member State collaboration in addressing hybrid threats by emphasising the necessity to:

- support the Member States to address vulnerabilities and risks;
- provide a suitable platform for raising awareness and sharing knowledge, expertise and best practices;
- explore through a table-top exercise the dependencies of the defence sector in the event that defence-related CEI is compromised or unable to function due to hybrid threats;
- promote synergies and complementarity and foster cross-border cooperation by developing joint collaborative projects, research studies and exercises.

In February 2022, the **European Commission** reiterated its commitment to contributing **to enhance European defence resilience** by boosting innovation and addressing strategic dependencies (European Commission, 2022a). Focus was also placed on combating hybrid threats and climate change challenges within the defence sector. In pursuit of these efforts, the Commission is dedicated to establishing a policy framework that promotes reduced energy demand and enhanced energy resilience for critical technologies used by civilian security actors and armed forces. Additionally, the Commission is determined to develop concrete climate-resilient solutions to address evolving challenges and ensure defence sustainability.

This momentum and actions are significant regarding European critical infrastructure, as set out in the **EU's Strategic Compass for Security and Defence** (Council of the European Union, 2022b). Specifically, the Strategic Compass identified the need to «harness innovation to enhance the energy efficiency of the defence sector (...) without reducing operational effectiveness... [and significantly] to develop common benchmarks and standards for the increased use of renewable energy sources and the resilience of defence-related critical infrastructure.» In addition, the identification of sectoral hybrid resilience baselines (European Commission, 2022b) covers sectoral legislation and policy documents grouped in domains prone to hybrid threat interference complementing the mapping of measures related to enhancing resilience and countering hybrid threats (European Commission, 2020b).

In this context, the issue of hybrid threats is high on the EU political agenda, and it can be considered as a vital element of concern for MoDs across Europe. Especially against the backdrop of the EU's shift to green technologies and renewable energy sources (RES), military officials have to consider not only the benefits of this transformation but also the associated risks and potential cascading effects. **As the EU pursues a climate-neutral and resilient Energy Union, it is essential to strike a balance between the defence transition and maintaining the operational effectiveness of armed forces.**

Acknowledged by the Council of the European Union, 2019, the Consultation Forum plays a pivotal role in developing resilient and sustainable energy models as well as strengthening cooperation in tackling energy security challenges. This includes energy efficiency, renewable energy solutions and the protection of critical energy infrastructure against hybrid threats and climate change cascading effects (Tavares da Costa et al., 2023). Through these efforts, the Forum assist the MoDs in advancing energy transition and enhancing climate change adaptability, while contributing to implementing the European Green Deal objectives (European Commission, 2021a, 2019a).

In this light, it is vital for the defence sector to consider the recently introduced **Directive on Critical Entities Resilience** (CER) (European Commission, 2022c). This directive expands upon and supersedes the previous European Critical Infrastructure (ECI) Directive (European Commission, 2008), further emphasising the importance of protecting critical infrastructure. In particular, the CER Directive looks at critical entities as providers of essential services «crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment» (European Commission, 2022c) whose interruption may lead to significant disruptive effects and cascades across society. In line with the CER Directive, the armed forces have the potential to significantly contribute to increasing the CEI's robustness and survivability. While the CER Directive aims at strengthening physical non-cyber resilience of critical infrastructure, the **EU Directive on the security of network and information systems** (NIS2) (European Commission, 2022d) provides legal measures to strengthen the overall level of cybersecurity in the EU as well as streamlines incident reporting obligations with more precise provisions on

The EU's comprehensive policy and diverse toolbox can support Member States' defence ministries in successfully mitigating the vulnerabilities and risks associated with hybrid threats.

reporting, content and timeline. Although hybrid threats may not be the primary focus of NIS2, the directive's wider goal of enhancing cybersecurity and protecting critical assets can help mitigate the impact of such threats.

As malicious activities will continue targeting European critical entities, it is imperative to **enhance joint situational awareness and cooperation between EU Institutions and Member States** (Council of the European Union, 2022b), factoring the level of interdependency into the planning of the defence sector. In view of that, the **EU's Action Plan on Military Mobility** (European Commission, 2022e) strengthens the need to enhance the protection of the transport sector, military mobility being reliant on civil transport infrastructure, especially with cross-border dimension, while reducing dependency on fossil fuels in military transport with implications for the availability of renewable energy sources and related technologies. Significantly, this work will draw on relevant results from the CF SEDSS, including research studies and project ideas.

2. ANALYTICAL FAMEWORK FOR COUNTERING HYBRID THREATS

2.1. The Conceptual Model: Actors, Tools, Domains, Activities, and Targets

The term hybrid threats refers to:

Actions conducted by state or non-state actors aimed at undermining or damaging a target through a combination of overt and covert military and non-military means.[1] *Such actions are coordinated and synchronised and deliberately target the vulnerabilities of democratic states and their institutions. The common denominator for hybrid threats actors is their aim to undermine or harm democratically established governments, countries or alliances* (Jungwirth et al., 2023).

Based on this definition, the conceptual model helps to understand hybrid threats and provides an initial analytical framework of this phenomenon (Giannopoulos et al., 2021). It is based on the following **five pillars** (see Figure 1):

- Actors
- Tools
- Domains
- Activities
- Targets

Significantly, the model seeks to answer **who, how, where, when** and **why** questions with respect to analysing hybrid threats.

The model identifies two main categories of actors, namely **state and non-state**. In addition, it identifies a list of possible tools (e.g., physical operations to infrastructure) and **13 domains** (infrastructure, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, political, diplomacy, information) which can be targeted by actors applying specific tools towards achieving their objectives.

Generally, an **actor** (state or non-state) can apply a combination of **tools** on one or more **domains** to perform certain hybrid threat **activities** to achieve one or a series of **targets**. The targets can be achieved either by the **direct effect** of the tool to the domain or due to **cascading effects** caused.

The structure of the conceptual model also makes it possible to capture the **temporal scale** of hybrid threats and the way an actor can use a **combination** of tools to achieve one or more objectives. An important parameter of this framework is, therefore, the **timeline** for hybrid threats.

1 https://www.hybridcoe.fi/hybrid-threats/

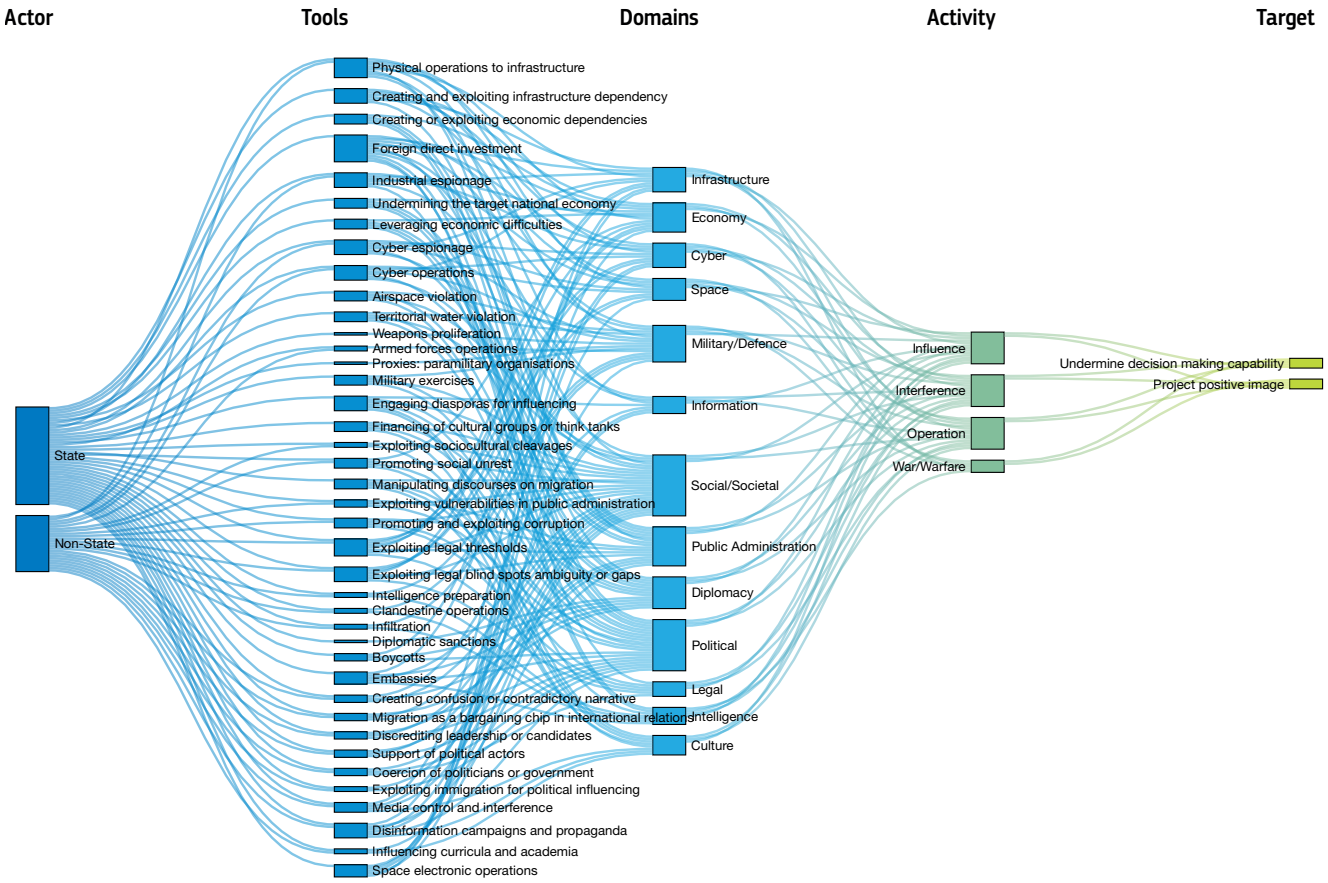

Figure 1. Visualisation of the conceptual model (Giannopoulos et al., 2021)

According to the model, hybrid threat activities posed by an adversary are characterised by different **escalation stages**, which are defining elements of the hybrid nature of threats. These are represented by three main phases (see Figure 2):

I. Priming
II. Destabilisation
III. Coercion

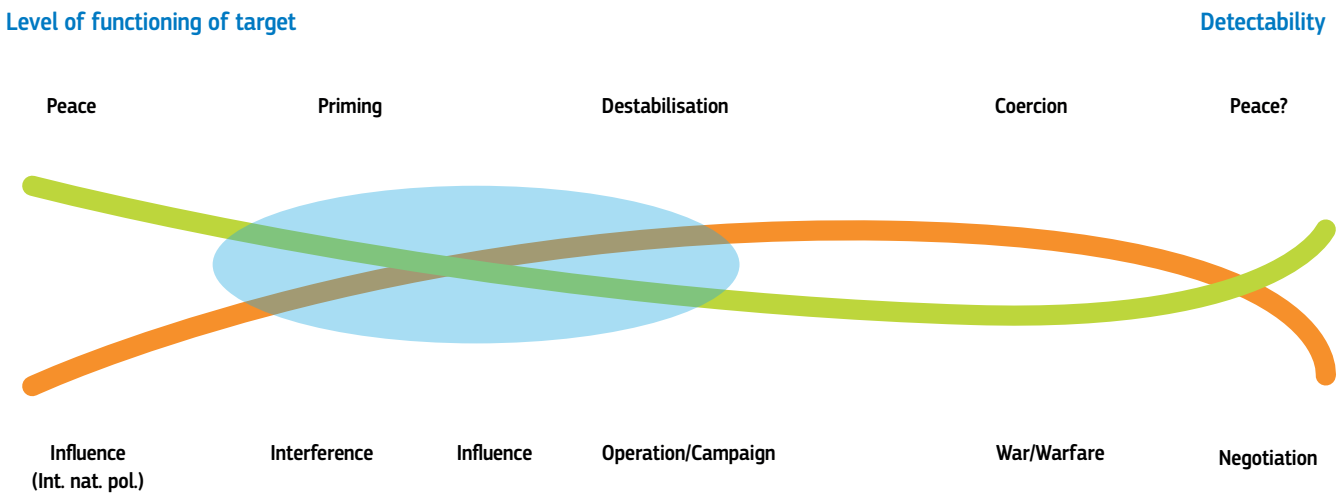

Figure 2. Escalation phases and associated activities (Giannopoulos et al., 2021)

The **priming phase:** it is particularly challenging for the **detection and attribution** of hybrid threat activities. In the priming phase, the actor's goal is for the **target** to voluntarily make harmful decisions. In this phase, if there is already a plan to escalate towards military conflict, the actor will try to infiltrate and position its subversive capabilities in the internal space of the target. This goal is pursued through **interference** that blurs situational awareness (Giannopoulos et al., 2021). However, during the priming phase the functioning of the targeted society is still high. It is ideally in the priming phase where hybrid threat activities must be detected and counter-measures taken. Considering that one of the main characteristics of hybrid threats is their blurred character and expansion across diverse jurisdictions, detection and attribution is rather cumbersome, hindering a coordinated response.

The **destabilisation phase:** it is characterised by an actor intensifying the hybrid threat activities in the manner of a **campaign** (multiple operations) or using it for an **operation** to achieve the intended goal. It is difficult to identify when an actor changes mode. In the destabilisation phase, the activity becomes more visible, aggressive and may involve more violence. This happens either according to the actor's need or an opportunity that presents itself, or because of the actor's frustration with the status quo. In this phase, the boundaries between acceptable and unacceptable and between legal and illegal actions become blurred (Giannopoulos et al., 2021). The destabilisation phase is accompanied by a gradual degradation in the ability of the target to respond to the threat.

The **coercion phase:** hybrid threat activities have now gone beyond insufficient detection and attribution and can be described as hybrid warfare. **Hybrid warfare** represents the «hard end» of the escalation spectrum of hybrid threat activities. Basically, hybrid warfare is a combination of covert and overt military operations, combined with political and economic measures, subversion, information/disinformation operations and propaganda/fake news, the covert or overt use of special forces, and military support or overt military actions, including cyber-attacks as part of the overall orchestration (Giannopoulos et al., 2021). This becomes vital given that while an open attack on energy infrastructure may lead to open warfare, hybrid threats may help adversaries to achieve their objectives. However, the impact on operational effectiveness of defence and armed forces could be irreversible.

2.2. The CORE Model: COmprehensive Resilience Ecosystem

Building upon the conceptual framework, the CORE model analyses the impact of hybrid threats and provides a more comprehensive (ecosystem) analytics to counter them. The CORE model is based on a **whole-of-society approach** (European Commission, 2021b; Wigell et al., 2021), including three **spaces** (civic, governance, services) and three **layers** (international, national, local), representing the different sectors and levels of society respectively (see Figure 3). The **13 domains** introduced in the conceptual model are considered as potential **entry points** into the ecosystem.

Resilience to hybrid threats requires strong **ecosystem foundations.** The seven foundations ensuring a resilient ecosystem (CORE model) are:

1. Feeling of justice and equal treatment
2. Civil rights and liberties
3. Political responsibility and accountability
4. Rule of law
5. Stability
6. Reliability / availability
7. Foresight capabilities

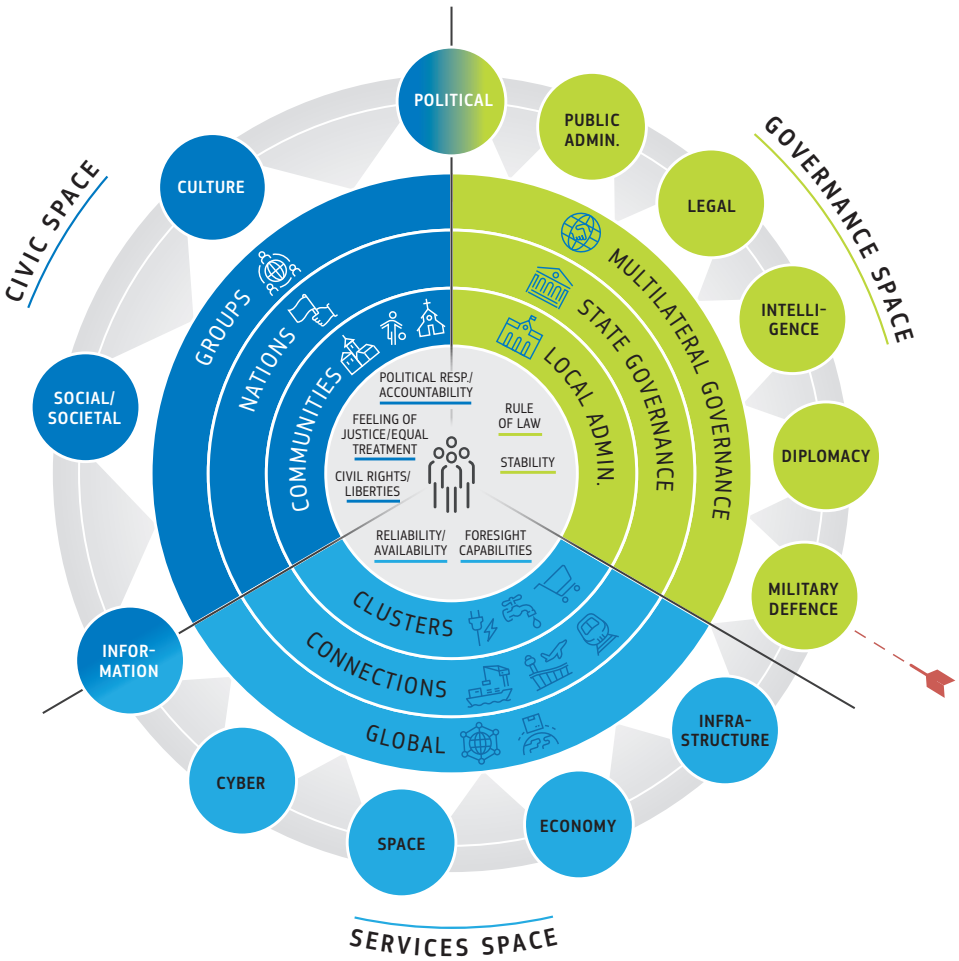

Figure 3. CORE-model – structure (Jungwirth et al., 2023)

At the heart of all foundations is trust and credibility, which is essentially the glue that makes **dependencies and connections** strong and healthy in democracies, and supports the foundations of democratic systems. The seven foundations are the basis of democratic society and are essential in building resilience against hybrid threats (Jungwirth et al., 2023).

2.2.1. Resilience vs. Resilience against Hybrid Threats

Resilience has a central function in the ecosystem's capacity to withstand hostile actions. Generally, resilience is used in many different fields, with specific definitions varying by discipline. In general terms, **resilience** means being resistant to and overcoming external shocks by adapting and moving towards a new stable equilibrium that can be close to the original one before the disturbance (Jungwirth et al., 2023).

Resilience in the context of hybrid threats requires instead an understanding of the EU as a whole-of-society system in which several interconnections and inter-dependencies must be considered. This approach is necessary as hostile actors seek to achieve primarily **three objectives** using hybrid threats to (Jungwirth et al., 2023):

a. undermine and harm the integrity and functioning of democracies;
b. change or challenge the decision-making processes and credibility;
c. create cascading effects (across the three spaces of the society, the three layers and the 13 domains).

Hybrid threats aim to undermine democratic integrity, challenge decision-making credibility, and cause cascading societal effects.

Building resilience against hybrid threats, for example, to protect and strengthen defence-related critical (energy) infrastructure therefore requires a perspective that goes beyond resilience in sectoral areas. Instead, it necessitates developing resilience while considering dependencies and interdependencies between the different domains and actors of society that are relevant for critical (energy) infrastructure in the defence sector (see Figure 4). Hence, the whole-of-society approach is needed to develop and increase resilience against hybrid threats.

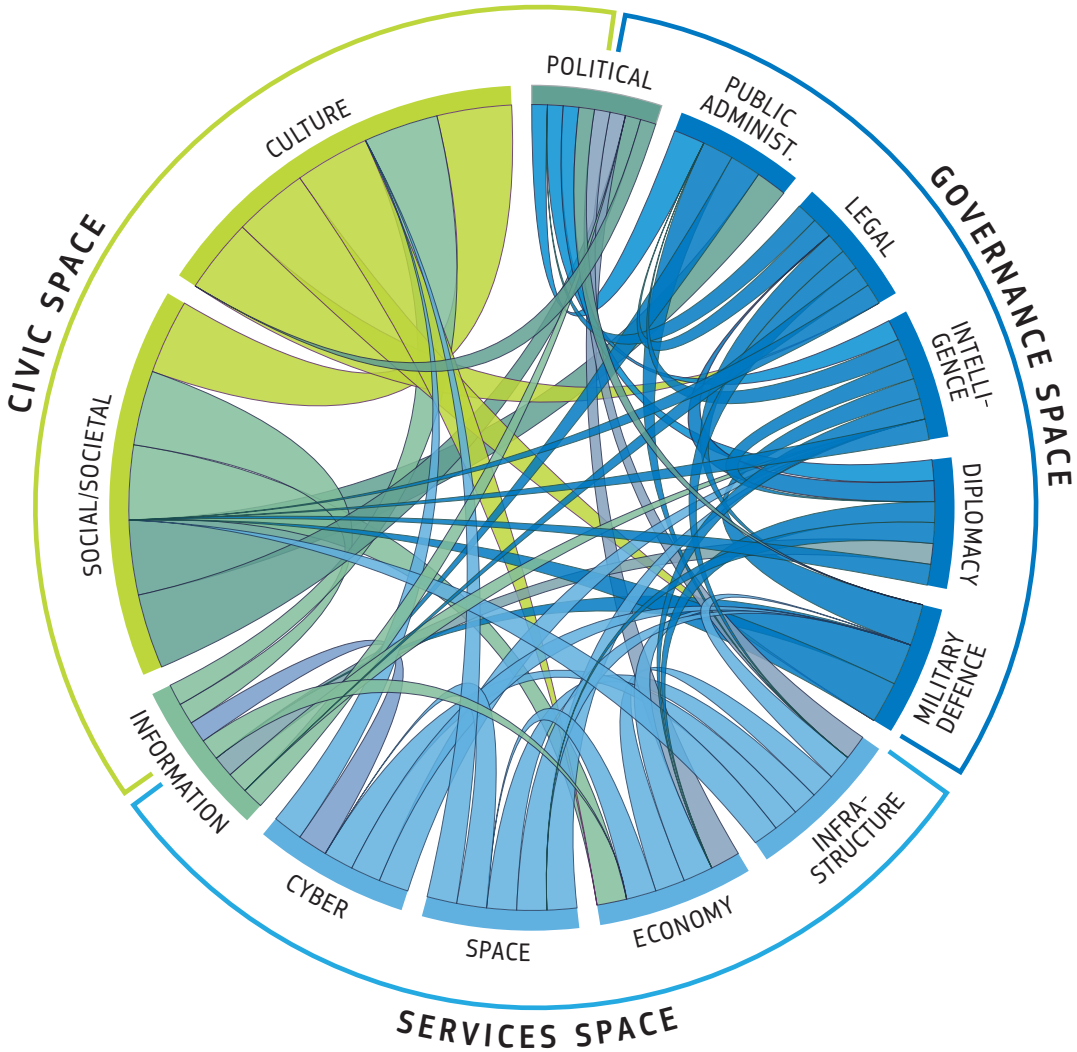

Figure 4. Resilience and interconnections between domains (Jungwirth et al., 2023)

When defences are inadequate, it is considerably easier for attackers to execute their plans and actions which aim at compromising several levels and layers across different locations. Using the CORE model and its whole-of-society approach, the interaction dynamics that connect domains with the three spaces and their layers are represented. Moreover, the CORE model is used to analyse and ultimately counteract hybrid threats and their impacts that seek to achieve one or more of the three objectives mentioned above.

Resilience against hybrid threats requires consideration of interdependencies across interconnected domains, crucial for the defence energy resilience.

3. HYBRID THREATS EFFECTS ON DEFENCE-RELATED CRITICAL ENERGY INFRASTRUCTURE

This chapter applies the analytical framework described above to the effects of hybrid threats to defence-related CEI. Using the rationale defined in the conceptual and CORE models, the focus is now on the infrastructure and military/defence domain. In a potential scenario, a **hostile actor** has two ways to exploit vulnerabilities to target defence-related CEI: **directly or indirectly**. The next sections discuss several relevant tools that can be used to directly or indirectly target the infrastructure and the military/defence domain to compromise their operational effectiveness.

3.1. Direct Target: the Infrastructure and/or Defence Domain

Hybrid threats actors are flexible in their choice of tools to achieve their strategic goals. Not only the combinations of different tools may vary, but also the **way, intensity and duration** in which they are applied. Due to technological innovations and other factors such as the context of conflict situations, new tools are constantly emerging and existing tools are being adapted (Giannopoulos et al., 2021). For these reasons, a listing of tools is always incomplete and must be constantly renewed. Nevertheless, this section resorts to the listing of the most important tools that can directly target the infrastructure and/or the military/defence domain (see Figure 5), including a hypothetical scenario as example (see Figure 6).

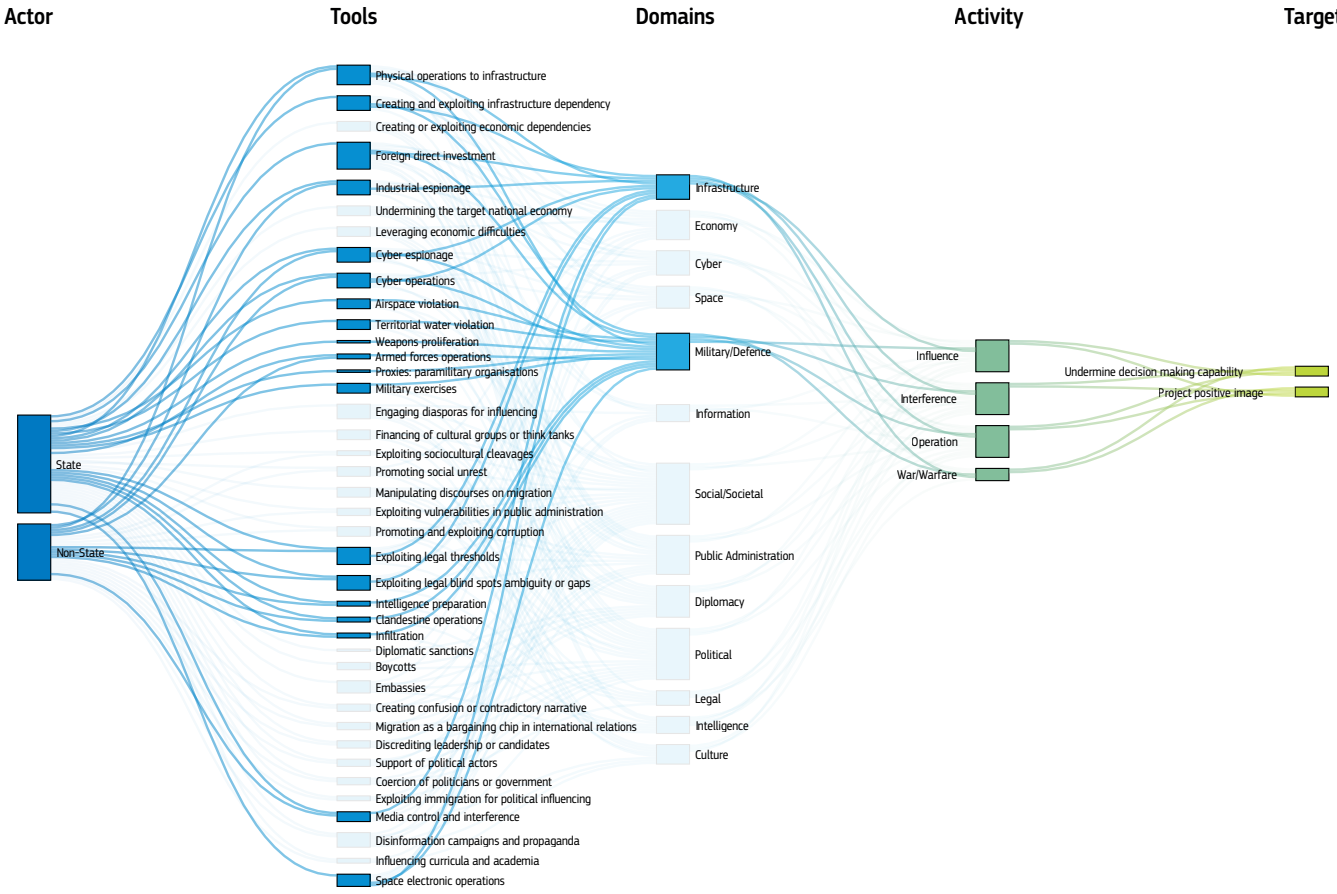

Figure 5. The conceptual model in relation to the list of tools that can be used to target the Infrastructure and/or Military/Defence domain

ACTOR
- State

TOOLS
- Cyber espionage
- Cyber operations

DOMAINS
- Infrastructure
- Military/ Defence

ACTIVITIES
- Influence/ Interference
- Operation
- War/Warfare

TARGET
- Undermine decision making capability

Figure 6. Example of a hypothetical scenario for defence-related CEI

Depending on the escalation stage, some tools are more likely to be used in a certain phase than in others due to their nature, although firm assignment of tools to a particular phase cannot be ensured. The following discussion is divided in two parts: priming phase and destabilisation/coercion phase, directly targeting the infrastructure and the military/defence domains.

3.1.1. Tools Used in the Priming Phase

Foreign direct investment: means «an investment (...) by a foreign investor aiming to establish or to maintain lasting and direct links between the foreign investor and the entrepreneur to whom or the undertaking to which the capital is made available in order to carry on an economic activity in a Member State, including investments which enable effective participation in the management or control of a company carrying out an economic activity» (European Commission, 2019b). Foreign direct investment can become a critical security threat in the energy sector. It can lead to profound dependencies and vulnerabilities of the state concerned. It can enable a hostile actor gaining access to sensitive information such as network structure as well as sensitive technologies. Moreover, overtaking strategic industries may enable hostile actors to exert political influence.

Creating and exploiting infrastructure dependency: Infrastructure dependency, including civil-military dependency, in the energy sector exists if the actions of a hostile actor can influence the amount of energy received by another country through a particular infrastructure. This kind of dependency can be a profound vulnerability and can make the targeted country susceptible to foreign interference up to strategic blackmail, e.g. if the hostile actors threatens to cut the energy supply. An example of the use of this tool is a state approach to abuse its dominant market position and ownership of gas supply to support foreign policy objectives (Korteweg, 2018).

Exploiting thresholds, non-attribution, gaps, and ambiguity in the law: Hostile actors may deliberately conduct hybrid threat activities in a way that remains below certain legal thresholds, in particular those governing the use of force. This allows to avoid the legal and practical consequences that crossing these thresholds would entail. As the EU energy market is huge, many actors have a special interest in it and try to push their agenda. The common market gives them not only important revenues but may also be used to influence EU decision-making in different areas. For example, the borders between lobbying the actors' own interests and bribery may become blurred.

Leveraging legal rules, processes, institutions, and arguments: Actors may use legal rules, processes, institutions and arguments both at the domestic and international level in support of hybrid threat activities. In such cases, law and the continued compliance with the law by targeted states and societies is employed as leverage against the latter. Hostile actors who understand the legal framework, the rules and processes may use this to their own advantage. In particular, non-EU countries can engage in investments or support of technologies by utilising legal possibilities, which do not guarantee European companies and vice-versa (Kratz and Oertel, 2021).

Cyber espionage: Cyber espionage is defined in this context as the illegal penetration of corporate cyber networks to obtain sensitive information to gain a comparative advantage over a competitive company or (governmental) entity. This approach can be advantageous as it often promises less effort, lower detectability and a higher chance of success, especially if the hostile actor possesses sophisticated cyber capabilities. This form of espionage is a major concern for many states, especially in the energy sector (European Commission, 2019c).

Industrial espionage: Industrial espionage usually refers to espionage with a commercial motivation. There may be overlaps with «Cyber espionage». In fact, Industrial espionage may include cyber means. For the purpose of this paper the definition shall be wider to include any kind of information gathering, including HUMINT, i.e. a person gathers intelligence

on the ground. This includes for example spying on energy infrastructure and its vulnerabilities by different means as well as stealing sensitive research results on new energy technologies, datasets or similar. It may also include the use of insiders[1].

Airspace / Territorial water violation: Airspace or territorial water violation can be defined as an unauthorised intrusion into the water or air borders of a country. A hostile actor uses this tool to test the detection and response capabilities of the targeted country, as well as to test the boundaries. Energy infrastructure are sometimes intrinsically exposed, e.g., if they are located near coastal waters and are therefore particularly susceptible to storms, erosion, but also hostile human interference. The latter challenge could become even more complex with renewables, as offshore wind farms are, for example, in the coastal foreshore of the oceans and are therefore particularly exposed (Staggs et al., 2017).

Intelligence preparation / Clandestine operations / Infiltration: Although these are three different tools, they can be put together in the context of this study and be considered as the covert takeover or weakening of a country's energy infrastructure. During the invasion of Crimea, Ukraine was not only deprived of part of its national territory, but also of a large part of its fossil energy infrastructure. The takeover of large parts of Ukraine's fossil fuel infrastructure was facilitated by due to corruption, which was also the result of targeted intelligence operations, clandestine operations and infiltration in the run-up to the annexation[2].

3.1.2. Tools Used in the Destabilisation/ Coercion Phase

Physical operations against infrastructure: Physical operations against energy infrastructure may include terrorist attacks, sabotage or vandalism in order to destroy, disrupt or overwhelm the infrastructure. This tool may cause severe damage in the targeted country while the hostile actor can maintain credible deniability remaining under the threshold of open hostile actions. Attribution of the hostile action to an actor is a political decision and targeted countries may be hesitant to attribute physical operations against infrastructure to a hostile actor. While any kind of energy infrastructure is vulnerable to physical attacks, it must be carefully analysed which influence the increase of renewable energies has on the resilience of the energy systems against physical operations. An example is the explosions that destroyed the North Steam 2 pipelines in 2022[3].

Cyber operations: In contrast to «cyber espionage», the main goal of cyber operations against energy infrastructure is not to gain information but to disrupt the normal functioning or even destroy the infrastructure. Cyber operations are not easily attributed, and the hostile actors have the advantage of credible deniability. Cyber-attacks can have a huge impact and may lead to a complete failure of certain parts of the energy infrastructure, e.g. the electricity network. This not only affects the civilian population and industry but also the military. In serious cases, military operations may be hindered which can give a strategic and battlefield advantage to a hostile actor.

1 https://www.reuters.com/article/denmark-security-russia-idUSKBN28J10E

2 https://www.forbes.com/sites/arielcohen/2019/02/28/as-russia-closes-in-on-crimeas-energy-resources-what-is-next-for-ukraine/

3 https://www.euronews.com/my-europe/2022/11/18/nord-stream-explosions-caused-by-gross-sabotage-swedish-prosecutor-says

Space electronic operations: Electronic operations may include attempts to disrupt position, navigation, and time solutions derived from Global Positioning System (GPS) by jamming and spoofing. It may also include the use of electromagnetic pulse (EMP) weapons against energy infrastructure. The aim is to disrupt or cause lasting damage to the energy supply. Unlike cyber-attacks, Global Navigation Satellite System (GNSS) jamming and spoofing could become more relevant, especially regarding renewable energies (Rügamer et al., 2015).

Promoting social unrest: A hostile actor may attempt to promote social unrest to destabilise a target country's government, generate and exploit social tension, or encourage a certain behaviour in the target country. On the defence side, social unrest may also increase desertions, draft dodging and general functioning of the military. Furthermore, a hostile actor may use existing societal cleavages over energy policy to promote social unrest. Social unrest may affect energy infrastructure in many ways. Violent protesters may destroy infrastructure or energy infrastructure may be occupied and blocked. Furthermore, social unrest may occur in case energy supply is disrupted. In any case, social unrest can destabilise a country and hinder the decision-making process.

Armed forces conventional/sub-conventional operations: Conventional/sub-conventional operations of the armed forces can be defined in the context of this study as those operations that aim to disrupt or completely prevent the energy supply through military actions. Since civil and military energy supply are difficult to separate completely, the application of this tool concerns both areas. The military attacks on the Ukrainian energy infrastructure in the context of the invasion is an example. Indeed, the attacks do not only affect the fossil energy infrastructure, but also the renewable one. For example, the invasion has crippled almost all of Ukraine's wind energy sector[4], potentially affecting the conduct of interconnected military installations and operations[5].

Paramilitary organisations (proxies): The use of paramilitary organisations, in the context of this study, can be defined as using them as a proxy to destroy energy infrastructure. This tool could be used in cases where a hostile actor does not want to be attributed. For example, on behalf of a state actor, it can employ kinetic actions. Furthermore, the use of such organisations often offers credible deniability, potentially affecting the interests of third countries (Markusen, 2022).

3.2. Indirect Target: the Infrastructure and/or Defence Domain

As mentioned in the previous chapter, a hostile actor can also **indirectly** target the infrastructure and/or the military/defence domain and ultimately achieve its objectives. There are many different dependencies between the domains, some of them are unidirectional, others are bidirectional. Through these dependencies, a hostile actor may use **other domains and tools** to ultimately affect the infrastructure and/or the military/defence domain through **cascading effects.** It is therefore necessary to focus not only on those tools and domains that can directly affect the infrastructure and the military/defence domain, but also on those that can indirectly affect these two domains.

The outset of this study is that the critical (energy) infrastructure and the military/defence domains are **interconnected**, relying on each other in most cases. On the one hand, this means that certain tools can be used by a hostile actor to affect both domains. On the other hand, it also means that an attack on one of the two domains can have cascading effects on the other.

4 https://www.bloomberg.com/news/articles/2022-09-14/russia-s-invasion-knocked-out-almost-all-of-ukraine-s-wind-power

5 https://www.csis.org/analysis/responding-russian-attacks-ukraines-power-sector

3.2.1. Dependencies Used as Entry Points

This section investigates several relevant dependencies between other domains of the ecosystem that could be exploited by adversaries to affect the infrastructure as well as military/defence domain (see Figure 7). In that view, the focus is to identify through which other domains (i.e., **political, economy, cyber, space, legal, public administration, intelligence and culture**) a combination of threats to defence-related CEI may occur. A result of the interdependent nature of the ecosystem, vulnerabilities in one domain might act as Trojan horses to cripple another.

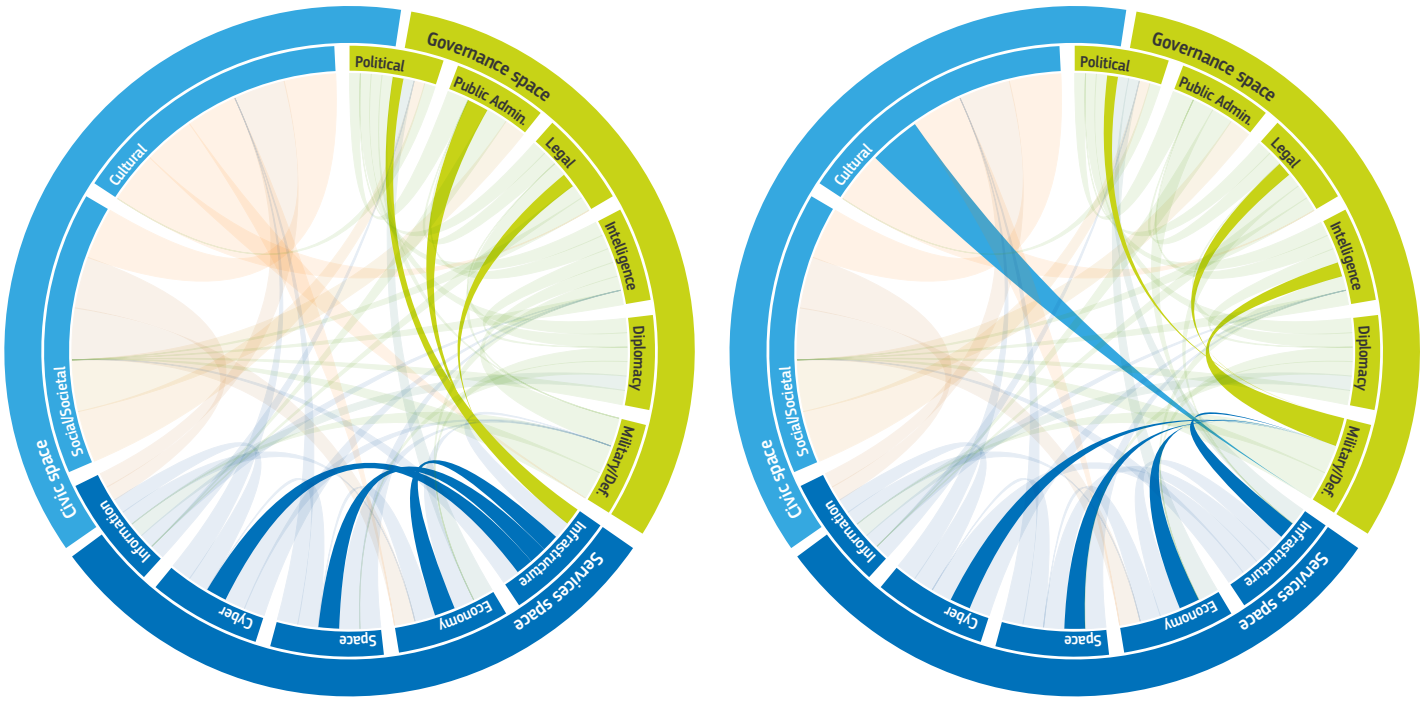

Figure 7. Unilateral and bilateral dependencies that can affect the Infrastructure (left) and Military/Defence (right) domain

a) Addressing Infrastructure and Military/ Defence Domain

Political: it is defined as «actors, organisations and institutions that exercise authority or rule within a territory through the application of various forms of political power and influence» (Giannopoulos et al., 2021). The political domain is closely interconnected with the (energy) infrastructure domain, e.g. through energy policy which governs investments into energy infrastructure. It is also connected with the military domain, which is governed by defence policy. Tools targeting the political domain attempt to impact individuals, political organisations and democratic processes, in order to influence the political agenda in the national and diplomatic arena and decision-making processes. Eventually, this kind of tools challenge the credibility of the target state by making citizens dispute decisions, laws and norms.

Opportunities as well as barriers for the energy infrastructure and defence sector are created by political decision-making. Moreover, due to the high dependence of industrialised societies on the energy sector, political decision may also be influenced by targeting the energy infrastructure. For example, if a hostile actor reduces energy

> *The armed forces must consider a new set of combined and blurred threats that can impair their operational effectiveness in peace and war.*

supplies, political leadership may be forced to release support funds or subsidising energy prices. Also, targeting the political domain - through the support of political actors or coercion of politicians - can influence strategic decisions in the energy sector (Jungwirth et al., 2023).

Governments are under constant scrutiny about resources allocation. In western democracies, and especially in peacetime, civil society is often sceptical about the allocation of defence resources, as citizens consider that taxpayers' money should rather be invested in other areas of society. This makes it more difficult for governments to advocate for defence investment and, for example, increase spending for the protection of defence-related CEI. This opens opportunities for a hostile actor to try to exert influence and consequently exploit gaps and vulnerabilities.

Economy: it is defined as «the production, distribution and consumption of all goods and services for a country and includes its economic development and distribution of wealth» (Giannopoulos et al., 2021). Tools targeting the economy domain aim at weakening the target state by making citizens lose trust on their government and in the democratic processes and institutions. The economy domain is mostly targeted in the priming phase, (e.g by foreign direct investments) through which hostile actors try to gain influence. However, the economy domain can also be targeted during the destabilisation/coercion phase (e.g. through boycotts and economic sanctions).

Energy infrastructure plays a great role in the economy domain and vice-versa. High energy prices as a result of one-sided dependencies hamper economic development. It is the private sector that owns or operates most of the infrastructure that ensures the supply of goods and services vital to the normal functioning of the communities they serve. For the defence sector, this poses a critical challenge as it relies on services provided by the private sector and without having direct control on these infrastructure. To be adequately prepared for situations in which defence is called upon, defence must continue to invest in specific areas to minimise vulnerabilities and ensure civil-military coordination, especially during energy crises.

Cyber: it is defined as «information environment, consisting of the interdependent networks of information technology infrastructure (including hardware, software, data, protocols), and information including the internet, telecommunications networks, computer systems, and embedded processors and controllers»[6]. This domain links many other domains together. Tools targeting the cyber domain can attempt to access data and information as well as cause degradation, disruption, or destruction of the networks (Giannopoulos et al., 2021).

The challenges posed by the cyber domain to the energy infrastructure and the defence sector

6 https://csrc.nist.gov/glossary/term/cyberspace

are manifold[7]. For example, a major strength in the functioning of CEI is the resilience of their critical information infrastructure in terms of its availability, authenticity, and integrity within the energy network. The **critical information infrastructure can be both an asset and vulnerability**. Critical information infrastructure ensures reliable functioning, security and safety of energy infrastructure. They can be provided by smart sensors, more complex supervisory control and data acquisition (SCADA) systems or even more complex integrated communications information systems. The main issue in protecting CEI is to identify the relevant critical information infrastructure and to proactively address the measures necessary to make them resilient against cyber-attacks.

Space: it is defined as «space-based services including navigation, communications, remote sensing, and science and exploration» (Giannopoulos et al., 2021). Since different domains increasingly rely on the space domain, tools targeted at it aim at exploiting its link with other domains. The space domain provides services to the infrastructure domain (e.g. GPS or timing signals) and to the military domain. Space-related technologies – including power supply and management systems – are being made available to address the burgeoning energy needs of military domain but also for providing communication and intelligence gathering for the protection of energy infrastructure, including technological synergies between space and terrestrial energy sector.

Legal: it is defined as «legal rules, actions, processes and institutions, including their normative and physical manifestations, that are or can be used to achieve legal or non-legal effects in the context of a hybrid threat activity» (Giannopoulos et al., 2021). Targeting the legal domain, for instance by exploiting legal thresholds or leveraging rule-compliance by the targeted state, hybrid threats actors may impact the energy sector and the defence sector indirectly[8]. For example, this may happen by abusing the rule of law or the right to freedom of speech. Also, breaching or disregarding international treaties and contracts falls under this category as such action ultimately undermines trust inside the targeted society and the institution's credibility.

b) Addressing Infrastructure Domain Only

Public Administration: it is defined as «the process, individuals and institutions involved in implementing the rules and laws» (Giannopoulos et al., 2021). Hybrid threats actors can target the public administration domain to delay or disrupt the approval and implementation of specific policies. For example, this may happen through corruption but also by exploiting disinformation campaigns. The CER Directive (European Commission, 2022c) covers eleven sectors including public administration which underlines its importance for the resilience of critical (energy) infrastructure.

7 Tools targeting the Cyber Domain should not be confused with Cyber Tools targeting other domains. Indeed, it is possible to target the Cyber Domain with non-cyber tools (e.g. foreign direct investments) which will have cascading effects to other domains.

8 The Legal Domain can be targeted by legal or non-legal tools. At the same time, other domains can be targeted by legal tools.

c) Addressing Military/Defence Domain Only

Intelligence: it refers to process of intelligence gathering which can be defined as «the process by which specific types of information important to national security are requested, collected, analysed and provided to policy-makers; the products of that process; the safeguarding of these processes and this information by counter-intelligence activities; and the carrying out of operations as requested by lawful authorities» (Giannopoulos et al., 2021).

Culture: Hybrid threat campaigns can cascade from the culture domain to the military/defence domain. Tools targeting the culture domain can be summarised as it refers to "cultural statecraft" by an aggressor to support an objective through hybrid threat activities. Although like the concept of soft power, cultural statecraft differs fundamentally in its origins. While soft power grows out of an autonomous civil society, cultural statecraft is essentially a state endeavour and specifically targets issues of national identity, history and religion (Giannopoulos et al., 2021). Although this is a rather long-term threat, it is to be expected that hybrid threats actor will try to exploit these specific elements of a country or society to gain an advantage[9].

9 For example, a hybrid threat actor could support the pacifist movement in a country in order to gain a strategic advantage by weakening the military/defence domain in this country in the long term.

4. ENHANCING RESILIENCE OF DEFENCE-RELATED CRITICAL ENERGY INFRASTRUCTURE

4.1. Recommendations for Resilience-Building

As the analysis of the tools, the domains and their interconnections in the previous chapters have shown, building resilience against hybrid threats means that a **whole-of-society** approach is required. This means that existing dependencies and interdependencies in society must be considered. Building sectoral resilience is not sufficient, as hybrid threats actors aim to create cascading effects and exploit vulnerabilities. Resilience against hybrid threats therefore needs to be designed and implemented at all levels of society, and must consider resilience measures, not only from multiple domains' perspective but as a **comprehensive approach**. In other words, developing resilience against hybrid threats necessitates looking **beyond resilience in individual areas,** building it systemically while considering interconnections between the different parts of society. Considering all this, fostering resilience of defence-related CEI against hybrid threats requires focusing beyond measures in the infrastructure and military/defence domains, including **cross-borders and cross-sectoral** elements.

A key challenge of every military operation is maintaining the energy supply and thus enable military performance and combat power. Military operations rely on civil infrastructure and civil society relies on military capabilities to respond to large-scale crises. Indeed, if a hostile actor is successful in disrupting or disabling the CEI, this could provide the actor with a compelling advantage on the battlefield, undermining the effectiveness of military operations linked to the **business continuity** of critical energy infrastructure. This demonstrates that military and civil are interrelated.

The **civil-military cooperation** at national level is a necessity and this is obviously projected (or vice-versa) also at international level. Both EU and NATO have recognised that in countering hybrid threats, a structured approach that enables the continuous exchange of information and intelligence on threat-related issues is essential . Thus, there is a need for a **coordinated response** to incidents, including «near-misses» meant as incidents that could have resulted in an injury or illness to people, danger or damage to property, including the environment. The latest can, indeed, represent worthy lessons learnt to improve capabilities and performances.

Building resilience against hybrid threats requires a whole-of-society approach that goes beyond sectoral resilience, considering all levels of society and interdependencies.

Cost-saving measures have often meant that militaries have become reliant on specific supply routes, communications means and sources of energy supply. Such dependencies could create vulnerabilities that may be exploited by a hostile actor and consideration should therefore be given to **diversification** to create resilience and continuity of supply in critical areas. Other vulnerabilities exist when, for example, CEI requires certain technology or parts that must be imported or that have long **manufacturing times** and are, therefore, particularly prone to hostile interference.

Even though hybrid threats are not an entirely new topic, **modern technology and capabilities** have increased the **disruptive potential** of such threats. Energy is a very important component of hybrid threats either as a direct objective or as part of a more comprehensive plan to destabilise a country and weaken its military and response capabilities. **Investing** in emerging technologies, innovation and foresight contribute to improving the capabilities of defence-related CEI against hybrid threat activities and, at the same time, enhancing resilience against disruptive technologies used as means to harm.

In this context, the development of **multinational and/or multi-sectoral exercises** or relevant training is a key activity to improve capabilities. Investments in education are expected to enhance **situational awareness** and collaboration between all parties involved in the operation and protection of the defence-related CEI as well as to establish **communication channels** between countries (competent authorities from the private, public and defence sectors) which can be exploited during crises, while at the same time helping to reveal dependencies in the energy sector which may not be always known a priori. For example, the Parallel and Coordinated Exercise (PACE) 2022[1] had a strong energy dimension; however, no reference to the dependency of the defence sector was made.

Hybrid threat activities, particularly those involving cyber threats, are dynamic and constantly evolving over time and space. As such, defence-related CEI operators should **conduct periodic vulnerability assessments as well as identify interdependencies and cascading effects** based on experiences, emerging innovations and latest knowledge in the field. By doing so, the EU member states can develop the most appropriate and **cost-effective measures** to address identified

1 https://www.eeas.europa.eu/eeas/eu-integrated-resolve-2022-eu-ir22-parallel-and-coordinated-exercisespace_en

gaps which could be potentially exploited by hostile actors.

Equally essential is the international collaboration, given the interlinked nature of CEI and the issues related to the ensuring continuity of supply. In this view, it is essential to have a structured approach that enables continuous **information and intelligence sharing** on threat-related issues to ensure coherence and prompt information exchange. Indeed, there are still some obstacles at operational level preventing information sharing among countries with respect to hybrid threats. Information sharing should also expand to more **strategic** layers (e.g., foreign direct investments and acquisitions) and **not only to operational or tactical ones.**

In particular, at operational level, it is paramount to embark on **practical projects** to improve the security posture with respect to hybrid threats in the defence-related CEI. To this end, collaborative projects for identifying criticalities, addressing interconnections and assessing potential consequences are necessary for states to obtain a **hands-on experience** on these issues.

Further **recommendations** and **measures** could also strengthen the **risk assessment process** and **enable a comprehensive response to hybrid threats**, both at the MoD and EU levels. These recommendations and measures are summarised below:

EU and MoD levels:

- **Dependencies analysis:** carry out a detailed analysis of how military functioning and operations depend on civil CEI, so that the impact of CEI outage becomes understood, which is needed to justify protection measures for CEI against hybrid threats. This should be done at national levels, and then possibly aggregated to an EU-wide picture.
- **Risk assessment:** consider hybrid threats when creating a dedicated risk management framework, including vulnerability and threat assessment, and inter-dependencies of other domains to CEI.
- **Technology investment:** create a new, innovative, state-of-the-art, intelligent communication and information system. This may support detection and mitigation of hostile attacks to CEI and may protect from sophisticated cyber-threats.
- **Intelligence threat landscape report:** develop national and EU reports for the resilience of defence-related CEI against hybrid threats.
- **Training and education:** these are essential for improving the skills, know-how and expertise of stakeholders involved in the critical (energy) infrastructure and defence/military relevant domains. Providing targeted training such as security awareness, threat intelligence and behavioural analysis can improve the ability to understand and respond to various challenges and ensure the resilience of critical infrastructure. This could be a major asset in risk assessment and timely identification of new emerging threats that have not been identified yet; therefore, difficult to detect and tackle.
- **Real scenario-based exercises:** stimulating major crises based on a realistic threat landscape can contribute to establishing or optimising crisis management processes and practices. By engaging in the exercise, the stakeholders and actors responsible for the operation and security of the CEI can streamline a comprehensive approach and foster synergies for increasing the resilience of defence-related CEI.
- **Civil-military collaboration:** further enhance interoperability and synergies and improve joint and comprehensive responses leading to a more resilient and effective defence-related CEI.

EU level:

- **Establish an EU collaborative platform for countering hybrid threats as a whole:** provide an appropriate platform to assist the EU Member States in addressing risks by exchanging best practices, promoting synergies, and fostering cross-border collaboration.
- **Establish EU communication channels for addressing hybrid threats:** develop dedicated channels (at strategic, tactic and operational levels) to ensure timely, secured, and effective communication between all relevant and responsible stakeholders involved in the operation and resilience of CEI. This will help to ensure interoperability with other relevant parties and disseminate information on threats as early as possible both within the EU and to associated partners outside the EU.
- **Establish an EU civil-military partnership to counter hybrid threats:** tackle common challenges for countering hybrid threats in EU Member States, building on the 2023 Joint Declaration on EU-NATO Cooperation[2]. This partnership could investigate hybrid threat activities against defence-related critical (energy) infrastructure by engaging in a series of initiatives and data exchange with stakeholders at strategic, tactic and operational levels.

MoD level

- **Keep track of ownership** of defence-related CEI.
- **Ensure (or develop) the existence of up-to-date plans** (measures and practices) in the domain of prevention, preparedness, response and recovery for ensuring defence contribution to maintain the resilience of defence-related CEI against hybrid threats.
- **Conduct on a regular basis vulnerability assessment** to improve situational awareness and mitigate risks in case of hybrid threats against defence-related CEI. Assessments should be specific to each military installation, consistent with risk assessments, and focused on optimising mitigation measures under different risk scenarios.
- **Systematically collect intelligence and post-event data on hybrid threats** incidents on defence-related CEI, analyse them at the national level and share lessons learned with other Member States and EU institutions.
- **Identify points of contact and establish priority relations** with responsible civilian critical entities/operators and competent public authorities to facilitate data exchange, training and early response action in case of incidents.
- **Ensure the existence of communication channels** and information flow in case of a crisis with the relevant departments and responsible actors.
- **Keep up with the existing EU instruments and ongoing initiatives for countering hybrid threats,** e.g., the EU Innovation Fund, the European Defence Fund, Horizon 2020 and Horizon Europe, the Permanent Structured Cooperation (PESCO), EDA's Energy and Environment capability technology group, CF SEDSS, the European Defence and Security College (ESDC), JRC publication repository and technical working groups.
- **Invest in upskilling and reskilling of defence and armed forces personnel** through dedicated education, seminars, and exercises at regional, national and supra-national levels, making sure that elements on hybrid threats and CEI resilience are included. By providing training opportunities and encouraging continuing education and expertise improvement, MoDs can guarantee that staff has the skills and know-how required to react and better counter hybrid threat activities against defence-related CEI.

2 https://ec.europa.eu/commission/presscorner/api/files/attachment/874309/EU-NATO%20declaration_EN.pdf

4.2. Way Ahead and Forward-Looking Perspectives

As hybrid threats will continue challenging the armed forces' capabilities and performance, it will be essential to keep investigating their nature and **development over time** and across domains, including *new modus operandi* and targets. EDA, with the support of the European Commission, in particular of DG ENER and DG JRC, as well as other partners such as the Hybrid CoE, will continue exploring how to better contribute to strengthening the resilience of defence-related infrastructure against hybrid threats. In that view, attention will be given in examining **emerging and future energy challenges** – ranging from technological to non-technological factors – as well as the potential of man-made or natural disasters from being exploited by hybrid threats actors, terrorists and cyber-attackers, with a view to enhancing the ways of addressing them when these challenges are combined or blurred.

Overall, hybrid threats need a hybrid response which will play a central role in the near future, contributing to EU policy-making process in a more cross-cutting manner. In particular, to identify the origin and features of hybrid campaigns, **strategic foresight** and comprehensive situational awareness would be enhanced and further embedded into defence operations and energy supply services.

In addition, as part of the CF SEDSS, EDA and DG JRC conducted a table-top exercise (TTX) on hybrid threats in May 2023. The TTX was held in Sofia under the auspices of the Bulgarian Ministry of Defence to enhance defence energy resilience and promote collaboration across Europe in response to hybrid threats. The exercise focused on identifying the dependencies of the defence sector in the event that defence-related CEI is compromised or cannot operate due to hybrid threats. It also enabled MoDs, armed forces, and relevant defence stakeholders to acquire critical insights to enhance their response against various hybrid threats, such as cyber and physical attacks, disinformation campaigns, and climate change cascading effects, by examining response strategies, prevention methods, and management techniques. Using a **real-world situation scenario**, the TTX provided a valuable opportunity for defence and civilian stakeholders to share information and best practices, improve their situational awareness and management skills, and interact with one another in a rapidly changing operational environment. EDA, JRC, and the CF SEDSS community will analyse the insights learned from the exercise to inform the planning of future TTX events.

Subsequently, EDA and DG JRC will continue exploring how to enhance **energy-related strategic autonomy** and resilience through diverse perspectives within the European energy network. Following the analytical framework of this study, the efforts will be focused on promoting the interaction between different domains and actors across the EU Member States and strategic partners, fostering sharing of information and best practices to support decision-making, situational awareness and management skills in a rapidly changing operational environment.

Strategic foresight and comprehensive situational awareness are key to identifying and responding to hybrid campaigns.

Following the January 2023 statement[3] by the EU and NATO to address common security and defence challenges in the Euro-Atlantic area, a joint EU-NATO **Task Force for Resilient Critical Infrastructure** has been launched[4]. This Task Force will assess the strategic vulnerabilities across four interconnected sectors – energy, transport, digital, and space – to identify key risks to critical infrastructure. Based on this assessment, the Task Force will develop key principles to enhance resilience and recommend mitigation measures and remedial actions.

Throughout multinational collaboration, research studies, project ideas and exercises, EDA and JRC will assist MoDs in improving national processes and procedures for strengthening the resilience of defence-related CEI against hybrid threats. By analysing the outcomes of these activities and **identifying gaps and opportunities**, the EDA and JRC will recommend **how the EU can complement national efforts and foster European civil-military collaboration.** By developing a more robust and comprehensive response to hybrid threats, the EU, its Member States, and strategic partners can achieve a higher level of security and resilience.

3 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_133

4 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_1705


Knowledge-sharing and cross-border cooperation are crucial for bolstering critical energy infrastructure resilience against hybrid threats.

Enhancing dialogue between the civil and military communities is a sine qua non for addressing hybrid threats against defence-related critical energy infrastructure.

CONCLUSION

This study offers a more **comprehensive and holistic view of the nexus between defence-related critical energy infrastructure and building resilience against hybrid threats.** The study has underlined that ensuring the resilience of defence-related CEI is imperative to tackle hybrid threats because of their blurred nature and cross-sector and trans-national cascading effects.

What is new about this perspective is not so much the individual threats or the individual tools that a hostile actor might use to harm the defence-related CEI, but the way in which vulnerabilities are created and eventually exploited. The **armed forces must consider a new set of combined and blurred threats that can impair their operational effectiveness in peace and war.** These new combined and blurred threats involve a mix of conventional and unconventional means that can negatively affect military operations and subsequently the society.

The study's analytical framework helps identify and incorporate the recent developments when designing policies to increase resilience of defence-related critical energy infrastructure against hybrid threats. In this light, the study provides an overview of the problem at hand, aiming at characterising it, and raising awareness of the issue that Member States, in particular MoDs and relevant defence stakeholders, must confront, given the complexity and stealth nature of hybrid threats.

Considering the volatile security and energy situation, the role of the defence is vital in preserving the uninterrupted provision of those services. In this regard, the study emphasises promoting civil-military collaboration at the EU level to further enhance the resilience of those infrastructure and supporting the MoDs to address associated risks.

In addition, key issues to consider when building resilience are listed, along with recommendations for sharing knowledge, expertise and best practices, promoting synergies and complementarity as well as fostering cross-border cooperation by developing joint collaborative studies, projects and exercises. These actions aim at assisting the MoDs in developing the necessary measures for ensuring the resilience of CEI on which the defence sector depends, with respect to hybrid threats by addressing vulnerabilities, identifying interdependencies and assessing cascading effects. In this context, the study aims, through the collection of lessons learned, to determine **how the EU can better complement the national efforts and promote a robust European comprehensive approach to maintain the resilience of defence-relate CEI against hybrid threats.**

To sum up, this study could help start a process which, at the end, should lead to a deeper understanding of hybrid threats, establishing a common terminology around this topic and fostering **collaboration and information sharing at the strategic level.** Enhancing the dialogue between the civil and military domains is a *sine qua non* for addressing hybrid threats against defence-related CEI. This study aims to highlight the relevance of these vital factors and ensure that they will continue to feature as the highest priority on both European and national policies and agendas.

REFERENCES

Council of the European Union, 2022a. Council conclusions on a Framework for a coordinated EU response to hybrid campaigns.

Council of the European Union, 2022b. A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security.

Council of the European Union, 2019. Council conclusions on security and defence in the context of the EU Global Strategy.

EEAS, 2022. Joint Progress Report on Climate Change, Defence and Security (2020-2022).

EEAS, 2020. Climate Change and Defence Roadmap.

European Commission, 2022a. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Commission contribution to European defence.

European Commission, 2022b. JOINT STAFF WORKING DOCUMENT Identification of sectoral hybrid resilience baselines.

European Commission, 2022c. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

European Commission, 2022d. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E.

European Commission, 2022e. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Action plan on military mobility 2.0.

European Commission, 2021a. Fit for 55: Delivering the EU's 2030 Climate Target on the way to climate neutrality.

European Commission, 2021b. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Second Progress Report on the implementation of the EU Security Union Strategy.

European Commission, 2020a. The EU Security Union Strategy.

European Commission, 2020b. JOINT STAFF WORKING DOCUMENT, Mapping of measures related to enhancing resilience and countering hybrid threats.

European Commission, 2019a. The European Green Deal.

European Commission, 2019b. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. Off. J. Eur. Union.

European Commission, 2019c. The scale and impact of industrial espionage and theft of trade secrets through cyber. Publications Office. https://doi.org/doi/10.2873/48055

European Commission, 2018. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats.

European Commission, 2016. Joint Framework on Countering Hybrid Threats: A European Union Response.

European Commission, 2008. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Giannopoulos, G., Smith, H., Theocharidou, M., 2021. The landscape of hybrid threats : a conceptual model : public version. Publications Office of the European Union. https://doi.org/doi/10.2760/44985

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., Giannopoulos, G., 2023. Hybrid threats : a Comprehensive Resilience Ecosystem. Publications Office of the European Union. https://doi.org/doi/10.2760/37899

Korteweg, R., 2018. Energy as a tool of foreign policy of authoritarian states, in particular Russia, Study Commissioned by the European Parliament's Committee on Foreign Affairs. https://doi.org/10.2861/951739

Kratz, A., Oertel, J., 2021. Home advantage: How China's protected market threatens Europe's economic power. Eur. Counc. Foreign Relations.

Markusen, M., 2022. A Stealth Industry.

Rügamer, A., Iis, F., Kowalewski, D., 2015. Jamming and Spoofing of GNSS Signals - An Underestimated Risk?!

Staggs, J., Ferlemann, D., Shenoi, S., 2017. Wind farm security: attack surface, targets, scenarios and mitigation. Int. J. Crit. Infrastruct. Prot. 17, 3–14. https://doi.org/10.1016/j.ijcip.2017.03.001

Tavares da Costa, R., Krausmann, E., Hadjisavvas, C., 2023. Impacts of climate change on defence-related critical energy infrastructure. Luxembourg.

Wigell, M., Mikkola, H., Juntunen, T., 2021. Best Practices in the whole-of-society approach in countering hybrid threats.

LIST OF ACRONYMS

CEI	Critical Energy Infrastructure
CER	Critical Entities Resilience
CF SEDSS	Consultation Forum for Sustainable Energy in the Defence and Security Sector
CORE	Comprehensive Resilience Ecosystem
DG	Directorate General
EC	European Commission
ECI	European Critical Infrastructure
EDA	European Defence Agency
EEAS	European External Action Service
EMP	Electromagnetic Pulse
ENER	Energy
ESDC	European Defence and Security College
EU	European Union
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HCoE	Centre of Excellence for Countering Hybrid Threats
JRC	Joint Research Centre
MoD	Ministry of Defence
MS	Member States
NATO	North Atlantic Treaty Organization
NIS	Network and Information Security
PACE	Parallel and Coordinated Exercise
PCEI	Protection of Critical Energy Infrastructure
PESCO	Permanent Structured Cooperation
RES	Renewable Energy Sources
SCADA	Supervisory Control and Data Acquisition
SUS	Security Union Strategy
TTX	Table-Top Exercise
WG	Working Group

LIST OF FIGURES

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels - Belgium

eda.europa.eu

Tel +32 2 504 28 00
info@eda.europa.eu

European Commission, Joint Research Centre (JRC)
Directorate E – Space, Security and Migration
JRC.E.2 – Technologies for Space, Security and Connectivity

joint-research-centre.ec.europa.eu

JRC-E2@ec.europa.eu