European Commission

EUROPEAN DEFENCE AGENCY

Protecting Critical Energy Infrastructure

A Defence Imperative in an Era of Uncertainty

Contact information:
European Commission, Joint Research Centre (JRC)
Directorate E – Societal Resilience and Security
JRC.E.2 – Space, Connectivity and Economic Security
Email: JRC-E2@ec.europa.eu
https://joint-research-centre.ec.europa.eu

European Defence Agency

Email: info@eda.europa.eu
www.eda.europa.eu

JRC142118

Print ISBN 978-92-68-26819-3 doi:10.2760/8872865 KJ-01-25-252-EN-C
Online ISBN 978-92-68-26818-6 doi:10.2760/2484288 KJ-01-25-252-EN-N

Luxembourg: Publications Office of the European Union, 2025

How to cite this report:
C. Hadjisavvas, M. Kuzel, A. Georgescu, E. Krausmann, I. Chatzialexandris, N. Nasikas, S. Leclerq, A. Lazzari (editors), Protecting Critical Energy Infrastructure: A Defence Imperative in an Era of Uncertainty, Publications Office of the European Union, Luxembourg, 2025, https://data.europa.eu/doi/10.2760/2484288, JRC142118.

Protecting Critical Energy Infrastructure

A Defence Imperative in an Era of Uncertainty

Consultation Forum for Sustainable Energy in the Defence and Security Sector

CF SEDSS
10 Years of Contributions
to the Defence Energy Transition

Editors

Constantinos Hadjisavvas, *European Defence Agency*
Maja Kuzel, *European Defence Agency*
Alexandru Georgescu, *National Institute for Research and Development in Informatics ICI Bucharest*
Elisabeth Krausmann, *European Commission Joint Research Centre*
Ioannis Chatzialexandris, *European Defence Agency*
Nektarios Nasikas, *Hellenic Army Academy*
Shana Leclerq, *European Defence Agency*
Alessandra Lazzari, *European Defence Agency*

Contents

Acknowledgements

The editors thank all the authors for their valuable contributions and insights. They also wish to acknowledge the substantial support of the CF SEDSS members from over 30 European countries, whose expertise greatly enriched this publication. Special thanks go to the EDA and the European Commission's leadership for supporting this publication and the ongoing efforts of CF SEDSS to advance the defence energy transition and climate adaptation.

The editors would also like thank Fabio Bortolamei of the JRC for creating and implementing the design of the publication.

Abstract

The defence sector is integral to safeguarding national security, and its operational effectiveness is strongly dependent on the resilience and reliability of critical energy infrastructure (CEI). However, the evolving threat landscape, ranging from hybrid threats to climate change-induced disasters, poses significant risks to these infrastructures. Disruptions to CEI can severely impact defence sustainability and readiness making it crucial for the armed forces to ensure the uninterrupted provision of these services. Given that the vast majority of CEI is owned and operated by the private sector, this task requires comprehensive, proactive planning and strong collaboration across sectors.

This publication, developed in the context of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) — the largest defence energy community in Europe — underscores the importance of enhancing the resilience of defence-related CEI. It leverages the expertise, capabilities, and strategic positioning of the armed forces to explore how the defence ecosystem can secure its energy needs while contributing to national and EU-level resilience strategies. Through a multidisciplinary approach, this research draws from CF SEDSS outputs and analyses to provide insights for advancing the defence energy transition and enhancing climate resilience within the armed forces.

The publication delves into the impacts of climate change, pandemics, financial markets, and hybrid threats on defence-related CEI. It highlights how extreme weather events, cyberattacks, and supply chain disruptions expose critical vulnerabilities within energy systems. Lessons from recent crises, such as the COVID-19 pandemic, emphasise the urgency of improving coordination between civilian energy providers and the military sector to secure a continuous energy supply. Additionally, the research explores offshore energy security, advocating for international cooperation to protect subsea infrastructure vital to Europe's energy transition.

Building on analyses of EU policies, strategies, and regulations, this publication offers actionable recommendations for bolstering CEI robustness, improving response and recovery mechanisms, and fostering collaboration between defence and energy sectors. It aims to address the complex interdependencies between defence operations and energy infrastructure, promoting enhanced national coordination and joint initiatives at the EU level. In a world of increasing uncertainty, energy resilience is crucial to the armed forces' operational effectiveness and critical to safeguarding the EU's resilience, strategic autonomy and decision-making capacity.

Preface

The Russian war of aggression against Ukraine, rising tensions in the Middle East, and the growing geopolitical challenges across the globe-from volatile political regimes to the weaponisation of immigration, disinformation, and cyber-attacks—have laid bare the vulnerabilities of the EU's critical energy infrastructure (CEI). This infrastructure is not just central to civilian life but is also indispensable to the operational effectiveness of the armed forces, both in times of peace and war. These complex and evolving threats call for a decisive shift from reactive to proactive measures in protecting the infrastructures that underpin our defence capabilities. The EU and its Member States can no longer afford to respond to crises as they arise; instead, they must anticipate and prepare for them.

This publication addresses these pressing issues, demonstrating through in-depth analysis and its findings that the defence sector is uniquely positioned to strengthen CEI resilience by leveraging its expertise, assets, and operational role. The vulnerabilities exposed by recent global events underscore the critical need for the EU to make the resilience of its CEI a top priority. This involves not only protecting energy systems but also ensuring their ability to withstand and quickly recover from crises. Our competitors are already adept at exploiting technological advancements, raw materials, and even migration patterns to their strategic advantage. It is time for Europe to match these efforts with a cohesive, forward-looking strategy.

The European Commission's Clean Industrial Deal, which aims to decarbonise and modernise the EU's industrial sector, the appointment of Andrius Kubilius as the first Commissioner for Defence and Space, and the strengthened role of the European Defence Agency, position the EU to lead in addressing these challenges. Backed by the scientific expertise of Commission key Directorates-General, such as the Directorate-General Joint Research Centre (JRC) and the Directorate-General for Energy (DG Energy), the EU is ready to support national and EU-wide initiatives to bolster CEI resilience. A truly common approach with a strengthened civil-military cooperation can help to build a secure and sustainable future, where defence and energy resilience are tightly interconnected and where more significant research, innovation, and technology investment is provided to defend against physical and digital threats.

We are proud to present this comprehensive, multidisciplinary publication, building on the invaluable research of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), an EU funded project. It offers practical recommendations for enriching the dialogue at both EU and national levels on how best to align defence strategies with broader EU objectives, such as achieving climate neutrality by 2050 and strengthening the resilience of energy systems.

We applaud the remarkable efforts of the CF SEDSS community, turning ten years, the authors, and the editors who have brought this important work to fruition. Policy frameworks must also evolve to prioritise resilience through energy efficiency, renewable energy, digitalisation, green procurement, and climate-adapted military planning.

We, therefore, invite all relevant stakeholders—across government, industry, and academia—to join us in this collective effort to enhance the resilience of Europe's critical energy infrastructure and ensure a more secure future for all.

Nathalie Guichard
Director Research, Technology & Innovation
EDA

Matthias Oel
Director Societal Resilience and Security
JRC

Executive Summary

This publication, developed in the context of the third phase of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS)[1], addresses the vital need to enhance the resilience of CEI that supports the operational effectiveness of the European defence sector. As modern threats evolve—from hybrid warfare to climate change-induced disruptions—ensuring the uninterrupted and resilient functioning of CEI has become a strategic priority. The majority of CEI is owned and operated by the private sector, making collaboration between governments, military forces, and civilian energy providers crucial. This multidisciplinary publication offers actionable insights for strengthening CEI against emerging threats, ensuring both the sustainability of armed forces' operations and the broader resilience of Europe.

The publication is organised in seven core chapters, along with a concluding chapter. It presents both abbreviated versions of key deliverables[2], as well as one-off contributions from a series of long-term CF SEDSS contributors within Working Group 3 which focuses on the protection of CEI. The contributions of WG3[3] extend far beyond those presented in this book, and consist also of project fact sheets, various policy documents and the contributions to the CF SEDSS Guidance on Advancing Sustainable Energy in Defence.

Chapter 1: Energy Resilience in Defence: Adapting to a Changing Security Landscape

This chapter underscores the critical role of CEI in sustaining defence operations and maintaining military readiness. It examines key risks, including geopolitical instability, cyber threats, natural disasters, and supply chain disruptions. As security challenges grow, energy resilience has become a strategic defence imperative. The chapter explores the interconnection between defence and energy security, emphasising the need for proactive measures, cross-sector collaboration, and long-term resilience strategies.

Chapter 2: Critical Energy Infrastructure Resilience: A Priority for Europe

This chapter explores the strategic importance of CEI resilience for European defence readiness, highlighting how climate change and hybrid threats increasingly threaten energy security. The growing complexity of these risks requires a comprehensive, multi-sector approach that strengthens cooperation between defence, energy, and private sector stakeholders. Given the blurring lines between conventional and hybrid threats, the chapter underscores the need for stronger EU-level coordination and proactive resilience strategies to safeguard critical infrastructure.

Chapter 3: Impacts of Pandemics on Defence-Related CEI

The COVID-19 pandemic revealed significant vulnerabilities in defence-related CEI, especially regarding supply chain disruptions, shifts in energy demand, and cyber threats. This chapter analyses how the pandemic acted as a large-scale stress test for CEI, demonstrating the need for greater collaboration between civilian energy providers and military sectors to secure continuous energy supply during crises.

Chapter 4: The Impact of Finance, Markets, and Ownership on CEI

This chapter examines the financial, market, and ownership structures that influence the security of defence-related CEI. With the majority of CEI owned by private entities, the chapter explores how market volatility, investment flows, and ownership fragmentation can pose risks to national security. It highlights the importance of developing robust regulatory frameworks that ensure the protection of CEI while maintaining market stability.

Chapter 5: Offshore CEI Protection Beyond National Sovereignty

Offshore energy installations, such as wind farms and subsea cables, play an increasingly important role in Europe's energy transition but are vulnerable to geopolitical threats and natural disasters. This chapter explores the challenges of securing offshore CEI in international waters and advocates for enhanced military engagement and international cooperation to protect these critical assets.

Chapter 6: Lessons Learned from Hybrid Threats Tabletop Exercise

This chapter summarises the outcomes of a tabletop exercise held in the context of CF SEDSS simulating hybrid threats against CEI. The exercise exposed the complexity of defending against these threats, including the difficulties of attribution and the potential for cascading impacts across interconnected infrastructures. It underscores the need for civil-military coordination, joint intelligence sharing, and pre-emptive defence policies and strategies.

Chapter 7: Critical Energy Infrastructure Protection in the Near Future

A forward-looking assessment of the emerging challenges for CEI resilience, including the role of artificial intelligence, subsea energy infrastructure, and the integration of cybersecurity into renewable energy projects is outlined in this chapter. It calls for a proactive, strategic approach that balances energy security, economic sustainability, and climate resilience to ensure the future protection of CEI.

Chapter 8: Conclusions and Recommendations

The concluding chapter outlines future priorities for enhancing the resilience of CEI, focusing on the growing role of artificial intelligence in defence, the critical importance of securing subsea energy infrastructure, and integrating cybersecurity into renewable energy projects. It calls for a proactive, forward-looking approach that balances energy security, economic sustainability, and climate resilience. The publication emphasises the need for the EU to shift from a reactive to a proactive stance, requiring action on three levels:
* EU Level: Strengthen coordination among

1 A European Commission initiative managed by the European Defence Agency to assist the European Union ministr.ies of defence to move towards green, resilient, and efficient energy models. More information is available here: https://eda.europa.eu/what-we-do/eu-policies/consultation-forum

2 Documents, reports and publications developed during phase III (2019-2024) of the CF SEDSS project. are available here: https://eda.europa.eu/what-we-do/eu-policies/consultation-forum/phase-iii/deliverables

3 For more information about the CF SEDSS working groups, including PCEI WG3 see here: https://eda.europa.eu/what-we-do/eu-policies/consultation-forum/phase-iii/factsheets

Member States through joint initiatives, research projects leading to products, and policy frameworks to address cross-border CEI vulnerabilities.
* National level: Ministries of Defence and Armed Forces: Integrate CEI resilience into national defence strategies and budget, ensuring preparedness for cyber, physical, and climate-related threats.
* Private Sector: Invest in resilient infrastructure and collaborate closely with military and government agencies, focusing on innovative technologies and enhanced cybersecurity to safeguard CEI.

The Editors
Brussels, August 2025

01

Energy Resilience in Defence: Adapting to a Changing Security Landscape

Alexandru Georgescu, *National Institute for Research and Development in Informatics ICI Bucharest*
Hadjisavvas Constantinos, *European Defence Agency*

1.1 Introduction

Since 2015, the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) has brought together Ministry of Defence (MoD) representatives, experts from academia and the private sector, and national and European authorities to explore the evolving relationship between energy and defence. Over the years, CF SEDSS has grown into the largest defence-energy community in Europe, involving over 30 European countries and fostering essential collaboration between the two sectors. These connections have become critical to European strategic objectives, especially in an era of heightened security threats and rapid energy transformation. Energy resilience is now a core defence priority, not only to ensure the military's ability to operate under any conditions but also because the defence sector itself is undergoing a major transformation. The need to enhance energy security, efficiency, and sustainability comes at a time when armed forces must also adapt to emerging threats, climate change, and geopolitical shifts.

To address these challenges and advance sustainable energy in defence[4], CF SEDSS has established itself as the leading European platform for sharing information, exchanging best practices, and fostering cross-sector collaboration. By bringing together stakeholders from across the EU Member States, the Forum facilitates the generation of innovative defence energy-related projects[5] and promotes joint initiatives aimed at strengthening energy security and sustainability. To achieve these objectives, the CF SEDSS operates through four dedicated working groups (WGs)[6]:

- **WG1**: Focuses on improving energy efficiency and building performance in the defence sector.
- **WG2**: Explores the utilisation of renewable energy sources to reduce dependence on fossil fuels.
- **WG3**: Works on enhancing the resilience of defence-related CEI.
- **Transversal Working Group**: Addresses cross-cutting themes, including energy management and policy, emerging energy technologies, and the identification of funding and financing instruments for defence energy initiatives.

This chapter argues that **CEI protection is no longer optional but a strategic defence imperative**, especially in an era of growing geopolitical instability, hybrid threats and evolving security threats. It sets the foundation for this publication by explaining the key themes and strategic priorities that will be explored in the following chapters. In this context, the chapter outlines the extensive contributions of WG3, which has led research on CEI resilience, the identification of hybrid and asymmetrical threats, and the development of strategic response frameworks. It also introduces a brief policy analysis on implementing key EU legislation on energy security. Finally, the chapter highlights the crucial role of the armed forces in ensuring CEI resilience, emphasising the need for proactive defence engagement, strategic planning, and cross-sector cooperation. By doing so, it sets the stage for the subsequent chapters, which will delve deeper into the technical, policy, and operational dimensions of CEI protection in the defence sector.

4 Hadjisavvas, Kuzel, Lazzari, et al. Guidance on Advancing Sustainable Energy in Defence, Brussels: Eu-ropean Defence Agency, 2024, https://eda.europa.eu/docs/default-source/consultation-forum/guid-ance-document/cf-sedss-iii-guidance-document.pdf

5 Hadjisavvas, Kuzel, Lazzari, 30 CF SEDSS Transformative Project Ideas for Advancing the Defence Energy Transition, Brussels: European Defence Agency, 2024, https://eda.europa.eu/docs/default-source/consultation-forum/project-ideas/cf-sedss-iii-project-ideas.pdf

6 For all CF SEDSS WGs see footnote number 3.

1.2 Balancing military readiness and energy transition

Europe is experiencing its most volatile security landscape since the Cold War, marked by the war in Ukraine, escalating geopolitical tensions, and increasing crisis response demands. These developments have placed additional pressures on EU Member States' armed forces, the defence industry, and public institutions to develop new capabilities, cost-effective technologies, and enhanced operational capacity. At the same time, the EU has reaffirmed its commitment to the energy transition, focusing on reducing dependence on fossil fuels, increasing energy efficiency, and decarbonising its economy—including its armed forces. Efficiency, sustainability, resilience, and carbon neutrality have become central pillars of EU energy and defence policies. However, these priorities must not come at the expense of military operational effectiveness. **The challenge lies in balancing climate and energy goals with the core mission of national defence**.

The armed forces are among the largest public consumers of fossil fuels in many EU Member States. While they must adapt to the digital and green transition, military operations remain heavily reliant on stable and secure energy supplies. The consequences of climate change—such as extreme weather events, wildfires, droughts, and flooding—already affect military bases and operations, forcing MoDs to divert resources for disaster response and infrastructure protection. Meanwhile, Europe's push for energy independence, accelerated by geopolitical instability and sanctions on Russia, further underscores the need for energy resilience in defence.

The CF SEDSS project has been instrumental in raising awareness among MoDs and supporting their alignment with EU energy and climate priorities. More importantly, it has demonstrated how energy efficiency, renewable integration, and sustainability strategies can enhance rather than weaken defence resilience. By fostering dialogue and cooperation, it has also enabled MoDs to proactively redefine their role not only as energy consumers but as potential energy producers—fully integrated within the Energy Union and the broader European energy market.

As most CEI is privately operated, military forces depend on uninterrupted services from civilian energy providers. Any disruptions—whether caused by cyberattacks, hybrid threats, or supply chain vulnerabilities—can have severe consequences, impacting not just defence readiness but also national security, economic stability, and public trust. To **maintain operational effectiveness, the defence sector must ensure energy affordability, sustainability, and resilience**. Achieving this balance requires an approach that integrates defence energy needs with the green transition, focusing on key priority areas:

- **Supply chain security** which includes affordable, sustainable, accessible and resilient supply of energy both during normal activities as well as during crisis and emergency situations.
- **Energy efficiency and renewable sources integration in military operations,** ensuring that armed forces enhance operational effectiveness while reducing dependence on fossil fuels.
- **Energy storage**, supply chain vulnerabilities, and diversification of energy sources, securing the resilience of military energy supply chains in times of crisis.
- **Climate change adaptation for defence infrastructure and operational readiness**, addressing risks from extreme weather events, rising temperatures, and natural disasters.
- **Cybersecurity risks in smart energy systems and digitalisation**, safeguarding energy assets used in defence also from the risks generated by the adoption of emerging digital technologies, such as AI in grid management, industrial control systems, data analysis and other roles.

- **Protection of offshore and undersea CEI**, especially against emerging threats to subsea energy networks and novel hybrid warfare means.
- **Evaluating the risks of foreign investments** in CEI and ensuring resilience against strategic dependencies.

1.3 EU policy evolution: Strengthening CEI protection

Ensuring the resilience of CEI is fundamental to military operational effectiveness, as modern defence depends on stable energy supplies, secure communication networks, and resilient logistics chains. However, the interdependencies between different critical sectors — such as energy, telecommunications, transport, and ICT — mean that **vulnerabilities in one sector can trigger cascading effects, ultimately jeopardising military and civilian security alike**.

Recognising these interdependencies and risks, the EU has developed a structured approach to Critical Infrastructure Protection (CIP). While some infrastructures are national and affect only a single Member State, many extend beyond borders and require EU-level coordination. The Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER Directive[7]) establishes minimum security standards, requiring mandatory identification and risk assessment of critical entities. Meanwhile, European Critical Infrastructures (ECIs)—which impact multiple Member States—demand coordinated security and resilience measures between the EU, hosting Member States, and affected Member States.

Furthermore, under the EU's new 'Blueprint for Resilience' (Council Recommendation 2023/C 20/01[8]), infrastructures of special importance—those impacting six or more Member States—demand enhanced strategic oversight and coordinated response mechanisms. As CEI threats increasingly transcend national borders, resilience-building requires pan-European coordination, strategic foresight, and public-private cooperation. The Energy Union framework further underscores the need for robust governance and crisis preparedness mechanisms. By recognising these emerging risks and adapting EU policy accordingly, the European regulatory framework now provides a stronger foundation for ensuring CEI security and resilience. However, continued defence-sector engagement, cross-border cooperation, and integration with private-sector stakeholders will be essential to safeguarding CEI in the evolving security landscape.

Over the past two decades, the European Programme for Critical Infrastructure Protection (EPCIP) has undergone significant transformation. Initially, its legal foundation was based on:

- Council Directive 2008/114/EC, which introduced the first framework for identifying and designating European Critical Infrastructures (ECIs).
- The NIS Directive (Directive (EU) 2016/1148), which laid the groundwork for enhancing cybersecurity across critical networks.

As threats to CEI have evolved, the EU's regulatory and strategic response has expanded significantly. The new framework now includes:

- The CER Directive (Directive (EU) 2022/2557)—which replaces the 2008 Directive, expanding CEI protections beyond just energy and transport to cover 11 key sectors, ensuring a more comprehensive resilience approach.
- The NIS 2 Directive (Directive (EU) 2022/2555)—which updates and strengthens cybersecurity requirements for critical infrastructure operators, reflecting the increasing digitalisation of CEI.

Recognising that cybersecurity is now integral to CEI resilience, the CER and NIS 2 Directives share a unified taxonomy of critical/essential entities, ensuring a coordinated approach to both digital and physical infrastructure protection. Beyond the CER and NIS 2 Directives, several EU regulations further reinforce CEI security, energy resilience, and crisis preparedness, including:

- Regulation (EU) 2019/941 – On risk preparedness in the electricity sector, ensuring contingency planning.
- Regulation (EU) 2019/942 – Establishing the European Union Agency for the Cooperation of Energy Regulators (ACER).
- Regulation (EU) 2019/943 – Governing the internal market for electricity, enhancing energy market stability.
- Regulation (EU) 2023/0109 – Strengthening solidarity and response measures against cybersecurity threats.
- The EU Cybersecurity Act (Regulation (EU) 2019/881) – Establishing ENISA as the leading agency for cybersecurity certification and incident response.
- The EU Strategic Compass for Security and Defence – For the first time, this policy explicitly calls on MoDs to integrate climate and energy resilience into national defence strategies.

While EU policy frameworks provide the foundation for CEI protection, their effectiveness depends on the active role of national defence authorities. Armed forces must not only comply whenever is relevant with these evolving regulations but also develop the operational capabilities and strategic foresight needed to secure CEI from emerging threats. This requires a shift from passive reliance on civilian infrastructure to proactive engagement in energy security and resilience efforts. The following section examines the crucial role of defence in protecting CEI and the challenges that must be addressed to ensure operational continuity in an increasingly volatile security environment.

1.4 The role of defence in protecting CEI

Energy is the foundation of all critical infrastructures, as sectors such as healthcare, finance, transport, and ICT rely on affordable, accessible, and sustainable energy to function with minimal disruption. This dependency makes security of supply a fundamental priority for Europe, particularly in today's evolving security environment, where energy systems have become both strategic assets and high-value targets. Since the launch of CF SEDSS's WG3 in 2016, it has become evident that defence-related CEI is inseparable from civilian CEI. Unlike other sectors, defence (MoDs and armed forces) cannot function without a reliable and resilient energy supply, yet they lack a fully independent military energy system. Instead, they rely almost entirely on civilian-operated infrastructure, with only limited emergency provisions in place for crisis situations. This interdependence has made CEI a prime target for hybrid warfare, particularly through cyber, physical, and electronic attacks designed to weaken national resilience and undermine military effectiveness.

The war in Ukraine has provided a stark example of how energy infrastructure is weaponised in modern conflicts. Attacks on power grids, oil depots, and energy transport networks have caused widespread blackouts, disrupted critical services, and placed enormous strain on military

7 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, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

8 Proposal for a COUNCIL RECOMMENDATION on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance, https://eur-lex.europa.eu/resource.html?uri=cellar:9d905b3c-4cbc-11ee-9220-01aa75ed71a1.0001.02/DOC_1&format=PDF

logistics. Hybrid warfare tactics - such as cyberattacks and sabotage - are particularly effective because they often operate below the threshold of armed response, making it difficult to justify a direct military response while the issue of attribution with a high level of certainty is also elusive.

Beyond kinetic attacks, cybersecurity vulnerabilities pose a growing risk to CEI and defence operations. Cyber threats can:

- Disrupt energy supply chains, compromising military readiness.
- Manipulate critical infrastructure systems, leading to cascading failures across multiple sectors
- Undermine public trust in energy resilience, creating economic and social instability.

MoDs and armed forces must rapidly adapt to these new realities with a proactive and integrated approach. **Cyber defence, energy security, and CEI can no longer be treated as separate domains — they are now fundamentally interconnected**. They need to equip with the most suitable capabilities and technologies, while investing in skills to ensure that they can **understand, detect, deter, prevent these threats and, if they fail to do so, to withstand the impact with as little damage as possible** and to **recover to a minimum acceptable level of functioning in as short a time** as possible while **learning from the incident to improve security outcomes** during future events of the same type. Despite the clear security implications of CEI vulnerabilities, many EU MoDs have struggled to engage effectively with the civilian energy sector. Several factors contribute to this challenge:

- **Awareness gaps:** CEI security has traditionally been seen as a civilian sector responsibility, leading to a lack of defence-specific expertise.
- **Limited resources and institutional barriers:** CEI governance falls primarily under Ministries of Energy or Interior, making direct MoD involvement complex.
- **Cultural and strategic differences:** The private sector operates on market-driven principles, while defence institutions prioritize security and national sovereignty.

CF SEDSS has played a crucial role in addressing these challenges. Starting in 2017 with the development of the first Concept Note on the Protection of Critical Energy Infrastructure (PCEI)[9], WG3 laid the groundwork for understanding the unique vulnerabilities of defence-related CEI and the growing threats posed by hybrid warfare, cyberattacks, and geopolitical tensions. This Concept Note was the first structured effort to outline the specific risks faced by the defence sector and propose initial policy recommendations for enhancing CEI resilience. It set the foundation for subsequent research, strategic discussions, and policy initiatives within CF SEDSS.

By fostering an integrated defence-energy community, CF SEDSS has helped MoDs build relationships with energy regulators, private sector operators, and cybersecurity specialists. This cooperation has been particularly valuable during Phase III (2019-2024) of CF SEDSS, which coincided with a major overhaul of the EU's critical infrastructure protection (CIP) and energy security frameworks. With direct input from DG ENER and DG Joint Research Centre (JRC), MoDs have been actively involved in shaping reforms driven by lessons learned from the COVID-19 pandemic, the prolonged conflict in Ukraine, and other geopolitical crises. This growing engagement represents a significant step forward in enhancing defence-related CEI resilience.

9 Protection of Critical Energy Infrastructure Conceptual Paper, Brussels: European Defence Agency, 2017, Conceptual Paper - https://eda.europa.eu/docs/default-source/events/eden/phase-i/informa-tion-sheets/cf-sedss---protection-of-critical-energy-infrastructure-conceptual-paper.pdf

1.5 Enhancing the role of defence in CEI resilience: from awareness to action

As threats to CEI become more sophisticated and widespread, EU MoDs must move beyond awareness and actively contribute to resilience-building efforts. MoDs and armed forces are uniquely positioned to support CEI protection by leveraging strategic foresight, operational planning, and cross-sector collaboration. CF SEDSS WG3 has played a crucial role in this transition, providing timely insights and policy recommendations on:

- **Offshore and undersea CEI security**, recognising its vulnerabilities even before the sabotage of the Nord Stream pipelines[10].
- **Impact of financial and commodity market volatility on energy security**, particularly for military operations[11].
- **Increasing reliance on space-based systems for CEI** monitoring and defence applications.
- **Cyber-physical vulnerabilities in the energy sector,** requiring stronger cybersecurity measures for critical infrastructure assets.
- **Legal and strategic challenges of MoD involvement in CEI protection,** including operations in international waters and special economic zones.
- **European tabletop exercise** (Sofia, Bulgaria, May 2023), bringing together MoDs, energy operators, and security experts to simulate real-world CEI disruptions[12].

The impact of these efforts is already evident. European MoDs are increasingly aware of their critical dependencies on CEI and are taking proactive steps to enhance resilience. MoDs and armed forces are transitioning from a passive reliance on civilian energy infrastructure to an active role in securing energy supply chains, integrating sustainability into defence planning, and adopting new technologies for energy resilience. However, ensuring long-term implementation requires overcoming key barriers such as funding constraints, inter-agency coordination gaps, and the integration of evolving technologies into existing defence structures.

To **sustain progress in CEI protection and resilience**, the future of defence energy security will depend on:

- **Greater collaboration between defence, energy, and cybersecurity communities**, ensuring a coordinated response to emerging threats.
- **Increased investment in the protection of digital-physical systems within critical infrastructure** from all hazards, including the emerging issue of electromagnetic spectrum threats as well as the use of drones for infiltration and sabotage.
- **Enhanced regulatory and policy frameworks that align energy resilience with military operational needs**, ensuring that sustainability efforts do not compromise mission effectiveness.
- On a case-by-case basis, **strategic investment in resilient and secure CEI** owned and operated by armed forces to achieve partial energy autonomy, especially situational, which can also feed back into societal resilience with these

10 https://eda.europa.eu/docs/default-source/consultation-forum/research-studies/offshore-critical-energy-infra.pdf

11 https://eda.europa.eu/docs/default-source/consultation-forum/research-studies/impact-of-finance-markets.pdf

12 Tabletop exercise and new study focus on protecting critical energy infrastructure - https://eda.europa.eu/news-and-events/news/2023/05/26/tabletop-exercise-and-new-study-focus-on-protecting-critical-energy-infrastructure

CEI being able to contribute to overall capacity within society.

- Greater **investment in awareness, education, and structured re-skilling and upskilling programs for MoD personnel**, ensuring they can operate, secure, and manage advanced energy technologies and smart energy systems in defence environments.

As Europe advances toward 2030, the challenges of energy security, hybrid warfare, and strategic autonomy will intensify. With the EU aiming to cut greenhouse gas emissions by 55%, the defence sector must accelerate efforts to enhance energy resilience, efficiency, and sustainability. The defence ecosystem—especially the armed forces—must not only adapt to the evolving energy landscape but also develop the skills and capabilities needed to operate and secure smart energy systems across infrastructure, installations, platforms, weapon systems, and personnel. Integrating these advanced energy technologies into defence operations will require not only technical expertise but also strong institutional leadership and investment in cross-sector collaboration to ensure seamless implementation. CF SEDSS must remain a driving force, equipping MoDs with the insights, technologies, and strategies necessary to safeguard CEI and ensure operational effectiveness in an increasingly complex security environment.

02

Critical Energy Infrastructure Resilience: A Priority for Europe

Constantinos Hadjisavvas, *European Defence Agency*
Elisabeth Krausmann, Ricardo Tavares da Costa, Georgios Valsamos, Georgios Giannopoulos and Rainer Jungwirth *European Commission Joint Research Centre*

2.1 Introduction

Constantinos Hadjisavvas, *European Defence Agency*
Elisabeth Krausmann, *European Commission Joint Research Centre*

CEI resilience is crucial for European security, especially amid rising geopolitical tensions and increasingly frequent climate-related disasters. In the defence context, CEI encompasses all energy systems and resources essential for military operations and logistics. These infrastructures face growing threats—not only from extreme weather events and natural disasters but also from hybrid threats such as cyberattacks, terrorism, and geopolitical instability. Europe's highly interconnected energy networks mean that disruptions in one region can trigger cascading effects across borders, jeopardizing military readiness and national security. Given that most CEI is privately owned and operated, strong cooperation between armed forces, energy providers, and policymakers is crucial. A coordinated EU-wide approach is needed to mitigate vulnerabilities, ensure rapid crisis response, and enhance infrastructure resilience.

This chapter explores two critical aspects of CEI resilience: (2.2) the growing risks from climate change, including extreme weather, resource scarcity, and their impact on military infrastructure, and (2.3) the increasing threat of hybrid attacks, where state and non-state actors exploit energy infrastructure vulnerabilities to disrupt operations and destabilize security. It emphasises the need for proactive adaptation, strategic planning, and cross-sector cooperation to safeguard defence capabilities. Drawing on lessons from recent crises, the chapter outlines concrete steps to enhance CEI resilience through risk management, innovation, and civil-military collaboration. Strengthening CEI protection is not just a security necessity—it is fundamental to Europe's strategic autonomy and defence readiness in an era of escalating global instability.

2.2 Climate change in defence: reshaping the current risk landscape

Elisabeth Krausmann, Ricardo Tavares da Costa, *European Commission Joint Research Centre*
Constantinos Hadjisavvas, *European Defence Agency*

According to the Intergovernmental Panel on Climate Change (IPCC), an expert group brought together by the United Nations to track and evaluate the global science on climate change, greenhouse gas emissions (GHG) linked to human activities (e.g., the burning of fossil fuels or changes in land use) are warming the climate at an unprecedented rate[13]. This contributes to shifts in the climate system which in turn affects weather patterns, giving rise to more frequent extreme weather events, and accelerates the melting of land and sea ice, and sea-level rise. As a result, more floods and droughts are expected in Western and Central Europe[14], and more frequent pluvial floods and fire weather in Eastern Europe. At the same time, higher temperatures and more heatwaves, droughts, fire weather and coastal flooding are predicted for the Mediterranean region, accompanied by a decrease in precipitation[13].

Climate change affects all sectors of society and the armed forces are no exception. In EDA's capability development analysis beyond 2040, **climate change is predicted to reshape the future security and operational environment**, thereby underscoring the urgency for EU countries' armed forces to adapt and prepare[15]. **Defence assets, workforce, capabilities, missions and operations are also at risk from climate hazards**[16].

Impacts of climate hazards can damage or destroy military assets or render them unfit for purpose under certain operating conditions (e.g., flooded runways – Figure 1). They can also give rise to higher costs for utility services (e.g., higher energy demand for cooling and ventilation during heatwaves) and for applying shorter inspection, maintenance, repair and overhaul (MRO) intervals (e.g., increased wear and tear during extreme temperatures). They can also endanger the safety and well-being of military personnel (e.g., heat-related illnesses).

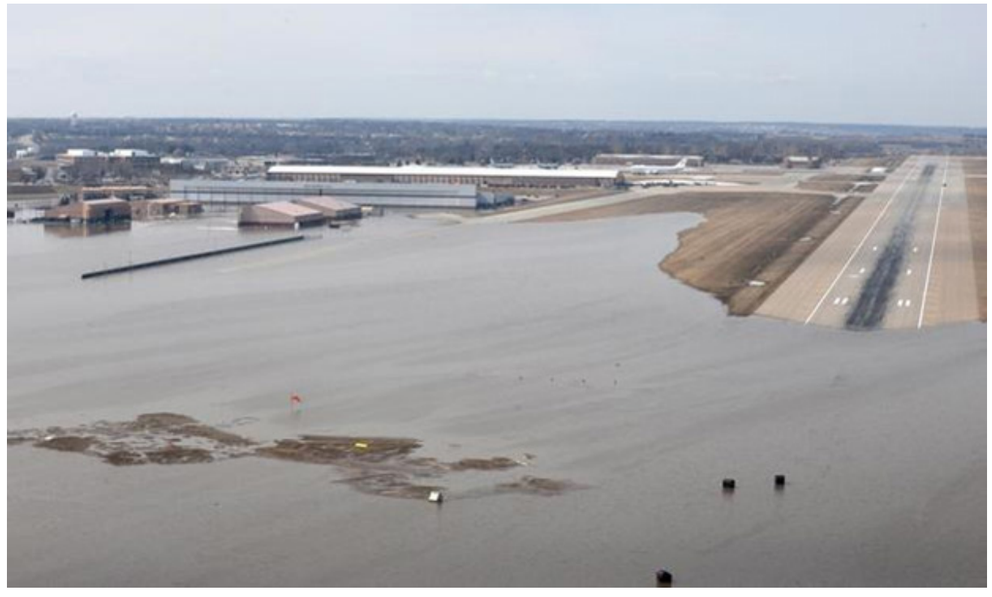


Figure 1 Flooded runway at a US Air Force Base, Photo credit: TSgt. R. Blake.

At the same time, **climate hazards are also a threat to civilian entities that provide essential services to the armed forces, such as power, water, or fuel**. If these services are interrupted by a climatic event, this disruption can cascade to military in-

13 IPCC (2021) Climate change 2021: The physical science basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change, Eds: Masson-Delmotte, V., Zhai, P., Pirani, et al., Intergovernmental Panel on Climate Change, Cambridge University Press, Cambridge, UK and New York, US. https://www.ipcc.ch/report/ar6/wg1/

14 Naumann, G., Cammalleri, C., Mentaschi, L. and Feyen, L. (2021) Increased economic drought impacts in Europe with anthropogenic warming. Nature Climate Change 11, 485-491.

15 EDA (2023) Enhancing EU Military Capabilities Beyond 2040 – Main findings from the 2023 Long-Term Assessment of the Capability Development Plan. https://doi.org/10.2836/360180

16 Tavares da Costa, R., Krausmann, E. (2021) Impacts of Natural Hazards and Climate Change on EU Security and Defence, Publications Office of the European Union, Luxembourg, doi:10.2760/244397, JRC126315.

stallations, thereby jeopardising operational effectiveness and readiness due to external dependencies.

Compounding the risk, climate hazards can also trigger technological accidents involving hazardous substances[17], causing oil spills, fires and explosions (Figure 2). Such accidents are of particular relevance in CEI and at military sites that handle such substances (e.g., oil and gas, explosives, ammunition). For example, in 2023, a wildfire in Greece led to multiple explosions at an ammunition depot within an air force base[18], while a heatwave in 2020 in Jordan caused the expansion of mortar shells, leading to a series of massive explosions[19].

Figure 2 Flooding in the San Jacinto river basin led to the rupture of oil pipelines which spewed flammable hydrocarbons into the floodwaters where they ignited. Photo credit: USGS

2.2.1 Analysing the climate-energy-defence nexus

Armed forces rely on stable energy supplies for everything from base operations to frontline logistics. However, climate-related disruptions—such as extreme weather, resource shortages, and blackouts—are directly impacting defence infrastructure, forcing armed forces to adapt. Consequently, **climate change poses multidimensional challenges to energy security** and infrastructure with profound repercussions for defence and national security. For example, climate change exacerbates geopolitical tensions over dwindling energy reserves and access to resources which can increase the likelihood of conflicts. At the same time, the energy sector accelerates climate change via its reliance on fossil fuels for energy production, which makes it a major contributor to the emission of GHGs.

To further complicate matters, the **energy sector is itself highly vulnerable and increasingly exposed to the effects of climate change**. Numerous energy supply chain disruptions due to climate hazards have already been documented, including instances of propagation through all (inter) connected systems and knock-on effects to military installations.

During a winter storm in the USA in 2021, with power blackouts lasting several days, an air force base had to rely on backup power for part of its nuclear missile field, and several military installations were damaged and down to mission-essential personnel. The severity and duration of the storm had been grossly underestimated prior to the event, as was the vulnerability of the power grid and the gas facilities to cold weather, and the power supply was unable to match demand[20]. The storm's impacts rippled through all sources of energy production (gas, nuclear, solar, wind, coal, hydro), with most outages and derates related to a shortfall in natural gas caused by the high demand and forced shut-ins, frozen pipelines and well-heads, and the near depletion of stored gas supplies (Figure 3).

This complex set of vulnerabilities in the energy sector amplifies concern for the armed forces, which rely heavily on secure and resilient energy sources to sustain operations and readiness.

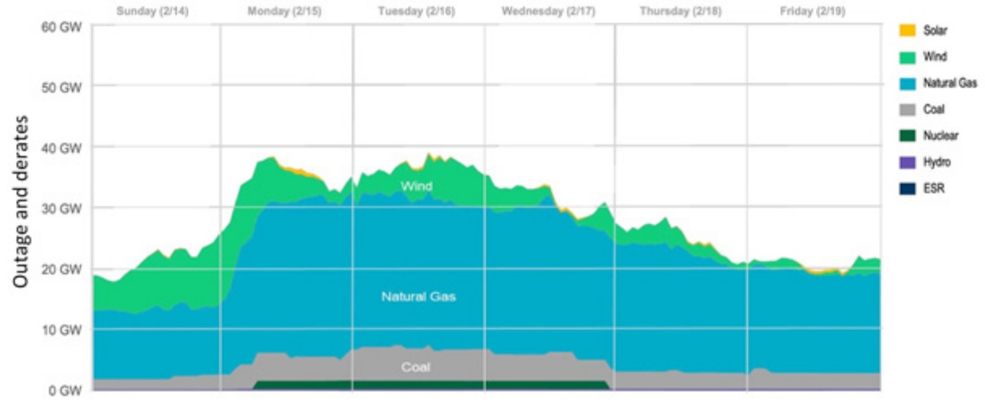


Figure 3 Net generation outages and derates by fuel type in February, 2021. Wind and solar values are estimated (ESR: energy storage resources). Source: ERCOT

A collaborative study by the European Commission's Joint Research Centre (JRC) and EDA, conducted in the CF SEDSS context, aimed to **shed light on the links between climate change, energy and defence in the EU**[20]. More specifically, the study's goals were three-fold:

1. Assess the impacts of climate change on defence-related CEI, military installations and capabilities, including via dependencies;
2. Identify gaps and propose options to strengthen resilience to climate change in defence-related CEI, military installations and capabilities;
3. Suggest ways forward for defence to reduce its climate footprint and increase its sustainability.

In addition to discussing the specific effects of each analysed climate hazard[21] in detail, the study found that some impacts on military facilities, equipment and personnel are common to all climate hazards and include an **increase in demand for securing critical infrastructure** (e.g., during a prolonged blackout) **and for MRO, a higher need for supplies, spare parts and staffing, limited access to facilities and equipment, delayed operations, degradation and loss of military land, reduced readiness, reduced cognitive performance of personnel, and higher operational costs**. It was also noted that **climate hazards may happen simultaneously and reinforce each other**. As an example, light-

17 Krausmann, E. and Necci, A. (2021) Thinking the unthinkable: A perspective on Natech risks and Black Swans, Safety Science 139, https://doi.org/10.1016/j.ssci.2021.105255.

18 Tavares da Costa, R., Krausmann, E., Hadjisavvas, C. (2024) Navigating climate change in defence – Climate risk management guide for Chiefs of Defence Staff, Publications Office of the European Union, Luxembourg. doi:10.2760/252092, JRC135952.

19 https://www.reuters.com/article/idUSKBN2613LD/

20 Tavares da Costa, R., Krausmann, E., Hadjisavvas, C. (2023) Impacts of climate change on defence-related critical energy infrastructure, Publications Office of the European Union, Luxembourg. doi:10.2760/03454, JRC130884.

21 High temperature and heatwaves, drought, extreme cold, floods and heavy rainfall, windstorm and lightning, wildfire.

ning can trigger a wildfire which can in turn be fanned by high winds. This can lead to multiple impacts associated with different hazard types.

With respect to CEI, each climate hazard exerts specific types of stress on the different components of an energy system. Following an in-depth analysis of the impact mechanisms and disruption paths, Tavares da Costa et al.[20] summarise potential impacts on CEI as well as their consequences. Also here, some consequences are common to all climate hazards and include loss, limited access to or unavailability of tools, means and/or facilities, increase in MRO, response and recovery operations, delays, staffing, parts and equipment needs, higher operational costs and danger of stranded assets. Table 1 provides an example of the expected impacts of drought on electricity, and oil and gas infrastructure.

Table 1 Example of climate hazard impact on different types of CEI [excerpt from Tavares da Costa et al.[20] (Table A.2)

	Electricity	Oil and gas
Drought	Damage to structures, equipment or components/network elements due to ground failure from soil dry-out.	Damage to oil and gas wells, pump/meter stations, tank farms and terminals due to ground failure from soil dry-out.
	Reduction of electricity generation, e.g., in hydropower due to low river flows, and restrictions associated with water use and environmental flows; in concentrated solar power (CSP) due to water use restrictions; in thermal power plants due to water use restrictions for cooling and emissions control systems (including carbon capture and storage), restrictions in the discharge of water, and due to limited inland water transport of fuels (e.g., coal transport); in biofuel power plants due to biofuel crops yield loss.	Damage to pipelines and components (small-bore connections, welds, flanged joints, concrete anchor blocks, aboveground storage tank foundations) due to ground failure from soil dry-out.
	Energy export restrictions (reduction of electricity interconnector capacity or curtailment of oil and gas exports).	
	Reduction of transmission and distribution efficiency of subsurface electric power lines and effectiveness of earth wires.	Releases of dangerous substances from damaged components.
	Increase in electricity demand due to an increase in water use (e.g., pumping, irrigation, desalinisation).	

The joint JRC-EDA study also found **significant climate adaptation gaps in defence** across multiple domains, e.g., the operational dimension, capability planning and development, multi-stakeholder engagement, governance, and R&D. Most importantly, **military installations in the EU may be operating with unknown climate risk** due to a lack of analyses on climate change impacts on defence. In addition, climate concerns are insufficiently integrated in capability planning, investment lifecycles, procurement criteria and R&D. Since CEI used by the military is often owned and operated by civilian entities, Ministries of Defence (MoD) have limited influence over managing climate risks in CEI and strengthening resilience. The problem is compounded by civilian entities that operate interdependent critical infrastructure (e.g., energy, water, transport, telecommunications) who often do not coordinate efforts across sectors or with MoDs to manage risks.

Strengthening resilience to climate change requires implementing a set of measures spanning different geographic scales, from national (e.g., MoD, CEI operators) to EU level. Tavares da Costa et al.[20] conclude that the sector needs to bolster its resilience which can be achieved, i.e., by **advancing the level of understanding of climate impacts in defence, performing climate risk assessments, investing in fortified infrastructure** and assets, reviewing risk management plans to identify gaps, and adapting planning processes to ensure they consider potential future climates. Integrating climate considerations into awareness-raising and training programmes is also essential. They also recommend the development of specific guidelines for the management of climate risk in defence, both at the leadership (chief of staff) and at the implementation level.

2.2.2 Guiding chiefs of defence staff towards effective climate risk management

Proactively addressing climate change via risk management and implementing tailored risk reduction and resilience measures, combined with efforts to lower GHG emissions, decreases future financial losses, preserves military capability and ensures operational effectiveness. This process can be facilitated by making use of dedicated guidance that helps defence to navigate the intricate climate risk management landscape.

Addressing the corresponding recommendation in Tavares da Costa et al.[20], the JRC, in collaboration with EDA, undertook the development of such guidance, targeting the senior leadership level[18]. Chiefs of Defence Staff (CHOD) exert a transformative influence, have the power to foster a risk-aware culture, and prepare the ground for effective climate risk management (CRM) implementation. **The guidance constitutes a comprehensive roadmap for CHODs to understand their organisation's exposure to climate hazards and the associated vulnerabilities of its elements, missions and operations.** This includes understanding the dependencies on external critical services (e.g., CEI). Hence, CHODs can and should promote action on risk reduction and resilience building with regard to climate change.

The guidance puts forward the following recommendations for the effective implementation of CRM across defence[18]:

- Align national defence strategies on climate change with the EU's objectives on climate change adaptation, energy resilience and net-zero GHG emissions by 2050.
- Harmonise CRM with the organisation's strategic goals.
- Integrate CRM into all the organisation's processes and across departments and functions.
- Allocate resources to risk reduction and resilience building.
- Establish a multidisciplinary team in CRM to analyse and propose measures for addressing climate risks.
- Foster a climate risk culture and enhance awareness.
- Ensure that CRM is equitable and inclusive of vulnerable groups.
- Develop and strengthen staff expertise in CRM.
- Encourage a culture of continuous learning and adaptation.
- Encourage intelligent and energy-efficient use of technology to reduce technological accidents and environmental impacts.

- Leverage procurement processes to facilitate climate action, e.g., by applying green procurement and circular economy principles.

It is essential that CHODs have a realistic view of the CRM status in their organization to understand strengths and areas for improvement. To enable this process,

Table 2 Self-assessment questions on prevention and risk treatment for CHODs (example checklist from Tavares da Costa et al.[18]).

	Prevention and risk treatment	Yes	Not sure	No
1	Do you ensure that you organisation's activities and practices are consistent with climate change adaptation and climate change mitigation?			
2	Are regular risk assessments conducted across your organisation?			
3	Are risk assessment approaches consistent across your organisation's departments and functions?			
4	Are risk assessments in your organisation coherent with existing national and regional risk assessments and climate projections?			
5	Do you think that resources allocated for climate risk management and resilience building are sufficient in your organisation?			
6	Do you make use of your organisation's in-house expertise to enhance risk assessments (e.g., Weather Officers)?			
7	Has your organisation implemented physical measures to prevent or control consequences (e.g., flood defences, redundant emergency power) associated with climate hazards?			
8	Does your organisation diversify energy sources and suppliers to prevent external disruptions or has contingencies in case of disruptions?			
9	Does your organisation incentivise and recognise employees who identify potential risks before they escalate?			
10	Has your organisation employed scenario building techniques (e.g., red teaming, scenario planning) to uncover potential climate vulnerabilities?			

the guidance also includes a set of checklists that allow CHODs to quickly evaluate the presence and adequacy of current strategies, identify vulnerabilities, and prioritize actions for mitigating climate risk. Table 2 shows an example of such a checklist. The self-assessment covers six key areas which address the following topics[18]:

1. Risk awareness (understanding climate change impacts)
2. Leadership and risk culture (proactive risk management, roles and responsibilities)
3. Risk information (accessibility, accuracy, use in decision-making processes)
4. Risk management expertise (assessment capabilities, staff training, skills development)
5. Prevention and risk treatment (adaptation and mitigation strategies, contingencies)
6. Emergency response and recovery (assessments, plans, resource allocation, resilience, effectiveness).

2.2.3 Climate proofing EU defence

The impacts of climate change on defence are expected to increase in the future, and the armed forces have to adapt to the changed risk landscape to avoid losses and remain operative. To support its Member States, the EU has created several policy instruments that underscore the importance of the link between climate, security and defence. These instruments call for action in both reducing GHG emissions (climate mitigation) and strengthening resilience (climate adaptation) in defence.

For example, the 2022 Strategic Compass for Security and Defence[22] highlights climate change as a threat multiplier that needs to be addressed by strengthening resilience and achieving net-zero GHG emissions. The Strategic Compass requires the EU Member States to develop national strategies to prepare the armed forces for climate change. More recently, the 2023 Joint Communication on the climate-security nexus[23], which complements the 2020 EU Climate Change and Defence Roadmap[24], the first EU action plan to address the links between defence and climate change, lays down EU-level actions to address climate change and environmental degradation in peace, security and defence.

Also of relevance in this context is the Critical Entities Resilience Directive[25] which aims to strengthen the resilience of critical entities, including against climate risk, and acknowledges the interdependence of critical infrastructure which is of great significance to defence.

While defence must increase its resilience to climate change, at the same time it has to reduce its GHG emissions without affecting operational effectiveness, readiness, or deterrence. The defence sector is a large consumer of fossil fuels and raw materials which is reflected in a large carbon footprint. Efforts to reduce GHG emissions are therefore crucial to help fight climate change. Such efforts can also create co-benefits, improving the autonomy and energy security of the armed forces through diversification, and decreasing exposure via the reduction of the amount of energy provided through the supply chains.

2.2.4 Conclusions

Climate change presents multifaceted risks to global security, necessitating a paradigm shift in how the defence ecosystem responds and operates. For the armed forces, the cascading effects of climate

22 Council of the European Union (2022) 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, 21 March 2022, 7371/22. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

23 EC/EEAS (2023) Joint communication to the European Parliament and the Council, A new outlook on the climate and security nexus: addressing the impact of climate change and environmental degradation on peace, security and defence, JOIN(2023)19 final. https://www.eeas.europa.eu/eeas/joint-communication-climate-security-nexus_en

24 EEAS (2020) Climate Change and Defence Roadmap, EEAS(2020)1251. https://data.consilium.europa.eu/doc/document/ST-12741-2020-INIT/en/pdf

25 EC (2022) 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. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

change, such as extreme weather events, sea-level rise, and temperature fluctuations, can compromise critical infrastructure, disrupt supply chains, and impact sustainability and readiness. These challenges underscore the urgency for MoDs to integrate climate resilience into their defence planning, procurement and budgets. By doing so, the armed forces can maintain operational effectiveness and safeguard national security while contributing to the EU's broader sustainability and climate adaptation efforts.

This chapter, which describes the outcome of extensive research partly conducted within the CF SEDSS context, led by the JRC and EDA, highlights the significant and growing impact of climate change on defence-related CEI. The respective findings and recommendations aim to enhance military resilience through multinational projects, innovative research, and the implementation of sustainable practices across the defence ecosystem. Prioritising the **development of an EU Defence Strategy on Climate Change and the establishment of an EU-led Competence Centre for Defence, Energy, and Climate is essential**. These initiatives can substantially contribute to EU MoD efforts to enhance resilience through long-term, coordinated, and cost-effective practices, fostering synergies with the public and private sectors as well as other strategic partners.

The armed forces have a unique opportunity to lead by example in transitioning to a more sustainable and climate-resilient future. Immediate and decisive action is essential to prevent military capability losses, mitigate rising costs, and ensure that armed forces are fully prepared to address the multi-layered threats posed by climate change. **Strengthening CEI resilience must become a core defence priority, as it directly impacts operational readiness, crisis response, and long-term strategic autonomy.** As the EU advances towards climate neutrality, the defence sector must accelerate its transition—adopting sustainable energy solutions, enhancing risk management, and integrating both climate resilience and digitalisation into every level of defence planning. Smart energy systems, AI-driven grid management, and digital monitoring tools will be essential for optimising energy efficiency, securing critical infrastructure, and ensuring rapid response to emerging threats. This is not just an environmental obligation; it is a strategic imperative to safeguard Europe's security, stability, and defence effectiveness in an increasingly volatile world.

2.3 Strengthening defence-related CEI resilience against hybrid threats

Georgios Valsamos, Georgios Giannopoulos, Rainer Jungwirth, *European Commission Joint Research Centre*
Constantinos Hadjisavvas, *European Defence Agency*

In an era where the boundaries between conventional warfare and peacetime operations are increasingly blurred, the concept of hybrid threats has emerged as a critical concern for national and international security. Hybrid threats are complex and multifaceted, combining military and non-military tactics, covert and overt operations, and spanning across various domains such as cyber, political, economic, and infrastructure. These threats exploit vulnerabilities within societies, institutions, and critical infrastructures, aiming to destabilise states, gain strategic advantages and coerce behaviour without escalating to open conflict by keeping under the threshold of armed response or by distorting attribution.

One of the most vulnerable and strategically important assets in this context is defence-related CEI. The term encompasses the energy assets, systems, resources and organisations that are essential for the functioning and operational effectiveness, readiness and sustainability of the armed forces. The resilience of CEI is paramount, as any disruption can have far-reaching consequences for national defence, civilian services, business continuity, quality of life and overall societal stability. The vast majority of CEI are civilian owned, operated and regulated, and do not exclusively provide energy and energy-related critical products and services just to the armed forces. Recognising the importance of this issue, EDA, in collaboration with the European Commission, initiated research on this vital topic in the context of the CF SEDSS.

This section delves into the complexities of hybrid threats and the strategies that can be employed to enhance the resilience of defence-related CEI. It draws insights from the extensive work and research undertaken in the context of the CF SEDSS, particularly in Working Group 3 on the Protection of CEI, as well as other relevant EU and scientific studies. It outlines the current policy landscape, presents an analytical framework for countering hybrid threats focused on the defence and infrastructure domains, and offers recommendations for how defence can effectively contribute to the resilience of CEI. Through this exploration, the section aims to underscore the critical role of defence in safeguarding national security in the face of hybrid threats affecting CEIs. This analysis is based on a joint study on hybrid threats by the EDA (CF SEDSS) and the Joint Research Centre of the European Commission[26].

2.3.1 The EU policy landscape

The EU is actively responding to the growing challenge of hybrid threats, which have become increasingly common and pose a significant risk to security. This response is reflected in the EU policy landscape which includes the Joint Framework on Countering Hybrid Threats[27] and the Joint Communication on increasing Resilience and Bolstering Capabilities to Address Hybrid Threats[28], both of which stress the importance of enhancing resilience and the ability to address hybrid threats effectively.

Likewise, the EU Security Union Strategy[29] underscores the critical need for resilience against hybrid threats, while the EU Climate Change and Defence Roadmap addresses the defence and climate change nexus, recognising the need to protect defence-related CEI from such threats. The European Commission has reaffirmed its dedication to boosting defence resilience by focusing on innovation and strategic (inter)dependencies, particularly in relation to hybrid threats and climate change challenges within the defence sector. The EU's Strategic Compass for Security and Defence[22] advocates for innovation to improve energy efficiency and the resilience of defence-related infrastructure, and it emphasises the creation of common benchmarks and standards for renewable energy use and infrastructure resilience.

The EU's resilience policies, such as the CER and NIS2 Directives, provide a foundation for strengthening CEI protection. However, effective implementation requires greater defence-sector engagement. New

26 Giannopoulos G., Jungwirth R., Hadjisavvas C., et.al., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EUR 31505 EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/58406, JRC133083

27 European Commission (2016) Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats, a European Union Response. EC JOIN (2016) 18 final

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

29 Communication from the Commission on the EU Security Union Strategy, COM(2020) 605 final.

critical infrastructure sectors—such as healthcare, financial markets, and space—have emerged, creating new interdependencies that can also impact CEI. These developments go beyond the original EU framework on Critical Infrastructure Protection (CIP) established under the now-superseded Directive 114/2008.

The 2022 Action Plan on Military Mobility 2.0[30] also mentions hybrid threats to military mobility networks and critical nodes, including in the context of climate change and cyber. It aims to address these threats in a holistic manner and introduces a new resilience and preparedness pillar that mentions also the climate resilience and energy security of the transport sector. As in other sectors, CEI are intertwined with defence issues also through the critical transport infrastructure.

The CF SEDSS can play a key role in initiating research and developing project ideas, including the Hybrid Threats Attack Response, to address these concerns, by fostering the largest energy and defence community in Europe and ensuring engagement with experts of diverse training and backgrounds, as well as institutional affiliation. It is through the activity of WG 3 of CF SEDSS that the studies summarized in this publication, including this chapter, were developed, and these and other efforts inform policymakers on how to construct and adjust the future frameworks for countering hybrid threats or promoting resilience of CEI in general in the complex security environment.

2.3.2 Analytical framework for countering hybrid threats

The landscape of hybrid threats: a conceptual model[31] defines hybrid threats as actions by state or non-state actors that undermine, coerce or damage a target through a combination of military and non-military means. These actions are coordinated and target the vulnerabilities of democratic states and institutions. The model defines hybrid threats using five key pillars (Figure 4): **Actors, Tools, Domains, Activities, and Targets**.

It answers key questions of - ***who is behind the attack, what methods they use, and which sectors they target***. It distinguishes between state and non-state actors, enumerates possible tools (e.g., physical operations against critical infrastructure), and identifies **13 domains** (e.g., infrastructure, cyber, space, economy) that can be targeted. Hybrid threats are characterised by escalation phases, including priming, destabilisation, and coercion, each with distinct activities and impacts on the functioning of the targeted society. Each phase has its own specificities: the priming phase is challenging for detection and attribution due to its low detectability level, the destabilisation phase becomes more visible and aggressive, and the coercion phase represents hybrid warfare with a combination of covert and overt operations. Detecting the hybrid activities early in the priming phase is essential while the targeted state's ability to activate countering mechanisms is still high. For example, cyberattacks on Ukraine's power grid (2015 – 2025) demonstrated how hybrid threats can cripple critical infrastructure without direct military confrontation. These attacks disrupted energy supplies, affecting both civilian populations and military operations.

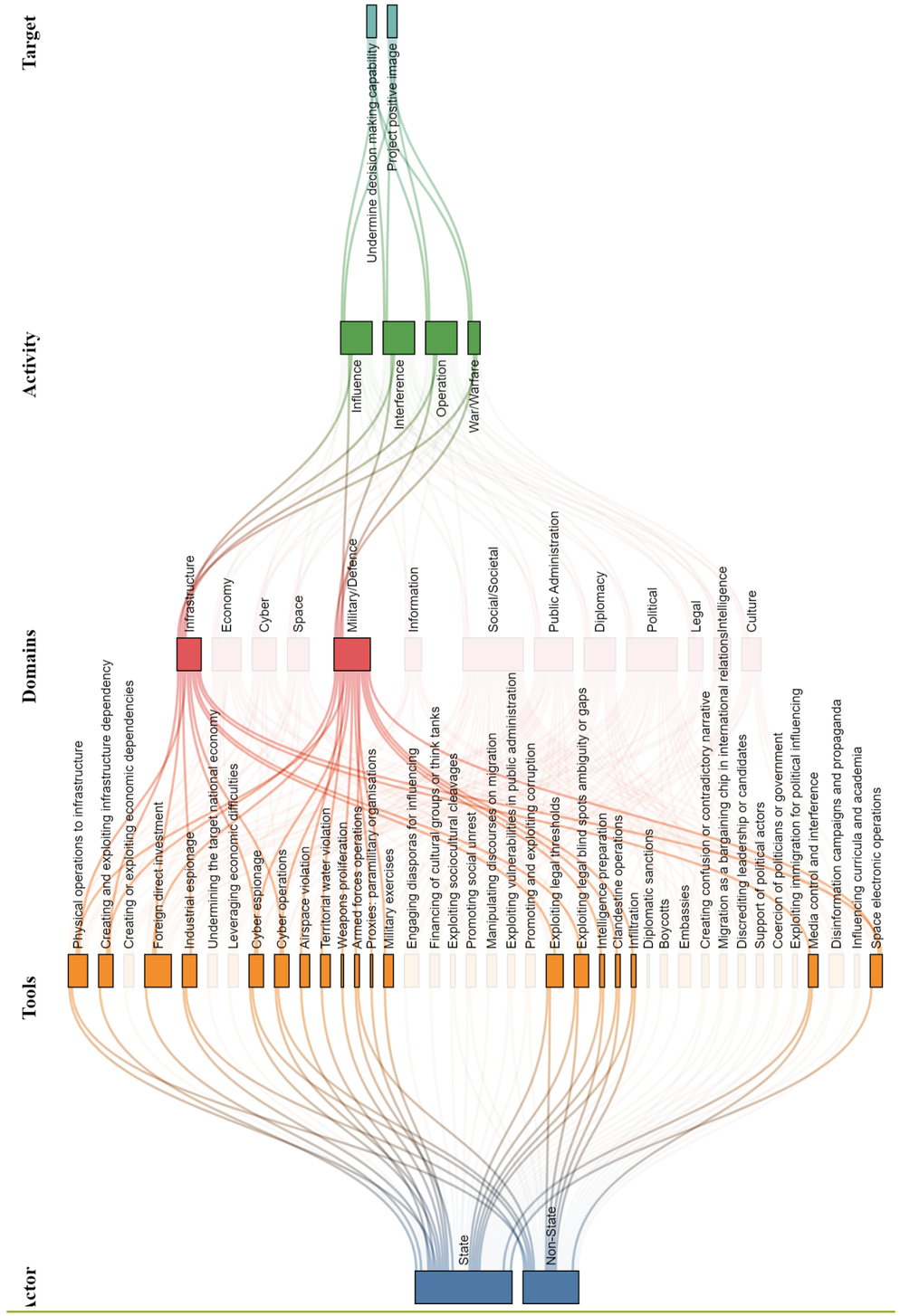


Figure 4 Conceptual model, highlighting the tools related to the infrastructure and/or military/defence domain[31].

30 European Commission (2022). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Action plan on military mobility 2.0. Brussels, 10.11.2022, JOIN(2022) 48 final

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

As a follow-up of the conceptualisation of hybrid threats, the JRC and the Hybrid CoE developed the Comprehensive Resilience Ecosystem (CORE) model[32] to support the Member States to enhance their resilience against hybrid threats. The CORE model builds upon the conceptual framework and serves as a sophisticated analytical tool that employs a comprehensive whole-of-society approach to understand and build resilience against hybrid threats.

It systematically categorizes society into three interconnected spaces—civic, governance, and services—and further stratifies these into international, national, and local layers. This structure reflects the multifaceted nature of societal sectors and the levels at which hybrid threats can operate. The 13 domains from the conceptual model are considered as potential entry points into the ecosystem (see Figure 5).

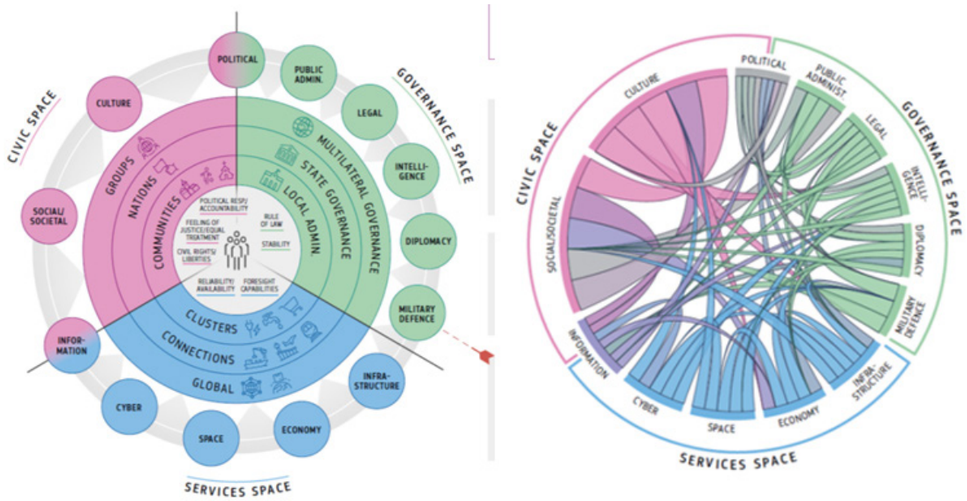


Figure 5 CORE-model and the interconnections between domains[32].

Central to the CORE model are seven foundational elements that are deemed essential for a society's resilience to hybrid threats. These include:

1. Justice and equal treatment, ensuring fairness across society.
2. Civil rights and liberties, safeguarding individual freedoms.
3. Political responsibility and accountability, demanding transparency and integrity from leaders.
4. Rule of law, maintaining legal norms and procedures.
5. Stability, fostering a predictable and controlled societal environment.
6. Reliability and availability, guaranteeing consistent access to services and systems.
7. Foresight capabilities, the ability to predict and prepare for future challenges.

Trust and credibility act as the glue that holds the societal structure together, reinforcing the democratic system and its ability to withstand hybrid threats. These foundational elements are not just theoretical constructs, they are practical necessities for a society to resist, recover from and adapt to the complex and multifaceted nature of hybrid threats.

Resilience against hybrid threats requires understanding the EU as a complex interlinked system, and to consider the interconnections and interdependencies. Hostile actors aim to undermine democracies, challenge decision-making processes, and create cascading effects across society. The CORE model is used to analyse and counteract hybrid threats and their impacts, which seeks to achieve these objectives by adopting a whole-of-society approach.

32 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://data.europa.eu/doi/10.2760/37899

2.3.3 Enhancing the resilience of defence-related CEI

The whole-of-society approach mentioned above is also required to fortify defence-related CEI against hybrid threats. This involves considering dependencies and interdependencies across different domains and levels of society. The JRC and EDA have developed a specific study[26] to substantiate the concept of hybrid threats in the domain of defence-related CEI. By applying the analytical framework discussed in the previous section, the study explores how hybrid threats can directly or indirectly target infrastructure and military/defence domains, compromising their operational effectiveness.

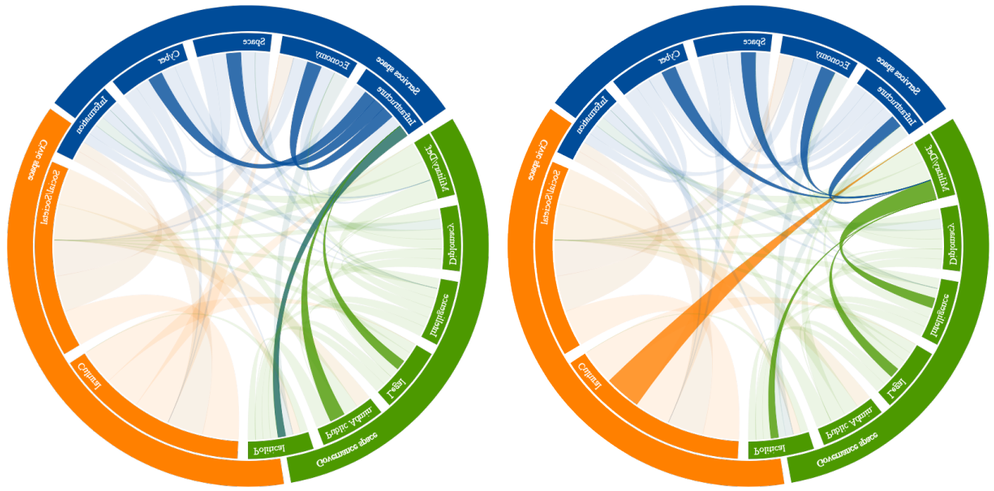


Figure 6 Interconnections related to the infrastructure (left) and military/defence (right) domain[26].

The first layer of complexity in safeguarding defence energy infrastructure arises from the direct threats posed by state and non-state actors. These actors deploy a range of tactics, from strategic economic manoeuvres to overt cyber and physical attacks, aiming to disrupt or control energy resources and systems. The priming phase often sees subtle yet strategic moves, such as foreign investments in key energy assets or cyber espionage aimed at gathering intelligence and identifying vulnerabilities within energy networks.

While the situation moved from the priming phase to the coercion phase these threats may manifest more aggressively and show signs of escalation. Cyber operations, for instance, may evolve from espionage to active disruption or sabotage, targeting control systems and causing widespread outages. Physical attacks on infrastruc-

ture, while less covert, remain a potent tool, capable of causing immediate and tangible damage, disrupting military operations, and spreading chaos within the civilian sector.

Beyond direct attacks, adversaries may exploit indirect methods to weaken defence energy infrastructures. The interconnected nature (see Figure 6) of modern societies means that political decisions, economic policies, and legal frameworks can all have far-reaching impacts on energy security. For example, political instability can lead to policy vacuums, economic sanctions can disrupt energy supplies, and legal loopholes can be exploited to gain undue influence over energy assets.

These indirect methods often aim to exploit the dependencies and interdependencies that exist within and between various societal domains. By manipulating these levers, adversaries can create cascading effects that amplify the impact and duration of their actions, often in novel and unanticipated ways, and extending far beyond the initial target while potentially crippling defence capabilities.

2.3.4 Recommendations

In the shadow of escalating hybrid conflicts, the imperative to secure defence-related CEI has never been more pressing. The recommendations below provide the MoDs with a strategic roadmap for bolstering the resilience of these vital systems and ensuring they remain robust in the face of multifaceted threats.

i. **Comprehensive Risk Management**

A detailed understanding of the risks posed to energy infrastructure is essential. This includes recognising the spectrum of threats, from cyber intrusions to physical sabotage, and the potential for these threats to disrupt military operations and national security. A comprehensive risk management framework is proposed, integrating vulnerability assessments, threat analysis, and the identification of critical interdependencies.

ii. **Innovative Defence Technologies**

Investing in cutting-edge technologies is crucial for safeguarding energy infrastructure. This includes the development of advanced cybersecurity measures, smart grid technologies, and autonomous systems that can enhance situational awareness and reduce response times. Emphasis is placed on innovation and digitalisation that defends against current threats and anticipates future challenges.

iii. **Intelligence and Information Sharing**

The flow of timely and accurate intelligence is the lifeblood of effective defence strategies. Establishing mechanisms for sharing information on threats, vulnerabilities, and incidents between military, government, and industry partners is vital. This shared situational awareness enables a proactive posture and a more coordinated response to incidents.

iv. **Training and Preparedness**

A well-prepared defence force is key to resilience. This involves regular training exercises that simulate hybrid attack scenarios, testing the readiness of military and civilian agencies to respond to energy disruptions. These exercises should be designed to refine protocols, improve interagency cooperation, and ensure that all stakeholders are equipped to manage complex crisis situations. Additionally, ongoing upskilling and reskilling of staff are crucial to adapting to emerging threats and technological advancements, ensuring that defence forces maintain a high level of expertise and preparedness.

v. **Civil-Military Synergies**

The interdependence between civilian energy infrastructure and military readiness necessitates a synergistic approach to resilience. Civil-military partnerships should be strengthened to facilitate the exchange of expertise, resources, and support. This synergy ensures that the defence sector can leverage civilian advancements in energy technology and infrastructure protection, while also contributing to the overall security of national energy systems.

vi. **Policy and Legislative Frameworks**

Robust policy and legislative frameworks provide the backbone for energy resilience. Policies should be crafted to incentivise the protection of energy assets, promote research and development in energy security technologies, and foster international cooperation on energy resilience. Legislation must also evolve to address the changing nature of hybrid threats and the need for rapid adaptation in defence strategies as well as the need for credible attribution. As the MoDs are, in general, neither the owners nor the operators or regulators of CEI, it is imperative for the MoDs to make their unique perspectives and concerns known during a multistakeholder process for crafting new policy and legislation. Whatever the form this input may take (consulting, interministerial reunions, review processes), the MoDs have both an abiding need and, increasingly, the awareness and expertise to make positive contributions to energy frameworks.

2.3.5 Conclusions

The final insights from this analysis underscore the urgent need to strengthen the resilience of defence-related CEI against increasingly complex and concealed hybrid threats. By blending conventional warfare with irregular tactics, these threats pose a significant challenge to military effectiveness, national security, and broader societal stability. Ensuring CEI resilience demands a unified, whole-of-society approach that fosters deep civil-military cooperation, particularly at the EU level.

To counter these evolving risks, Europe must prioritise **knowledge-sharing, cross-sector collaboration, and the integration of advanced digital technologies** such as AI-driven monitoring, smart grid security, and predictive analytics. Strengthening cyber resilience and securing critical infrastructure through innovative defence technologies will be key to **enhancing strategic autonomy and ensuring uninterrupted military readiness and sustainability**.

This section concludes with a call for collective action. **A coordinated European approach to hybrid threat resilience is no longer optional - it is a strategic necessity**. Defence institutions, policymakers, and industry must work together to build a robust, adaptable, and future-proof CEI protection framework, ensuring that Europe's critical infrastructure remains secure and operational in an era of growing uncertainty and global instability.

03

Impacts of Pandemics on Defence-Related Critical Energy Infrastructure: Lessons from the COVID-19 Pandemic

Christos Makropoulos, *School of Civil Engineering, National Technical University of Athens*

Nothing in life is to be feared, it is only to be understood.
Now is the time to understand more, so that we may fear less.
Marie Curie

3.1 Introduction

The defence sector is heavily dependent on civilian critical energy infrastructure (CEI), and disrupting its stable operation could result in challenges for the security, safety, and operational effectiveness of the armed forces. In this light, it is essential for Europe to re-examine its strategic energy autonomy, using the COVID-19 pandemic as a 'wake up' call. This chapter maps direct and indirect effects of the pandemic on CEI, also highlighting relevant insights, and states key recommendations towards increased resilience for the civilian and defence energy sectors. The main thesis of the chapter is that the COVID-19 pandemic crisis, seen as a large scale '**stress-testing**' exercise for defence-related CEI, could provide lessons towards improving the sector's resilience and readiness in anticipation of similar future risks. To this effect, we identify **key impacts** of the COVID-19 pandemic on CEI and services; **identify and present lessons learnt** from the pandemic and summarise transferable **insights,** and **provide recommendations** on how the civilian and defence energy sectors can increase their resilience. *It should be noted that the work was completed by December 2021 and as such preceded the invasion of Ukraine. We argue however that the insights gained by this work became even more relevant after the 24th February 2022.*

The conceptual approach adopted to trace COVID-related direct and indirect impacts can be seen in Figure 7. Our research findings are grouped into **three main topics** (energy demand, energy supply and power grids operation) and **three cross-cutting topics** (human challenges, cyber-security threats and supply chain disruptions) that together capture both direct and indirect vectors of influence of COVID-19 on CEI.

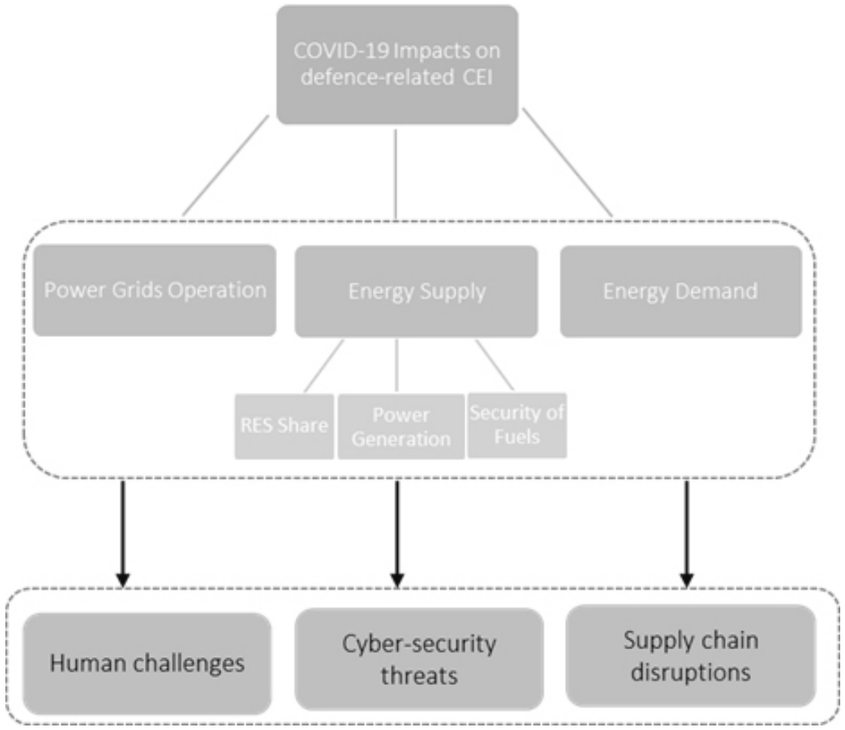


Figure 7 Aspects of impact of COVID-19 pandemic on defence-related CEI. Source: Author

An extensive **evidence base** was created through an "information mining" process. An **expert-driven desk study**, augmented using an **artificial intelligence (AI) driven tool**, leveraging advanced natural language processing (NLP) algorithms identified **multi-dimensional effects** of COVID-19 to CEI through an extended literature review. Over **250.000 peer-reviewed academic papers** were processed by the AI tool and **over 350** were finally retrieved and added to the study's database.

3.2 Setting the scene: a typology of extreme-impact events

Extreme-impact events (of negative outcome, implying harm, loss, or danger) are essentially hazards (e.g. physical, cyber or a combination of them) to which businesses, infrastructure, systems, societies are exposed to. As disruptive and unexpected events are becoming the norm in today's world (also termed 'the New Normal[33]'), it is considered important to first define a typology of such events and then attempt to link them with the notions of risk and uncertainty. To establish such a typology for extreme-impact events we employ here a number of "animal metaphors". The use of such metaphors dates back to Aesop's fables, but interestingly, such "animal metaphors" have also been used much more recently by the influential economist J. M. Keynes in his "General Theory of Employment, Interest, and Money", and through that work have passed into the everyday vocabulary of the financial sector to describe market behaviour (e.g. bull and bear markets). To describe extreme-impact events (see Figure 8) we employ the metaphors of pink elephants, grey rhinos and (the iconic) black swans. A brief definition of each metaphor is provided next.

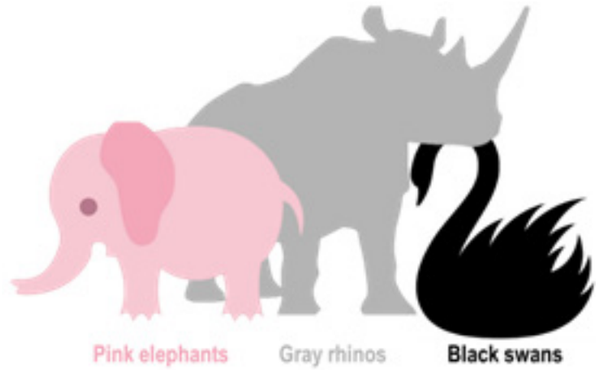


Figure 8 Common animal metaphors for extreme-impact events. Source: Author

Pink Elephants: A concept similar to that of "the elephant in the room". It regards known/anticipated hazards with notable impact (often underestimated), which can be quantified, attributed to events that have already taken place, or are happening now, yet no actions are taken to mitigate their consequences (for example, climate change, as recognised by several countries 20-30 years ago. Interestingly, it can be ar-

33 Nikolopoulos, D., van Alphen, H.J., Vries, D., Palmen, L., Koop, S., van Thienen, P., Medema, G. and Makropoulos, C., 2019. Tackling the "New Normal": A resilience assessment method applied to real-world urban water systems. Water, 11(2), p.330.

gued that climate change has now evolved into a grey rhino - see below). The idea is that if we ignore the problem long enough, the catastrophic risk of failure/conflict will (hopefully) pass us by.

Grey Rhinos[34]: Similar to the previous type of events, such events are characterised by large and apparent impacts that can be foreseen with reasonable certainty, but these have not yet occurred. The risk of such events can be quantified by embedding potential uncertainties into risk quantification approaches, yet it is typically neglected and/or underestimated. The metaphor of Grey Rhinos builds on the fact that although such animals are very big (high impact) they are considered slow (and as such not an immediate threat). Yet, surprisingly, rhinos have an average speed of 50 km/h, emphasising that the consequences/impact of such events can escalate fast and get out of control very easily.

Black Swans[35]: These are unpredictable, extremely improbable, yet impactful events (a real "poster animal" of uncertainty). Such events cannot be foreseen prior to their appearance and as such we tend to only be able to explain their occurrence/risk a posteriori (i.e. with a hindsight). Although such "explanations" and ex-post analysis of black swan events abound, they are of limited use since, as the Danish philosopher Soren Kierkegaard [1813-1855] said, "*Life can only be understood backwards; but it must be lived forwards.*" The origins of the term can be traced back to ancient Greece, where it was used to refer to an impossible event. For centuries Europeans had only seen white swans, believing that black swans do not exist, yet at some point this belief changed abruptly, since black swans were discovered in Australia[36].

3.3 Classifying the COVID-19 event

Considering the above, one may reasonably wonder what kind of "animal" the COVID-19 pandemic was[37]. At the beginning of the crisis, the general view was to consider COVID-19 as a black swan event (i.e. an unpredictable event ruled by deep uncertainty). An explanation for this initial categorisation was due to ambiguity aversion, which makes people think that something "that bad" can be only caused due to deep uncertainty.

We argue that COVID-19 should not be classified as a black swan event as it cannot be reasonably considered as extremely improbable. On the contrary, it could better be described as a grey rhino event, and as such fitting the notion of "known unknowns", to be treated within a risk management under uncertainty/resilience perspective. In particular, we have known that the threat existed, but there were many unknowns[38] such as the population fatality, the virus reproduction rates, the rate of prevalence of some virus variation, the ratio of asymptomatic and symptomatic infections, the seasonality of infections, the mechanics of immunity, as well as the impact of restrictive measures (e.g. social distancing) in societies, which of course may also have cascading effects, influencing the population and societies in multiple ways (from the economy to mental health). It is further argued that in such situations, posing the right questions, while recognizing and embracing related uncertainties is a more pragmatic approach than providing predictions, often using spurious and fragile assumptions. This suggestion is in line with the recently published "modelling manifesto"[39] in *Nature*, highlighting key principles for models and predictions to better serve society and politics with insights.

3.4 COVID-19 and the day after

In view of the discussion above, we argue that to better deal with / prepare for extreme-impact events of the grey rhino variety, we need to evoke the concept of resilience (and possibly also explore antifragility attributes[40]).

Resilience refers to the ability of systems to retain some of their function and recover quickly when exposed to stressors/shocks/failures[41]. *Antifragility* refers to the ability of systems to actually improve or even thrive when experiencing stressors/shocks/failures. Antifragility can be identified, for example, in learning/training procedures (where examinations can be considered a form of external stress through which performance is improved). Another indicative example is the process of evolution (e.g. Darwinian Theory) where through time populations adapt to different environmental stresses.

In concrete terms, such an approach would focus on grey rhino events, since these are more common than black swans (i.e. the unknown unknowns), and also entail some degree of predictability, and try to both spot them but also act pro-actively. It is also argued that it is important to recognise and attempt to transform (if possible) the "known unknowns" to "known knowns" by combining data-mining and multiple research domains and as a result promote proactive action-plans and decision making. Some of these concepts in relation to COVID-19 and CEI will be discussed in the recommendations and insights sections of this chapter.

3.5 The COVID-19 pandemic and its impact on defence-relevant critical energy infrastructure

3.5.1 How dependent on civilian CEI is the defence sector for its energy needs?

The European Union unequivocally rec-

34 The notion of gray rhinos has been popularized Michele Wucker (writer and policy analyst) in a 2016 book, where she refers to obvious and impactful challenges that ignored, rather than addressed (e.g. by policy makers). M. Wucker came up with the term after the 2012 Greek financial crisis.

35 A termed popularized in 2007 by Nassim Nicholas Taleb after the publication of his book "The Black Swan: The Impact of the Highly Improbable".

36 In 1697 by the Dutch explorer Willem de Vlamingh

37 Appleyard, B. (2009). Books that helped to change the world. The Sunday Times

38 See for instance: Kissler, S. M., Tedijanto, C., Goldstein, E., Grad, Y. H., & Lipsitch, M. (2020). Projecting the transmission dynamics of SARS-CoV-2 through the postpandemic period. Science, 368(6493), 860-868. doi:10.1126/science.abb5793.

39 Saltelli, A., Bammer, G., Bruno, I., Charters, E., Di Fiore, M., Didier, E., Nelson Espeland, W., et al. (2020). Five ways to ensure that models serve society: A manifesto. Nature, 582(7813), 482–484. https://doi.org/10.1038/D41586-020-01812-9

40 The concept of antifragility was introduced by Nassim Nicholas Taleb, in his book "Antifragile: Things That Gain from Disorder." According to Taleb's own definition: "Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better."

41 Makropoulos, C., Nikolopoulos, D., Palmen, L., Kools, S., Segrave, A., Vries, D., Koop, S., Van Alphen, H. J., Vonk, E., Van Thienen, P., & Rozos, E. (2018). A resilience assessment method for urban water systems. Urban Water Journal, 15(4), 316–328.

ognizes the strategic importance of civilian energy infrastructure in supporting its broader defence sector, which includes the armed forces, relevant government agencies, and the defence industry. This civilian infrastructure is critical not only for everyday operations but also for ensuring the security, safety, and effectiveness of military activities. The dependency is substantial-EU armed forces rely heavily on national electricity grids, as they generate only a minor proportion of the electricity they consume themselves. According to data from the EDA[42] for 2016-2017, nearly 99% of the electricity requirements for EU armed forces operations were met through civilian electricity networks. The reliance on civilian CEI underlines a crucial vulnerability: disruptions to these systems, whether due to technological failures, human errors, or deliberate attacks, could severely compromise military readiness and operational capabilities. The ongoing conflict in Ukraine exemplifies the risks associated with such dependencies. Since the onset of hostilities, there have been numerous reports of targeted attacks on Ukraine's energy infrastructure, aimed at destabilizing the country by crippling both civilian and military operations. These assaults demonstrate how civilian energy grids can become strategic targets for geopolitical adversaries, thereby highlighting the necessity for robust, resilient energy systems that can withstand such challenges.

As such, ensuring a continuous, high-quality power supply to the defence sector is not merely a matter of maintaining operational readiness; it is also critical for national security. The defence sector's ability to function effectively without interruption is paramount, especially during extreme circumstances like the COVID-19 pandemic or natural disasters such as hurricanes and wildfires. Enhancing the resilience of energy infrastructure against potential aggression becomes even more crucial in light of the vulnerabilities exposed by the conflict in Ukraine. The Armed Forces require secure power supply for critical systems that must be online 24/7, year-round. Although military infrastructures usually rely on generators for accidental power cuts, this backup is, for the most part, inadequately sized for longer outages. Scenarios of prolonged electrical outages are characterised as high-impact low-probability (HILP) events but what needs to be better understood that that low probability events happen more often than one would assume[43].

3.5.2 Enter COVID-19

The advent of the COVID-19 pandemic, besides a severe health emergency, signalled an unprecedented disruption in the lives of billions of citizens around the world. This disruption negatively affected the global economy, which suffered its most steep recession in nearly a century, dropping global economic growth in 2020 to a rate of -3.2%[44]. The International Monetary Fund (IMF) estimated that governments across the globe spent around USD 11 trillion to combat the pandemic, resulting in a deficit of 14% GDP in 2020[45]. The time in which the pandemic struck was already difficult for the global energy sector[46]. The effects of COVID-19 during the global lockdown periods were significant, stressing the global economy, disrupting supply chains, and (initially) decreasing electricity demands to unprecedented levels. It is no exaggeration to claim that the pandemic has pushed the world to a new era of economic activity whose mid- to long-term effects are still unfolding. In the following sections we will sketch some of these effects grouped under the vectors identified in Figure 7.

3.5.3 A high-level summary of key effects

- **Electricity demands** deviated from their expected volumes and shapes causing increasing load forecasting errors that stressed power grids. Increased distributed energy resources (mainly renewables) caused stability issues in some distribution systems.
- Fossil fuel **electricity generation** dropped by up to 25 GW in EU countries by April 2020 with direct effects on European **energy companies' financial sustainability**. The drop in fuel consumption caused a turmoil with cascading effects for refineries.
- Initially, **natural gas** growth projections dropped by 5-10%. However, in 2021, a **natural gas crisis** erupted, influenced by the COVID crisis through a combination of cascading effects. The gas crisis highlighted **an over-reliance of the EU on imported natural gas** and should be considered as a major lesson to be learned.
- **Renewable energy sources** (RES) were a success story **increasing their share** of the (reduced) energy load **surpassing fossil fuels for the first time**. This increase should, however, be contextualised in view of their priority access to the grid guaranteed through contracts and due to intermittency and difficulties in adjusting RES production due to hydroclimatic uncertainties.
- **Delays** in **infrastructure maintenance and new projects deployment** due to personnel constraints caused by the lockdowns were often reported.
- **Severe supply chain bottlenecks** emerged that will continue to cause knock-on effects in the energy market for the foreseeable future.
- The pandemic also **catalysed a rapid digitalisation** for most sectors – a fact that can be seen as an **anti-fragility effect**. However, a dramatic increase in **cyber-threats**, tripling above average pre-COVID numbers, **was also reported**, affecting CEI as these also became more digitalised and adopted working from home practices.

In the following sections we briefly expand on and provide evidence for these effects following the conceptual approach identified earlier.

3.5.4 Effects on electricity demand

The outbreak induced unprecedented challenges to energy utilities and system operators, as the pandemic arguably caused one of the biggest global crises since WWII, hitting healthcare, finance, commerce and business systems around the world[47]. The energy sector, as a mirror to this global impact, was directly influenced especially due to significant changes in electricity demand (in terms of both volume and temporal distribution, i.e., shift of energy peaks and load profiles). In its global review for 2020, the International Energy Agency (IEA) states that the drop of energy demand was the largest recorded in the last 70 years. Global energy demand in 2020 declined by 6% compared to 2019[48] while in the EU, in the first quarter of 2020 demand reduc-

42 European Defence Agency, Energy and Defence. https://eda.europa.eu/docs/default-source/eda-factsheets/2019-06-07-factsheet-energy-defence

43 Papalexiou, S. M., Koutsoyiannis, D., & Makropoulos, C. (2013). How extreme is extreme? An assessment of daily rainfall distribution tails. Hydrology and Earth System Sciences, 17(2), 851–862.

44 Jackson, J., Weiss, M., Schwarzenberg, A., & Nelson, R. (2021). Global Economic Effects of COVID-19. Congr. Research Service.

45 Akhtaruzzaman, M., Boubaker, S., Chiah, M., & Zhong, A. (2021). COVID-19 and Oil Price Risk Exposure. Finance Research Letters, 42 (January).

46 Myers Jaffe, A. (2020). Geopolitics and the Oil Price Cycle - An Introduction. Economics of Energy & Environmental Policy, 9(2), 1–9. https://doi.org/10.5547/2160-5890.9.2.ajaf

47 Juutilainen, K. H., & Grinkitytė, U. (2020). Impact of COVID-19 on NATO Energy Security - View on Fuels, Gas and Renewable Energy.

48 Jiang, P., Fan, Y. V., & Klemeš, J. J. (2021). Impacts of COVID-19 on Energy Demand and Consumption: Challenges, Lessons and Emerging Opportunities. Applied Energy, 285 (November 2020). https://doi.org/10.1016/j.apenergy.2021.116441.

tions reached a 5% drop compared to 2019. Such significant reductions in energy consumption and peak demands directly impact energy utilities' revenues and viability. Indicative examples include the Danish power trading company (Nordstrom Invest A/S) which shut down their operation due to energy prices surge[49], nineteen energy companies that went bankrupt in the USA under COVID-19 cascading tensions, the French Distribution System Operator, Hydroption, which went bankrupt[50] as well as Elia, a Belgian Transmission System Operator which was forced to stop over 80% of its construction activities[51]. Further to these examples, the European Network of Transmission System Operator (ENTSO-E) reported that several energy-related development projects were seriously delayed due to COVID-19 pandemic.

This electricity demand reduction was directly related to social distancing measures and mitigation policies. The Council of European Energy Regulators[52] (CEER) reported that from its member countries, 21 of them imposed at least one nation-wide lockdown and 15 of them two lockdowns. Societies which faced more total movement restrictions and closing of workspaces were impacted the most[53].

Indicatively, power consumption for EU countries in April 2020 dropped to 181 TWh from 207 TWh in April 2019[54]. According to IEA, financially strong European countries encountered a demand fall by at least 15% during full lockdowns (Figure 9). A study[55] estimated the average reduction during the first lockdown using a Demand Variation Index (DVI) for selected European countries. The DVI in Spain, Italy, Belgium, UK, and the Netherlands was 25%, 17.7%, 15.6%, 14.2%, and 11.6% respectively. In contrast, in Sweden, the percentage was reduced by -2.1%, meaning that electricity demand slightly increased.

49 Paulsson, L. (2021, September 13). Danish Energy Trader Files for Bankruptcy as Turmoil Bites. Bloomberg. https://www.bloomberg.com/news/articles/2021-09-13/energy-trader-files-for-bankruptcy-as-market-turmoil-bites.

50 Le Figaro. (2021, October 22). Première défaillance d'un fournisseur d'électricité. Le Figaro. https://www.lefigaro.fr/societes/premiere-defaillance-d-un-fournisseur-d-electricite-20211022.

51 IEEE Power & Energy Industry. (2020). Sharing Knowledge on Electrical Energy Industry's First Response to COVID-19. IEEE Power and Energy Society.

52 Council of European Energy Regulators. (2021, March). First Analysis of the COVID-19 Pandemic's Effects on the Energy Sector. https://www.ceer.eu/documents/104400/-/-/31d2aad0-f7b3-46cf-b7e9-1ef382ad2e87

53 Werth, A., Gravino, P., & Prevedello, G. (2021). Impact Analysis of COVID-19 Responses on Energy Grid Dynamics in Europe. Applied Energy, 281 (January), 254–266. https://doi.org/10.1016/j.apenergy.2020.116045

54 Bompard, E., Botterud, A., Corgnati, S., Huang, T., Jafari, M., Leone, P., Mauro, S., Montesano, G., Papa, C., & Profumo, F. (2020). An Electricity Triangle for Energy Transition: Application to Italy. Applied Energy, 277 (November), 115525. https://doi.org/10.1016/J.APENERGY.2020.115525

55 Wormuth, B., Wang, S., Dehghanian, P., Barati, M., Estebsari, A., Filomena, T. P., Kapourchali, M. H., & Lejeune, M. A. (2020). Electric Power Grids Under High-Absenteeism Pandemics: History, Context, Response, and Opportunities. IEEE Access, 8, 215727–215747. https://doi.org/10.1109/ACCESS.2020.3041247

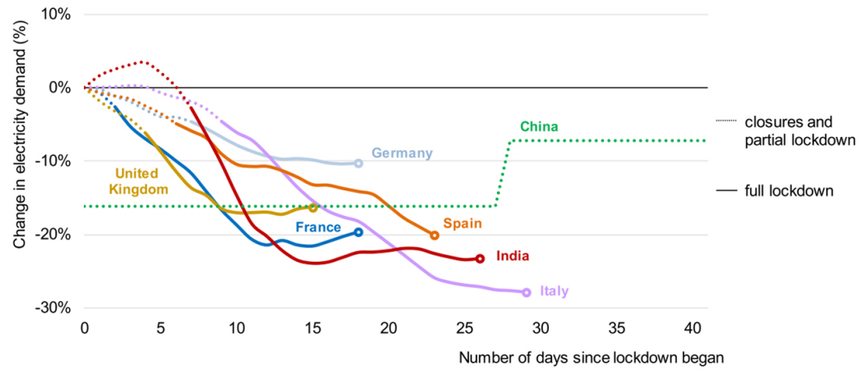


Figure 9 Reductions of electricity demand after implementing lockdown measures[56]

During the restrictions, residential demand load soared, by almost +40% in some European countries[57], as expected due to the prolonged stay of people at home. However, this increase was far outweighed by reductions in the services sector including commercial, office, hospitality, education and tourism activities that sharply declined. In Italy, one of the hardest-hit countries in the EU, nearly 75% of the services paused their activities due to stringent COVID-19 policies undertaken[56].

It should be noted that the industrial sector, which constitutes the highest energy consumer in Europe, was, on average, impacted much less, registering energy demand decreases of the order of 12%. This is mainly attributed to the fact that factories managed to continue operations despite the pandemic outbreak through a combination of advanced automation implementation and precautionary measures for necessary personnel.

It is important to note that lockdown measures greatly affected not only demand volumes, but also reshaped load demand profiles. Although each country follows different scheduling habits, in many cases significant temporal shifts in demand peaks were observed. This caused serious challenges for the utilities in terms of forecasting loads. For example, in Spain, during the lockdown, it was observed that morning and afternoon demand peaks were shifted to later hours of the day as seen in Figure 10. Similar behaviour was observed also in other countries such as the United Kingdom.

56 International Energy Agency. (2020). Global Energy Review 2020. https://doi.org/10.1787/a60abbf2-en

57 Zhong, H., Tan, Z., He, Y., Xie, L., & Kang, C. (2020). Implications of COVID-19 for the Electricity Industry: A Comprehensive Review. CSEE Journal of Power and Energy Systems, 6(3), 489–495. https://doi.org/10.17775/CSEEJPES.2020.02500.

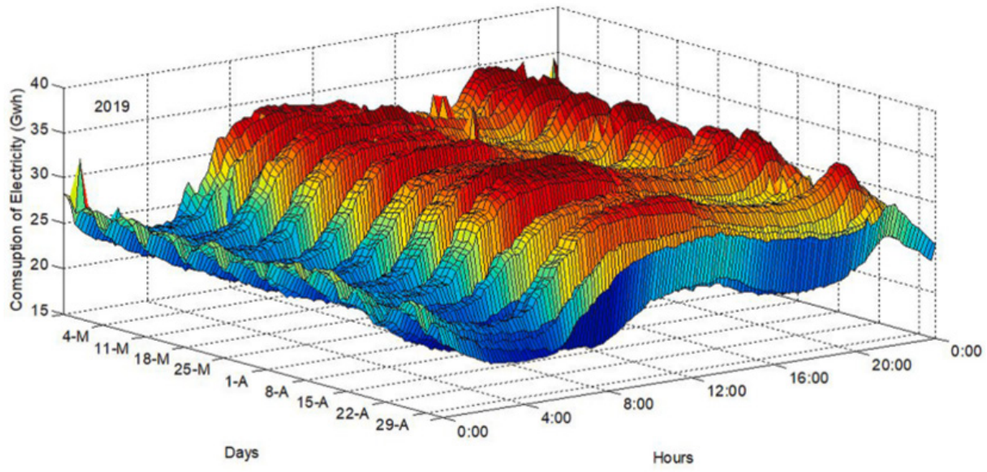


Figure 10 Daily profiles of electricity demand during March and April 2020 in Spain[58]

3.5.5 Effects on energy supply

Since early 2020, containment policies due to the COVID-19 pandemic have been a major setback for fuel supply and power generation. The drastic measures, including movement restrictions, bans on all non-essential travel, transition to remote learning and working, reduced energy demand to unprecedented levels. The significantly disrupted transport sector caused a subsequent reduction in fuel consumption. Specifically, according to IEA, vehicle transport in Europe declined by 50-75% and aviation activity by over 90%. A prolonged amplified freezing of international airline fleets was observed just four weeks after the beginning of the outbreak in January 2020 leading to a total aviation fuel consumption drop by -62.5% compared to the previous year[59,60].

The pandemic also compromised maritime cargo transportation. A study[61] suggested that ports ran at 20-30% of their full capacity during the second half of 2020 as products manufacturing plunged both in China and the EU. This drop and the consequent disruption of global maritime commerce which represents more than 90% of global trade had significant repercussions for the energy sector in Europe. This will be discussed in more detail in the following sections.

The dramatic drop in fuels consumption, combined with reduced electricity demand, created a wide range of impacts on the energy industry, mainly for coal, oil and gas, including a crash in prices, employment and long-term effects that are still researched and assessed from a global perspective[62, 63,64]. On the other hand, this (temporary) demand dip paved the way for a more pronounced role for renewable energy during the COVID-19 crisis.

In the next subsections the effects of the crisis to several aspects of energy supply are briefly discussed. The first and second subsections review the impact on the conventional energy industry highlighting impacts on power generation in Europe and considering the near-term and longer-term impacts on fossil fuels. The third subsection refers specifically to the role of renewable energy sources during the crisis while investigating their outlook as part of energy production for the medium term.

3.5.5.1 Impact on power generation

The significant demand reduction, the shifts in peaks, and turmoil in electricity wholesale market prices led to major changes in electricity generation. According to a study[53], in April 2020, the total mean generation in 16 EU countries decreased by 25 GW (-9%) compared to the previous five years. Fossil fuel generation saw the highest drop (24 GW, -28%), followed by nuclear (11 GW, -14%), while renewables increased by 15 GW (+15%). Nuclear power's reduction was less severe due to its inflexible operation, unlike coal-fired power stations, which reduced output more significantly to balance demand[57]. Combined-cycle gas turbines (CCGT) responded well due to their flexibility[58].

Countries that switched from coal to gas increased gas-based power generation (+3% in Germany, +9% in Poland, +10% in the Netherlands) due to its flexibility and (at the time) low prices. Countries unable to switch saw a decline in gas-based generation[65] (-31% in the UK, -18% in France). The IEA reported a 2.6% decrease in global generation in Q1 2020. In the EU, fossil fuel generation dropped significantly during lockdowns: coal (-35%), natural gas (-25%), and nuclear (-20%) (Council of European Energy Regulators 2021). Coal generation saw the highest decrease (28.3%), followed by gas and nuclear (13.9%) during the intense lockdown months. France downgraded its nuclear outlook by 8-12%[66]. The largest drops in conventional generation among high-demand countries (>5 TWh) were in Germany (-28.7%), the UK (-25.4%), Italy (-18.3%), Belgium (-16.4%), France (-15.0%), Poland (-14.1%), and Spain (-10.7%)[54]. Different impacts were due to varying electricity system structures. Gradual increases occurred after May 2020 as economies reopened[67].

3.5.5.2 Impact on fuels

The pandemic impacted almost every

58 Santiago, I., Moreno-Muñoz, A., Quintero-Jiménez, P., García-Torres, F., & González-Redondo, M. J. (2021). Electricity Demand during Pandemic Times: The Case of COVID-19 in Spain. Energy Policy, 148 (May 2020), 111964. https://doi.org/10.1016/j.enpol.2020.111964

59 Mhalla, M. (2020). The Impact of Novel Coronavirus (COVID-19) on the Global Oil and Aviation Markets. https://doi.org/10.18488/journal.2.2020.102.96.104.

60 Xue, D., Liu, Z., Wang, B., & Yang, J. (2021). Impacts of COVID-19 on Aircraft Usage and Fuel Consumption: A Case Study on Four Chinese International Airports. Journal of Air Transport Management, 95, 102106. https://doi.org/10.1016/j.jairtraman.2021.102106

61 Tardivo, A., Sánchez, C., Armando, M., Zanuy, C. S. M., & Zanuy, A. C. (2020). European Rail Research Network of Excellence COVID-19 Impact in Transport, an Essay from the Railways' Systems Research Perspective. https://www.worldometers.info/coronavirus/

62 Ibn-Mohammed, T., Mustapha, K. B., Godsell, J., Adamu, Z., Babatunde, K. A., Akintade, D. D., Acquaye, A., et al. (2021). A Critical Analysis of the Impacts of COVID-19 on the Global Economy and Ecosystems and Opportunities for Circular Economy Strategies. Resources, Conservation and Recycling, 164(May 2020), 105169. https://doi.org/10.1016/j.resconrec.2020.105169.

63 Norouzi, N. (2021). Post-COVID-19 and Globalization of Oil and Natural Gas Trade: Challenges, Opportunities, Lessons, Regulations, and Strategies. International Journal of Energy Research, 45(10), 14338–14356. https://doi.org/10.1002/er.6762.

64 Smith, L. V., Tarui, N., & Yamagata, T. (2021). Assessing the Impact of COVID-19 on Global Fossil Fuel Consumption and CO_2 Emissions. Energy Economics, 97. https://doi.org/10.1016/j.eneco.2021.105170

65 Honoré, A. (2020). Natural Gas Demand in Europe: The Impacts of COVID-19 and Other Influences in 2020. Oxford Energy Comment. https://www.oxfordenergy.org/publications/natural-gas-demand-in-europe-the-impacts-of-covid-19-and-other-influences-in-2020/

66 Combs, J. (2021). COVID-19 and Nuclear Energy. IAEE Energy Forum, 22. https://www.iaee.org/en/publications/newsletterdl.aspx?id=875

67 Ghenai, C., & Bettayeb, M. (2021). Data Analysis of the Electricity Generation Mix for Clean Energy Transition during COVID-19 Lockdowns. Energy Sources, Part A: Recovery, Utilization and Environmental Effects,. https://doi.org/10.1080/15567036.2021.1884772

aspect of society, bringing a staggering plunge in demand for nearly all major fuels, especially for coal, oil and gas (Figure 11). The collapse of fossil fuel demand brought significant financial stresses to the power industry, as prices slumped immediately because of the global lockdowns. In 2020, the global coal industry was hit the hardest, falling almost 8% according to IEA, whereas in the EU, imports of coal plunged by almost two-thirds, the lowest levels in the last 30 years[68]. In the US, the total number of fuel exploration and exploitation projects decreased[63] from 805 to 265. It is estimated that investments that were expected to grow by around 2% prior to COVID-19 in the energy sector, fell by 20% (almost $400bn) in 2020, mainly influencing new oil and natural gas projects[47]. In total, it is estimated that due to less oil spending, the power sector lost more than $1tn[69]. The repercussions of these declines include, but are not restricted to, an accelerated momentum of decarbonisation of the energy sector and a (not unrelated) surge in natural gas prices.

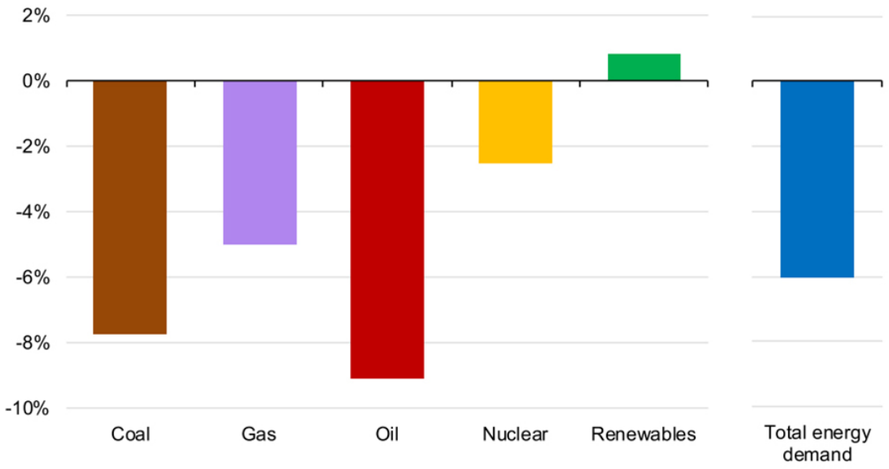


Figure 11 Change in primary energy demand by fuel in 2020 relative to 2019[56]

OIL INDUSTRY

During COVID-19 the oil industry experienced its third collapse in 12 years. The pandemic aggravated the state of an already volatile market due to the dissolution of the OPEC+ agreement in March 2020[70]. The failure in negotiations to agree on production cuts between the Organization of Petroleum Exporting Countries (OPEC) and Russia signified a period where the global crude market had more oil than it could potentially use and store. In early March 2020 the combination of the two crises created a deep plunge in oil markets, dropping oil prices to unprecedented levels. Brent crude, an international oil marker, dropped below $20 a barrel, signifying an 18-year low. The slow recovery in oil demand due to the relaxation of the sanitary measures lifted the oil price to $40-$45 price range in mid-April. However, the demand remained at low levels during the whole year with a small improvement observed by the end of 2020. Specifically, IEA reported that oil demand in 2020 decreased by about 9.2 mb/d compared to 2019 while December improved but remained lower than 2019 (-2.7 mb/d). Regarding supply, average production in 2020 dropped by 2.3 mb/d while in May 2020 the steepest drop was recorded – by 12 mb/d compared to 2019. Figure 12 depicts the downfall of oil consumption during the Q1 of 2020 in the US[71].

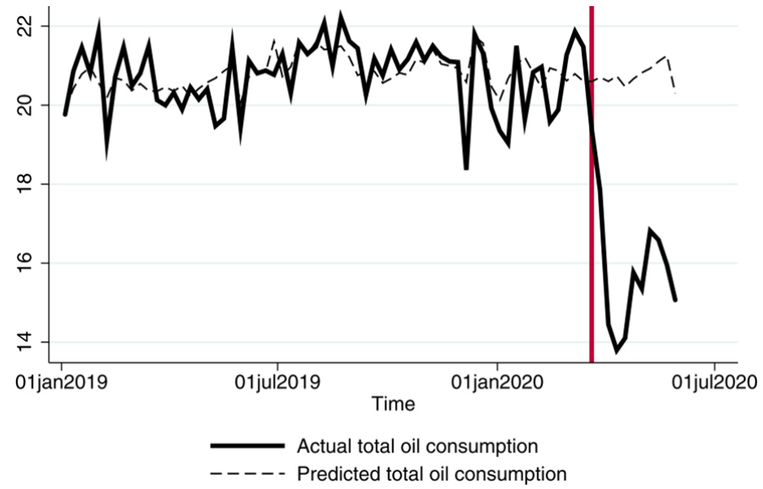


Figure 12 Actual and predicted total oil consumption in the US in 2020 in million barrels per day (mb/d)[71].

Plummeting demand during the pandemic lead to record volumes of stranded crude cargo and almost no storage space left on land to store crude. During the deepening crisis at least 160 million barrels were reported to be stored at sea outside shipping ports[72]. Oil drilling was reported to halt their operations for 2020 due to the low-price regime, as drilling (especially offshore) constitutes a capital-intensive investment. Before the pandemic, predictions of oil markets development were uncertain due to the challenges of the energy transition. IEA considered that after the pandemic rebound, these uncertainties would only escalate due to combining efforts to meet climate goals. However, as early as November 2021, oil prices had already reached their highest levels in 6 years, signifying a better-than-expected industry recovery.

NATURAL GAS INDUSTRY

Due to the crisis, it is estimated that total

68 Watts, Jonathan, and Jillian Ambrose. 2020. "Coal Industry Will Never Recover after Coronavirus Pan-demic, Say Experts." The Guardian. https://www.theguardian.com/environment/2020/may/17/coal-industry-will-never-recover-after-coronavirus-pandemic-say-experts

69 Carbon Brief. (n.d.). IEA: Coronavirus accelerating closure of ageing fossil-fuelled power plants. https://www.carbonbrief.org/iea-coronavirus-accelerating-closure-of-ageing-fossil-fuelled-power-plants

70 Al Jazeera. (2020, March 12). The fall of OPEC and the age of oil price wars. https://www.aljazeera.com/opinions/2020/3/12/the-fall-of-opec-and-the-age-of-oil-price-wars

71 Gillingham, K. T., Knittel, C. R., Li, J., Ovaere, M., & Reguant, M. (2020). The Short-Run and Long-Run Effects of Covid-19 on Energy and the Environment. Joule, 4(7), 1337–1341. https://doi.org/10.1016/j.joule.2020.06.010

72 The Guardian. (2020, April 19). Supertankers drafted in to store glut of crude oil amid coronavirus. https://www.theguardian.com/business/2020/apr/19/supertankers-drafted-in-to-store-glut-of-crude-oil-coronavirus

demand of natural gas also fell initially by 2-4%[73], significantly less than coal and oil. Despite this fall, the demand levels were still higher than 2014 (+12%) and 2015 (+2%), when gas demand reached its lowest level due to its limited utilization in heating and power generation[65].

In Europe, gas demand was low before COVID-19 as the winter of 2019-2020 was mild and wet especially in Northwest Europe, conditions that do not require heat. In February 2020, renewables exploited the strong winds, resulting in limited need for gas-fired generation. The IEA estimated that in Europe, natural gas demand dropped by 8% during Q1 2020 relative to 2019, consumption for domestic use dropped 3% and gas-fired power generation by over 5%[56]. Analyses indicate that variations in gas consumption are mostly dominated by the temperature factor[74]. Countries that use natural gas primarily for heating faced less challenges compared to those using it for electricity generation and industrial purposes. Significant impacts of COVID-19 in gas demand started to appear after March as during that month, an unusual increase in heating demand was observed, mainly due to lockdown which constrained people staying at home during cooler temperatures. At a national level, biggest year-on-year changes in gas consumption during the lockdowns were reported in France (-23%), Spain (-22%), the UK (-17%) and Italy (-16%) mainly due to reduction in production of the industry sector[75]. However, starting from mid-2021, the world has been in the grip of a natural gas crisis as the global economy continued its gradual recovery from the COVID-19 pandemic. During 2021, the crisis deepened as turbulence in the gas market led gas prices to soar by +250% compared to 2020 in Europe (price surges in the US market were also of the order of +100%[76]) (Figure 13). In October 2021, CNN reported that natural gas prices in Europe went from below $2 per million BTU in 2020, to almost $55. The next month, the Dutch TTF hub – a European benchmark for natural gas – set a new record high, by trading at 118 € per MWh in London, reaching almost a 400% rise since the start of the year[77].

Admittedly, for Europe, this gas crisis was soon dwarfed by the repercussions of the war in Ukraine to imported natural gas from Russia. But it is worth remembering that the evidence for Europe's over-reliance to imported natural gas was already there well before the invasion, as clearly seen in the pandemic era data collected in this work.

73 Hoang, A. T., Nižetić, S., Olcer, A. I., Ong, H. C., Chen, W.-H., Chong, C. T., Thomas, S., Bandh, S. A., & Nguyen, X. P. (2021). Impacts of COVID-19 Pandemic on the Global Energy System and the Shift Progress to Renewable Energy: Opportunities, Challenges, and Policy Implications. Energy Policy, 154 (April), 112322. https://doi.org/10.1016/j.enpol.2021.112322

74 Ciais, P., Bréon, F.-M., Dellaert, S., Wang, Y., Tanaka, K., Gurriaran, L., Françoise, Y., et al. (2021, April). Impact of Lockdowns and Winter Temperatures on Natural Gas Consumption in Europe. https://arxiv.org/abs/2104.14990v1

75 Sönnichsen, N. (2020). Coronavirus: Impact on the Global Energy Industry - Statistics & Facts. Statista. https://www.statista.com/topics/6254/coronavirus-covid-19-impact-on-the-energy-industry/

76 Reuters. (2021, September 20). Global markets: Gas. https://www.reuters.com/business/energy/global-markets-gas-2021-09-20/

77 CNBC. (2021, October 5). Gas price surges to a record high in Europe on supply concerns. https://www.cnbc.com/2021/10/05/gas-price-surges-to-a-record-high-in-europe-on-supply-concerns-.html

Figure 13 Gas prices soar in Europe in 2021. Source: Reuters.com

The search for the causes of this initial gas crisis points towards a combination of events including economic, geopolitical and weather factors, eventually creating a "perfect storm" for gas markets. In this combination of causes, the influence of the COVID-19 pandemic is irrefutable. The economic recovery in the post-lockdown era, especially in Asia, bounced-back with more vigour than expected by energy analysts and energy suppliers. In Europe, this led to significant shortages that pushed prices up, as increases in gas demand also followed an already cold winter which lasted up to the end of spring, leaving many European gas storage facilities depleted[78]. The surge in natural gas demand was also influenced by the global progressive phase-out of coal in electricity generation that was significantly accelerated during the lockdowns, as many countries and especially China, resorted to gas as a transitional resource towards renewables to achieve environmental goals. In China, this caused increased imports of natural gas up to 25% compared to the previous year. This situation restricted even the available gas supply for the European market. Furthermore, disruptions in LNG supply were reported, caused by maintenance work delayed during the COVID-19 pandemic[79].

In 2021, the growing demand for fuels aggravated the already challenging situation

78 Reuters. (2021, September 20). German households face 11.5% rise in gas bills. https://www.reuters.com/business/energy/german-households-face-115-rise-gas-bills-2021-09-20/

79 The Economist. (n.d.). Natural gas prices are spiking around the world. https://www.economist.com/finance-and-economics/natural-gas-prices-are-spiking-around-the-world/21804953

of ongoing supply chain disruptions and shortages inflicted by COVID-19, leading to unprecedented inflation in wholesale gas prices. It is indicative that on average, a 5.25% consumer-price inflation was estimated in early December 2021, attributed to supply chain strains. The duration and intensity of disruptions of sea freight, contrary to initial assessments of being transient, proved to be persistent and had cumulative effects on activities and prices, while researchers estimate that the knock-on effects will most likely remain for years ahead[80]. In its Review of Maritime Transport for 2021, the United Nations Conference on Trade and Development estimated that the maritime trade could experience a slow-down until 2026 (up to 2.4%), whereas global import price levels could increase by up to 11%, as a result of high freight rates[81]. The supply chain bottlenecks induced from the pandemic mainly created logistical difficulties and labour shortages which were unsolvable for the maritime sector, such as strict border controls, unanticipated and extensive mobility restrictions and the unavailability of global vaccine pass for seafarers and related industry personnel. These obstacles had a significant effect on fuels supplier delivery times which in turn led to high transit costs (Figure 14) that pushed consumer prices upwards. In addition to price inflation, the persistent challenge of supply chain bottlenecks in the maritime sector remains a challenge for natural gas alternatives which depend on shipping transporting. Since almost 61% of global crude oil and petroleum products are transported by sea[82], such bottlenecks will affect oil and related products which, in turn, exacerbates natural gas demand in a vicious circle – in the absence of credible domestic alternatives for power and electricity generation in Europe.

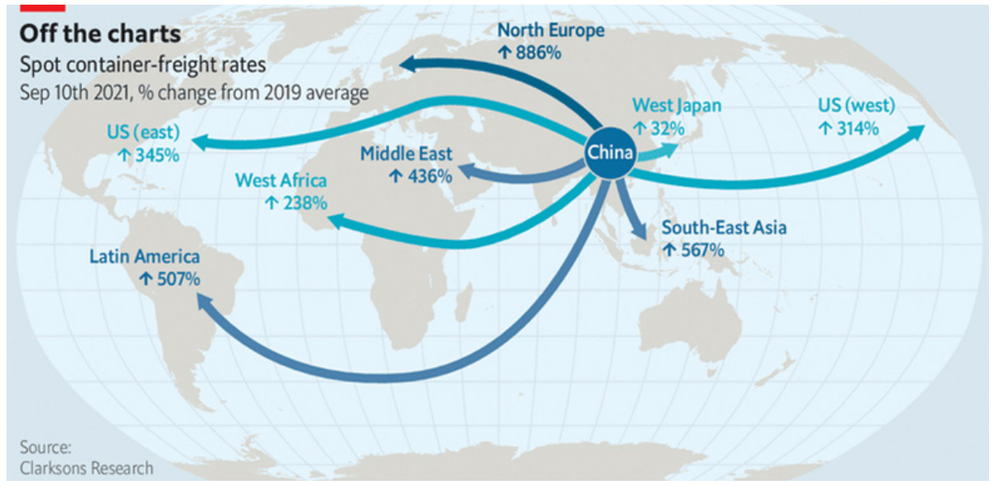


Figure 14 Increase of freight rates as of the Sep 10th, 2021, compared to 2019. Source: Economist.com

80 BBVA Research. (n.d.). Spain and EMU: Effects of Bottlenecks on Inflation and Activity. https://www.bbvaresearch.com/en/publicaciones/spain-and-emu-effects-of-bottlenecks-on-inflation-and-activity/

81 UNCTAD. (2021). Maritime Trade Weathers COVID-19 Storm but Faces Far-Reaching Knock-on Effects. https://unctad.org/news/maritime-trade-weathers-covid-19-storm-faces-far-reaching-knock-effects

82 Talk Business. (2017, August). 61% of global crude oil and petroleum products transported by sea. https://talkbusiness.net/2017/08/61-of-global-crude-oil-and-petroleum-products-transported-by-sea/

REFINERIES

The initial significant drop in fossil fuels demand and supply due to the spread of the pandemic and related restrictions also created disturbances in downstream petrochemical sectors and especially for the European refineries. The plunge of demand for refined products dropped by almost 20% at a global scale[83] which, combined with the oil price crash and oversupply pressured even more regional refineries, many of which were already operating at a loss. Figure 15 shows the sudden leap of refining margins, a proxy indicating profitability, from HELPE refineries due to COVID-19. According to expert assessment, the refinery sectors should shut down at least 6 mb/d to allow rates to return to normal levels, as excess capacity was the main struggling task. By February 2021, 1.72 mb/d of refining capacity across 15 refineries shut-down their production permanently or announced their closure. Additional 584.000 b/d of capacity were reported to be under stress[84].

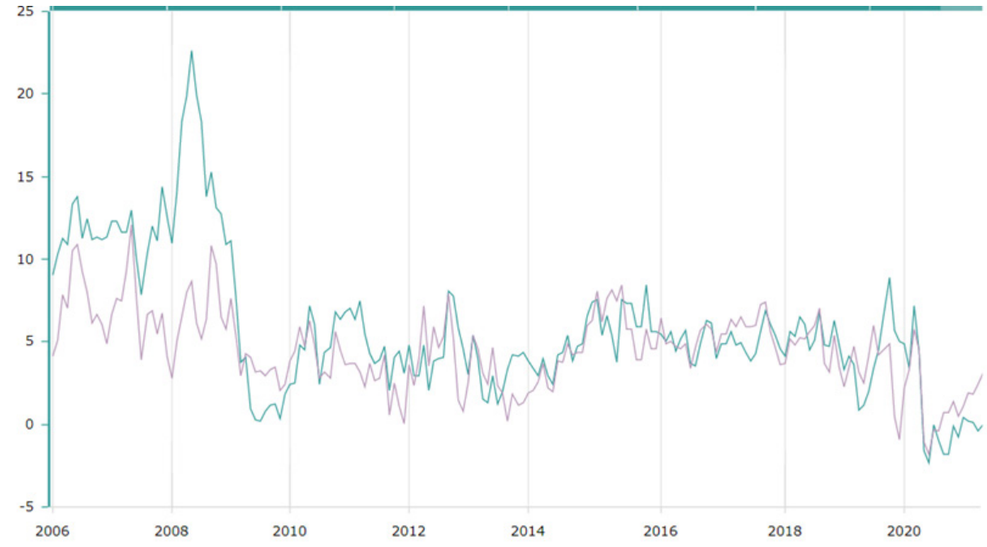


Figure 15 Refining margins from 2006 until 2021 from HELPE company. The two lines depict two different refining processing. Source: HELPE.gr

3.5.5.3 RES Share

While the conventional power generation industry struggled, the renewables sector proved to be a success story of the COVID-19 era. Renewables demonstrated high robustness during this period adding more than 256 GW of global power capacity during 2020 and being the only source that marked a growth in demand (+3% in 2020 according to IEA). During 2020, the renewable energy systems share in the EU surpassed the share of fossil fuels for

83 McKinsey & Company. (n.d.). Oil and gas after COVID-19: The day of reckoning or a new age of opportunity? https://www.mckinsey.com/industries/oil-and-gas/our-insights/oil-and-gas-after-covid-19-the-day-of-reckoning-or-a-new-age-of-opportunity

84 IHS Markit. (n.d.). COVID-19 accelerates refinery shutdown. https://cdn.ihsmarkit.com/www/pdf/0221/IHS-Markit-COVID-19-accelerates-refinery-shutdown.pdf

the first time ever (38% against 37%)[85]. This was not only an EU phenomenon: in the UK, solar power, at its peak, reached almost 30% of demand in April 2020, where all renewables at their peak hours reached 73% of the total demand. It should be noted however, that these share increases refer to a significantly reduced demand, as detailed before. In any case, the increase should be attributed to three main drivers: (i) significantly low operating/variable cost of electricity production (ii) priority access to the grid guaranteed for RES through regulations (iii) practical difficulties in adjusting RES production due to their inherent uncertainties.

In terms of costs, it is interesting to note that the cost of electricity generation from renewables reduced significantly according to the International Renewable Energy Agency (IRENA) especially of wind and solar. The Agency reported that almost everywhere in the world, utility-scale wind and solar PV generation became cost-competitive to coal energy production. According to the REN21 2020 annual report, the global weighted average levelized cost of electricity from solar photovoltaics declined by 85%, while wind power costs fell by 56% during the same period.

In terms of priority, it was reported[86] that during the pandemic, renewables were constantly receiving priority in the grid and were not asked to adjust their output to match demand due to contractual and regulatory constraints.

This increased prioritization and thus share of RES is also partly attributed to the (practical) difficulty in precisely managing RES production (due to the uncertainty related to hydrometeorological processes driving renewable energy generation). As such, regulators and energy utilities opted to adjust production in more (deterministically) manageable power plants (e.g., thermal or nuclear power plants) to counter the decrease in demand due to COVID-19 by limiting excess supply.

Only demand for biofuels dropped (-13% in 2020) due to reduced transportation, with biofuel production plants having to idle or reduce their output[56].

An indicative table reporting on RES share increasing in several European countries is presented in Table 3, using data from the Council of European Regulators. Germany reported the highest renewable energy generation (98.32 TWh) from wind, solar and biomass during the lockdowns[67], while France generated almost 50 TWh from hydro, solar and wind. It was reported that in April 2020, Denmark, Germany and Ireland covered almost 50% of their demand by wind generation[87]. Hydropower was the second largest renewable source producing more than 126.1 TWh.

In summary it can be stated that during the crisis, European countries overall managed to produce clean energy and cover (decreased) energy demands while also reducing greenhouse gas emissions. It is estimated that CO_2 emissions went down by up to 20% during April 2020 year by year (this number also includes the reduction in transportation). In a way, as the IEA also highlights, the pandemic acted as "a real-time experiment" to evaluate the operation of higher shares of variable renewables, thus boosting confidence and experience[56].

85 European Commission (2021). State of the Energy Union Report 2021. Directorate-General for Energy, 25 November 2021, Brussels, https://commission.europa.eu/news/2021-state-energy-union-report-2021-11-25_en

86 Khanna, M. (2021). COVID-19: A Cloud with a Silver Lining for Renewable Energy? Applied Economic Perspectives and Policy, 43(1), 73–85. https://doi.org/10.1002/aepp.13102

87 Renewable Energy World. (2020). Renewables Achieve Clean Energy Record as COVID-19 Hits Demand. Renewable Energy World. https://www.renewableenergyworld.com/energy-business/energy-finance/renewables-achieve-clean-energy-record-as-covid-19-hits-demand/

Table 3 Reported RES share percentage for different time periods and their relative increase from 2019. Data: CEER

Country	RES Share percentage (%)	Time in 2020	Increase relative to 2019 (%)
Germany	52.5	January to June	+8.1
Spain	43.3	January to November	+13.4
Great Britain	45	April to June	+9
Greece	34.6	April	+15

As such, COVID-19 offered an early glimpse of a future energy landscape, with declining demand for fossil fuels and increasing shares of electricity in the final energy market. It also highlighted challenges as renewables output remains uncertain and volatile in the absence of large-scale electricity storage technologies. It is expected that investments in renewable capacity will increase in the aftermath of COVID-19 as a result of both public (mostly EU-driven) and private initiatives. It is interesting to note that the pandemic caused significant reductions in CO_2 emissions[88] possibly well beyond what international treaties (UN Climate Change Conference of the Parties - COPs) have agreed. This creates a **unique opportunity to study the effects of these drastic reductions in CO_2 on climate phenomena** (e.g., extreme events etc.) thus providing evidence of the true impact of decarbonisation policies, beyond the results of simulation models.

3.6 Effects on grid resilience

The impacts of COVID-19 on network operations can be differentiated into direct and indirect. Direct impacts include power instabilities and outages. Indirect impacts include longer term effects to power grids operation such as delays in new projects, consequences of delayed maintenance etc. In this section we describe direct impacts. Longer-term, indirect effects are discussed in the following sections, under the headings of human challenges and supply chain disruptions. At a micro scale the consequences of reduced demand peaks and irregular consumption patterns (Figure 16) create risks in the safety, efficiency and reliability of the power systems and power grids from an operational perspective.

88 Lalas, D., Gakis, N., Mirasgedis, S., Georgopoulou, E., Sarafidis, Y., & Doukas, H. (2021). Energy and GHG Emissions Aspects of the COVID Impact in Greece. Energies, 14(7), 1955. https://doi.org/10.3390/en14071955

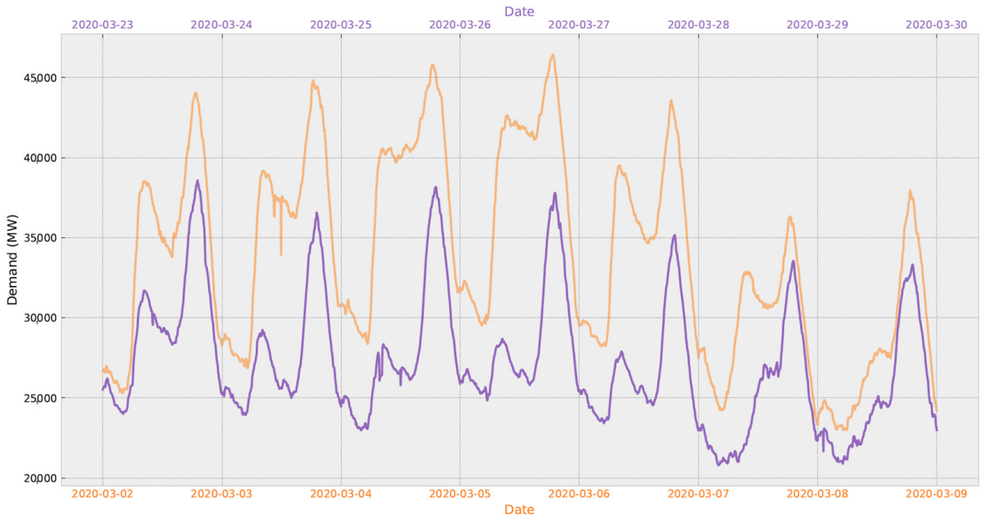


Figure 16 System demand before and during COVID-19 lockdown in Great Britain[89].

These operational challenges can be classified into two categories based on the time frame of disruption as discussed by the Electric Power Research Institute[90] in a technical report for COVID-19 guidance for system operators. These include:

a. *Slowly unfolding risks* that can lead to longer time failures (minutes to days) and are relevant to demand or renewable mix and load forecast errors, non-expected flows to networks, exceeding voltage levels or insufficient conditions that can lead to failures in the electric supply chain,

b. *Fast-acting, dynamic* risks that have a narrower timeframe of impact (seconds to minutes) and are related to frequency imbalances and voltage stability.

Real-time discrepancies in demand and supply are the main factors of grid frequency deviation. Reported data prove the existence of highly increased average forecasting errors during the initial lockdowns in Spain and France compared to previous years (Figure 17). Electricity utilities oversee the keeping of grid frequency within a specific range. A surplus in power generation or decline in demands and vice versa can increase a network's frequency. Therefore, maintaining power balance proved a decisive challenge because of the continual uncertainties of the demand due to fast-changing mitigating policies. This process is harder especially in coal-dominated regions where in-unit commitment has to be decided on a longer time basis[57].

89 Kirli, D., Parzen, M., and Kiprakis, A. (2021). Impact of the COVID-19 Lockdown on the Electricity System of Great Britain: A Study on Energy Demand, Generation, Pricing and Grid Stability. Energies, 14(3), 635. https://doi.org/10.3390/en14030635

90 Electric Power Research Institute. (2020). COVID-19: Flexibility and the Grid

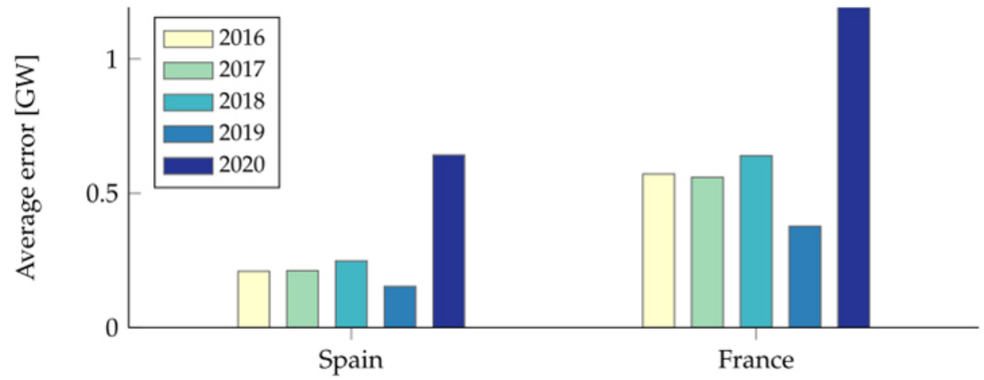


Figure 17 Average daily load forecasting error between 15 March and 15 April[91]

Several studies[54, 92] have discussed the challenges of utilities and system operators in addressing problematic frequency stability issues in short-length forecast accuracy due to COVID-19 measures in different countries. An example of unstable frequency during the first lockdown is presented in Table 4 based on data from a study for the Israeli power grid. It is observed that during the lockdown the grid frequency appeared significantly more unstable, as evidenced by the increased deviation of the time during which the frequency deviated from its nominal value (50 Hz).

Table 4 Duration (in sec) of frequency deviations (in Hz) from its nominal value before, during and after 1st lockdown in Israel, March-May 2020[91]

Week	<49.8	[49.8, 49.9)	(50.1, 50.2]	>50.2
02 – 08/03 (before 1st lockdown)	0	801	2195	32
23 – 29/03 (during 1st lockdown)	20	1612	2903	13
30/3 – 05/04 (during 1st lockdown)	128	4245	3716	667
11/05 – 17/05 (after 1st lockdown)	7	57	1547	0

Another issue that arises from changes in demand patterns is related to voltage regulation of the power system. Voltage regulation ensures that electrical products and equipment operate optimally. During the pandemic an increasing penetration of distributed energy resources (DER) was observed e.g. roof-top PVs, an idea of demand side management that is growing in recent years[93]. However, the surplus that occurs due to the high demand drops on the one hand and the stable generation by DERs on

91 Navon, A., Machlev, R., Carmon, D., Onile, A. E., Belikov, J., & Levron, Y. (2021). Effects of the COVID-19 Pandemic on Energy Systems and Electric Power Grids—A Review of the Challenges Ahead. Energies, 14(4), 1056. doi:10.3390/en14041056

92 Halbrügge, S., Schott, P., Weibelzahl, M., Buhl, H. U., Fridgen, G., & Schöpf, M. (2021). How Did the German and Other European Electricity Systems React to the COVID-19 Pandemic? Applied Energy, 285. doi:10.1016/j.apenergy.2020.116370

93 Tsagkari, M. (2020). Impact of Coronavirus on Distributed Energy Generation with the Application of Demand-Side Management. IAEE Energy Forum / Covid-19 Issue 2020

the other hand may aggravate voltages issues in some distribution system[51,57]. It is therefore important for utilities to mitigate these over voltage issues by undertaking preventive measures. For example, in the UK the disconnection of distributed generation has been proposed to diminish operational risks due to these imbalances[94].

3.7 Direct and indirect human challenges

To protect human health during the pandemic and comply with social distancing, many energy utilities restricted their workforce and implemented teleworking. Workers were encouraged to work remotely, avoiding non-essential interactions, while businesses provided remote system access. The reduction of on-site employees was significant, especially since experienced, often older, workers were more vulnerable to the virus. Human expertise and communication are crucial for smooth operations, particularly in the nuclear sector, where specialized tasks cannot easily be reassigned. International travel restrictions further impacted projects at the commissioning stage due to difficulties in site access and accommodation. Critical roles in the energy industry, including utility workers, engineers, and technicians, support various operations such as development, fuel procurement, generation, and distribution of electric power. These roles also encompass the mining, processing, and logistics of fuels like coal, natural gas, crude oil, and nuclear. Services requiring physical presence were delayed, and virus outbreaks among employees caused project delays[95]. For instance, Kazatomprom, a major uranium producer in Kazakhstan, reduced on-site staff to mitigate the virus spread, leading to a 19% drop in 2020 production[96]. Similarly, Poland's top coal mining company, PGG, suspended operations due to COVID-19 among workers, and the installation of a 382.7 MW wind farm in the Netherlands was delayed due to the pandemic and bad weather[97].

Furthermore, due to COVID-19, essential maintenance actions, such as periodic grid service and inspections were postponed or even cancelled[98]. In Belgium, grid maintenance was reported to be undertaken for minimal risk level[51]. Delayed or negligent maintenance of electricity networks can potentially lead to severe consequences for network operation. It also raises additional environmental and safety concerns because power-line grids often extend to areas covered by woodlands and forests: a serious risk of wildfires is known to arise from poorly maintained electric transmission lines. In Greece in 2017 two devastating wildfires that incinerated 15.000 acres of forest were attributed to negligent maintenance of pylons and power cables[99] and the significant wildfires that hit Greece again in the summer of 2021[100] could also be, partly, attributed to indirect effects on maintenance caused by the pandemic.

94 PV Tech. (n.d.). UK solar at risk of switch-offs as ESO seeks urgent disconnect powers. https://www.pv-tech.org/news/uk-solar-at-risk-of-switch-offs-as-eso-seeks-urgentdisconnect-powers

95 Global Energy Monitor. (n.d.). Impact of Covid-19 Pandemic on Major Fossil Fuel Projects. https://www.gem.wiki/Impact_of_Covid-19_Pandemic_on_Major_Fossil_Fuel_Projects#References

96 Decena, K. (2021). COVID-19 Drags down Kazatomprom's Q4'20, FY'20 Uranium Outputs YOY. S&P Global Market Intelligence. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/covid-19-drags-down-kazatomprom-s-q4-20-fy-20-uranium-outputs-yoy-62408782

97 Windpower Monthly. (n.d.). Bad weather, COVID-19 delay Dutch lake project. https://www.windpowermonthly.com/article/1717172/bad-weather-covid-19-delay-dutch-lake-project

98 Bahmanyar, A., Estebsari, A., & Ernst, D. (2020). The Impact of Different COVID-19 Containment Measures on Electricity Consumption in Europe. Energy Research and Social Science, 68 (July), 101683. doi:10.1016/j.erss.2020.101683

99 Lampropoulos, V. (2017). The Oversights of the PPC That Set the Forests on Fire. To Vima. Retrieved from https://www.tovima.gr/2017/08/25/society/oi-ablepsies-tis-dei-poy-bazoyn-fwtia-sta-dasi/

3.8 Direct and indirect challenges due to disruptions in supply chains

An important vulnerability of CEI that sometimes goes undetected is the vulnerability to supply chains[101]. Disruptions in supply chains can influence both exporting and importing countries – reduced export damages financially local firms and reduced imports leads to material shortfall. In this context, a study[102] claimed that in the U.S. more than 75% of companies reported disruptions in their supply chain during the COVID-19 pandemic. Disruptions in supply chains translate to direct impacts on power systems due to resulting disruptions in operation, delayed maintenance implementations or postponed installations and construction[57]. As manufacturing of most energy-related equipment inevitably decreased, utilities had to secure alternative supply chains to ensure continuity of operations. Shortages in supply chains were caused by problems and delays in production, transportation and warehousing. Critical products included personal protective equipment (PPE) for workers (e.g. safety helmets, rubber voltage gloves etc.), different parts and components of energy systems (e.g. photovoltaic cells, gearboxes, rotors), and other materials. Depending on the duration of the lockdowns in each region, disruptions in supply chains also caused delays in the construction of energy projects.

Slowdowns from China, which was the epicentre of the pandemic, exacerbated the deficits of product supply, not only in the electricity sector, but also in the renewable energy industry[55,103]. Most renewable systems rely on critical raw material such as lithium and cobalt that are used in wind turbine generators, solar panels, batteries and electric motors for electric vehicles and were on shortfall due to temporary factories shut-down or reducing capacity. Global solar PV manufacturing and wind power supply chain were hit hard as they are highly concentrated (over 70% for PVs) in Chinese factories[104]. In France, Germany, Spain and the UK onshore capacity additions were reduced by around 10% mainly due to delays[105]. These issues are important to take note of in the context of a RES-based approach to the EU's Strategic Energy Autonomy challenge.

Nuclear utilities around the world announced minor impacts on their short-term uranium supply processes. However, in the long-term, reactor construction schedules were also impacted in France and the United Kingdom. The delays were mainly attributed to significant disruptions in supply chains[66]. Supply chains at national levels were also affected. Energy projects that relied on local suppliers for materials like

100 DW News. (n.d.). Greece wildfires: New blaze hits Evia island. https://www.dw.com/en/greece-wildfires-new-blaze-hits-evia-island/a-58954794

101 Excluding supply chains of fuels – discussed earlier

102 Fernandes, N. (2020). Economic Effects of Coronavirus Outbreak (COVID-19) on the World Economy. SSRN Electronic Journal, March. Elsevier BV. doi:10.2139/SSRN.3557504

103 Ivanov, D., & Dolgui, A. (2021). OR-Methods for Coping with the Ripple Effect in Supply Chains during COVID-19 Pandemic: Managerial Insights and Research Implications. Int. Journal of Production Economics, 232. doi:10.1016/j.ijpe.2020.107921

104 The World Bank. (2020). COVID -19 Operational Disruptions in Infrastructure

105 IRENA. (2020). Post-COVID Recovery: An Agenda for Resilience, Development and Equality. Int.Renewable Energy Agency

concrete also slowed down[106].

3.9 Effects on cyber-security

It is important to note that the pandemic reshaped, to a large extent, work and lifestyles and created new challenges for businesses as "working from home" became the new normal for millions of employees. This new operating model started out of necessity for utilities to conform with the social distance restrictions and resulted in an (ongoing) digitalisation acceleration across multiple sectors – from business to government. However, cyber-security issues also rapidly accelerated (Figure 18). The European Union Agency for Cybersecurity (ENISA) reported that COVID-19 put organizations under serious pressure while ranking the technology industry as one of the most attractive targets for cyber-attackers[107]. Similarly, the European Cyber Security Organization (ECSO), reported that increases in fraud, cybercrime and cyber-attacks became a number one priority for organizations during the pandemic due to these newfound challenges. In June 2020, a Swiss survey reported that cyber-attacks had tripled above the average during the first lockdown[108].

Energy infrastructure had already been tar

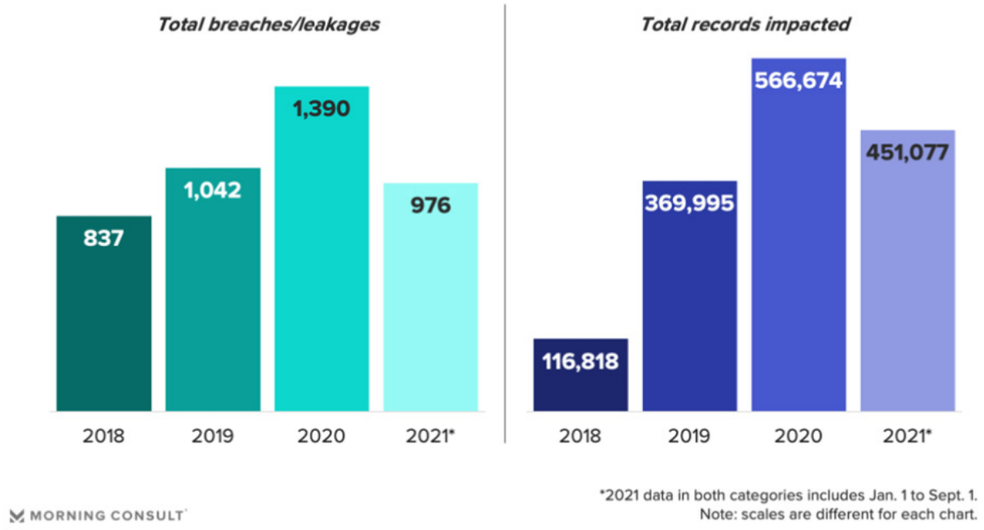


Figure 18 Total energy sector credential exposures – both breaches and records impacted – of top 20 energy companies on the Fortune Global 500 list. Source: Constella Intelligence Inc.

geted by attackers, that are getting more sophisticated, with every passing year according to surveys[109]. The Organization of American States reported that hackers of CEI are becoming more interested in operational technology and physical devices that support the systems, as most of the recorded cyber-attacks have targeted mainly industrial controls rather than attempting to steal data[110]. Different adversaries were profiled by a study[111] who consider nation-states and insider attacks as key actors aiming at the destruction of critical infrastructure. The same study also identifies as possible adversaries, for the power sector, organized criminals, hacktivists, competitors and skilled individual hackers, the motives of which are an array from financial thefts, business disruptions to damaging reputation etc.

In recent years critical infrastructure, including the energy sector, such as power grids, fuel industries, nuclear power plants, dams, and others, have become more digitalized as well as automated[112]. Examples of cyber disruptions in energy utilities have been reported around the world. As recent as in 2021, the Colonial Pipeline Network in the USA, was hit by a ransomware, forcing the company to temporary halt the main 5.500 miles pipeline transporting gasoline[113]. In Europe, one of the most well-known examples is the blackout of part of the Ukrainian capital Kiev on December 2016[114]. These instances and many others highlight the importance of maintaining critical energy infrastructure well-protected from cyber-threats.

The pandemic increased cyber-threats as many utilities had employees work from home, creating breaches and makeshift solutions that compromised security. For example, an oil refinery used smartphones with a videoconferencing app to monitor a pilot flame[115]. Such workarounds, however, can be exploited by adversaries. Arguably, there was a lack of method statements and guidance for employees on avoiding risky cybersecurity behaviours, especially with personal computer use[116]. This led to increased social engineering attacks, phishing scams, lack of multifactor authentication, and outdated antivirus software[117]. Working from personal computers heightened the risk of accessing and potentially misusing sensitive company data. The long-term implications of COVID-19 on remote work and unmanned facilities are still unclear, but as digitalization accelerates post-pandemic, cybersecurity risks are expected to rise. Therefore, the energy sector needs to focus more on protecting critical IT systems against these new challenges.

106 Chesson, M. (2020). Impact of COVID-19 on Power Projects. https://www.joi.or.jp/wp-content/uploads/2022/10/Mag_202007_07_SIMMD.pdf

107 ENISA. (2020). Main Incidents in the EU and Worldwide. Enisa Threat Landscape, no. April, 1–26

108 Swissinfo. (n.d.). Jump in cyber-attacks during COVID-19 confinement. https://www.swissinfo.ch/eng/jump-in-cyber-attacks-during-covid-19-confinement/45818794

109 Desarnaud, G. (2017). Cyber Attacks and Energy Infrastructures

110 AGCS Allianz. (n.d.). Cyber Attacks on Critical Infrastructure. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

111 Livingston, Sanborn, Slaughter, & Zonneveld. (2019). Managing Cyber Risk in the Electric Power Sector. Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html

112 Erbach, G., & O'Shea, J. (2019). Cybersecurity of Critical Energy Infrastructure. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642274/EPRS_BRI(2019)642274_EN.pdf

113 The New York Times. (2021). Cyberattack Hits U.S. Pipeline. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

114 BBC News. (n.d.). Power Cut Disrupts Olympics. https://www.bbc.com/news/technology-38573074

115 Baily, T., Maruyama, A., Malashenko, E., & Wallance, D. (2020). The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities. Power Magazine, no. November, 1–16. https://www.powermag.com/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities/

116 Wang, L., & Alexander, C. A. (2021). Cyber Security during the COVID-19 Pandemic. AIMS Electronics and Electrical Engineering, 5(2), 146–157. doi:10.3934/electreng.2021008

117 Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. SN Computer Science, 2(2), 78. doi:10.1007/s42979-020-00443-1

3.10 Insights and recommendations

Here we present the main insights for civilian energy infrastructure based on the findings of this chapter and spell out key recommendations to **enhance the resilience of the defence sector against possible similar future extreme events**.

This chapter's findings are aligned with the rationale of the EU Critical Entities Resilience (CER) Directive[118] where it is suggested that what is needed is to "*fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them*". The evidence collected here suggests that indeed, through direct and indirect cascades, the resilience of CEI depend on much more than the integrity of infrastructure assets and as such a widening of the protective umbrella **to include all relevant critical entities** is warranted. Of direct relevance for MoDs in the context of this expanded protective umbrella for CEIs are **hybrid threat considerations**, such as those outlined in the relevant JRC report[119] entitled "The Landscape of Hybrid Threats". As such it is strongly recommended that a **wider protective "net" is cast around CEI**, beyond 'just' infrastructure.

From a technology perspective, new AI tools are needed to increase **load forecasting accuracy** and **system flexibility** under extreme events. In this regard, readers are referred to the *Artificial Intelligence for Energy and Environmental Technologies* report of the EDA ARTENET project[120]. But, perhaps the most important lesson from the crisis, is that the EU should seek to **urgently decrease its energy dependency**. It is suggested that this over-reliance on imported natural gas **needs to urgently decrease** for three main reasons: (a) gas is not a carbon-free fuel and as such it represents a deviation from EU decarbonisation objectives (b) related pipeline projects, aiming at diversifying the sources of natural gas imports are **very demanding** in terms of financial resources, political capital and time (c) and perhaps more importantly, as evidenced by the COVID crisis and especially the winter of 2021, natural gas makes the EU **over-dependent on a few major suppliers** with the obvious risk that **competing market demands** (e.g. of China[121]) or potential **spill-over effects of political disputes** between the EU and these suppliers, as the recent events in the Ukraine have clearly shown, **could affect the EU** (socially, politically and militarily) by turning the **Union's energy security**, into a *de facto* '**bargaining chip**' in geopolitical tensions beyond the EU's direct control. This recommendation is directly supported by the 2022 report published by the High-Level Group convened by EU Commissioner Gentiloni to reflect on the post-COVID economic and social challenges[122], which although completed before the Russian invasion of Ukraine (as was the case with this work), suggests that accelerating the energy transition is critical to reduce the dependency on Russian gas.

This dependency makes it ever more critical for the EU to **bridge the gap** between the current state of the EU energy system and a future energy landscape that will be dominated by renewable energy sources thus minimising energy dependencies. In this regard, the EU should address the 'elephant in the room' and **heavily (and rapidly) invest in the development of technologies for large scale energy storage** (e.g., large scale hydropower with pump-storage capabilities and hydrogen). It is encouraging that in its Hydrogen Strategy[123] released in July 2020 the EU pledged the development of 100% clean hydrogen production from renewable electricity, with plans to install at least 6 gigawatts of electrolysers in the EU by 2025 and at least 40 gigawatts by 2030. In this regard, we would argue that **we need to be even more ambitious**.

However, even the most rapid of technological developments and storage capacity deployment, still results in a temporal gap which needs to be bridged without exacerbating the over-reliance of the EU on imported natural gas evidenced during the COVID crisis. In this regard it is suggested that the EU needs to focus on **increasing the diversity of imported fuels** (e.g., increase **LNG terminals capacity** in key ports throughout the EU) but also rethink the appropriate role of **fuels already available in the EU**, including coal.

As energy security is a key concern for the EU military and since EU defence is heavily reliant on civilian CEI for energy security, **vulnerabilities on the civilian side are translated into vulnerabilities on the defence side**. Although this was well known before the pandemic, COVID-19 demonstrated some of these problems, which were previously considered as theoretical possibilities, in practice. It is suggested that the pandemic should act as a 'wake-up call' for the defence sector to build its resilience (and to also think about antifragility opportunities) in preparation for future events. The strategy towards such resilience could be summarize as: less fuels, more options. In particular it could include:

- Casting a **wider net in risk assessment and management** of energy dependencies (and other linked civilian services, such as water) of military installations and bases, adopting an **end-to-end** approach that includes financial and supply chain issues on the civilian side.
- Reducing energy/fuel consumption by **increasing energy efficiency** (especially in heating and transportation) **needs to be accelerated** to reduce dependency from civilian CEI. Recent advances in hybrid power generation and micro-grids in deployed military camp settings, provide early evidence that such solutions are becoming more feasible. What this report suggests is that equal (or even more) attention should be given to **retrofitting existing home bases** (and not only deployable installations). It is further suggested that potential failures of civilian CEI, for periods of time beyond a few hours, would result in disruptions of **other civilian services** that home bases depend on, **such as water**. As such, it is strongly suggested that water and energy autonomy is pursued in combination and that related autonomous infrastructure is conceptualized as **integrated water-energy systems**, rather than as separate, independent infrastructure.
- Investment in novel technologies of **energy generation** and **longer-term storage**, to be owned and operated by the military. In this context RES, biofuels, and hydrogen (e.g., fuel cells, hydrogen power plants, but also hydrogen for synthetic fuel production) should be carefully considered and prioritised.
- Furthermore, and perhaps somewhat controversially, we suggest that MoDs at the national level could also examine the possibility of **placing civilian coal power plants**, that are flagged for de-commissioning as part of the decar-

118 European Commission. (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN

119 European Commission. (2020). The landscape of Hybrid Threats: A Conceptual Model. https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

120 ARTENET: Artificial Intelligence for Energy and Environmental Technologies (Contract Number: 19.RTI.OP.373). https://www.uwmh.civil.ntua.gr/projects/69-artenet.html

121 Reuters. (2022, February 4). Russia, China agree 30-year gas deal using new pipeline: https://www.reuters.com/world/asia-pacific/exclusive-russia-china-agree-30-year-gas-deal-using-new-pipeline-source-2022-02-04/

122 European Commission. (n.d.). https://economy-finance.ec.europa.eu/economic-recovery/high-level-group-post-covid-economic-and-social-challenges_en

123 European Commission. (n.d.). https://energy.ec.europa.eu/system/files/2020-07/hydrogen_strategy_0.pdf

bonisation transition, **in 'cold reserve'**, to be used in emergencies – including for reasons of national security. It is noted here that such a 'plan b' policy **is not conflicting with the EU's decarbonisation efforts**, since power plants in cold reserve do not result in CO_2 emissions under normal circumstances and would be used as an **energy source of last resort**, playing an important role in the collective security of European citizens.

- **Cyber-awareness and related cyber-security technology** development and deployment should be accelerated in the civilian and defence sectors. This **need for cyber-awareness and related cyber-security technology development and deployment** is expected to be ever more relevant in the next years and is also directly relevant to MoDs and security agencies in the context of hybrid threats as suggested earlier. In this sense, it is also suggested that **MoDs engage even more actively in shielding defence relevant civilian CEIs from cyber-attacks**, working together with relevant civilian authorities.

Finally, it is recommended that MoDs become **more engaged** in the planning and operational resilience of civilian CEI, by communicating **armed forces requirements** to ensure uninterrupted operational readiness under the most challenging conditions (such as future, even more disruptive, pandemics). In this regard, we argue that the concept of '**military energy resilience**' should be introduced as an equivalent to 'military mobility' in the energy domain. The concept of "military mobility"[124](MM), adopted by the EU through the relevant 2018 Action Plan acknowledges[125] that "*facilitating the movement of military troops and assets is essential for the security of European citizens, and to build a more effective, responsive and joined-up Union*". The Military Mobility Action Plan spells out the required steps in terms of developing an appropriate **vocabulary for this dialogue**, compiling **military requirements** to be taken into account **by civilian planners and operators** and **by creating** new (or streamlining existing) **legal** and **financial instruments** that allow **greater synergies** between civilian and defence domains in terms of planning and operation of transport infrastructure (e.g., financial instruments that allow necessary upgrades of existing infrastructure to be funded from suitable budgets). Here we argue that an equivalent **EU Action Plan on "Military Energy Resilience" (MER)** in the aftermath of the COVID crisis and the war in Ukraine would be highly advisable so that relevant military requirements can be communicated, and appropriate legal and financial instruments leveraged to ensure that civilian CEI, that are important for defence, are designed, built and operated appropriately for their (effectively) dual use purpose.

In the meantime, and before such an Action Plan can be adopted at the EU level, it is suggested that MoDs could better prepare by undertaking (or updating) **risk/vulnerability assessments**, extending the scope of these assessment beyond military infrastructure to **include civilian CEI**, looking also at **indirect cause-effect vectors** such as those identified in this work for the specific COVID crisis (incl. personnel, cyber, financial and supply chain disruptions affecting critical civilian energy entities). Based on such studies, identify **critical control points** and related **upgrade requirements**, when necessary, to be communicated to civilian stakeholders as appropriate. As this communication is highly sensitive in nature, it must be undertaken in collaboration with national security agencies.

Such bottom-up efforts could also be facilitated by the development of **dedicated civilian-military collaboration units** or agencies (similar for example to US DoD Defence Logistics Agency DLA[126]) where military and civilian personnel could collaborate in continuously and proactively undertaking the above risk assessment and management tasks, adopting an **end-to-end protection** logic that conceptualises **critical civilian and military energy systems as truly interconnected**.

Furthermore, the concept of **antifragility**, invoked in this work as an approach to thinking about desirable system properties beyond robustness and resilience, in other words the property of a system not only to bounce back from an impact but to **recover at an improved state** is indeed evident in the pandemic era. The significant acceleration of digitalisation of significant parts of the economy and government due to the pandemic is a **good example of anti-fragility at work**: the stress from the pandemic resulted in an improved situation in terms of digital transformations – accelerated even against the most optimistic forecasts of the EU's twin transition targets. It remains to be seen if wider lessons for the civilian and defence sectors related to energy autonomy (such as those identified in this chapter) will be taken up by relevant actors and as such increase the resilience of defence relevant CEI, **in an act of *de facto* antifragility display**, in a post-COVID world, by both the EU defence and energy sectors.

124 European Commission. (n.d.). Military Mobility. https://ec.europa.eu/defence-industry-space/eu-defence-industry/military-mobility_en

125 European Commission. (n.d.). https://ec.europa.eu/commission/presscorner/detail/en/IP_18_2521

126 Defense Logistics Agency. (n.d.). https://www.dla.mil/

04

The Impact of Finance, Markets and Ownership on the Operational Security and Effectiveness of Defence-Related Critical Energy Supply and Infrastructure

Thierry Bros, *Sciences Po Paris*

4.1 Introduction

The armed forces rely on civilian critical energy supply and infrastructure (CESI)[127] in and outside the EU to ensure affordable, sustainable, and accessible energy for their everyday activities within the European territory. This critical dependence entails risks, threats and vulnerabilities that can affect operational effectiveness.

Back in 1974, an off-market organisation, the International Energy Agency (IEA) was created by the Organisation for Economic Co-operation and Development (OECD) to increase and ensure their collective security of oil supply. For the last two decades, the EU has relied more and more on markets for its broad energy security as markets can provide some short-term balance in a cost-effective way. Unfortunately, markets cannot cope with malign interferences or massive supply disruptions and are vulnerable to abrupt shifts in perception and sentiment with real-world financial impact. The 2021-2022 weaponisation of natural gas by Russia was a wakeup call, with the EU needing to rethink its long-term energy security with both market and off-market elements.

After a lengthy period of peace and economic prosperity, the return of war in Europe was the wake-up call for EU governments which are realising that energy security is paramount to national and economic security. MoDs with a longer time horizon and time preference than most civilian organisations are therefore ideally suited to help different EU organisations in this redesign of improved security of supply for the benefit of both the civilians and the armed forces to secure abundant clean energy. The energy transition will expose misalignments between exporters and importers, potentially reshaping commodity markets and relationships along the way. As these disagreements are bound to increase as nations accelerate efforts to clamp down on climate change, policymakers may need to balance emissions reduction rules with ensuring that energy keeps flowing to their citizens.

In this context, it is also important to investigate the ownership of companies operating defence-related CESI, encompassing issues such as non-European companies acquiring (minority) stakes and controlling stakes in strategic energy companies, especially when they are directly or indirectly influenced or supported by systemic rivals or adversaries. China's move to restrict exports of key metals used for chip-making and electric batteries, due to its trade dispute with the United States (US), is a reminder that economics is an extension of politics by other means.

Energy is a core driver of socio-economic outcomes and geopolitical landscapes. The on-going energy transition is set to induce far-reaching and transformative changes and has demonstrated yet again how the global energy system is intricately intertwined with geopolitics. As such, MoDs should, firstly, have an educated view and, secondly, be an active stakeholder to protect EU interests.

Failure to properly address security of energy supply leads to economic recession and massive increase of state debt burden. Mechanisms to avoid a security of supply issue always look costly in isolation but must be compared with the effective cost on the economy of the manifestation of supply failures.

The unbundling of supply and infrastructure on one side and the inter-fuels competitions have made looking into security of energy supply a more fragmented problem. As only Member States can have a complete view of the energy chain, MoDs should liaise with their respective energy ministries to rethink the security of energy supply by adding their non-market views. In a complex and volatile energy security environment, the EU should take steps to enhance its security of supply.

There has not yet been a clear instance when the energy security of a European armed force has been affected by defence-related CESI ownership issues, but concerns have been outlined regarding the regulatory and strategic impact of non-EU investment in European energy as part of a state strategy for growth in influence. Such actions could also conceivably raise concerns for MoDs regarding security of supply in all its dimensions (affordability, accessibility, sustainability), security of information and overall security in the face of hybrid threats comprising economic, legal and industrial measures. Therefore, the strategy of state-supported and state-financed actors from outside the EU to enter the European energy market by buying shares of European companies operating European energy could have an adverse impact on security governance and on energy security and requires scrutiny which has so far been lacking.

In this context, there is an emerging need for the defence sector, as an energy-intensive consumer, to further investigate and enhance its understanding and insights on the (cascading) effects of financial and market vulnerabilities of defence-related CESI with the potential of affecting armed forces operations in European countries. In addition, there is a need to explore the concerns and risks that the ownership of those CESI creates for MoDs and to define and propose the appropriate measures and responses to enhance armed forces' resilience towards the abovementioned risks.

This chapter investigates how financial, market, regulation, and ownership issues impact CESI operators, and to examine the resulting effects on the resilience of the European Union Member States' armed forces within the territory of the EU. The chapter is split into four topics:

- Electricity producers (mostly produced in the EU);
- Critical EU energy infrastructure (as the EU has unbundled energy infrastructure);
- Producers of coal, oil and gases (provide the buffer and mostly produced outside the EU);
- Energy reseller/supplier as MoDs contract via resellers.

An additional section is dedicated to how security of energy supply should be addressed in a world in transition where inter-fuels competition is increasing. The old silo-analysis per fuels is becoming less and less relevant and should be modernised. It needs to address not only the security of supply but also the storage of energy.

4.2 Electricity producers

As electrification is paramount to the energy transition, MoDs should advocate for as much as possible decarbonised electricity production and for measures to ensure the transition is as smooth as possible by avoiding decommissioning any plants (in particular decarbonised ones) if enough additional supply is not already available. By closing down / decommissioning electricity production plants too early or too fast, Member States are de facto tightening the EU electricity supply-demand balance pushing prices up and increasing the risks of blackouts/brownouts.

The EU is independent in electricity production (with some marginal connections with neighbouring countries, Figure 19) and should not become dependent either on electricity directly or on raw materials. China not only controls the rare earths that are

127 Due to EU unbundling regulation, the study splits production on one side and transportation on the other hand. To take this into account the wording will be Critical Energy Supply and Infrastructure (CESI) and supply will mean both outside and inside the EU

desperately needed in wind and solar electricity production but could be tempted, once it owns energy companies in Europe, to limit investments to make Europe more dependent on electricity produced far away or by tightening the EU supply-demand balance making prices more expensive and the EU *de facto* less competitive.

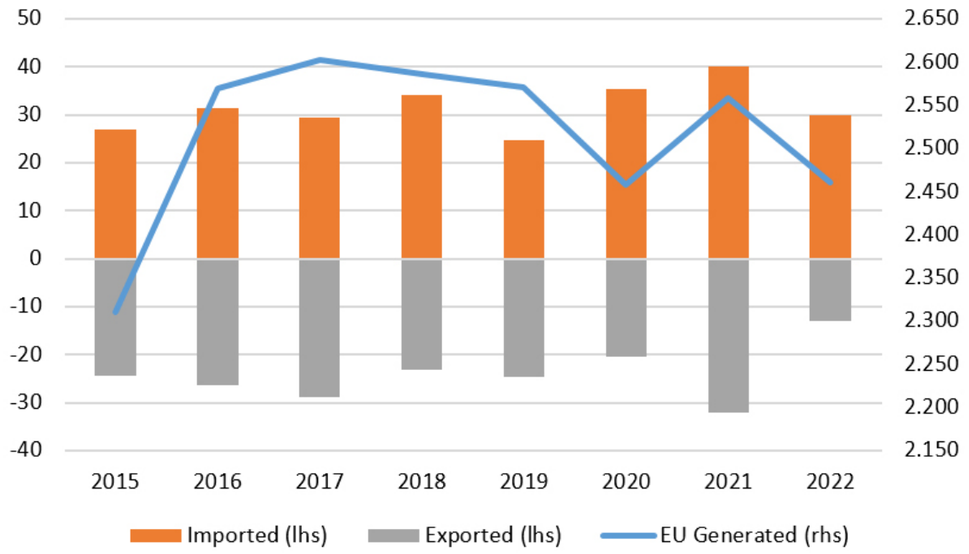


Figure 19 Electricity generated inside the EU, exported and imported[128] (TWh) - Source: energy-chars.info, thierrybros.com

The marginal imports/exports account for less than 2% of electricity generated inside the EU and this should be viewed as optimal. The increased electrification cannot be outsourced to third countries as this could generate unwelcome outcomes as we have seen in oil and gas for example. The only constraint is investment, and this should be monitored on a yearly level to make sure EU production capacity matches EU peak demand.

It is also important to make sure that the available capacity can meet the peak demand. After liberalisation, most of the owners have decided to 'sweat'[129] their production assets to increase their profitability and reduced their capex. Hence the production margin available has been reduced and the Agency for the Cooperation of energy regulators (ACER) adequacy concern has been growing. The European Network of Transmission System Operators for Electricity (ENTSO-E) is tasked with providing winter and summer outlooks to assess the net generating capacity overview and to compare it with the highest expected demand. On top, ENTSO-E's 10-year network development plan is the pan-European electricity infrastructure development plan that looks at the future power system in its entirety and at how power links and storage can be used to make the energy transition happen in a cost-effective and secure way.

128 Flows are netted for each country on a yearly basis. Actual exchanges are much higher

129 In a monopoly situation, the electricity producer tends to overinvest to make sure most risks are covered. In a liberalised world, electricity producers are in competition and tend to make sure their assets are used more, hence the term 'sweating'. This means that overall, the system is less resilient as no-one wants to overinvest to cover very unlikely risks not covered by regulation

The ownership of those assets could be an issue if too many foreign countries that are not considered as allies are investing. A major Chinese player involved is the state-owned company, Three Gorges Corp., established for the management of the eponymous dam, which has rapidly diversified into asset management abroad which led to the purchase of 20.9% of the Portuguese energy company EDP[130]. China Three Gorges Corporation (CTG) 2021 annual report states that: "Closely focusing on the strategic goal of building a world-class clean energy enterprise, CTG continuously accelerated the pace of "going global", and actively participated in the construction of the "Belt and Road Initiative". By the end of 2021, CTG's business covered nearly 50 countries around the world, with a consolidated installed capacity of 11 GW."[131] CTG has installed over 1 GW of renewable energy in Spain[132]. This proves the willingness of China to enter the EU electricity market. Chinese state-owned Power Investment Corporation Limited (SPIC) also owns a few production assets[133] in Germany (wind farm) and Malta (gas-fired power plant and Rooftop PV projects).

Even leaving the opportunity for systemic rivals to finance new power investments could be problematic as seen in the UK with the government removing[134], in 2022, China General Nuclear Power Group (CGN) of its 20% stake in the construction of Sizewell C nuclear plant. And the 75% 0.6 GW Markbygden Ett wind power project in Sweden[135] acquired in 2018 is now facing bankruptcy[136].

Any new purchase in electricity production assets should not be allowed without a full investigation where MoDs should voice their concerns. It is striking to see that foreign companies are more willing to buy EU electricity producing assets than invest in new ones in the EU. In an energy transition where capex is badly needed, new foreign investment could be allowed but acquisition of operating assets by systemic rivals should be severely limited. The same should apply for share in capital structure. Non-OECD ownership in EU companies should be limited to a set threshold avoiding any indirect control. For new investments, systemic rivals should nevertheless be severely scrutinised to avoid any risk later.

Also, MoDs should challenge the concept of the electricity capacity mechanism[137] where a state pays a company for available capacity if this is in the hands of companies owned by systemic rivals like China or Russia as there could be a risk, when supply is short, for the foreign company to renege on its contract in order to engineer an energy crisis inside the EU.

Being independent in electricity is paramount as demonstrated in October 2023 when Israel cut power supply to the Gaza Strip after Hamas attacks. The EU cannot afford to have its electricity being imported from non-EU countries or produced by systemic rivals.

The race to decarbonise the economy,

130 EDP generation capacity is 26 GW (51% renewable, 29% hydro, 11% gas and 8% coal) https://www.edp.com/en/what-we-do/energy-management

131 CTG latest annual report (2021) p.37

132 CTG latest annual report (2021) p.41

133 http://eng.spic.com.cn/2021/whatwedo/internationalpresence/europe/

134 UK removes China from Sizewell C nuclear plant amid tensions https://www.dw.com/en/uk-removes-china-from-sizewell-c-nuclear-plant-amid-tensions/a-63926813

135 CGN buys into Swedish power project https://global.chinadaily.com.cn/a/201807/19/WS5b4fe451a310796df4df756a.html

136 Sweden's largest wind farm faces bankruptcy https://www.arctictoday.com/swedens-largest-wind-farm-faces-bankruptcy/

137 Capacity mechanisms https://www.acer.europa.eu/electricity/security-of-supply/capacity-mechanisms

starting with the energy sector itself, is global. The EU understands that it competes versus not only systemic rivals but also allies and needs to adapt fast. Policy makers should not try to pick the winner but if MoDs believe in some specific technologies, they could help fast-track them via collaboration with research centres.

China should be viewed as a tough competitor that is not only the leading provider of solar panels today but is willing to dominate electric storage technologies going forward. The EU must start, as soon as possible, to think about an electricity storage strategy that encompasses not only the raw materials, the technology but also the operation of storage in the EU. With the 2021 experience of Gazprom not refilling its EU gas storage ahead of the war in Ukraine, electricity storage assets cannot be in the hands of a hostile nation. This condition needs to be implemented for actual storages (dams) as well as future storages (batteries). MoDs have, with the Gazprom gas storage, the perfect example to ask policymakers and regulators to ban hostile nations from entering this strategic sector.

The creation of national regulators at the beginning of this millennium was the cornerstone to avoid political interferences and ill-conceived decisions, but in practice having national regulators leaves each Member State interfering with its national regulator. To avoid further fragmentation of 27 markets and set an EU level playing field, there should only be one powerful EU electricity regulator (as in the banking sector after the financial crisis). Making ACER a true European regulator would lead to a single European regulation applied in the same way in all Member States. In the aviation sector, air traffic control is managed by a single entity (Eurocontrol) that shows that organising the Europe wide exchange of electricity could be done efficiently by a single entity.

ACER should be tasked with checking and reporting ex-post, each year, the electricity generated inside the EU, exported and imported and making sure the marginal imports/exports account for less than 2% of electricity generated inside the EU. If this was to increase, MoDs should voice their concerns at the regulatory level and ask for remedies. This could be part of the ACER Electricity Market monitoring report[138] on top of the adequacy concern. Once an adequacy concern is identified in a Member State, MoDs should be informed, and they can then advocate for some fast-track solutions.

MoDs should, following the weaponisation of gas by Russia, ask ACER to review its "Technical specification for cross-border participation in capacity mechanisms"[139]. The wording 'foreign' relates to a Member State, bidding zone or control area where a capacity provider is located. This Member State, bidding zone or control area is outside the Member State(s) applying the Capacity Mechanism, in which the capacity provider intends to participate."[140]

There should effectively be no distinction between EU companies but foreign companies with capital in the hands of a non-EU state should not be able to participate on the simple basis of EU security. This should be flagged as early as possible to avoid any issues going forward as, for now, no power asset is fully in the hands of a non-OECD entity. This is a very basic first step of any de-risking strategy with systemic rivals: better safe than sorry.

Any purchase by non-EU entities of electricity production assets already in operation should not be allowed without a full investigation where MoDs should voice their concerns. The legal basis for the Commission's action in the field of EU Merger Control is Council Regulation (EC) No 139/2004, the EU Merger Regulation. The EU Merger Regulation prohibits mergers and acquisitions which would significantly reduce competition in the Single Market. In assessing proposed mergers, the Commission considers whether they can be expected to significantly impede effective competition in the EU. In this respect, EU merger reviews solely concern the competition effects of proposed transactions and protection of energy supply and infrastructure security is not, per se, within the remit of EU competition rules. While merger control, and competition policy in general, may indirectly contribute to energy supply and infrastructure security by protecting competition on these markets, the Commission is strictly bound by the framework of the EU Merger Regulation, which does not empower it to intervene against a merger on grounds other than the protection of competition. Nevertheless, EU merger rules also do not stand in the way of Member States who want to take appropriate measures to protect legitimate interests other than those related to competition including public security, prudential rules and or any other public interest, as provided for by Article 21(4) of the EU Merger Regulation, as long as such measures are compatible with EU law. In other words, the EU Merger Regulation foresees that Member States can intervene against a merger to protect their legitimate interests, based on their national laws. Most Member States do have rules in place which submit mergers and acquisitions to foreign direct investment control, allowing them to intervene against transaction based on concerns of public security and public order.

The Foreign Direct Investment (FDI) Screening Regulation (Regulation (EU) 2019/452) has provided, since October 2020, a cooperation mechanism that allows the Commission and Member States to identify, assess and mitigate potential risks for EU security or public order in relation to FDI. The regulation applies to all sectors; therefore, it allows screening FDI in the energy sector and Member States may take action (i.e., impose conditions or, in extreme cases, prohibit the investment) if they conclude that the particular FDI is likely to affect security or public order in their country or in other Member States. The final decision on any FDI is the responsibility of the Member State where the investment takes place. The regulation specifies possible factors for determining whether an FDI is likely to affect security and public order. These factors include the potential effects of the FDI on critical infrastructure (including energy), critical technologies (including energy storage), the supply of critical inputs (including energy) and access to sensitive information. However, Member States are free as to whether they maintain a screening mechanism and if so, whether the mechanism covers the energy sector or energy-related economic activities. On 24 January 2024, as part of the five initiatives to strengthen the EU's economic security, the Commission proposed the revision of the FDI Screening Regulation. This legislative proposal builds on the experience gained by the Commission and Member States with reviewing over 1,200 FDI transactions notified by Member States over the previous three years under the existing FDI Screening Regulation. The legislative proposal aims to address existing shortcomings and improves the efficiency of the system. Therefore, the reinforcement of investment screening in the EU and the cooperation between the Commission and Member States will also increase the protection of the EU's energy sector.

The EU's Carbon Border Adjustment Mechanism (CBAM) entered into application on 1st October 2023. The CBAM will initially apply to imports of certain goods and selected precursors whose production is carbon intensive and at most significant risk of carbon leakage; electricity being one of the six sectors covered. Once the permanent system enters into force, on 1st January 2026, importers will need to declare each year the quantity of goods imported into the EU in the preceding year and their embedded

138 ACER-CEER Market Monitoring Report (MMR) https://www.acer.europa.eu/monitoring/MMR

139 ACER - Technical specifications for cross-border participation in capacity mechanisms https://www.acer.europa.eu/Individual Decisions_annex/ACER Decision 36-2020 on XBP CM - Annex I - technical specifications_0.pdf

140 Ibid. P7

greenhouse gas emissions. They will then surrender the corresponding number of CBAM certificates. The price of the certificates will be calculated depending on the weekly average auction price of the Emissions Trading System (EU ETS)[141] allowances expressed in €/tonne of CO_2 emitted. A review of the CBAM's functioning during its transitional phase (2023-2025) will be concluded before the entry into force of the definitive system. MoDs should take part in this review to make sure that the EU doesn't become more import dependent with this new mechanism. CBAM should not lead to the EU relying more on foreign electricity producers than it does today. CBAM is also covering hydrogen and MoDs should make sure that the EU doesn't perpetuate its gas dependency with hydrogen. Only after an in-depth analysis of what happened in electricity and hydrogen during this transitional phase, could CBAM be potentially extended to other fuels later.

4.3 Critical EU energy infrastructure

Following EU unbundling in the early 2000s, electricity and gas infrastructure are separated from the production and commercialisation sides. This was done to provide a level-playing field for competition between national incumbents and new players. This means that electricity and gas infrastructure must be analysed separately from the production side.

4.3.1 Electricity infrastructure

The main foreign structure active in asset purchases in the field of transmission and power distribution in Europe is the state-owned State Grid Corp. of China (SGCC), covering 80% of the country, giving it unparalleled economic investment capabilities in the sector of electrical operators (Figure 20). State Grid acquired 25% of Portuguese REN in 2012 giving it a de facto ENTSO-E membership. In 2014, SGCC's next move was in Italy, where it partnered with the Italian state in buying 35% of the CDP Reti fund from the Italian Cassa dei Depositi. Thanks to this important participation, SGCC obtained a blocking minority over the activities of SNAM (gas network operator), Italgas and Terna (electricity transmission network operator)[142]. SGCC also continued its development in the Greek networks by acquiring 24% of Public Power Corp. to the Greek state in 2016 and the purchase of 75% of the private group Copelouzos, becoming de facto the key player in transport and distribution in Greece. In 2014, Shanghai Electric Power[143] signed[144] a deal with the Maltese government to acquire 33.3% of the local utility Enemalta[145] as well as a 90% in the Delimara 3 gas-fired power plant[146]. This could lead to creative accounting[147] with one of the partners becoming weaker due to loss facing business. **In a broader security-based assessment, China is therefore acquiring (directly and indirectly) the same extensive knowledge of the whole European energy network that Russia had in gas!**

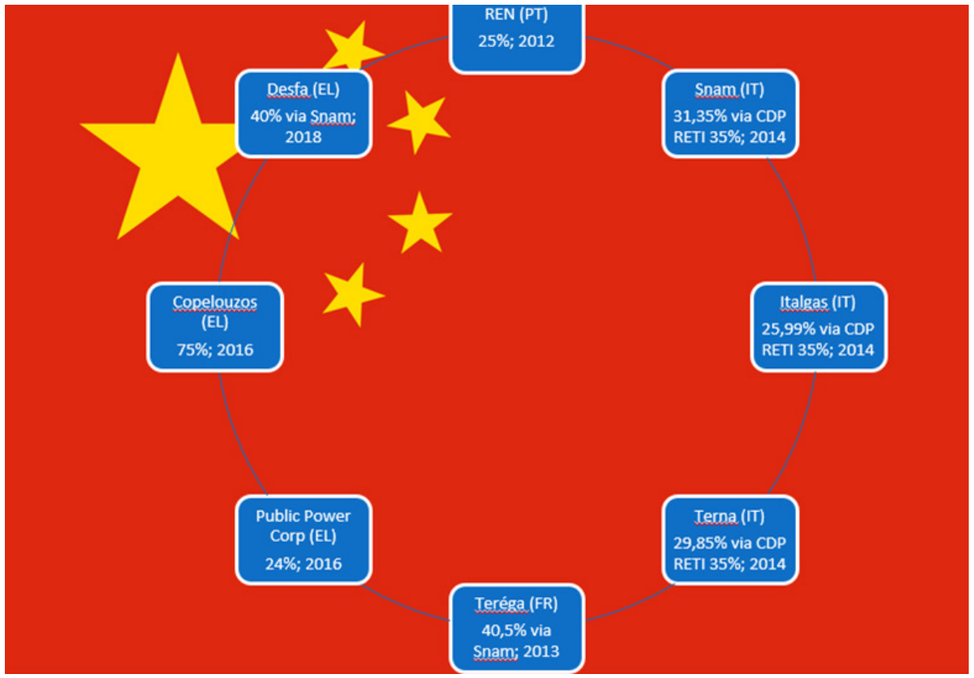


Figure 20 China's SGCC many direct and indirect energy acquisitions in the EU
Source: thierrybros.com

On and off-grid storage is a key to integrating renewable into the electrical systems. High performance battery technologies are a must to solve the problems of intermittency and availability of production inherent to renewable energies. Smart grids are also an important element for the future of electricity. The EU should make sure that systemic rivals are not allowed to invest in or control new seasonal electricity storages, once the technology is readily available. When this would become available, policymakers should keep in mind what has been painfully achieved with gas storage (minimum storage requirement) and request the same for seasonal electric batteries.

4.3.2 Gas infrastructure

Europe learned the hard way that it cannot put critical infrastructure in the hands of non-friendly state-owned companies. Russia's Gazprom had until recently the best analysis on the EU gas situation thanks to its high market share (up to 40% of EU demand prior to COVID) and its cooperation with the European Network of Transmission System Operators for Gas (ENTSOG). In 2021, Gazprom didn't refill its EU gas storage. This puzzling move in fact turned out to be the first step of weaponization of gas by Russia, just a few months ahead of the Ukrainian war. Germany did nationalise those assets after the beginning of the war in Ukraine. Those pipes and storage assets

141 EU Emissions Trading System (EU ETS) https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets_en

142 https://www.cdp.it/sitointernet/en/cdp_reti.page

143 Shanghai Electric Power is a subsidy of China state-owned Power Investment Corporation Limited (SPIC), one of China's five power generation groups http://eng.spic.com.cn/2021/whatwedo/internationalpresence/europe/

144 https://www.ccmalta.com/insights/news/china-power-investcorp-in-largest-fdi-in-malta?lang=hy-AM

145 https://www.enemalta.com.mt/about-us/

146 https://cdn-others.timesofmalta.com/fce759c0a91a01f83a5f9cfdf01ac0b5f3918cc6.pdf

147 Enemalta posts €35 million losses while its Chinese partner turns a profit | The Shift News - https://theshiftnews.com/2023/01/25/enemalta-posts-e35-million-losses-while-its-chinese-partner-turns-a-profit/

should not be sold to actors outside the EU. China has, in 2019, unbundled its pipe[148] company that could, in theory, bid for EU gas critical infrastructure. This should not be allowed without a full investigation where MoDs should voice their concerns.

The immediate resulting price spikes from June 2021, without any need of political intervention, have efficiently led to LNG flows reconfiguration from Asia to Europe and to demand adjustments in both regions. As all the regulation was in place, this happened smoothly and efficiently with some regasification terminals operating even above nameplate capacity at some stages.

The EU Commission also provided a very useful regulation since the starting of the Ukrainian war, by mandating EU gas storage to be filled at 80% by 1st November 2022 and at 90% by 1st November each year thereafter. Ahead of each winter, this regulation provides a buffer in case of any additional shocks. This is in line with the IEA strategic oil stocks that have been implemented since the 1970s. The drop in Russian gas witnessed in 2022 vs 2021 amounts to a worldwide supply disruption of less than 2%. But as gas markets are regional, for the EU, this amounted to 22% of its demand. For the EU, this gas disruption was therefore higher than the IEA definition of a severe oil disruption that entails a loss of 7% of world supply.

After the start of the war in Ukraine, some European nations launched new LNG receiving infrastructure. Germany became an LNG importer in early 2023. Nevertheless, having the necessary infrastructure in place without corresponding long-term supply commitments does not necessarily guarantee European security of energy supply.

4.3.3 Recommendations and way ahead

The electricity grid must be adapted to the increased risk of severe storms. MoDs should liaise with their respective national regulator to make sure that, after each major storm that affects their specific locations, technical solutions are implemented like moving overhead power lines underground or improving grid interconnections or having local batteries. The regulator would then adapt the remuneration of the transport operator for this grid resilience to be better remunerated than the weak grid points that suffered damages.

Making ACER a true European regulator would lead to a single European regulation applied in the same way in all Member States. The same is valid for the transmission system operators in charge of balancing the system. Their competences are limited to regional or national territories when interconnections have created an almost true European market as shown by all exchanges taking place between Member States and beyond. The limitations placed by the national regulators on their Transport System Operator is a major obstacle to the creation of a true European market and to the optimisation of the system. MoDs should push for a single energy regulator with increased power[149]. MoDs should be represented at ACER level as both a particular buyer and an entity that can provide views when dealing with security of energy supply.

MoDs should have a say when the EU Commission or Member States deal with controlling acquisition of energy assets by systemic rivals or adversaries. As seen with Gazprom's storage in Germany, this should not have been allowed from the beginning. This is going to be extremely important when dealing with electricity storage. The EU should make sure that systemic rivals are not allowed to invest in or control those strategic assets.

148 China Oil and Gas Pipeline Network Corp., commonly referred to as PipeChina, was founded by the Chinese government in December 2019 to centralize control of the country's oil and gas pipelines

149 National regulators have to ensure the protection of consumers, while the EU wide regulator has to regulate and monitor the European market

4.4 Producers of coal, oil and gases

4.4.1 Exiting coal

The EU Green Deal strategy aims to fast-track coal phase out, but coal still represents 12% of its energy mix, (Figure 21) vs 27% at the global level.

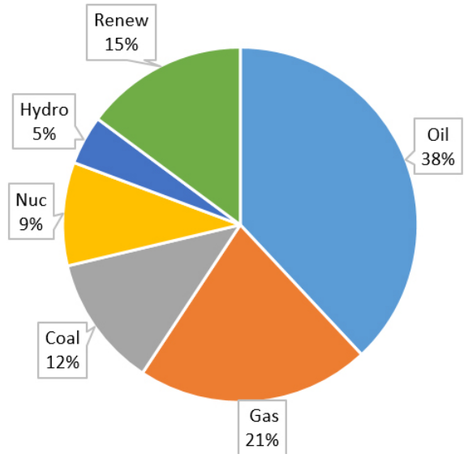


Figure 21 EU 2022 Primary energy mix.
Source: EI Statistical Review 2023

Since 1970, the share of coal has steadily declined from 35% to a record low of 11% in 2021, just before the energy crisis hit. Thanks to changing its primary energy mix, the EU managed to spare 57% CO_2 emissions during this period compared to what it would have emitted had the energy mix stayed the same (Figure 22).

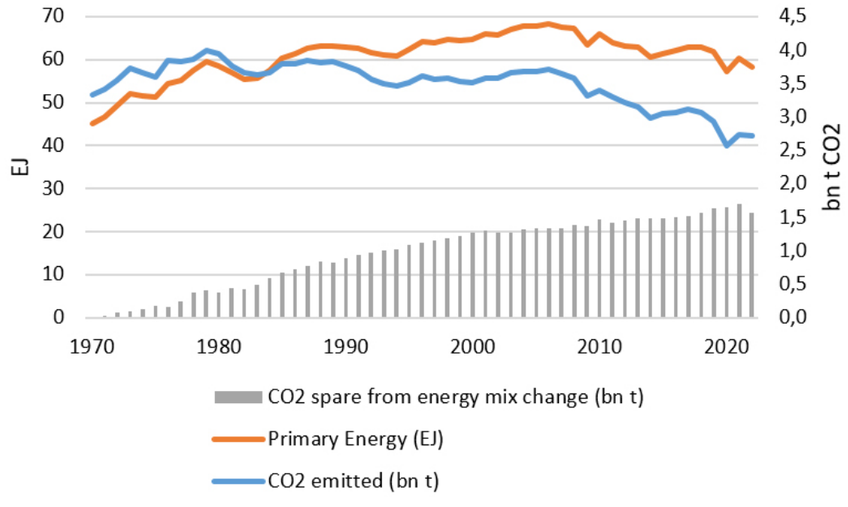


Figure 22 EU Primary energy mix and CO_2 emissions from energy - evolution 1970-2022
Source: EI Statistical Review 2023

This proves that any energy transition is a lengthy process that needs to be analysed over decades.

4.4.2 Dealing with old and new risks in oil

It is worth remembering that, as for all commodities, in oil it is the marginal or additional barrel that sets the price for all barrels. There is therefore an asymmetry in prices. Too little supply/too much demand leads to skyrocketing prices while too much supply/too little demand provides very cheap prices (and even negative prices at some stages as seen during COVID). In oil, there is no relation between the cost of production (as low as 10 $/b for conventional oil in Saudi Arabia or Russia to above 50 $/b for shale oil or deepwater oil) and the international prices (c. 90 $/b) as some major producers are part of a OPEC cartel which aims to increase their oil rent thanks to curtailing exports.

For both markets and security of supply what is paramount is the amount of oil spare production capacity (Figure 23). Spare capacity is commonly defined as the volume of production that can be brought on within 30 days and sustained for at least 90 days. Saudi Arabia, the largest oil producer within OPEC and the world's largest oil exporter, historically has had the greatest spare capacity. Saudi Arabia has usually kept more than 2 mb/d of spare capacity on hand for market management. Private companies do not hold any spare capacity as this is very costly (the investment is de facto stranded) and their shareholders would not tolerate such move[150].

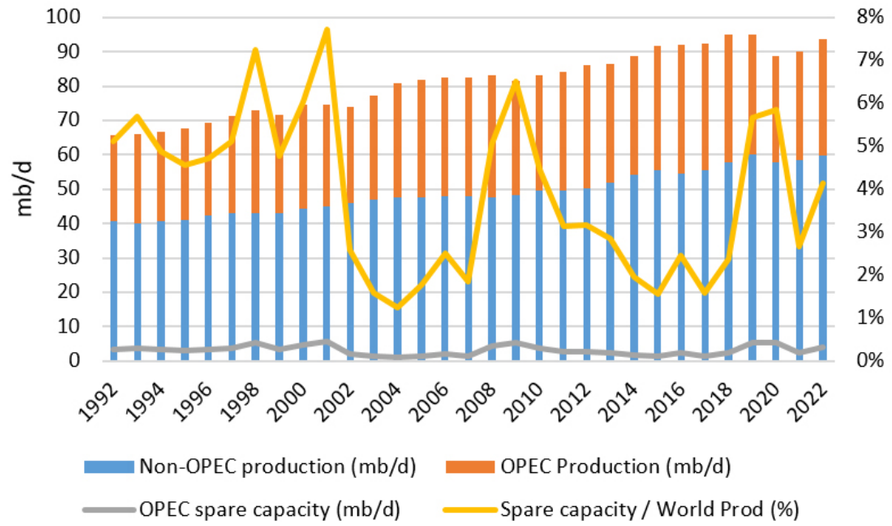


Figure 23 Oil spare production capacity. Source: EI Statistical Review 2023, US DoE

The % of spare capacity compared to the total effective oil production has moved inside a narrow range from 1 to 8%. This could be viewed as de facto storage, but this is in the hands of a cartel that might have a geopolitical agenda.

The International Energy Agency (IEA) Net Zero Emission by 2050 Scenario[151], published in May 2021 and updated in September 2023[152], had negative consequences for the financing of fundamentally necessary hydrocarbon projects after it stated in its "Summary for policymakers" that there should be "no new oil and gas fields approved for development". This led the Western banking industry to conclude that financing hydrocarbon projects was deemed unacceptable to OECD political leaders. Given the completely impractical nature of the IEA's stance, it was only natural that the premise started to unravel quickly.

1. The first to move away from this IEA scenario was US President Joe Biden when he repeatedly asked domestic oil companies to boost production in 2021 to mitigate the on-going high prices. In his 2023 State of the Union Address, President Biden baldly stated "We're going to need oil for at least another decade…and beyond that."
2. Subsequently, following Russia's illegal war against Ukraine and the reduction of oil and gas imports to Europe, Norway's role as a key energy supplier for Europe became further elevated. Hence, the Norwegian Ministry of Petroleum and Energy announced[153] its intention to offer a record-level of oil and gas exploration areas in the Arctic as part of the 2023 concession round.
3. Finally, the UK Prime Minister stated in July 2023 that "hundreds of new oil and gas licences will be granted". And this was followed by The North Sea Transition Authority granting consent for the development of a new field[154] in September 2023 and 27 new licence offers for oil and gas exploration in the North Sea in October 2023.

So, within 2 years, 3 major IEA hydrocarbon producing countries have turned their backs on this IEA report, while the others (mainly importers) must provide billions of dollars of subsidies to their citizens and industries that cannot afford the record energy prices. It is clearly time to start to question the validity of this IEA report.

The IEA 2021 net-zero scenario describes well the increased OPEC market power in oil with "supplies become increasingly concentrated in a small number of low-cost producers. OPEC's share of a much-reduced global oil supply grows from around 37% in recent years to 52% in 2050, a level higher than at any point in the history of oil markets." This is something OECD countries should be extremely worried about. The IEA should keep to its mandate[155] and its business-as-usual energy analysis that was based on "Current Policies Scenarios that assume only existing policies in its long-term energy forecasts."

The reduction of Western finances to upstream oil projects drastically reduced the competitive landscape and is now leaving the world with a tighter oil supply-demand balance.

4.4.3 Recommendations and way ahead in oil

The old risk of spare production capacity exclusively in OPEC+ hands is there to stay and cannot be addressed by any market / finance solutions.

150 There is also a risk that competition authorities in the EU and the US could view this as market manipulation

151 Net Zero by 2050 IEA - https://www.iea.org/reports/net-zero-by-2050

152 Net Zero Roadmap: A Global Pathway to Keep the 1.5 °C Goal in Reach - 2023 Update - https://iea.blob.core.windows.net/assets/6d4dda5b-be1b-4011-9dad-49c56cdf69d1/NetZeroRoadmap_AGlobalPathwaytoKeepthe1.5CGoalinReach-2023Update.pdf

153 A continued responsible and long-term management of the oil and gas resources - https://www.regjeringen.no/en/aktuelt/a-continued-responsible-and-long-term-management-of-the-oil-and-gas-resources/id2960540/

154 The Rosebank field to progress in the UK - https://www.equinor.com/news/20230927-rosebank-field-to-progress-in-the-uk

155 The IEA was created to help OECD countries co-ordinate a collective response to major oil supply disruptions

MoDs do not share green NGOs views that have a hidden agenda of curtailing fast hydrocarbon supply to force the economy to adapt (by degrowth). MoDs, especially since they rely on oil products for transportation, should push the EU and their respective Member States to be more pragmatic vis-à-vis oil. The smart way to achieve a successful energy transition is to push oil demand down first, either through efficiency, sobriety, pricing CO_2 emissions or electrification, and not to constrain supply.

Thanks to its Emissions Trading System (EU ETS), the EU has been at the forefront of putting a price on CO_2 emissions. This should be the best mechanism to push oil demand down in the EU. It has been a very slow process since its inception in 2005 but the 2021 "fit-for-55" package with reduced free allowances and increased sectors covered should now help.

The narrative on upstream oil as a stranded asset, as it developed since 2021, has tightened the global supply and increased both price and OPEC power. Higher oil prices have a recessionary effect in the EU and boost oil producers' profitability. The EU and Member States should further tighten the EU ETS to push CO_2 prices higher.

MoDs should remind their respective states that indirectly interfering in the financing of privately owned upstream hydrocarbon is both increasing the oil rent for producers and the power of OPEC as analysed in the IEA net zero scenario.

The rerouting of Russian oil away from the EU where it is embargoed to China and India with Russia providing on top a price discount should be viewed in the global geopolitical arena and not just as a simple reshuffling of voyages along a supply chain. This helps Russia to keep countries willing to continue to interact as the price discount is materially significant. It could also in the medium term pose competitive issues in the EU that has to pay international prices for oil and top prices for gas, while some Asian countries are benefiting from the Russian discount on oil.

To remind EU policymakers of OPEC+ power, MoDs should have a seat at the table when the EU, the G7 and the IEA draft position papers that have an impact on world energy supply/demand. MoDs should challenge impossible-to-follow scenarios.

4.4.4 Increased risks in gas

Russia started, in the third quarter of 2021, limiting gas pipeline exports to Europe[156] and not refilling its EU gas storage capacity ahead of the 2021/2022 winter. The EU was caught off guard with low gas storage level at the end of summer 2021. The invasion of Ukraine by Russia, in February 2022, further impacted Russian (pipeline) gas. Russian pipeline volumes massively dropped from more than 160 bcm/y pre-2020 to 26 bcm in 2023 (Figure 24), allowing Gazprom to still sell contracted gas to Austria, Croatia, Greece, Hungary, and Slovakia. REPowerEU is targeting to reach zero before the end of this decade. The EU has not eliminated its Russian gas dependency. Gazprom reduced its exports that used to represent 40% of EU demand in 2019 down to 7% but the market is using Russian LNG to mitigate part of this. Hence the EU is still 15% dependent on Russia to satisfy its demand. The EU needs to wait for extra LNG from the US and Qatar to benefit from a less tight supply-demand balance and being able to implement an embargo on Russian gas.

156 Gazprom reduced sales on its Electronic Sales Platform, with volumes falling to 0 from October 2021

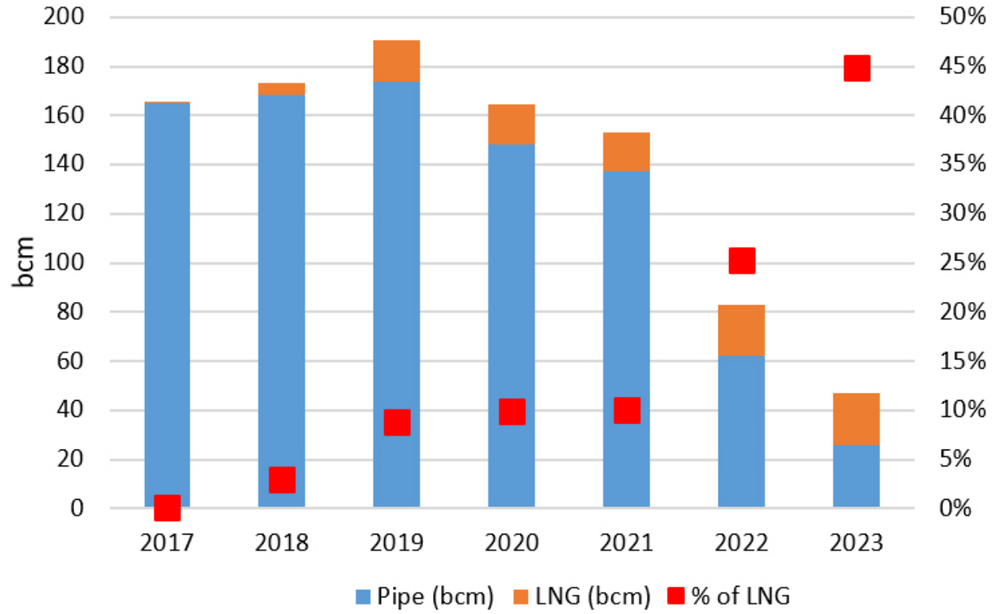


Figure 24 Russian gas exported to the EU - Source: Gazprom for pre-2021 data, Entsog, GTSOU, thierrybros.com

It is worth underlining that this Russian pipeline gas was mostly contracted under a long-term basis. It can be estimated that between 2021 and 2023, the EU lost at least 110 bcm/y of long-term contracted gas with Gazprom (Figure 25). Long-term contracts are needed to make sure European citizens and industries can access affordable and secure gas. To improve security of gas supply, some long-term contracts need to be resigned to replace those lost volumes. If the EU wanted to only revert to the position it had prior to the war in Ukraine in terms of contracted gas, it would need to contract on a long-term basis between 88[157] and 110 bcm/y (65 to 81 mtpa). Failure to do so will leave the EU market in the hands of volatile spot markets where portfolio players have a vested interest in maximizing their profit. In addition, China has deliberately over contracted gas, and will be able to (or not) swing LNG supply to the EU.

Failure of EU utilities to contract are pushing industries[158] to do so as they cannot operate profitably in a highly volatile premium energy market. 40% contracted volumes are too low for security of supply. This is a very good example for MoDs, as major end users, to step in as the actual system does not guarantee security nor affordability of supply. It is unlikely that MoDs should start to contract directly for oil or gas as it is a cumbersome process that needs to deal with international risks.

157 Assuming a drop of 20% of overall demand translate in 20% less contracted volumes

158 Cheniere and BASF Sign Long-Term LNG Sale and Purchase Agreement: https://lngir.cheniere.com/news-events/press-releases/detail/284/cheniere-and-basf-sign-long-term-lng-sale-and-purchase

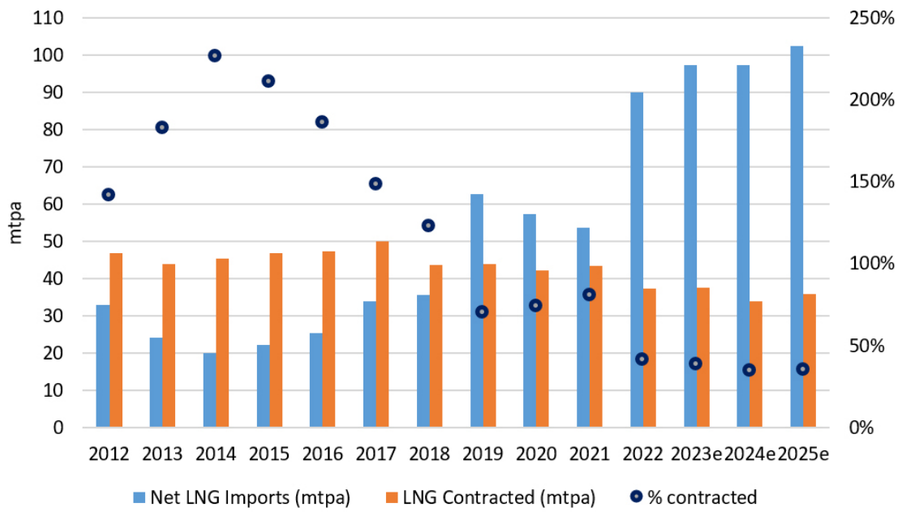


Figure 25 EU LNG demand vs contracted by utilities and industries - Source: thierrybros.com

Like in oil, there used to be spare production capacity in gas. But since the weaponisation of gas by Russia from 2021, there is de facto no spare production available (Figure 26).

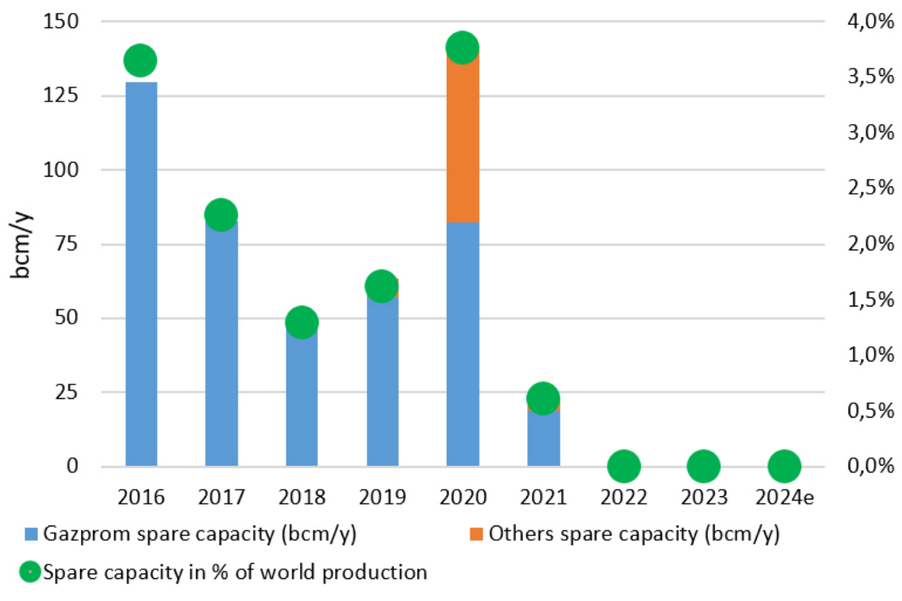


Figure 26 Gas spare production capacity - Source: thierrybros.com

Hence the EU faced an acute energy crisis in 2021/2023 as it could not turn to alternative suppliers that had spare capacity. The EU had to overbid LNG cargoes. The overall oil and gas system is de facto having 1/3 less spare capacity; the only spare production capacity left for all energy is OPEC+ oil spare capacity that amounts to around 1% of total worldwide energy consumption!

With no spare gas production capacity left, it is important to analyse what the Chinese could do now to systematically weaken Europe. 2022 has been the year when China has overtaken the EU as the 3rd largest world gas market (after the US and Russia, both exporters) (Figures 27 - 29).

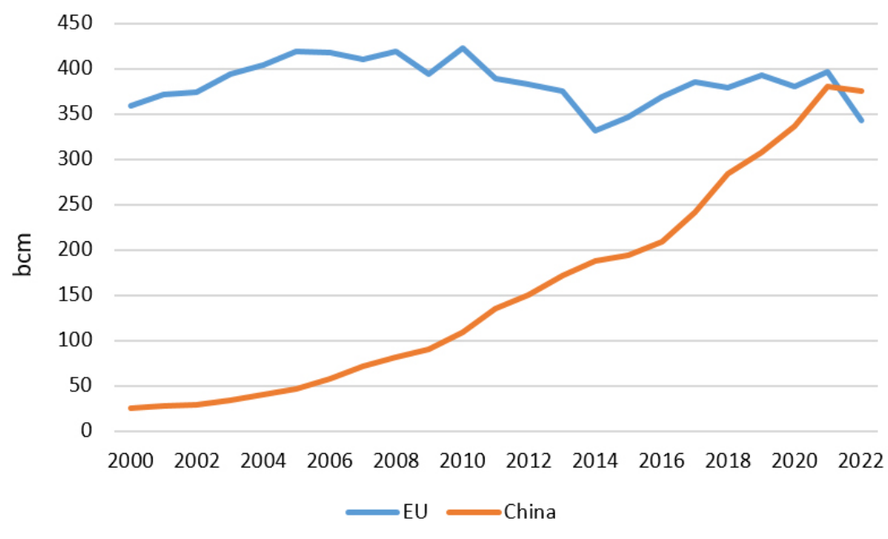


Figure 27 Evolution of EU and Chinese annual gas demand - Source: EI Statistical Review, thierrybros.com

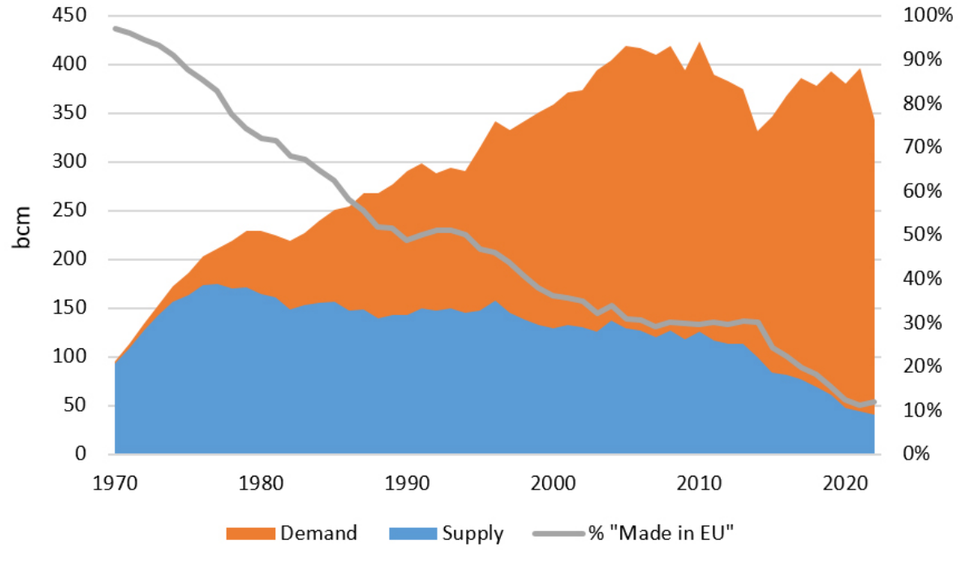


Figure 28 Evolution of EU gas supply-demand - Source: EI Statistical Review, thierrybros.com

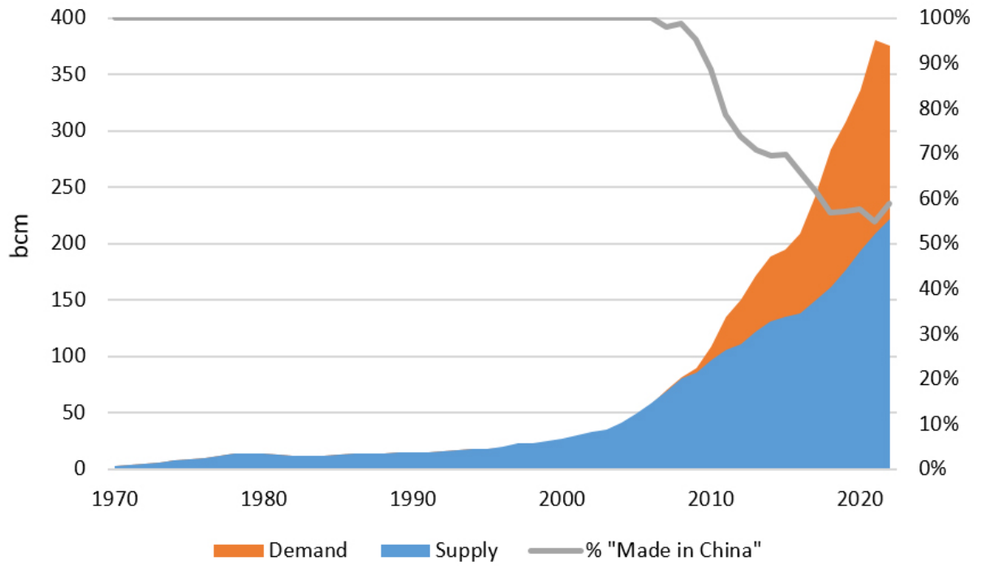


Figure 29 Evolution of China gas supply-demand - Source: EI Statistical Review, thierrybros.com

The EU is bound to continue to be more gas import dependent. China has also become more import dependent since 2000 but, to mitigate this, many exploration programmes are underway in China and domestic proven reserves are rising, accounting today for 4.5% of the world. Chinese gas security of supply comes from a strategic long-term thinking about diversification. China gets pipeline gas from Central Asia and from Russia and LNG from around the world. China is now not only the biggest LNG buyer since 2021 but the country that signs the most long-term contracts. As European buyers are shy to sign those contracts (due to a limited visibility on EU gas demand post 2035), if EU gas demand stays at those level, Europe could become dependent on China for its LNG. The LNG would still be produced by the top 3 producers (US, Qatar, Australia) but will be long-term contracted by China that could decide or not to resell it to Europe. China is doing this for 3 reasons: 1. security of supply/diversification; 2. economically China wants to make sure that going forward Europe will have to pay a premium for its gas vs China and 3. a geopolitical agenda that could be used if needed. The worrying factor is that, as its economy was slowing down in 2023, China not only continued to contract gas but is also building its LNG presence in Europe with:

- PetroChina having underwritten part of the Dutch regasification Gate's capacity expansion[159]
- Starting up[160] or expanding trading desks in London, UK

On top of this, as discussed earlier, China SGCC controls directly or indirectly stakes in gas infrastructure in France (Teréga), Greece (Defsa, Copelouzos), Italy (Snam and Italgas) and Portugal (REN). This tends to prove that China absolutely wants to be over-contracted to play a role in Europe. European demand for LNG has risen sharply during the war in Ukraine as the region scrambled to replace gas that came from Russia through pipelines. Faced with less pipeline gas altogether, a race between international energy groups to lock in LNG is driving investment in a range of export projects. But unfortunately, as Europe has been shy of signing long-term LNG contracts it will rely on international portfolio players that will sell LNG to Europe if it is profitable. As for the Chinese, they could have an added geopolitical aim: making sure Europe always pays a premium vs Asia for gas to negatively impact European competitiveness.

159 https://www.gateterminal.com/en/nieuwsberichten-archive/bp-and-petrochina-international-london-underwrite-gates-capacity-expansion/

160 China LNG buyers expand trading after adding more US, Qatari contracts https://www.reuters.com/business/energy/china-lng-buyers-expand-trading-after-adding-more-us-qatari-contracts-2023-08-21/

4.4.5 Recommendations and way ahead in gas

Spare capacity in gas production is gone and isn't going to materialise again any time soon as new projects will only slowly rebalance the global supply-demand balance. The 2022 EU regulation, requesting to fill up gas storage ahead of each winter, is a smart way to provide EU customers with some security and flexibility in front of this tight supply. In the medium term, gas storages are still going to be needed until seasonal batteries can be deployed in a cost-effective way.

The Churchillian view that security of supply lies only in diversification is shared by the European Commission, but some Member States are still too close to the industry that only views prices and therefore has little incentive to pay for the premium of security of supply as was the case in Germany in gas prior to the Ukrainian war. Here again the latest geopolitical development should provide MoDs the ability to support the Commission's initiatives.

To avoid EU dependency on gas to start in favour of China, MoDs should have a seat at the table when the EU, the G7 and the IEA draft position papers that have an impact on world gas supply/demand. The recent willingness by Japan to foster LNG worldwide projects could be viewed as some move back to pragmatism by a highly energy-dependent country… The Japanese April 2023 G7 Climate, Energy and Environment Ministers' Communiqué[161] clearly states "investment in the gas sector can be appropriate to help address potential market shortfalls provoked by the crisis, subject to clearly defined national circumstances, and if implemented in a manner consistent with our climate objectives and without creating lock-in effects… We expect that the IEA's functions and role in gas security will be further strengthened through dialogue between gas producing and consuming countries taking into account longer-term perspectives."

MoDs should challenge impossible to follow scenarios like the 2022 ENTSO-G Ten-Year Network Development Plans where "on the demand side this means a strong commitment to reduce energy consumption through (…) a decrease in individual mobility"[162]. If the scenario cannot explain how this is achieved, it should not be viewed as acceptable. MoD should be able to challenge any scenario hypothesis to check that it is reasonable.

In October 2023, Singapore decided[163] to centralise gas purchases to boost energy security. The nation will aggregate demand from power generating companies, which will create economies of scale and allow Singapore to negotiate more favourable gas contracting terms and procure fuel from diverse sources. This is a fundamental shift toward gas procurement. This is believed necessary to create a more stable

161 https://www.env.go.jp/content/000127828.pdf

162 P 10 TYNDP 2022 Scenarios Final Storyline Report, April 2021 - https://2022.entsos-tyndp-scenarios.eu/wp-content/uploads/2021/09/entsog_entso-e_TYNDP2022_Joint_Scenarios_Final_Storyline_Report_210421.pdf

163 Singapore Centralizes Gas Purchases to Boost Energy Security - https://www.bloomberg.com/news/articles/2023-10-23/singapore-to-centralize-gas-purchases-to-boost-energy-security

and secure power system that will ultimately benefit the consumers. This is in line with the EU Energy Platform[164], launched in 2022. The platform helps to coordinate EU demand with external gas suppliers and to match potential buyers with sellers.

It is of particular importance to see that, in the middle of a tough commercial LNG dispute between Western companies, both parties[165] asked the US-EU Task Force on Energy Security[166] to intervene. This proves that energy security is off market limits and that going forward, if the Chinese risk could materialise, a defence section could be added. Hence, on the EU side, this group should be extended to include a MoD representative.

4.4.6 Hydrogen as a potential energy vector, but later

The EU pushed very hard in 2019-2022 for hydrogen (H_2) to become a green energy vector. On the R&D side, this is not a failed option, but, on the supply-demand side, there is a major difference between theory and practice. Fostering a hydrogen market is in the remit of the Commission. MoDs should watch latest technological developments to be ready to adapt if and when needed.

MoDs should warn EU institutions of the risks of producing H_2 in unstable countries. Either H_2 is to become a decarbonised fuel and needs to be produced in the EU or it won't become a fuel and production location is irrelevant; the EU cannot start a H_2 policy assuming this is going to be produced abroad!

Even if it could be possible to repurpose gas pipes into hydrogen ones, this looks much more challenging for the LNG chain as it would require massive technological innovation and close collaboration between producers, shippers and consumers to develop a stable, supportive and adaptive regulatory framework. Some scenarios hope for green hydrogen produced in the Global South to be consumed in the EU. This looks improbable as it would be easier for the renewable electricity to be consumed locally and for the gas to continue to be exported to the EU either via existing pipelines or liquefaction plants. The latter would allow countries like Algeria and Egypt and potentially others to keep both for their population the growing renewable production and the financial gas rent, instead of risking billions of dollars in unproven technologies that would not solve their thirst for more energy.

In 2023, with a new Green Deal Chief, the EU Commission is becoming more pragmatic and appears to be waking up now rather than later to the fact that its hydrogen targets outstrip reality. Nevertheless, hydrogen is now one of the six sectors targeted by the new CBAM and MoDs should take part in the review of the CBAM's functioning during its transitional phase (2023-2025) before the entry into force of the definitive system.

4.4.7 Minimum impact of critical materials for the energy transition

Many reports are available on this subject as the world needs to rethink its critical materials strategy. In particular, the European Commission mapped in 2023 the list of critical raw material with rare earths needed for energy. The Commission proposal for a Critical Raw Materials Act is a comprehensive response to the risks of critical raw materials supply disruption and the structural vulnerabilities of EU critical raw materials supply chains. The Critical Raw Materials Act will ensure EU access to a secure and sustainable supply of critical raw materials, enabling Europe to meet its climate and digital objectives, keeping EU industrial competitiveness, and ensuring the well-functioning of the single market.

Critical material supply has, for now, a minimum impact on energy security and dependency risks and supply dynamics differ from those of fossil fuels, given vastly different characteristics and patterns. A prominent concern is that energy transition entails trading dependency on fossil fuels for dependency on critical materials. Such an analysis is outside the scope of this study.

4.5 Energy reseller/supplier

As MoDs contract via resellers, the final link between energy and MoDs is the reseller. For oil and oil products, MoDs have a long experience of markets, and some even implemented hedges to be able to forecast costs of those volatile fuels bought on international markets.

To kick start the electricity liberalisation process, largely opposed by traditional monopolistic producers, Member States allowed suppliers with no production to address consumer needs. The assumption was that as production takes time to be built, a few years down the road all suppliers will then produce the required electricity. This not only failed as many suppliers did not bother to even consider becoming producers, but it also gave traders exorbitant power. With the energy crisis that is hitting Europe since 2021, leading to many small resellers gone bankrupt, some MoDs even decided to build their own energy generation capacity to bypass energy resellers.

For electricity, if MoDs were making sure more EU supply was available, the likelihood of both blackouts and skyrocketing prices would be vastly reduced. This could be done by using the flexibility of EU market that allows signing power purchasing agreements (PPAs). In their respective states, by signing PPAs with utilities willing to invest in new supply, MoDs will not only provide a market information on their increased demand but foster new decarbonized supply in line with their state mix (renewable, hydro, nuclear).

This energy crisis also led Member States requesting the EU Commission to revise the EU electricity market design that was not fit for purpose any longer. This has been a very difficult process, as for all commodities, in electricity it used to be the marginal electron that sets the price for all MWh and this without considering if the additional electron was decarbonised or not. This change in electricity market design is going to be far reaching with Member States reasserting their power on this vital part of their economy. With the French nationalisation of EDF and German capital injection in Uniper in 2022[167] and the 2023 German loan to Siemens[168] States are back in the driving seat.

As energy markets face an inflexion point away from full liberalisation to more state control, MoDs have an ideal position and can push what is the most relevant for them. It might not be to focus themselves on producing decarbonised electricity or signing long-term gas contracts with foreign suppliers. It could, instead, be to part-

164 EU Energy Platform https://energy.ec.europa.eu/topics/energy-security/eu-energy-platform_en

165 https://www.linkedin.com/posts/venture-global-lng-inc._cp-activity-7129104712712290304-RiH_/

166 https://energy.ec.europa.eu/topics/international-cooperation/key-partner-countries-and-regions/united-states-america_en

167 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0651

168 German government grants Siemens Energy a loan guarantee to help secure the company - https://apnews.com/article/germany-siemens-energy-government-guarantee-24bbcf3b974f18f87cadc9737cfd273f

ner with the local utility in a win-win position with the blessing of the state. MoDs should request that the domestic 'supplier of last resort'[169] has an obligation to provide a contract to its domestic MoD with electricity and gas. Two designs could be envisaged: either an increased obligation on the supplier of last resort or an obligation on both sides: MoDs having no choice but to contract with the supplier of last resort. The first option could still allow MoDs to shop around for cheaper contracts. If properly designed the second option could be a win-win for both parties with states providing to their designed 'supplier of last resort' a minimum amount of guaranteed volumes outside market competition.

In the EU where security of energy supply would have to be redefined, MoDs should consider contracting exclusively with suppliers of last resort. Resellers with too little production or non-EU foreign entities should be disqualified. This could potentially increase the bill but that could be a win-win situation between selected suppliers and MoDs. Instead of a burdensome assessment of a utility's ability to meet security of supply requirements, MoDs could prefer to sign with the domestic 'supplier of last resort' for gas and power.

4.6 Security of energy supply

4.6.1 Cost of energy security and affordability

If energy security is defined as the uninterrupted availability of energy sources at an affordable price, it is interesting to assess the cost of failure. In front of skyrocketing energy prices, €390bn (or 2.5% of EU GDP) is estimated[170] to have been effectively spent in 2022 at the EU and Member States level (Figure 30) to reduce the burden of record high energy prices by direct subsidies without taking into account the German Uniper €34bn capital injection nor the French EDF €9bn nationalisation. If we assume that the €124bn dedicated to renewable, nuclear R&D and energy efficiency are long term subsidies to fast track the energy transition, these leaves €266bn (or 1.7% of EU GDP). This represents the failure of properly addressing EU security of energy supply. Any mitigation measures for the future should be compared with this cost of failure.

169 Supplier of last resort is used in EU directives. Some countries have also a default supplier. It is not unusual that the default supplier also acts as the supplier of last resort, or vice versa

170 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0651

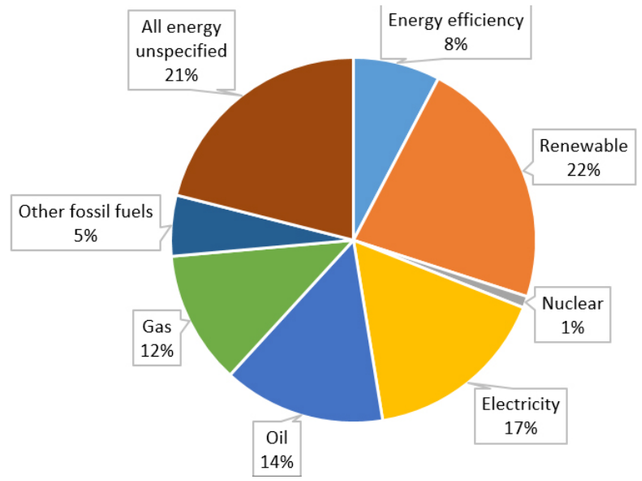


Figure 30 Split of EU 2022 €390bn energy subsidies - Source: 2023 Commission Report on Energy Subsidies in the EU, thierrybros.com

The 2022 subsidies amounted respectively to 55 €/MWh, 15.2 $/b and 4.2 $/Mbtu for electricity, oil and gas. This is more than the effective cost of production.

4.6.2 Who should be in charge of security of energy supply?

The unbundling of supply and infrastructure has made looking into security of energy supply a more fragmented problem. As only Member States can have a complete view of the energy chain, MoDs should liaise with their respective Energy Minister to rethink the security of supply by adding their non-market views.

In the event of a severe oil supply disruption[171], the collective OECD security of supply is managed by IEA thanks to strategic stocks in each country. A severe disruption could be viewed as a loss of more than 7% world supply. For smaller hiccups, the market is best suited to efficiently balance day-to-day supply and demand as oil is a fungible commodity than can be shipped all over the world. With electricity storage not readily available (except with dams), the security of supply was done by ad-hoc silos from strategic oil stocks to commercial gas storages. Recent events show the inter-fuels competitions leading for example some industries to having to switch away in 2022 from too expensive gas into less expensive fuels (coal or diesel).

Before the liberalisation of EU energy markets, security of gas supply was taken care of at each state level by its respective domestic utility. Since then, security of supply was pushed more and more to markets for efficiency and cost cutting measures. Security of supply can be, up to a certain level of disruption, left to markets. But above a certain level, this must be dealt with by non-market mechanisms. The EU is the relevant geography/entity to deal with gas supply disruption as pipeline gas is not a fungible commodity (contrary to LNG).

After the Russian gas weaponisation, the EU had to turn to LNG to keep the lights on (Figure 31). The massive demand destruc-

171 Oil security – Emergency response and energy security - IEA - https://www.iea.org/about/oil-security-and-emergency-response

tion helped further to rebalance the market. This crisis could help redesign EU security of gas supply. For a regional supply disruption below 10% of total demand, markets should be left alone as the best place to re-route LNG cargoes and reduce/destroy demand, but for something like above (as seen in 2022) some non-market measures must be in place like minimum storage requirements or solidarity mechanisms. Like in oil, MoDs should be an active stakeholder for gas.

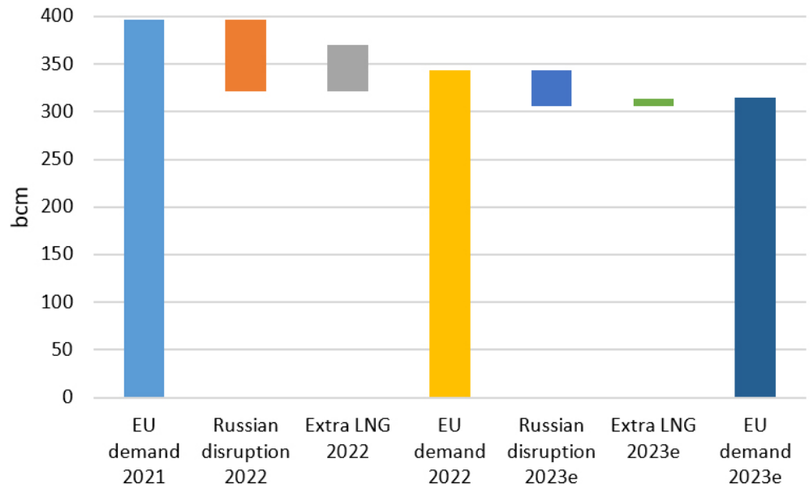


Figure 31 2021/2023 evolution of Russian disruption and extra LNG in front of EU demand - Source: EI Statistical Review 2023, GIIGNL Annual Report 2023, thierrybros.com

In 2022, some European nations launched new LNG receiving infrastructure. Nevertheless, having the necessary infrastructure in place without corresponding long-term supply commitments does not necessarily guarantee European security of supply. A rebound in LNG demand in China or a drop in global supply would put additional pressure on the market. So, after having been shy of signing long-term contracts in 2022, European utilities are slowly changing their views and started to sign new contracts, in 2023, to increase security of supply and reduce price volatility.

If European utilities do not invest enough in gas for Europe either upstream or via long-term contracts, in the future additional required supply will be in the hands of portfolio players and China. Portfolio players are doing this for profit. China could do it for geopolitical reasons. It makes little sense for the Chinese Communist Party to invest in energy in Europe knowing that worldwide capital available is not enough to meet growing energy needs, instead of concentrating investment in China (and Africa for raw materials access) unless it has a hidden agenda. In short, if Europe fails to reduce further its gas demand it will move from a Russian gas dependency to a Chinese energy dependency. This should be a wakeup call for EU leaders regarding the need to foster energy sovereignty.

To avoid always paying a premium vs Asia, EU utilities and major end users will need to contract more LNG on a long-term basis. For a sustainable economic growth, the EU cannot be both a place with higher cost of labour and higher cost of energy as the Japanese example, of the last decade, is showing. With China and portfolio players signing 20-year long-term contracts, the EU will have to either continue to be a volatile premium market relying mostly on spot or sign new long-term contracts.

In a complex and volatile energy security environment, the EU should beef up its security of energy supply thinking. On top of the Churchillian diversification of supply, there is a need to address the EU wide energy storage. This needs to be a combination of market and off-market mechanisms.

Member States should soon all have suppliers of last resort. MoDs should engage with regulators to see if the default option for them (unless they sign dedicated PPAs) should not be to contract exclusively with the domestic 'supplier of last resort', on the basis that security of supply is paramount for defence and trumps economic interests. If this simple option is not available, MoDs should, when tendering, request that resellers have minimum owned production or long-term contracts.

4.6.3 Benefit of an all-fuels approach

With coal hopefully on its way out in the EU and no more spare production in gas on one side and more intermittent power production on the other side, security of energy supply must be looked at, not on a fuel-by-fuel basis any longer, but globally at EU level.

The global energy system lost not only 12% of Russian production in 2022 but also the flexibility spare Russian gas production capacity provided prior to 2021. For all energies, the only spare production capacity is OPEC+ oil spare capacity that amounts to around 1% of total worldwide energy consumption! And this is used as a political tool to influence oil prices. As no one else wants to finance unproductive energy assets, the world will have to live with more volatile and interconnected energy prices.

Saving energy is the cheapest, safest and cleanest way to reduce EU reliance on fossil fuel imports from foreign countries but this is far from enough. The EU and its Member States should do their best to curb demand at home inside a democratic process without intending to curb production anywhere.

It could foster, thanks to non-market mechanism, green solutions at all levels.

The best energy and climate strategy for the EU should be to focus on effective CO_2 emissions that should be dealt with thanks to the EU ETS. The EU has embarked on a Green Deal transition, where what matters most is a massive reduction in CO_2 emissions with uninterrupted availability of energy sources at an affordable price.

Whenever climate targets prove unreachable or too costly, politicians often relax near-term targets in favour of more ambitious future targets (only to eventually relax those too). This pattern raises a cautionary flag for investors betting on policy-driven imminent peak oil demand. Those political moves are delaying overall CO_2 reductions and are the consequences of too dogmatic ideas that are loudly voiced by a small minority of voters. MoDs that both use all kind of energies and have technological expertise should make pragmatic recommendations to both regulators and policymakers to avoid those "slow-and-fast" changes that are detrimental to both elected policymakers and the climate. Finally, overinvesting in supply reduces prices and if demand does not materialise then it becomes the supplier problem more than the customer problem.

4.7 Recommendations and way ahead

The study produced key recommendations and actions at EU level on how MoDs can manage their growing financial, market, regulation and ownership risks that arise due to their dependence on CESI and help their respective states to foster a pragmatic and sustainable energy transition:

For electricity production

- MoDs should, by default, contract with the 'supplier of last resort' as security of energy supply trumps economics. Other less desirable options could be using the EU market mechanisms and contracting via PPAs to new projects or directly investing in producing decarbonised assets.
- MoDs should have a say when European Commission and Member States deal with controlling acquisitions of EU electricity production assets by systemic rivals or adversaries.
- MoDs should voice their concerns to their national electricity regulator and to ENTSO-E (legally mandated to coordinate the planning and the development of the infrastructure) to avoid the risk of under forecasting electricity demand.
- MoDs should take part in the review of the new CBAM before the entry into force on 1 January 2026 of the permanent system, to make sure that the EU does not become more electricity import dependent.
- For electricity capacity mechanism, MoDs should ask ACER to review its "Technical specification for cross-border participation in capacity mechanisms". Foreign companies with capital in the hands of a non-EU state should not be able to participate on the simple basis of EU security.

For EU energy infrastructure

- MoDs should be represented at ACER as both a particular buyer and an entity that can provide views when dealing with security of supply.
- MoDs should have a say when European Commission and Member States deal with controlling acquisitions of EU energy infrastructure assets by systemic rivals or adversaries.
- MoDs should voice their concerns at national electricity and gas regulator and at ENTSO-E and ENTSOG levels in particular during the 10-year network development plans.
- MoDs should liaise with their respective national regulator for technical solutions to be implemented (like moving overhead power lines underground or improving grid interconnections or having local batteries) for the electricity grid to sustain more and more severe storms.

For producers of coal, oil and, gases

- It would be wrong to assume that oil and gas would be out overnight in the EU energy mix. As we are seeing now, the world uses record volumes of all energy sources (coal, oil, gas, renewable).
- In gas, MoDs should, by default, contract with the 'supplier of last resort' as security of energy supply trumps economics.
- To avoid EU dependency on oil to further increase in favour of OPEC+ and on gas to start in favour of China, MoDs should have a seat at the table when the EU, the G7 and the IEA draft position papers that have an impact on world supply/demand to counterbalance vocal NGOs that have a hidden degrowth agenda.
- MoDs should voice their concern at their respective state level that too little investments in energy is unsustainable (it should not only be a question of climate change but also of energy sovereignty).
- With the hype for hydrogen disappearing, MoDs should remind their respective state that for now the only way to massively store energy is through oil and gas and that a crusade against those fuels will: 1. delay the worldwide energy transition as coal will be the default option, 2. weaken the EU position on the international scene.
- MoDs should take part in the review of the new CBAM before the entry into force on 1st January 2026 of the permanent system, to see what extra sector could be covered.

Governments once again are realising that energy security is paramount to national and economic security. Lengthy periods of peace and economic prosperity lull nations into letting their guard down. The recent weaponisation of gas by Russia was the wake-up call for EU governments.

05

Protection of Offshore Critical Energy Infrastructure Beyond National Sovereignty: Military Rules of Engagement and Barriers

Roxana Andrei, *Center for International Studies of the University Institute of Lisbon (CEI-ISCTE)*

5.1 Introduction

Mitigation of risks at European level requires a European answer

At present, the European Union navigates through a complex and volatile geopolitical and security context, prompted by the invasion of Ukraine, the overlapping energy crisis and the first attacks on its **offshore critical energy infrastructure (OCEI)**. Europe's maritime areas have become hotspots of ongoing warfare (Black Sea), zones of security alert due to their proximity to regional conflicts (Eastern Mediterranean), place of deliberate attacks on subsea pipelines and cables (Baltic Sea), and areas of intensified activities of espionage around the offshore energy installations (North Sea-Atlantic).

An unprecedented proliferation of **physical, cyber and hybrid risks, threats and vulnerabilities** acting in synergy, as well as a plethora of state-led, state-sponsored, private, non-state and transnational actors concur and pose pressure on the security and resilience of the European OCEI. The offshore critical energy infrastructure exhibits specific vulnerabilities compared to the onshore infrastructure, stemming from its location and accessibility, as well as from its legal regime, that all require a different protection, security and defence approach compared to the onshore infrastructure. At policy level, the OCEI is regulated by sector, with oil and gas aside from the offshore renewable infrastructure, and with the lack of a single policy framework that would address the safety and security of all existing OCEI under an integrated, all-hazard approach.

In this context, the study emerged as an initiative of the Working Group 3 ('Protection of Critical Energy Infrastructure') of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), as an effort to work in real-time in order to reach the following objectives:

- Identify an **up-to-date set of existing and emerging security risks, threats and vulnerabilities** of the OCEI in the EU.
- Provide an overview of the complex **legal regime governing the OCEI** to highlight the opportunities as well as the limits of engagement for the ministries of defence (MoDs) to protect the offshore critical energy infrastructure in the EU.
- Provide **key recommendations and guidelines for policy update and development** that would integrate all the relevant OCEI under a single policy umbrella, as well as for adopting **security-enhancing measures** for the protection of OCEI in the EU.

The study analyses three types of OCEI: **oil and gas, windfarms and subsea power cables**, due to the fact that they represent the majority of the offshore critical energy infrastructure currently deployed, and thus, their disruption or destruction would have the largest impact on the energy and maritime security. Newly developed and emerging offshore technologies, such as hydrogen, wave and tidal power will gain importance in the energy transition of Europe, and they would require future dedicated research, based on their own specificities.

The research intends to **inform the military and the civilian sector** with respect to the up-to-date risks, threats and vulnerabilities to the offshore critical energy infrastructure in Europe, the existing gaps and limitations pertaining to enhancing the protection and resilience of the OCEI, as well as the complex and specific legal regime governing the sector.

5.2 Internal challenges and limitations to the protection of the offshore critical energy infrastructure (OCEI) in the EU

The European Union has the largest maritime space and the largest combined exclusive economic zone in the world[172]. The safety and security of seas and oceans is of crucial importance for the EU's economy and its vital societal functions, as about two-thirds of the world's oil and gas supply is either extracted at sea or shipped by maritime routes, and as more than 80% of global trade is seaborne and almost 99% of global data flows are transmitted through undersea cables[173].

The transition to green energy has also led to a step-up in the deployment of offshore renewable energy infrastructure, with an increased number of windfarms and subsea electricity cables connecting the offshore installations to the onshore facilities as shown in Figures 32 and 33. As an effect, the EU has at present an installed offshore generation capacity from renewable energy sources of 34 GW[174]. In its *EU strategy on Offshore Renewable Energy of 2020*, the European Commission aims at an installed capacity of 300 GW offshore wind by 2050, with an intermediate goal of 60 GW by 2030, and takes into account the high natural offshore potential of the Baltic Sea as well, in addition to the confirmed one in the North Sea.

The offshore critical energy infrastructure exhibits specific vulnerabilities compared to the onshore infrastructure, stemming from its location and geography, environmental and weather conditions, as well as from its legal regime, which all require a different protection, security and defence approach compared to the onshore infrastructure. Most offshore facilities are located in remote, deep-water, and usually difficult to access areas, with frequently severe meteorological conditions, which can lead to difficulties in reaching the installations in case of an imminent or occurring threat or risk, in a timely manner. Even more, as a considerable part of the OCEI is located under the sea and on the seabed (such as pipelines and electricity cables), it renders it almost invisible to aerial and maritime means of conventional surveillance, and consequently more vulnerable to potential attacks.

The Nord Stream pipelines explosions in September 2022, the Balticconnector incident in October 2023 and the Estlink2 cable damage in December 2024 revealed **the particular vulnerability of the subsea critical energy infrastructure, pipelines and cables**. The "invisible" underwater infrastructure[175] is crucial in the process of energy transmission and is a key element for the EU energy and maritime security. In addition to the subsea communication cables that are responsible for up to 95% of all global communication and on which Europe's digital economy and military operations depend, the seabed of the European

172 European Commission (2020a) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. An EU Strategy to harness the potential of offshore renewable energy for a climate neutral future. Brussels, 19.11.2020 COM(2020) 741 final

173 European Commission (2023a). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the update of the EU Maritime Security Strategy and its Action Plan". An enhanced EU Maritime Security Strategy for evolving maritime threats". Brussels, 10.3.2023. JOIN(2023) 8 final

174 ENTSO-E (2024). Offshore Network Development Plans Paving the way towards an integrated onshore-offshore system planning. https://www.entsoe.eu/outlooks/offshore-hub/tyndp-ondp/

175 Bueger, C. and Edmunds, T. (2023) The European Union's Quest to Become a Global Maritime-Security Provider. Naval War College Review. Vol. 76: No. 2, Article 6, 1-20

waters is crossed by electricity cables as part of its offshore critical energy infrastructure. Given their security relevance, the subsea cables are potentially vulnerable to hybrid and cyber-attacks, terrorism, and acts of warfare. Landing stations where the cables reach the onshore are also vulnerable, as they are easier to reach and access by potentially malicious actors and their damage or destruction may disrupt the functioning of the offshore sections of the cables as well. Other offshore energy installations, such as those using wave and tidal power, also depend on the submarine cable infrastructure for energy transmission.

The security of the underwater OCEI is still under-researched and it benefits from an **uneven level of awareness and engagement from different EU Member States**. Countries more exposed to suspicious subsea activity by third parties and in some cases possessing relevant naval submarine capabilities tend to express a higher degree of awareness and to include the cable protection on their military agenda, with Russian naval and subsea activities being reported by the authorities of Denmark, Estonia, France, Ireland and Portugal[176].

Along with the specific vulnerabilities stemming from **location and geography, environmental and weather conditions**, the seas and the oceans are governed by a very complex and often ambiguous **legal regime**, as a large part of the offshore critical energy infrastructure is located beyond the territorial waters of the coastal states, leading to differing interpretations of the law of the sea with regard to sovereignty, sovereign rights and jurisdiction over the

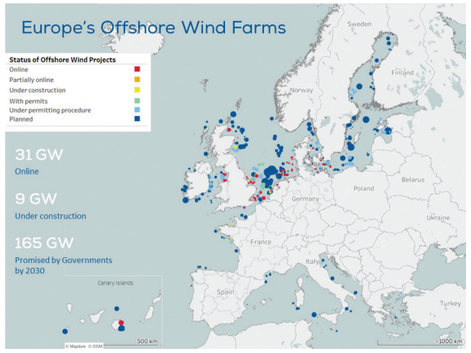


Figure 32 Europe's Offshore Wind Farms[177]

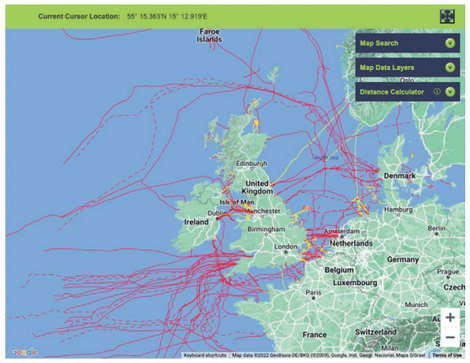


Figure 33 Subsea power cables[178]

OCEI.

Nonetheless, as this study will explain in detail, **fragmentation and interdependencies represent the main internal challenges to the effective protection of the OCEI**.

176 Bueger, C., Liebetrau, T. and Franken, J. (2022) Security threats to undersea communications cables and infrastructure – consequences for the EU. European Parliament, Directorate General for External Policies of the Union. PE 702.557. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557

177 WindEurope (2024) Wind Energy Fact Sheets. https://windeurope.org/wp-content/uploads/images/about-wind/fact-sheets/Slide27.JPG

178 ISSUU (2023) Protecting the subsea cables on which the global economy depends. https://issuu.com/magazineproduction/docs/professional_diver_issue_05/s/25808076

5.2.1 Fragmentation

5.2.1.1 Policy-level fragmentation

Fragmentation at the level of policies and actors in the maritime field stands out as a major challenge, with a multi-layered set of vulnerability areas. A major fragmentation-related limitation stems from **the absence of an integrated OCEI protection and resilience policy framework at EU level**, that would reunite under a single umbrella all offshore energy sectors (oil, gas, renewables), in an all-hazard approach (physical, hybrid and cyber threats).

- The two cornerstone Directives, both entered into force on 16 January 2023, the new ***Directive on the Resilience of Critical Entities ('CER Directive')***[179] and the revised ***Directive on Measures for High Common Level of Cybersecurity across the Union ('NIS2 Directive')***[180], although marking major progress in the EU security landscape, do not tackle the specificities of the offshore critical energy infrastructure.
- Also, the European Parliament and the Council's ***Regulation (EU) 2019/941 on Risk-Preparedness in the Electricity Sector***[181] does not address the issue of offshore critical energy infrastructure.
- Previous initiatives of the EU in support of enhancing its maritime security, the ***Blue Growth Strategy*** (2012) and the ***Security Union Strategy*** (2020), approach mostly threats related to terrorism and crime in the maritime domain, and do not cover hybrid threats.
- In its effort to counter the threats posed by the fast-evolving hybrid warfare techniques, the EU's Strategic Compass provides for the realisation of an ***EU Hybrid Toolbox*** (EUHT), meant as a coordinated action across EU Member States to reunite all military and civilian instruments that can be employed in order to prevent, respond and recover from hybrid threats and attacks[182].
- In November 2020, the Commission published the ***EU Strategy on Offshore Renewable Energy*** (COM(2020)741), focused on boosting the development of the offshore wind capacity in Europe, towards the decarbonisation goals of the Union[183]. Nonetheless, the Strategy concerns only the offshore wind sector and it does not entail a security component, it is not designed under a threat assessment perspective.

Thus, **none of the other security strategies and policy initiatives above mentioned is specifically dedicated to the protection of the OCEI, in an integrated, cross-sector and all-hazard approach**. However, a significant step further has

179 European Parliament and the Council (2022a) 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, L 333/164

180 European Parliament and the Council (2022b) 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 (EU) 2016/1148 (NIS 2 Directive), L 333/80

181 European Parliament and the Council (2019) REGULATION (EU) 2019/941 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

182 European Council (2022) 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 Strategic Compass. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

183 European Commission, Directorate-General for Energy, Andrey, C., Barberi, P., Florez, E. et al. (2022) Offshore renewable energy and grids – An analysis of visions towards 2050 for the Northern seas region and recommendations for upcoming scenario-building exercises, Publications Office of the European Union. https://data.europa.eu/doi/10.2833/693330

been taken on 21 February 2025, when the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy released the ***EU Action Plan on Cable Security***[184] focused on prevention, detection, response and repair, as well as deterrence, and covering both communication and electricity cable infrastructure. Although initially dedicated only to submarine cables, the Commission opens the possibility for some of its actions to be leveraged or extended in the future to other maritime critical infrastructures, such as pipelines or offshore wind fields.

5.2.1.2 Institutional fragmentation at EU level

- Several **EU agencies** hold specific responsibilities related to the protection of the maritime domain: the European Maritime Safety Agency (EMSA); the European Border and Coast Guard Agency (FRONTEX); the European Defence Agency (EDA); the European Environmental Agency (EEA); the European Fishery Control Agency (EFCA); the European Union Agency for Cyber Security (ENISA).
- Specifically in the field of gas, the ***Gas Coordination Group*** has been envisaged by the EU as an advisory body to the Commission, in charge with coordinating the security of supply measures in the case of a Union or regional emergency[185].
- The EU also conducts its own naval operations, ***Atalanta*** and ***Irini***, as part of its ***Coordinated Maritime Presences (CMP)*** concept, along with its ***EUNAVFOR Operation ASPIDES*** in the Red Sea established in 2024 under the EU Common Security and Defence Policy (CSDP).
- It also implements the ***Copernicus*** space-based maritime and border surveillance operational systems, through the cooperation between EMSA and FRONTEX, in addition to the navigation, positioning and timing services offered by the Galileo Global Navigation Satellite System (GALILEO GNSS).
- The EU has also stepped up its efforts in the field of maritime awareness and operational cooperation through the work of the ***European Coast Guard Functions Forum*** and the ***Mediterranean Coast Guard Functions Forum***, and through the inter-agency cooperation established between the European Fisheries Control Agency (EFCA), EMSA and FRONTEX, as a support to national coast guard authorities[173].

Nevertheless, **none of the above-mentioned EU bodies has specific delegated responsibilities for the protection of OCEI**.

5.2.1.3 Actors, data and information fragmentation

- **Fragmentation also affects the actors operating in the field of OCEI**, with a large range of state, non-state, public and private actors playing the field. The more entities involved, the more difficult it is to implement risk preparedness plans, which raises the need for developing comprehensive national and Union-wide mapping strategies that would identify and later involve all players.
- Significant **data gaps** still persist making data collection for maritime security particularly difficult. While data that generate commercial interest are generally largely available (such as data related to ship positioning, piracy or illegal fishing), other data that attract little commercial interest are still under-reported and dispersed (data that concern illegal mining, dredging, or oil bunkering), despite the EU's efforts in recent years to develop the voluntary CISE and MARSUR mechanisms, to enhance the collaboration in the field of surveillance and intelligence networks[175].
- At the same time, although progress has been made, **fragmentation in the exchange of information and intelligence cooperation** between Member States still persists[186]. Specifically with regard to the critical infrastructure, further fragmentation at intra-EU level is fuelled by the fact that similar types of entities are considered critical in some Member States, but not in others, while those identified as critical are subject to divergent requirements in different Member States[187].
- **Information fragmentation** poses challenges too, as conflicting situations may arise regarding the level of **information disclosure**, between public information on the one hand, and restricted, confidential, secret or top secret on the other hand. While for safety reasons, some information may be publicly available and contributes to maritime safety, such as the positioning of submarine cables in coastal and shallow waters to avoid anchoring and dredging incidents by ships, the same public disclosure may render the cable infrastructure vulnerable to malicious attacks, by making their location available to everyone with access to navigation charts. In addition, in many cases, the OCEI is privately owned, managed or operated. Private actors, such as energy and shipping companies, are at times reluctant to report and disclose information related to incidents, for reasons related to reputation, market movements, commercial and trade secrets, or competitive issues.
- The Nord Stream incidents in September 2022 revealed also challenges at national level, with the existence, in some cases, of a **lack of coordination** between the energy industry, the police and the military, which have different security responsibilities regarding onshore and offshore installations[188].

5.2.2 Interdependencies

Interdependencies account for the other major internal vulnerability of the offshore energy infrastructure, along with the fragmentation encountered at policy, institutional and actors level.

- **The OCEI and maritime infrastructures are closely interlinked**, as the functioning, repairing and transmission of energy produced offshore depends on the maritime transportation and port facilities. Disruptions in the maritime infrastructure can impact the proper functioning of the OCEI. Similarly, a major event affecting the OCEI, such as an oil spill from an offshore platform or the explosion of an underwater gas pipeline, can significantly disrupt the safety of maritime operations.
- The electricity systems and the gas transmission infrastructure are **increasingly interconnected across borders**, which means that, in the event of a disruption, its consequences can rapidly

184 European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2025) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. EU Action Plan on Cable Security. Brussels, 21.2.2025. JOIN(2025) 9 final

185 European Commission (2023b) Register of Commission expert groups and other similar entities. GROUP - X01096 - Gas Coordination Group. https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=1096

186 European Commission (2020b) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Security Union Strategy. Brussels, 24.7.2020 COM(2020) 605 final

187 European Commission (2022a) Projects of Common Interest in energy infrastructure in the Western Europe and North Seas. https://energy.ec.europa.eu/system/files/2022-12/Infrastructure_factsheet_WestEurope.pdf

188 Stroemmen, in Buli, N. (2022) Norway to deploy military to protect its oil and gas installations. Reuters.https://www.reuters.com/business/energy/norway-beefs-up-security-across-oil-gas-sector-2022-09-28/

spread to more countries and regions, in a cascading effect, as the transborder infrastructures often link more countries directly and indirectly. Cascading disruptions enhance the damages resulting from a negative event and prolong crises, making prediction and effective incident management more difficult for the authorities, and raising uncertainties for all stakeholders.

- In addition, disruptions in the energy sector may rapidly **impact other sectors in the society**, such as hospitals, transport, telecommunications, governmental services, or the police. The military forces may also be severely affected and their capacity to respond, deploy and intervene in an effective and timely manner can be degraded, as the defence sector largely depends on the public and private civilian infrastructure. This may even be a reason for an adversary to target such infrastructures in the first place. Interdependencies between various infrastructures can thus lead to a cascading effect, should a threat to one or more of them materialise.
- The role of private actors in potentially enhancing the vulnerabilities of the OCEI reveals the fact that their fragmentation can pose **risks to supply chains**, as many of the critical components and critical raw materials, such as the ones needed for the renewable offshore infrastructure, are produced at present outside the EU and NATO countries, making their monitoring challenging[189].
- In addition, there is a **critical interdependency between a large variety of entities** that play a role in the operation of the OCEI, from owners, operators, supply chain distribution, insurance companies, digital services providers, or private security actors. **Various entities have different levels of security and protection in place**. A lower level of security or the absence of security protocols may be exploited by malicious actors as a 'backdoor entrance' in order to perform attacks on the OCEI, be they in physical, cyber or hybrid form.

5.3 External challenges to the protection of the OCEI: an updated threat landscape

The maritime domain and, implicitly, the security of OCEI are exposed to a rapidly expanding array of risks, threats and vulnerabilities, widely ranging across physical, cyber and hybrid activities. Until the invasion of Ukraine in 2022, the main concerns related to maritime security in Europe have concerned illicit and illegal activities, primarily in relation with acts of terrorism, trafficking of arms and narcotics, smuggling of migrants, piracy and armed robbery, or illegal fishing. Similarly, the policy and the political focus has been mainly on preventive and reparatory measures addressing the safety of OCEI, and less on enhancing its security against deliberate acts orchestrated by a plethora of state-led, state-sponsored, non-state, transnational or private actors. **The focus has been predominantly on safety rather than on security**. Nevertheless, the recent geopolitical events in the aftermath of the Ukraine war, as well as the Baltic Sea incidents, **urge for broadening and updating the policy framework in order to pay due consideration to the security of the OCEI**.

For this purpose, three sets of threats to the security of the OCEI in the EU have been identified by the study: **physical, cyber and hybrid threats**, which may be employed independently or frequently in synergy by various state, non-state and transnational actors, requiring the need to adopt an all-hazard approach for preventing and countering risks, threats and vulnerabilities of the OCEI in Europe.

5.3.1 Physical threats to the OCEI

Conventional physical threats to the security of the OCEI continue to pose a significant risk, with a large variety of state-led or state-sponsored actors, along with transnational and non-state players being able to perform fast attacks on oil and gas rigs, subsea power cables and offshore windfarms. Physical attacks can be employed by surface, submarine or aerial means, with the support of both traditional means (boats, aircrafts, submarines, remote explosive devices), as well as advanced technological means (drones and other unmanned surface, submarine and aerial vessels). The attacks can range from: explosions; breaking and tapping oil and gas rigs, windfarms, underwater pipelines and cables; anchoring and dredging of cables; acts of terrorism involving seizure of assets and hostage taking; or missile firing at offshore installations.

Out of the means employed to cause physical attacks on OCEI, the **Maritime Improvised Explosive Devices (M-IEDs)** stand out as a fast-evolving threat that may be directed against all types of OCEI, be it offshore windfarms, oil and gas installations or submarine cables, being easily available to various actors due to their relatively small costs and unsophisticated production requirements. M-IEDs can be employed in the form of: drifting explosive devices, disguised as rafts, life boats, unattended boats, plastic bins, large bags, or floating mines, that can be denotated remotely, or upon contact with a person or an object; suicide borne devices; remotely controlled M-IEDs, which can be enhanced by using drones or powerful telescopic equipment in order to compensate for the distance of the target; drones and unmanned aerial vehicles that can be used for observation and intelligence gathering, or to perform kamikaze attacks on offshore and maritime targets; underwater M-IEDs with time-delayed mechanism and remote control mechanism[190]. Offshore windfarms can be damaged through the crash of a flying object, damage of submarine or land cables, shelling, occupation, intentional collision, bombing or explosion, vandalism, intentional shutdown, or intentional electro-magnetic pulse[191]. Deliberate attacks on the cable infrastructure may target the cable connections, as well as landing stations and repair infrastructure[176], being able to cause significant disruptions in the power supply, if also taking into account the usually longer time needed to intervene in order to repair or to replace an offshore cable compared to one located onshore.

5.3.2 Cyber Threats to the OCEI

The progressive **digitalisation** of the energy infrastructure in recent years, both onshore and offshore, renders it more vulnerable to the rapidly evolving cyber risks and threats. As the energy system is becoming more interconnected, with electricity systems and gas transmission infrastructure often crossing more borders, the disruptive events taking place in one part of the system can rapidly spread to the other parts of the system, in a **cascading effect**[192]. The

189 European Union and NATO (2023) EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf

190 Ceyhun Ture, H. (2023) Maritime Improvised Explosive Device (M-IED) Threat to Energy Security. NATO ENSEC COE. https://www.enseccoe.org/publications/maritime-improvised-explosive-device-m-ied-threat-to-energy-security/

191 Köpke, C., Mielniczek, J., Roller, C., Lange, K., Sill Torres, F. and Stolz, A. (2023). Resilience management processes in the offshore wind industry: schematization and application to an export-cable attack. Environment Systems and Decisions (2023) 43:161-177. DOI: https://doi.org/10.1007/s10669-022-09893-9

192 European Commission (2019a) COMMISSION RECOMMENDATION of 3.4.2019 on cybersecurity in the energy sector. Brussels, 3.4.2019. C(2019) 2400 final

system management is posing new security challenges on the transmission system operators (TSOs), as a consequence of the incorporation in the system of more actors, stakeholders, customers, local grid and market operators, some with lower levels of protection and security of their IT systems[193].

- The critical energy infrastructure finds itself exposed to an ever **increasing and fragmented network of players**, be it state-led, state-sponsored, transnational, non-state or private actors, that also includes hackers and hacktivists, with capabilities and means to inflict malicious cyber-attacks.
- The vulnerability of the critical infrastructure is enhanced by the persisting **heterogeneity of industrial systems** responsible for monitoring and controlling the physical processes in critical energy infrastructure, since some systems have a higher degree of digitalisation and automation, while others, in particular the older ones, still rely on analogue or manually controlled operations[194].
- Attackers can employ various **techniques** to exploit the vulnerabilities of the critical energy infrastructure, with the most frequent being malware infection, the manipulation by the attackers of the supply chains of OT systems, and the exploitation of poor cybersecurity practices related to encryption, authentication, patch management and configuration management[195].
- **Windfarms** may be vulnerable to smart cyber-attacks, which can target their industrial control system networks, such as the supervisory control and data acquisition (SCADA) systems that are used to connect wind turbines to the windfarm network operator[196]. Various stakeholders operate in the offshore wind sector, among which are owners, operators, maintenance providers, logistic companies, grid connection, public authorities, coast guard, trade control, rescue forces, vessel and air traffic services, insurance companies, investors, society, fishery, and shipping[191]. Threat actors may exploit the fragmentation of the sector, where a high diversity of public and private stakeholders co-exist, with different levels of security in place.
- Modern **offshore oil and gas installations** employ OT systems in support of their operations and components, including the process of extraction, and the monitoring of temperature and pressure during extraction, as well as critical parts such as the valves controlling oil and gas flow[197]. The attackers may be particularly attracted by the socio-political location of the target installation and by the potential cascading effects of the attack, which may result not only in disruptions of supply, but also in severe impacts on humans and environments, due to the release of hazardous materials[198].

193 ENTSO-E (2020) ENTSO-E Research, Development & Innovation Roadmap 2020 – 2030. https://www.entsoe.eu/2020/10/14/entso-e-research-development-innovation-roadmap-2020-2030/

194 Butrimas, V. (2022) Guide for Protecting Industrial Automation and Control Systems Against Cyber Incidents in Critical Energy Infrastructure. NATO Energy Security Centre of Excellence. https://www.ensec-coe.org/publications/guide-for-protecting-industrial-automation-and-control-systems-against-cyber-incidents/

195 Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D. and Karamperidis, S. (2021) Perspectives on Cyber Security for Offshore Oil and Gas Assets. J. Mar. Sci. Eng., 9:112, 1-27. https://commons.wmu.se/lib_articles/502/

196 Badihi, G., Jadidi, S., Yu, Z., Zhang, Y. and Lu, N. (2021) Diagnosis and Mitigation of Smart Cyber-Attacks on an Offshore Wind Farm Network Operator. 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS) | 978-1-7281-6207-2/21/$31.00 | DOI: 10.1109/ICPS49255.2021.9468268

197 GAO - United States Government Accountability Office (2022). Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure. GAO-23-105789. https://www.gao.gov/products/gao-23-105789

5.3.3 Hybrid threats to OCEI

Hybrid threats are purposefully ambiguous operations that blur the distinction between deliberate and unintentional events, as they often employ apparently harmless non-state actors, such as fishing or cargo vessels, in order to perform seemingly accidental operations, camouflaging in this way the real malicious intent and the occurrence of a state-backed or state-sponsored attack. Thus, the concepts of **hybrid threats and grey zone warfare** "refer to situations where states use disruptive measures that fall below the threshold of direct military actions, making it difficult to attribute them directly to a government"[199].

The maritime space is particularly vulnerable to these practices, given its vastness and the **large number of public and private actors**, which further blur the lines between state-sponsored and private activities[176]. At the same time, **foreign control of critical infrastructure and of strategic materials and supply chains** is considered by the EU and NATO to be a vulnerability of the critical infrastructure to hybrid threats, as it could allow malicious actors to gather sensitive information about EU and NATO activities, and also deny and disrupt access to critical infrastructure or tamper with the services it provides[189].

In response to the evolving threat landscape, the European Defence Agency, the European Commission Directorate-General Joint Research Centre (JRC), and the Working Group 3 of the Consultation Forum for Sustainable Energy in the Defence and Security Sector jointly released in 2023 the study ***"Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats"***. The study finds that interdependencies are key vulnerabilities, as dependencies between various domains of the ecosystem (i.e., political, economy, cyber, space, legal, public administration, intelligence and culture) could be used as entry points and exploited by adversaries to affect the infrastructure as well as the military/defence domain[200].

Particularly with regard to the maritime space, we identified specific predominant **hybrid techniques employed by malicious actors** to purposely blur the nature of their intervention, as well as their identity:

- When performing illegal or criminal activities, ***ships often switch off their AIS*** (automatic identification system) transponders, an automatic tracking system installed on ships and used by vessel traffic services to identify a vessel's course, position, identity and speed. Such technique has been regularly employed in illegal fishing and human trafficking activities at sea. Nevertheless, there are increased concerns that the practice is currently being used to perform undetected attacks on the OCEI in Europe. Among the possible attacks that can target the OCEI using this technique, a ship navigating with the AIS switched off can pass undetected and approach an offshore installation to perform a physical attack on the platform or its stations, by placing explosives or carrying out an armed attack in order to take control over the installation. A sim-

198 Iaiani, M., Tugnoli, A., Cozzani, V., Reniers, G. and Yang, M. (2023) A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. Ocean Engineering 273, 114010, 1-13

199 Bueger, C. and Liebetrau, T. (2023) Critical maritime infrastructure protection: What's the trouble? Marine Policy 155-105772, p. 5

200 Giannopoulos, G., Jungwirth, R. and Hadjisavvas, C. (2023) Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EN, Publications Office of the European Union, Luxembourg. DOI:10.2760/58406, JRC133083

ilar ship can get involved in intentional anchoring and dredging acts with the purpose of damaging and destroying the undersea electricity and data cables. Additionally, these vessels can also act as side-players, acting in pairs and attacking the coast guard, the military and the rescue ships that would intervene in the case of an attack on an OCEI asset. Adversaries, be it state-led, state-sponsored or transnational criminal groups may also subcontract apparently inoffensive vessels navigating with their AIS disconnected and having their activity disguised. As such, the vessels may perform remote attacks without closely approaching the installations, by carrying and launching maritime improvised explosive devices (M-IEDs) with the help of submersible attack technologies, such as underwater drones.

- ***AIS spoofing***, referring to the manipulation of the AIS, including of ships' location and identity, is becoming increasingly widespread and more sophisticated, encompassing fast-evolving techniques that can be employed for malicious purposes at sea. Among these, a threat actor can engage in: identity tampering (the deliberate falsification of a vessel's broadcasted data on AIS and/or alterations to its physical features); identity theft (when one vessel assumes the identity of another operating vessel, creating a duplication of the same transmitted identifiers); location tampering (manipulation of the global navigation satellite system to disguise the true location of the vessel); 'AIS handshake' (the use of a decoy vessel as a disguise, sailing in close vicinity of the malicious ship, which thus assumes the identity of the decoy)[201]. AIS spoofing tactics targeting warships during sensitive geopolitical times may lead to the escalation of tensions and of conflicts, in maritime hotspots such as the Black Sea or the Baltic Sea. The manipulation of their location to transmit a fake location, such as falsely showing warships approaching foreign naval bases, entering territorial or disputed waters, or even near OCEI, may be employed by an adversary to justify an alleged retaliation and defensive attack[202]. In this way, AIS manipulation and disinformation act together as hybrid threats techniques that may be engaged in the maritime ecosystem and in connection with the European OCEI.
- **Misinformation and disinformation**, the spread of **fake news**, as well as the **mobilisation of civil society actors for protests** grounded on environmentalist motivations, may also be diverted or orchestrated by malicious actors in order to employ hybrid attack techniques targeting the OCEI, blurring in this way the distinction between peaceful acts and disguised attacks to the security of the installations and consequently affecting the time and the nature of response.

5.4 Maritime hotspots in the EU: risks, threats and vulnerabilities of the OCEI

In the current geopolitical threat landscape in Europe, we identified for the purpose of the study **four maritime hotspots in the EU**, each with specific challenges to the security of the OCEI located in their waters: the North Sea-Atlantic region, the Baltic Sea, the Black Sea and the Mediterranean Sea.

201 Windward (2022) AIS spoofing: new technologies for new threats. https://windward.ai/blog/ais-spoofing-new-technologies-for-new-threats/

202 Harris, M. (2021) Phantom Warships Are Courting Chaos in Conflict Zones. WIRED. https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/

5.4.1 The North Sea-Atlantic Region

The North Sea-Atlantic region hosts 12 coastal states: Belgium, Denmark, France, Germany, Iceland, Ireland, the Netherlands, Norway, Portugal, Spain, Sweden, and the UK. With the exception of Norway, Iceland and the UK, all of them are members of the EU. **Most of the European Union's production of offshore energy takes place in the North Sea-Atlantic region**, where 80% of all the EU's domestic oil and gas (16 264 kilotons of oil equivalent) is produced[203] and where the world's largest deployed capacity and expertise in offshore wind is also located[172].

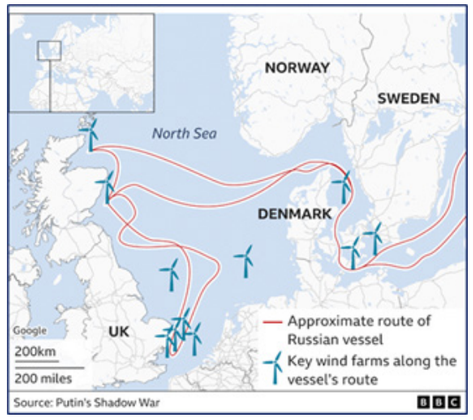


Figure 34 The presence of the Russian vessel Admiral Vladimirsky around the OCEI in the North Sea[204]

The North Sea in particular benefits from a high offshore wind potential, due to its steady wind regimes and to its shallow waters allowing for the deployment of bottom-fixed wind turbines and other types of installations at longer distances from the shore.

In the recent context of the war of aggression against Ukraine and the subsequent changing geopolitical dynamics in Europe, the North Sea-Atlantic region has been reportedly exposed to intensified suspicious activities of intelligence collection, frequently in the proximity of the OCEI located in the area (Figure 34). More incidents have thus been reported in the region:

- David Cattler, NATO's assistant secretary general for intelligence and security, warned about an increased presence of civilian ships commissioned by Russia for potential activities of espionage, the so-called '**spy ships**' in the Atlantic, North Sea and the Baltic sea[205].
- In February 2023, the Norwegian authorities released the National Threat Assessment for 2023, underlying the possibility of the Norwegian energy sector being targeted by **Russian activities of espionage**[206]. In September 2022, the presence of a number of unidentified drones in the proximity of the oil and gas platforms situated on the Norwegian continental shelf has been investigated by the Norwegian police[207].
- The Dutch General and Military Intelligence and Security Services (AVID and

203 European Commission (2024) Annual Report from the European Commission on the Safety of Offshore Oil and Gas Operations for the Year 2022. Brussels, 17.5.2024. COM(2024) 187 final

204 Corera, G. (2023) Ukraine war: The Russian ships accused of North Sea sabotage. BBC. https://www.bbc.com/news/world-europe-65309687

205 Cattler, in Cooper, Charlie (2023) NATO warns Russia could target undersea pipelines and cables. POLITICO. https://www.politico.eu/article/nato-warns-russia-could-target-undersea-pipelines-and-cables/

206 Duff, R. (2023) UK oil sector 'engaged' with government as Norway prepares for Russian spies. Energy Voice.https://www.energyvoice.com/oilandgas/483346/oeuk-remains-engaged-with-government-as-norway-prepares-for-russian-spies/

207 Kool, T. (2022) Norway Investigates Mysterious Drone Sightings Near Offshore Oil & Gas Fields. Oil Price. https://oilprice.com/Latest-Energy-News/World-News/Norway-Investigates-Mysterious-Drone-Sightings-Near-Offshore-Oil-Gas-Fields.html

MVID) have issued, in February 2023, a joint update on recent potentially harmful actions carried out by the Russian Federation in the vicinity of the Dutch energy infrastructure in the North Sea, identifying **mapping activities around the gas pipelines, offshore windfarms, and data cables** located in the Dutch waters as an indicator of possible espionage and preparatory work for disruption and sabotage[208, 209].

- The Belgian authorities have in their own turn reported, in November 2022, a series of potentially **suspicious activities in the Belgian and Dutch waters**, in the proximity of the gas, cables and windfarms offshore infrastructure in the North Sea[210].
- The head of the UK's armed forces, Adm. Tony Radakin warned that the British navy has been tracking **intensified Russian submarine activity in the Atlantic**[211].
- According to a study produced in 2021 for the NATO Energy Security Centre of Excellence (NATO ENSEC COE), **Russia owns a top-level military fleet located in Olenya Guba**, on the coast of the Barents Sea[212], close to the shores of Norway and the northern part of Finland. The fleet is under the authority of the Russian Main Directorate for Deep Sea Research (GUGI) and it consists of traditional submarines, intelligence ships and auxiliary submarines, as well as "special mission ships" or "oceanographic vessels", capable to be employed as reconnaissance vessels, such as the project 22010-class ship "Yantar", already spotted near the east coasts of the United States, Canada, Portugal, Ireland and in the Mediterranean, in the proximity of critical subsea data cables[212].
- In June 2024, maritime patrol crafts from France, Norway and the UK launched a joint search operation for a **Russian submarine spotted off the western coast of Ireland**, in close vicinity of the critical underwater infrastructure located in the area. The incident followed the May 2023 report of the Irish Naval Service of some Russian ships conducting unusual manoeuvres close to a newly laid cable off the Irish coast. Ireland is a particularly vulnerable spot in the region, due to its limited high-end capabilities able to perform surveillance of the subsea critical infrastructure and seabed warfare[213].

5.4.2 The Baltic Sea

The Baltic Sea is home to 9 littoral countries: 8 EU and NATO Member States (Denmark, Germany, Estonia, Lithuania, Latvia, Poland, Finland and Sweden), plus the Russian Federation. **The Baltic Sea ranks second after the North Sea-Atlantic region, in terms of its potential and planned offshore wind capacity** in the EU. In the low scenario, it could produce 17 GW by 2050, up from 2.5 GW at present, while in the ambitious scenario the production could go up to 32.1 GW in 2050[214].

The Baltic Sea region has been traditionally heavily reliant on a single natural gas supplier, namely on Russia. The Nord Stream explosions under the Baltic Sea (Figure 35), in September 2022, the Balticconnector incident in October 2023 and the Estlink2 cable damage in December 2024, brought to surface the stringent need for the countries of the region to enhance their cooperation to strengthen the resilience of their OCEI. The largest operational offshore natural gas project in the Baltic Sea, at present, is the **Baltic Pipe**, inaugurated on 27 September 2022 and representing a milestone project of the EU to diversify away from Russian gas imports. The Baltic Sea region is also one of the best interconnected regions in the EU and it benefits from an integrated electricity market with the Nordic countries.

Figure 35 Location of the damaged Balticconnector and of the Nord Stream leaks[215]

The EU has funded between 2006 and 2015 important projects for electricity interconnectors (the submarine cables NordBalt, Estlink 1 and 2, and the overhead cable LitPol Link), and in February 2025 the three Baltic States (Estonia, Latvia and Lithuania)

208 Ministry of Defence Netherlands (2023) 24/2 De Russische aanval op Oekraïne: een keerpunt in de geschiedenis. Ministry of Defence Netherlands. Available at: https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/downloads/publicaties/2023/02/20/publicatie-aivd-en-mivd-24-2

209 Buljan, A. (2023) Dutch intelligence warns Russia may be preparing to sabotage offshore wind, gas and cable infrastructure in North Sea. Offshore Energy. https://www.offshore-energy.biz/dutch-intelligence-warns-russia-may-be-preparing-to-sabotage-offshore-wind-gas-and-cable-infrastructure-in-north-sea/

210 Loctier, D. and Euronews (2023) 'A wake-up call': How to protect Europe's vital marine infrastructure from emerging threats? Euronews Green. https://www.euronews.com/green/2023/05/30/the-threat-of-sabotage-to-critical-infrastructure-is-real-belgian-navy-official-warns

211 Radakin, in The Guardian (2022) UK military chief warns of Russian threat to vital undersea cables. The Guardian. https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables

212 Trakimavičius, L. (2021) The Hidden Threat to Baltic Undersea Power Cables. NATO Energy Security Centre of Excellence. https://www.enseccoe.org/data/public/uploads/2021/12/the-hidden-threat-to-baltic-undersea-power-cables-final.pdf

213 Willett, L. (2024) UK, French, Norwegian MPAs combine to hunt reported Russian submarine. https://www.armadainternational.com/2024/06/uk-french-norwegian-mpas-combine-to-hunt-reported-russian-submarine/

214 European Commission (2019b) Directorate-General for Energy, Study on Baltic offshore wind energy cooperation under BEMIP – Final report, Publications Office. DOI: https://data.europa.eu/doi/10.2833/864823

215 Kauranen, A. and Luoma, E. (2023) U.S. supports Finland, Estonia as it probes Baltic Sea pipe burst, says Blinken. Reuters. https://www.reuters.com/business/energy/finland-cant-rule-out-state-actor-involvement-pipeline-damage-intelligence-chief-2023-10-12/

LitPol Link), and in February 2025 the three Baltic States (Estonia, Latvia and Lithuania) have disconnected from the Russian-led BRELL network, advancing for their full synchronisation with the EU continental grid. The planned subsea Harmony Link 700 MW high-voltage cable between Lithuania with Poland is part of the strategy to achieve the full synchronisation of the Baltic countries to the EU grid[216]. In line with UNCLOS, the Russian Federation has the right to a legitimate presence in the Baltic Sea, due to its coastal location.

Except for Russia, all the littoral states are members of the EU and NATO. The new security reconfiguration around the Baltic Sea has set the framework for a **more integrated capacity of reaction and cooperation** in the case of a potential, emerging or imminent threat to the security of the littoral states and to their OCEI. It has nonetheless also coincided with an escalation of **threats, risks, incidents and attacks on the subsea OCEI in the Baltic Sea**:

- **Russia has consolidated in past years its military capabilities at the Baltic Sea**, building forward defence and area denial capabilities with modern weapons systems in and around Kaliningrad and St. Petersburg[217].
- Since the invasion of Ukraine, more suspicious activities have been reported, such as the **occurrence of drones** in the vicinity of critical civilian and military infrastructure, and the potentially **non-innocent presence of vessels** in sensitive areas of the Baltic Sea, close to the OCEI.
- The increase in the number of existing and planned submarine cables raises their vulnerability to **potential malicious attacks on the subsea power infrastructure**, which can be performed by means of physical attacks (deliberate anchoring, dredging, cutting, placement of explosives via manned and unmanned devices), cyber-attacks on the digital infrastructure or broader hybrid warfare, including by the employment of high-tech alleged oceanographic and research vessels, or of apparently innocent fishing and cargo ships.
- The invasion of Ukraine has profoundly altered the threat landscape and the geopolitical dynamics of the Baltic Sea region. Critical events have brought to surface the exposure of the OCEI in the Baltic Sea to the rapidly evolving geopolitical changes in Europe since 2022 to a new set of risks, threats and vulnerabilities: the **Nord Stream gas pipelines explosions** on 26 September 2023, the **damage of the Balticconnector subsea gas pipeline** between Finland and Estonia, on 8 October 2023 and the **Estlink2 power cable plus four data cables damage** in the Finnish Exclusive Economic Zone (EEZ), in December 2024, by a ship suspected to belong to the Russian shadow fleet.

The Baltic Sea incidents revealed the vulnerability of the OCEI in the Baltic Sea, in particular of the subsea infrastructure, in front of larger-scale potential attacks that may occur undetected and would be difficult to prevent. At the same time, it unfolded the crucial role of cooperation and communication at regional and EU level, as well as with the EU's strategic partners, in order to increase the prevention, response and resilience capabilities, in the face of an unprecedented upscale of the threat landscape in the maritime hotspots of Europe and of its neighbours.

216 European Commission (2022b) Projects of common interest in energy infrastructure in the Nordic and Baltic Sea region. European Commission. https://energy.ec.europa.eu/topics/infrastructure/high-level-groups/baltic-energy-market-interconnection-plan_en

217 Swistek, G. and Paul, M. (2023) Geopolitics in the Baltic Sea region: The "Zeitenwende" in the context of critical maritime infrastructure, escalation threats and the German willingness to lead. SWP Comment, No. 9/2023, Stiftung Wissenschaft und Politik (SWP), Berlin, 1-8. DOI: https://doi.org/10.18449/2023C09

5.4.3 The Black Sea

The Black Sea is currently the most vulnerable maritime area of the European Union, with a full-scale war ongoing and with associated maritime warfare following the war of aggression against Ukraine. It is home to 6 coastal countries: Bulgaria, Georgia, Romania, Russia, Turkey and Ukraine. As a consequence of the invasion of Ukraine in 2022 and of the annexation of Crimea in 2014 by the Russian Federation, there are nowadays **disputed areas in the Black Sea**, with a number of areas of the Ukrainian territorial waters and EEZ claimed by Russia.

Although the exact volumes of natural gas in the Black Sea are still unknown, as most of the natural gas potential remains largely untapped, the most recent discoveries in the Turkish waters and the estimations of the Romanian and Ukrainian reserves indicate nonetheless towards **high quantities of natural gas**. There are currently 21 oil and gas wells drilled at sea depths exceeding 500 m in the Black Sea: Romania (10), Turkey (8), Bulgaria (2) and Russia (1), with no well yet drilled in the Ukrainian and Georgian deep water segments[218]. In the EU waters of the Black Sea, Romania is a well-established offshore oil and gas producer in the region and plans to develop its offshore production further. With the Netherlands closing the domestic natural gas production, Romania is expected to step up, albeit at a smaller production level, as the EU's largest domestic producer of natural gas.

Beyond the EU waters, Turkey is currently emerging as a new gas producer, following the large discoveries in the deep-water Sakarya field, expected to produce 10 million cubic metres (mcm) in the first phase and up to 40 mcm by 2027-2028[219]. Turkey is also a key player in two major subsea gas pipeline networks that cross the seabed of the Black Sea, transporting Russian natural gas: the TurkStream and the Blue Stream. Bulgaria has at the moment only one installation with limited oil and gas production[220,203]. Ukraine's gas reserves remain mainly untapped, as before the war the country was producing an average of only 20 bcm/y. The discovered proven reserves are estimated by the government at 778.2 bcm. Nevertheless 80% of these reserves are located in Eastern Ukraine, currently under partial Russian control or in war-affected areas.

The Black Sea is lagging behind the other maritime zones of the European Union in terms of deployment of offshore renewable energy projects. According to the World Bank, the Black Sea has a vast technical potential of 166 GW floating offshore energy[221], as seen in Figure 36. Romania and Georgia are also collaborating in order to install a 1,100 km long, 1 GW **electricity cable under the Black Sea**, joined by a subsea communication cable expected to become operational by 2029, and being included on the list of planned projects by the ENTSO-E[222].

218 Kobolev, V. (2023) The Black Sea's oil and gas potential: the reality and prospects of drilling a unique ultra-deep well on Zmiiny Island. Oil & Gas of Ukraine. https://oil-gas.com.ua/news/The-Black-Seas-oil-and-gas-potential-the-reality-and-prospects-of-drilling-a-unique-ultra-deep-well-on-Zmiiny-Island

219 Sykes, P. (2023) Turkey to begin production at "biggest" natural gas field in Black Sea. World Oil. https://worldoil.com/news/2023/4/17/turkey-to-begin-production-at-biggest-natural-gas-field-in-black-sea/

220 European Commission (2023c) REPORT FROM THE COMMISSION Annual Report on the Safety of Offshore Oil and Gas Operations in the European Union for the Year 2021. Brussels, 12.5.2023. COM(2023) 247 final

221 Vujasin, M. (2023) BLOW project – pioneering 5 MW floating offshore wind turbine in Black Sea. Balkan Green Energy News. https://balkangreenenergynews.com/blow-project-pioneering-5-mw-floating-offshore-wind-turbine-in-black-sea/

222 Todorović, I. (2022) Georgia, Romania plan power interconnection under Black Sea. Balkan Green Energy News. https://balkangreenenergynews.com/georgia-romania-plan-power-interconnection-under-black-sea/

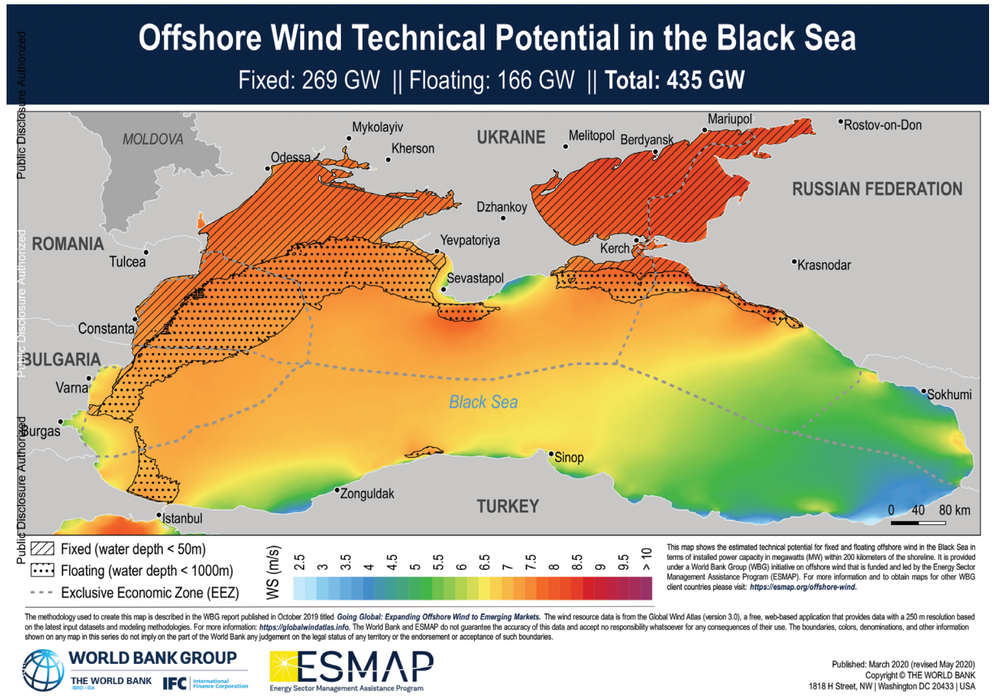


Figure 36 Offshore Wind Technical Potential in the Black Sea[223]

Nonetheless, the deployment of any new offshore project in the Black Sea is marred by the current **high-risk security environment** generated by the war in Ukraine, which may discourage developers and investors and delay governmental commitments for new projects.

- One of the main threats to the OCEI and to the maritime security in the Black Sea is represented by the **unexploded ordnance (UXO)**. The intense naval activity and the warfare in the Black Sea triggered by the invasion of Ukraine led to the dislocation of UXO, some dating from World War 2, and others deployed during the war in Ukraine. Since the start of the war in Ukraine, several explosions of mines have already been reported in very close proximity to the Romanian and Bulgarian shores of the Black Sea, along with an incident where a Turkish cargo boat hit a mine, 11 miles from the Romanian shore. Other unexploded devices have been identified and neutralised since the start of the conflict, according to the Romanian Navy[224].
- **Third-party interventions on the OCEI**, similar to the incidents in the Baltic Sea, may occur given the fact that the Black Sea is the most exposed to the war in Ukraine and constitutes itself a war zone. In particular **the subsea infrastructure (pipelines and cables) is vulnerable** to both unintended damage, as well as to potential malicious attacks, as the surveillance of the area is exceptionally difficult due to the ongoing hostilities.
- Moreover, the drilling ships and oil cargoes may be either accidentally or deliberately hit by **missiles and drones carrying explosives**, or damaged following an impact with **drifting mines**. While not all acts may intentionally target the OCEI installations and the ships, they are particularly vulnerable given the intense military activity and associated warfare in the Black Sea, as some assets, notably the Romanian ones, are located closely to areas with reported presence of UXO, missiles and drones.
- At the same time, the OCEI may be targeted by **cyber-attacks**, especially as the newly-deployed and planned facilities are increasingly digitalised and reliant on the subsea data cables.
- **Hybrid warfare techniques** may employ AIS spoofing of the vessels, for the purpose of taking control of their navigation system, disguising ships' identity, or to transmit a fake location, such as falsely showing warships approaching foreign naval bases, entering into territorial or disputed waters, or even near the OCEI. Several instances of **AIS spoofing** in the Black Sea, mostly by falsification of location, have already been reported since the beginning of the Russian invasion of Ukraine. The purpose may be related to evading the international sanctions on Russian oil exports, or the illicit transportation of weapons from the Mediterranean Sea into the Black Sea. Repeated instances of **GPS jamming** have also been reported by the coastal states.
- In 2023, Russia has enforced a **partial blockade of the Bulgarian EEZ**, closing the area for navigation under the pretext of ongoing military exercises, and raising in this way concerns about the maritime security and the security of the existing and planned OCEI in the Black Sea.

5.4.4 The Mediterranean Sea

8 EU Member States are coastal countries at the Mediterranean Sea and its marginal seas: Croatia, Cyprus, France, Greece, Italy, Malta, Slovenia and Spain. Along with them, 14 more countries are littoral states at the Mediterranean (Albania, Algeria, Bosnia and Herzegovina, Egypt, Israel, Lebanon, Libya, Monaco, Montenegro, Morocco, Palestine, Syria, Tunisia, Turkey), plus the UK's oversea territory of Gibraltar and its sovereign bases, Akrotiri and Dekhelia, located on the island of Cyprus. In addition, Albania, Croatia, France, Greece, Italy, Montenegro, Slovenia, Spain, Turkey and the UK are NATO members.

According to the European Commission[203], in 2022 there were 164 **oil and gas offshore installations** in the EU waters of the Mediterranean Sea, with Italy owning 45% of all installations (140), followed by Croatia (19). In the Eastern Mediterranean, Egypt is the largest natural gas producer, with 770 bcm of proven reserves followed by Israel with 622 bcm[225] (Figure 37). In the Western part of the Mediterranean, Algeria stands out as the third largest natural gas supplier to the EU, linked to Europe via two major subsea natural gas pipelines crossing the seabed of the Mediterranean Sea: the Medgaz pipeline to Spain and the TransMed pipeline to Italy, via Tunisia. Italy is also connected to Libya via the 540 km Greenstream undersea gas pipeline. The Mediterranean sea has a recognised **high potential of offshore wind energy**, mostly floating, a good potential for wave energy and localised potential for tidal energy[172]. However, at present, the deployment of offshore technologies for electricity generation in the Mediterranean Sea is still lagging behind and it consists mainly of floating offshore wind, wave, and tidal pi-

223 World Bank (2020) Offshore Wind Technical Potential in the Black Sea. https://documents1.worldbank.org/curated/en/718341586846771829/pdf/Technical-Potential-for-Offshore-Wind-in-Black-Sea-Map.pdf

224 Forțele Navale Române (2023) Forțele Navale Române desfășoară permanent misiuni de monitorizare în Marea Neagră. Statul Major al Forțelor Navale, 17 august 2023, Comunicat nr. 73. https://www.navy.ro/comunicat.php?id=747

225 Worldometer (2023). Natural Gas. Worldometer. https://www.worldometers.info/gas/

lot projects. The European Commission's moderate production scenario estimates a 4 GW offshore wind capacity by 2030 and 32.7 GW offshore wind by 2050[226]. More **subsea power link projects** are in place or underway in the EU waters of the Mediterranean Sea: the existing Malta-Italy Interconnector; the planned Great Sea Interconnector between Cyprus, Greece and Israel; the planned Euro-Africa Interconnector, between Greece, Cyprus, Israel and Egypt; the planned Greece-Italy link; the planned Cyprus-Egypt connection cable; and the planned undersea power link between Egypt and Greece – GREGY.

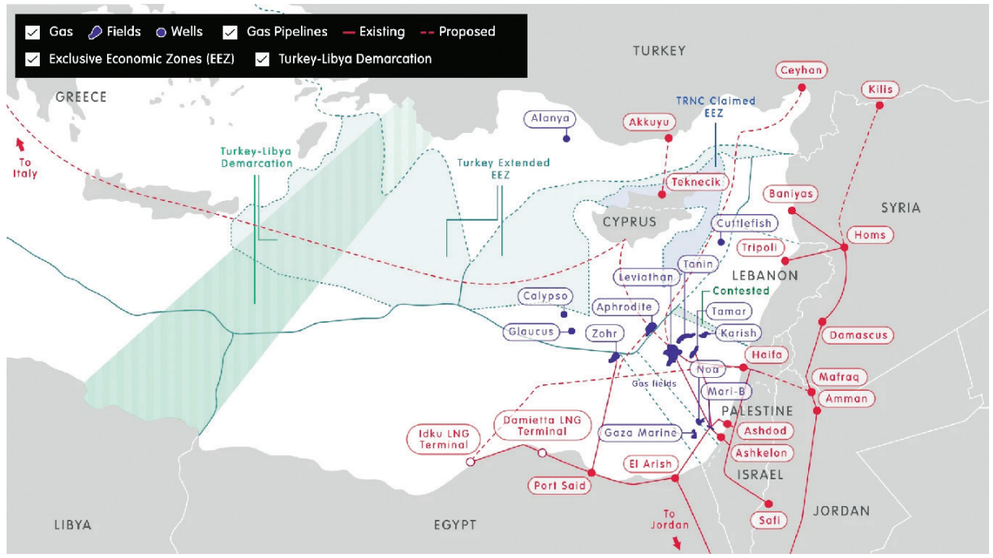


Figure 37 Main gas fields, pipelines and EEZ in the Eastern Mediterranean[227]

Nevertheless, the deployment of future offshore projects in the Mediterranean Sea is restricted by the complex economic, geographical and defence-related specificities of this maritime region. As such, many of the areas that have the highest potential for offshore renewable energy are located in sections with very intense human activity related to fishing, industrial shipping, cruise ship passage, tourism and military training zones, which limit the options for installing new facilities [226]. In addition, high and moderate geopolitical risks may impact on the prospects of any new offshore project. **The most stringent risks, threats and vulnerabilities to the OCEI in the Mediterranean Sea are currently focalised in its Eastern parts**.

- Following the **October 2023 attacks on Israel**, the EU's immediate Mediterranean neighbourhood is still at risk of an escalation of hostilities, which may also damage indirectly or deliberately the OCEI located in the region. Albeit not directly targeted, **the offshore oil and gas infrastructure is vulnerable to missiles exchange, drone attacks, and other activities of aerial and naval warfare**, which may accidentally hit the installations. In addition, potential **cyber-attacks** on the OCEI are to be taken into consideration, as part of the existing hybrid warfare.
- Furthermore, the **presence of the Russian naval forces** poses a stringent security concern, with potential risks for both the Black Sea and the Mediterranean Sea. With the Bosporus and Dardanelles straits closed for military vessels since the beginning of the war in Ukraine, it has nonetheless been reported that Russia has militarised civilian ships in order to circumvent the embargo and thus it has been able to move weapons several times between Tartus in the Mediterranean and Novorossiysk in the Black Sea, by switching off the ships' AIS tracking system[228].
- Another subject of discontent in the Eastern Mediterranean, this time of a legal and political nature, is represented by the **Cyprus issue**. The problem of the exploitation of the gas reserves recently discovered in the waters of the Republic of Cyprus has been a topic of discontent between Cyprus and Turkey, as Ankara has not signed and ratified the United Nations Convention for the Law of the Sea (UNCLOS) and claims that the Republic of Cyprus does not have the sovereignty to explore and exploit offshore resources in the absence of an agreement with the Turkish Republic of Northern Cyprus entity, which, in Turkey's understanding, has equal rights to issue exploitation licences for the gas reserves located offshore the island. Turkey denies Cyprus' right to establish an EEZ, as provided by the UNCLOS, and has engaged in naval activities and military exercises in some of Cyprus offshore blocks[227]. The Cypriot gas discoveries are important for the European Union's energy security, as the EU has included since 2013 a planned project, the **EastMed subsea gas pipeline**, on the list of its PCIs, aiming to bring natural gas from Cyprus and Israel, further to Greece and Italy. The original plan is nonetheless being re-evaluated and alternatives have been explored, such as the construction of a shorter pipeline from Cyprus to Egypt's well-developed LNG infrastructure (able to absorb also the Israeli gas, from where it could be exported further to the EU), or a pipeline linking Israel to Cyprus.

The current complex geopolitical and security dynamics are still impacting on the prospects of future offshore projects in the Eastern Mediterranean, with both public and private actors practicing caution.

5.5 The legal regime of the OCEI: limits of engagement for the military

5.5.1 The legal regime governing the OCEI

The United Nations Convention for the Law of the Sea (UNCLOS), adopted in 1982 and entered into force in 1994, establishes a comprehensive legal framework to regulate all ocean space, its uses and resources, and it defines the maritime zones (the territorial sea, the contiguous zone, the continental shelf, the exclusive economic zone and the high seas), while also considering the protection and preservation of the

226 European Commission, Directorate-General for Energy, Staschus, K., Kielichowska, I., Ramaekers, L. et al. (2020) Study on the offshore grid potential in the Mediterranean region – Final report, Publications Office of the European Union. https://data.europa.eu/doi/10.2833/742284

227 Hafner, M., Raimondi, P. P. and Bonometti, B. (2023) The Energy Sector and Energy Geopolitics in the MENA Region at a Crossroad: Towards a Great Transformation? Springer Cham. DOI: https://doi.org/10.1007/978-3-031-30705-8

228 Palmer, A., Duff, D., Jun, J., Bermudez Jr., Joseph S. (2023) A Wolf in Ship's Clothing: Russia's Militarization of Civilian Vessels in the Black Sea, CSIS. https://www.csis.org/analysis/wolf-ships-clothing-russias-militarization-civilian-vessels-black-sea

marine environment (Figure 38).

It is also the legal reference point at global level for the exploration and exploitation of the resources of the seabed and ocean floor and subsoil, beyond the limits of national jurisdiction. The Convention has been acceded by 168 states and the European Union. 15 United Nations member and observer states have neither signed nor acceded the Convention, while 14 more countries have signed it but have not ratified it.

The exclusive economic zones and the continental shelf are the areas where most of the natural resources and offshore energy installations are located. Art. 60 of UNCLOS regulates **the regime of artificial islands, installations and structures in the EEZ**. In these areas, the coastal States have the exclusive right to construct, and to authorise and regulate the construction, operation and use of: artificial islands; installations and structures for the purposes of exploring and exploiting, conserving and managing the natural resources; installations and structures which may interfere with the exercise of the rights of the coastal State in the zone. Also, the coastal States have exclusive jurisdiction over such artificial islands, installations and structures, and may establish reasonable safety zones, up to 500 metres around them, where they may take appropriate measures to ensure their safety and that of navigation. The same provisions apply, mutatis mutandis, to **artificial islands, installations and structures on the continental shelf** (Art. 80). Artificial islands, installations and structures do not have the status of islands and thus they do not own a territorial sea. Also, as observed by Art. 60, their presence does not affect the delimitation of the territorial sea, the EEZ or the continental shelf[229].

The legal regime of submarine pipelines and cables is set by the UNCLOS, together with the domestic and private law instruments[230]. According to the UNCLOS, all States, be they coastal or land-locked, are entitled to lay submarine cables and pipelines in the EEZ (Art. 58), on the continental shelf (Art. 79), and on the bed of the high seas beyond the continental shelf (Art. 112). Thus, the coastal State cannot, in principle, impede the laying of cables and pipelines on its continental shelf (only for environmental reasons and hydrocarbon-related activities). Its consent is required only with respect to the delineation of the course for the laying of pipelines (but not cables) on the continental shelf (Art. 79).

The legal status of cables, as established by UNCLOS, differs according to the different legal zones where they are laid. As such, in the territorial waters (up to 12 nautical miles), countries have full jurisdiction over the cables. In the contiguous zone (up to 24 nautical miles), States exercise particular law enforcement duties and obligations. **The jurisdiction of coastal States over the cables ends beyond the limits of the contiguous zone**. Thus, in the EEZ (up to 200 nautical miles) and on the high seas, the provisions of the UNCLOS regarding the legal status of cables and the rights and responsibility to protect them is considered to be ambiguous[176]. The Convention provides, in Art. 58, that all coastal and landlocked countries have the right to lay submarine cables and pipelines in the EEZ. Art. 79 provides for similar rights for all States to lay cables and pipelines on the continental shelf of other countries, limited, in this case, by the coastal State's right "to take reasonable measures for the exploration of the continental shelf, the exploitation of its natural resources and the prevention, reduction and control of pollution from pipelines". The same provisions stipulated in Art. 79 apply to cables and pipelines laid on the bed of the high seas beyond the continental shelf, according to Art. 112[229].

The ambiguity of the UNCLOS provisions related to the national jurisdiction over the submarine cables may become an issue of contention in areas of competing claims or with competitive regulative measures. **Possible contested maritime areas in the EU which contain cable systems** are the Aegean Sea (Greece versus Turkey) and the Levantine Sea (Greece and Cyprus versus Turkey)[176], where Turkey has not signed and ratified the UNCLOS.

According to the UNCLOS, **coastal States have the right, but not the obligation, to adopt regulations to protect subsea cables in their territorial waters**. Beyond this limit, States have no obligation to protect them, only the obligation to adopt regulations that provide for punitive measures for ships under their flag that would break or injury a submarine cable (European Parliament, 2022:14). The same obligation applies to submarine and electricity cables, as well as to subsea pipelines, according to Art. 113 of UNCLOS[229].

Nevertheless, it has been noted that, at global level, the majority of States do not comply with the obligations set by the UNCLOS, as they have not adopted legislation that would criminalise the damage or breaking of subsea cables. Moreover, "in contrast to ships that have a clearly assigned nationality, cables do not have a flag"[231], **as most of the subsea cables are owned by the private sector**, who is responsible for the planning, production, operation, and maintenance of cables[176].

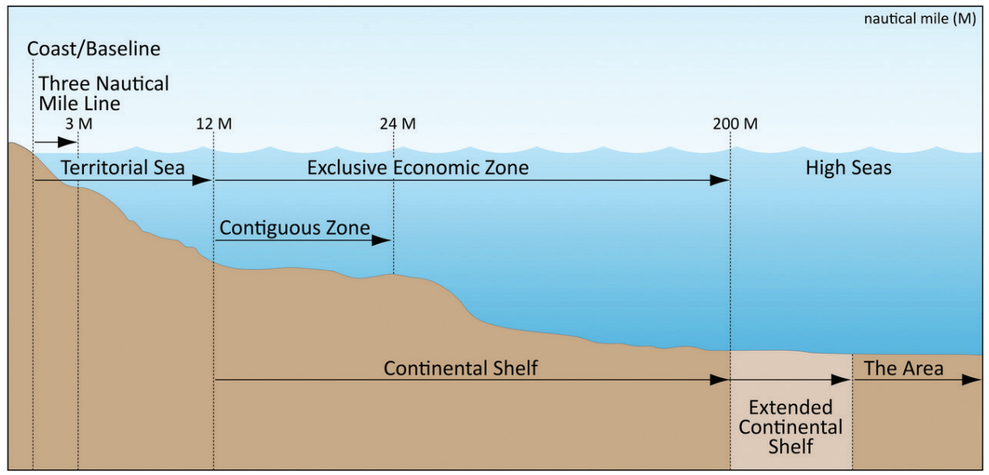


Figure 38 Maritime Zones under International Law (Image credit: U.S. Department of State as modified by NOAA to add Three Nautical Mile Line)[232]

229 United Nations (1982) United Nations Convention on the Law of the Sea (UNCLOS). Montego Bay, 10 December 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

230 Shvets, Daria (2021) The International legal regime of submarine cables: a global public interest regime. Universitat Pompeu Fabra. http://hdl.handle.net/10803/671344

231 Bueger, C. and Liebetrau, T. (2021) Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42:3, 391-413, DOI: 10.1080/13523260.2021.1907129

232 https://www.noaa.gov/maritime-zones-and-boundaries

5.5.2 Limits of engagement for the military in protecting the OCEI

The legal regime of the EEZ as established by the UNCLOS has been subject to criticism due to its sometimes ambiguous provisions. One of the reasons for concern is **the extent to which a coastal State may understand to enforce their authority in order to protect the offshore installations**.

According to the UNCLOS (Art. 111), **the right to hot pursuit** refers to the right of the coastal State to engage in the pursuit of a foreign ship that has violated the laws and regulations of that State. The hot pursuit must however commence when the foreign ship or one of its boats is within the internal waters, the archipelagic waters, the territorial sea or the contiguous zone of the pursuing State, and may only be continued outside the territorial sea or the contiguous zone if the pursuit has not been interrupted. The right to hot pursuit applies, mutatis mutandis, to violations of the laws and regulations of the coastal State applicable, in accordance with the Convention, to the EEZ or the continental shelf, including safety zones around continental shelf installations [229].

In line with the UNCLOS, **military activities at sea have certain limitations**:

- Art. 19 allows for the **innocent passage** of foreign ships in the territorial seas, as long as this is not prejudicial to the peace, good order or security of the coastal State. Thus, certain activities are prohibited, such as: the threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State; exercises or practice with weapons; any collection of information to the prejudice of the defence or security of the coastal State; acts of propaganda aimed at affecting the defence or security of the coastal State; launching, landing or taking on board of any aircraft and of any military device; carrying out of research or survey activities; acts aimed at interfering with any systems of communication or any other facilities or installations of the coastal State.
- Also, in the territorial sea, submarines and other underwater vehicles must navigate on the surface and show their flag (Art. 20)[229].
- Coastal States have the right, under Art. 21, to adopt laws and regulations in conformity with the Convention relating to innocent passage through the territorial sea, with regard to more activities, including the **protection of cables and pipelines**.
- The Convention does not make however clear provisions regarding **warships**. Nonetheless, Art. 17 stipulates that "ships of all States, whether coastal or land-locked, enjoy the right of innocent passage through the territorial sea"[229]. This lack of clarity has left some states to understand that the provision applies to all ships, including military ones, while other countries request prior authorisation and notification before allowing the passage of warships in their territorial waters. Countries like Germany, Italy, the Netherlands and the United Kingdom consider that claims from other states for prior authorisation and notification are incompatible with the UNCLOS[233].
- Also, **the Convention only covers maritime vehicles operated by a physical crew** and not the unmanned maritime vehicles, being thus unclear if these qualify as vessels, warships, or devices and equipment[234]. And furthermore, although military operations are allowed, the **UNCLOS does not define specifically what 'military operations' are**[235]. Therefore, the existing rules stated by the Convention need to be interpreted in such a way that they address the current security and defence challenges.
- **UNCLOS does not however restrict the right of all nations to conduct military activities in the EEZ**. Art. 58 stipulates that all States, whether coastal or landlocked, enjoy the right to navigation and overflight in the EEZ, provided they have due regard to the rights and duties of the coastal State and shall comply with the laws and regulations adopted by the coastal State. The same freedom applies in the high seas, according to Art. 87[229]. This provision has been interpreted to extend also to all lawful military activities, limited by the reciprocal respect of rights and freedoms of other states[236].

5.5.3 The Black Sea and the Baltic Sea challenging cases

5.5.3.1 The Black Sea: a specific case of a warfare zone

In the current geopolitical context triggered by the invasion of Ukraine, the Black Sea occupies a particular space in the realm of the legal regime, as it is a **warfare zone**, where, unlike the other three maritime areas in the EU, **legal instruments pertaining to the law of war, namely naval warfare, could also apply**. The provisions of UNCLOS, albeit a peacetime convention, continue to apply during an armed conflict, among neutrals and between neutrals and belligerents. **Other binding and non-binding legal instruments operate in junction with UNCLOS** during warfare at sea, among which the UN Charter and the Law of **Naval Warfare**, applying between belligerent parties or between neutrals and belligerents. According to the Law of Naval Warfare, naval warfare is not permitted in the internal waters, territorial seas, including waters comprising a strait used for international navigation, or archipelagic waters, of neutral states, as well as in permanently neutralised waters, such as those around Antarctica or the Åaland Islands, located between Sweden and Finland[235].

Regarding the status of the EEZ and continental shelf where most of the OCEI is located, it is worth noting however that **during naval warfare, the contiguous zone, the EEZ and the continental shelves of neutral states are considered areas of high seas, where armed conflict at sea can take place,** with 'due regard for the rights and duties of the coastal State', including the exploration and exploitation of the economic resources of the EEZ. Warring parties are entitled to lay mines in the EEZ and on the continental shelf of a neutral state, provided that the neutral state is notified of the danger and the size of the minefield, and that the type of mines does not pose danger to the artificial islands, installations, and structures. Although belligerents should avoid interfering with the safe exploration or exploitation activities of the EEZ by the neutral state, where such interference cannot be avoided, according to the San Remo Manual on International Law Applicable to Armed Conflicts at Sea adopted in 1994, **a belligerent party may inhibit the coastal State's economic prerogatives in the EEZ**[235].

5.5.3.2 The Baltic Sea: responses in times of hybrid warfare

The precipitated **incidents in the Baltic Sea** that led to the Nord Stream and Balticconnector gas pipelines incidents in 2022 and

233 Tanaka, Yoshifumi (2015) Navigational Rights and Freedoms, in Rothwell et al. (eds.). The Oxford Handbook of the Law of the Sea, p. 537-558. Oxford University Press: Oxford.

234 House of Lords (2022) UNCLOS: the law of the sea in the 21st century. HL Paper 159. House of Lords, International Relations and Defence Committee. 2nd Report of Session 2021–22, HL Paper 159

235 Kraska, J. (2015) Military Operations, in Rothwell et al. (eds.). The Oxford Handbook of the Law of the Sea, p. 867-887. Oxford University Press: Oxford

236 Pedrozo, Raul (Pete) (2009). Military Activities In and Over the Exclusive Economic Zone, in Nordquist et al. (eds.). Freedom of Seas, Passage Rights and the 1982 Law of the Sea Convention, p. 235-248. Martinus Nijhoff Publishers: Leiden, Boston

2023, as well as to the Estlink2 electricity and neighbouring cables damage in 2024, belong to the category of **hybrid warfare attacks**, not specifically regulated by the existing international legal instruments. The incidents have also raised questions about the limits of engagement for the military, as well as about the right of the coastal States to intervene beyond the limit of their territorial waters. UNCLOS and other legal instruments are insufficiently clear with respect to **the right of the coastal State to board and inspect a suspicious ship outside its territorial waters**, with the exception of the existence of a prior agreement in this sense from the flag State. The Balticconnector incident and the Estlink2 damage both took place in the Finnish EEZ, where the coastal State cannot exercise the right to board, inspect and arrest a suspicious ship, unless, as it happened in the case of the Estlink2 incident, the ship commander agrees for the vessel to be hauled into the territorial waters of the coastal State. Nonetheless, it has been suggested that the UNCLOS Art. 110 *The Right of Visit*, which for now allows boarding a suspicious ship on the high seas on grounds of piracy, slave trade and unauthorised broadcasting, could be extended in the future to also include suspected acts of sabotage[237].

5.6 Way forward

5.6.1 Recommendations for the MoDs and the defence sector to further contribute to the protection of OCEI in Europe

As noted by the European Defence Agency in its "Enhancing EU Military Capabilities Beyond 2040" study[238], **technological superiority is expected to be a major factor in future warfare**, posing challenges for the EU armed forces. Higher and more heterogeneous energy demand prompted by increased digitalisation, logistic and sustainment dependencies on energy sources, high level of electrification of future systems, new weapon systems implying a high energy demand will impact on the operational environment.

In this rapidly evolving environment, **the armed forces need to upgrade their military capabilities** in a number of areas identified as priority by the European Defence Agency:

- **The armed forces need cyber-resilient networks**, along with new advanced sensors based on quantum technologies able to collect more available data and gain an advantage through situational understanding.
- The MoDs can also make **increased use of artificial intelligence**, as AI-enabled systems will play a significant role in information control and counter-intelligence activities.
- This will also allow **the development of smart munitions** with greater precision, power, and range, while improvements in energy production and storage will enable the development of directed energy weapons (DEW) with increased range and power.
- The armed forces are encouraged to broadly **integrate robotics and autonomous systems** into their operations, reducing in this way the risk to human lives[238].
- Among the technological updates that can be used in order to strengthen the security of the maritime hotspots in the EU and of the OCEI located in the Union's waters, **countering AIS manipulation and spoofing** in order to prevent possible malicious acts by so-called 'dark ships' comes as a priority. Adding digital signatures to the unencrypted message transmitted by the AIS transponders is one possible solution that would increase the security of navigation[202].

Maritime security and specifically the protection of the OCEI can be enhanced through the **combined use of unmanned surface, submarine and aerial technology**:

- Thus, **unmanned surface vehicles (USV)** may be employed to perform fast and safe inspection of the offshore installations, in combination with the existing ROVs and divers[239].
- The recent disruptions to the subsea energy infrastructure in the Baltic Sea highlight the need for enhancing the underwater surveillance and detection capabilities. For this purpose, the use of **autonomous underwater vehicles (AUVs)** by the MoDs, already employed by energy companies for maintenance, can be successfully engaged in activities of intelligence and reconnaissance missions, in mines location operations, and in anti-submarine and seabed warfare.
- Maritime security surveillance can be additionally enhanced with the support of recent and innovative means of **unmanned aerial systems (UAS)**, for fast monitoring and detection of suspicious activities and potential damage of the offshore installations.

The group of experts that met in 2023 for the Third Ad-hoc Experts Group Meeting, "Protection of Offshore Critical Energy Infrastructure in the EU: Implications for the Defence Sector", which took place in Lisbon in partnership with the Portugal MoD as part of the CF SEDSS, identified a set of **opportunities for the MoDs to actively contribute to the protection of the OCEI**:

- The **establishment of a dedicated OCEI Protection Forum at EU-level**, reuniting the MoDs and the OCEI public and private stakeholders was proposed, to include also the EU's partners, such as Norway and the UK. The comprehensive OCEI Forum could be set up on the model of the existing European Offshore Oil and Gas Authorities Group working under the European Commission's Directorate General for Energy.
- In response to the proliferation and increased heterogeneity of hybrid attacks on the European critical energy infrastructure, the experts also proposed **the creation of a EU-level Practice-Sharing Framework** composed of an incident-triggered technical task force, a regular indicator of compromise (IoC) sharing program and a series of regular multistakeholder meetings that will allow for the dissemination of one or more incident-related case studies and best practices among critical infrastructure representatives from all participating Member States, in which the MoDs should play an active role.
- **Establishing a Hybrid Actions Reaction Team** for preventing and countering attacks on OCEI would involve the participation of MoDs in joint exercises and would allow for an uniformised framework of response at EU level, with a higher degree of homogeneity of practice and methodology across Member States, and established channels of communication and points of contact that would ensure a rapid and efficient response.
- ***Mitigation of risks at European level requires a European answer***. For this, the

237 Lott, Alexander (2024) Christmas Day Cable Cuts in the Baltic Sea. https://www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/

238 European Defence Agency (2023a) Enhancing EU Military Capabilities Beyond 2040: Main findings from the 2023 Long-Term Assessment of the Capability Development Plan. European Defence Agency, Isdefe September 2023. Catalogue number: QU-07-23-206-EN-N, DOI: 10.2836/360180

239 Offshore Source (2023) Protecting Offshore Energy Infrastructure Using Unmanned Surface Vessels (USVs). Offshore Source. https://www.offshoresource.com/news/oil-gas/protecting-offshore-energy-infrastructure-using-unmanned-surface-vessels-usvs

MoDs' efforts to enhance the protection and resilience of the OCEI should be developed under an integrated approach. As an example, the MoDs should use an **EU-level Standardised Methodology Framework** to evaluate their own reliance on OCEI and to identify risks, threats and vulnerabilities to their own security. Based on the national assessments, the MoDs can further elaborate integrated plans of action and response at regional and EU-level.

- In addition, **the MoDs' personnel should be provided with upskilling** and reskilling through dedicated academic modules, seminars, and vocational training, with regard to countering the new and emerging cyber and hybrid threats to the OCEI, including the upgrade of the know-how related to the specificities of the legal framework that govern the offshore field and the geopolitical dynamics that impact on the security of the OCEI. **Co-operation between military academies, and the civilian academia and experts** is key to enlarging the knowledge-base of the military staff, by providing it with up-to-date education and training skills and capabilities in the field of protecting and defending the OCEI.
- The **set up of an EU level Observatory for OCEI Risk Assessment** with the joint participation of the MoDs and civilian experts from academia and the industry was proposed by the CF SEDSS members, as part of the effort to monitor and update in real-time the sets of fast-evolving risks, threats and vulnerabilities to the OCEI, under the military-civilian cooperation component.

Building up on the recommendations provided by the "Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats" study[200] produced by the EDA, JRC and CF SEDSS III, as well as on the recently EDA-released "2023 EU Capability Development Priorities"[240], we consider that the MoDs should also:

- **Keep track of ownership of defence-related OCEI.**
- Develop or update **plans for the prevention, preparedness, response and recovery** necessary to maintain the resilience of defence-related OCEI against physical, cyber and hybrid threats.
- Conduct on a regular basis **vulnerability assessments** to improve situational awareness and mitigate risks in case of threats against defence-related OCEI.
- Systematically **collect intelligence and post-event data on cyber and hybrid threats incidents** on defence-related OCEI, and share lessons learned with other Member States and EU institutions.
- Perform **real scenario-based exercises**.
- Enhance and develop the **civil-military collaboration** towards developing comprehensive underwater surveillance capabilities.
- Integrate manned, unmanned, and fixed-sensor systems into a **common operational picture for critical infrastructure protection** on land, at sea and on the seabed.

5.6.2 Recommendations for the European Union to further enhance the security of the OCEI in Europe

Enhancing the resilience of the OCEI is key to the overall European security ecosystem facing an unprecedented escalation of hybrid risks, threats and vulnerabilities in the current geopolitical context. For this purpose, we brought together an aggregated set of recommendations and guidelines developed through this study and intended to suggest **key actions at EU level for reinforcing the protection and resilience of the OCEI**:

240 European Defence Agency (2023b). The 2023 EU Capability Development Priorities. DOI: 10.2836/229505. https://eda.europa.eu/docs/default-source/brochures/qu-03-23-421-en-n-web.pdf

- Keeping at core the need to overcome the existing policy fragmentation and taking into account that all OCEI and submarine cables work in synergy and are interdependent on each other, we strongly encourage **the extension of the recently released EU Action Plan on Cable Security to include all the major OCEI** (windfarms, oil and gas and cables) in a cross-sector and all-hazard approach. For the same purpose, we also recommend the development of an "**Offshore Security Toolbox**", in line with the Action Plan, that would go beyond the realm of cables to include all OCEI.
- Due to the potential escalation of risks, threats and vulnerabilities to the OCEI in Europe's maritime hotspots, and bearing in mind the recent incidents in the Baltic Sea, we recommend for the European Union's upcoming **Strategic Foresight Report to acknowledge the importance of enhancing the protection and resilience of the OCEI**, in a tailored approach adapted to its specificities as highlighted in this study.
- The policy fragmentation of the OCEI sector needs to be reduced by establishing an aggregated **EU Strategy for the Defence and Protection of the OCEI in Europe**, reuniting all existing and emerging offshore energy technologies (oil, gas, wind, wave, tidal power, hydrogen), under a single-hazard approach, addressing physical, cyber and hybrid threats jointly.
- The Consultation Forum for Sustainable Energy in the Defence and Security Sector (**CF SEDSS**) should continue in its fourth phase, which started on 1 October 2024, its ground-breaking work, by focusing particularly on **enhancing the protection and building resilience of the European subsea critical energy infrastructure (SCEI) against hybrid threats**.
- The necessity of **creating an EU-level Information Disclosure Mechanism** for countering physical, cyber and hybrid attacks, between Member States, as well as between Member States authorities and private OCEI stakeholders is a priority.
- The sector fragmentation, with the OCEI being split between public and private actors, should also be overcome by organising **regular real-life scenarios and tabletop exercises**, with the participation of public and private stakeholders.
- **Synchronised protocols of prevention and response strategies** among EU Member States, specifically dedicated to the protection of OCEI and maritime security, should be put in place.
- We also take note of the Council's recommendations on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure for Member States to encourage and support **critical infrastructure operators in the energy sector to conduct stress tests against malicious man-made threats**, as well as cybersecurity penetration testing to identify vulnerabilities, with the support of the cybersecurity preparedness services offered through the short-term support programme implemented with ENISA[241].

We also endorse the European Commission's recommendations for measures designed to enhance the maritime security in Europe, which implicitly adds up to the security of the OCEI, as included in the updated EU Maritime Security Strategy[173]:

- **Strengthening the defence maritime surveillance information exchange network** (MARSUR) by launching a dedicated programme through the EDA, and enhancing links between MARSUR and

241 Council of the European Union (2023). COUNCIL RECOMMENDATION of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Official Journal of the European Union, C 20/1. 20.1.2023

CISE.

- **Integrating high-end technologies for maritime security**, such as: space-based technologies, remotely piloted aircraft systems and radar stations, maritime patrol aircraft, and manned and unmanned seaborne means through innovative, cyber-resilient tools to boost maritime situational awareness.
- **Enhancing coastal and offshore patrol vessel surveillance** and upscaling it with digitally networked high-end naval platforms, including naval unmanned platforms to enhance prevention and response capabilities.
- **Elaborating new and updating existing risk assessments, contingency plans** and disaster recovery plans, at EU and national level for ports, coastal infrastructure, as well as passenger ship security and transport / supply chains.

5.7 Conclusions

The unprecedented escalation of warfare and overlapping security crises that have affected the European Union and its neighbourhood since 2022, along with the rapid expansion and diversification of physical, cyber and hybrid risks, threats and vulnerabilities to the security of the European OCEI, have prompted the EU to ramp up its efforts in order to enhance the protection and resilience of its critical offshore infrastructure.

Nevertheless, **fragmentation** still persists and it is posing limitations to the efforts to implement an effective and comprehensive strategy of prevention and response to potential attacks on the OCEI. Among the main challenges identified by the study, a major limitation stems from the absence of an integrated OCEI protection and resilience framework at EU level, that would reunite under a single umbrella all offshore energy sectors (oil, gas, renewables), under an all-hazard approach addressing physical, cyber and hybrid threats jointly. Fragmentation also affects the actors operating in the field of OCEI, with a large range of state, non-state, public and private actors playing the field.

In addition, there is a critical **interdependency** between a large variety of entities that play a role in the operation of the OCEI, from owners, operators, supply chain distribution, insurance companies, digital services providers, or private security, as various entities have different levels of security and protection in place. In addition, growing interdependencies resulting from increasingly cross-border and interdependent network of service provision across the EU reveal additional vulnerabilities of the OCEI, as in the event of a disruption, its consequences can rapidly spread to more countries and regions, in a cascading effect. Cascading disruptions in the energy sector may rapidly impact other sectors in the society and they may limit the military forces' capacity to respond, deploy and intervene in an effective and timely manner, as the defence sector largely depends on the public and private infrastructure.

Moreover, the seas and the oceans are governed by a very complex and specific **legal regime**. As a large part of the offshore critical energy infrastructure is located beyond the territorial waters of the coastal States and given the multinational character of many projects, differing interpretations of the law of the sea with regard to sovereignty, sovereign rights and jurisdiction over the OCEI frequently occur, on which the study shed light and provided clarifications related to the limits of authority and engagement of the MoDs for their protection.

The study compiled an **up-to-date set of specific risks, threats and vulnerabilities** to the European OCEI (oil and gas infrastructure, offshore windfarms and subsea power cables), by mapping the **physical, cyber and hybrid threats**, as well as the related techniques that can be employed independently or in synergy by various state-led, state-sponsored, non-state and transnational actors in order to perform attacks on the OCEI.

Conventional threats to the security of the OCEI continue to pose a significant risk, as physical attacks can be employed by surface, submarine or aerial means, with limited financial and technological effort. The subsea cables and pipelines are particularly vulnerable due to their location on the seabed, which makes them invisible and difficult to access.

The progressive digitalisation in recent years of the energy infrastructure renders it more vulnerable to the rapidly evolving **cyber risks and threats**. While cyber-attacks on the maritime infrastructure are not new, at present, the critical energy infrastructure finds itself exposed to an ever increasing and fragmented network of players, with high-end capabilities and means to inflict malicious cyber-attacks, even with limited costs and technological support.

Hybrid threats are purposefully ambiguous operations that blur the distinction between deliberate and unintentional events, as they are often employing apparently harmless non-state actors, such as fishing and cargo vessels, to perform seemingly accidental operations, camouflaging in this way the real malicious intent and an often state-backed or state-sponsored attack. At the same time, foreign control of critical infrastructure and strategic materials and supply chains is considered to be a vulnerability of the critical infrastructure. Tampering with the Automatic Identification System (AIS) of ships has been identified by the study as one of the most frequent techniques of hybrid warfare, with notable events occurring in the Black Sea and the Baltic Sea.

Having in view the set of risks, threats and vulnerabilities identified, the study performed a mapping of the **EU's main four maritime hotspots**: (1) the Black Sea (the most vulnerable maritime hotspot in Europe, the seat of the ongoing warfare between Ukraine and Russia in the vicinity of existing offshore oil and gas installations; (2) the Baltic Sea (the place of deliberate attacks on subsea pipelines and cables); (3) the Mediterranean Sea (where zones of high security alert exist due to their proximity to regional conflicts in the Middle East); (4) and the North Sea-Atlantic region (with areas of intensified activities of espionage around the offshore energy installations).

In its last part, the study provided a comprehensive set of **recommendations and guidelines** addressed to the EU and to the ministries of defence, in order to overcome the existing limitations and gaps in the protection of the European OCEI and to enhance the prevention and response capabilities.

In order to overcome the existing fragmentation and to successfully enhance the protection and resilience of the European offshore critical energy infrastructure, we conclude that cooperation within the EU and with its strategic partners, as well as cross-sector collaboration are crucial, as **mitigation of risks at European level requires a European answer**.

06

Increasing the Resilience of Defence-Related CEI: Lessons Learned from the Hybrid Threats Tabletop Exercise

***Gintaras Labutis**, Military Academy of Lithuania "General Jonas Žemaitis"*
***Hadjisavvas Constantinos**, European Defence Agency*
***Maja Kuzel**, European Defence Agency*
***Ioannis Chatzialexandris**, European Defence Agency*
***Alexandru Georgescu**, National Institute for Research and Development in Informatics ICI Bucharest*
***Nektarios Nasikas**, Hellenic Army Academy*
***Alessandra Lazzari**, European Defence Agency*
***Shana Leclerq**, European Defence Agency*

6.1 Introduction

In the face of growing geopolitical tensions and environmental challenges, how should the EU and its Member States respond if their energy production and transport infrastructure were targeted by hostile entities or unfriendly authoritarian regimes? Moreover, how would the EU react to climate-related emergencies that threaten critical energy infrastructure? Ensuring the protection of defence-related critical energy assets against a broad range of emerging hybrid threats is paramount.

This chapter emphasises the critical role of tabletop exercises (TTX) as a strategic approach to building competence in energy security and resilience within the framework of the Consultation Forum for Sustainable Energy in the Defence and Security Sector. It delves into the methodology of designing and executing energy-focused TTXs, tailored specifically to enhance the preparedness and response capabilities of EU Member States. This chapter explores the structured process involved in the design and execution of TTXs, focusing on scenarios that test the EU's ability to manage crises affecting its critical energy infrastructure. It highlights the collaborative efforts of various stakeholders—including the CF SEDSS Project Management Team, TTX design team, moderators, external service providers, participants, and stakeholders—to create realistic and challenging scenarios that reflect current and emerging threats.

6.2 The role of tabletop exercises in training and competence-building

TTXs are informal, discussion-based sessions where groups or teams review their roles and their responses during predefined emergencies by walking through realistic hypothetical scenarios. The primary purpose of TTXs is to evaluate and improve preparedness, coordination, and decision-making in simulated emergency or crisis situations, while fostering a collegial and exploratory environment, encouraging participants to discuss potential responses in a low-stress, no-risk setting. The outcomes of the TTX activities highlight areas for further improvements in readiness and effectiveness for real emergencies and crises.

TTXs are used to prepare for various emergencies, including energy and climate-related scenarios. They are less intense than functional exercises or full-scale exercises, where the functional or dedicated emergency teams respond to simulated crises in the field. Instead, TTXs take place around tables, with participants responding to scenarios designed by professionals and led by instructors and facilitators.

These exercises enhance critical thinking, problem-solving, and collaboration, while identifying gaps in existing plans or procedures. They provide a realistic understanding of roles and responsibilities in emergency or crisis situations, testing the effectiveness of an organization's plans without deploying resources. The following aspects highlight the importance of including TTXs in competence-building exercises:

a. **Evaluating preparedness**: TTXs assess an organisation's ability to handle emergencies, identifying gaps in plans, improving coordination, and enhancing overall readiness.
b. **Discussing scenarios**: Participants engage with predefined and hypothetical emergency scenarios, such as energy generation or energy supply or energy interruptions or natural disasters, tailored to specific risks faced by the organization or a network of interconnected organizations.
c. **Practicing roles**: Participants assume their actual or assigned roles, practicing their duties and understanding the responsibilities of others.
d. **Fostering critical thinking**: Unlike full-scale drills, TTXs focus on discussions, allowing participants to critically explore various aspects of response plans.
e. **Debriefing and improvement**: After the TTX, debriefing sessions evaluate team performance, discuss successes, and identify areas for improvement. These insights refine emergency plans, improving coordination and communication among team members. This process boosts participants' confidence in their ability to respond effectively to real emergencies. Scheduled follow-up activities ensure action plans are implemented, which might include additional training, updates to emergency plans, or subsequent exercises to test the changes made.
f. **Guided facilitation**: TTXs are led by a facilitator or a team of facilitators who present scenarios and support structured discussions

One can conclude that TTXs are a vital component of training and competence-building models, offering a unique platform for enhancing preparedness and response capabilities in a controlled, collaborative environment.

6.3 CF SEDSS hybrid threats tabletop exercise

In 2023, EDA, within the framework of the CF SEDSS, invited EU MoDs, particularly members of the PCEI WG3, along with relevant stakeholders, to participate in a Hybrid Threats TTX. This event was held in Sofia, Bulgaria, on 25-26 May 2023. The exercise was organised with support from the European Commission (JRC) and hosted by the Bulgarian Defence Institute (BDI) under the auspices of the Bulgarian Ministry of Defence (BG MoD). As a part of this TTX, EDA and the European Commission DG JRC presented a joint study "Fortifying Defence: Strengthening Critical Energy Infrastructure Against Hybrid Threats", which was a deliverable of CF SEDSS III WG3[242]. The key findings of this study were tested in TTX, and included in TTX scenarios that simulated real-world situations and were based on threats pertinent to the CF SEDSS III discourse, including cyber and physical attacks, disinformation campaigns, and climate change effects.

This TTX, which marked the first one organised by the EDA within the CF SEDSS framework, aimed to enhance defence energy resilience and boost European collaboration in this critical area. It also sought to explore the dependencies of the defence sector when CEI is compromised or inoperative due to hybrid threats. Given recent events, the exercise proved timely, drawing inspiration from relevant case studies and anticipating future issues by extrapolating from identified vulnerabilities and the current state of mapping hybrid threats to EU member states. Radostin Iliev, Director of the Defence Policy Directorate at the Bulgarian Ministry of Defence, echoed this summation of TTX objectives: "*This table-*

242 Giannopoulos G., Jungwirth R., Hadjisavvas C., et.al., Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats, EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/58406, JRC13308, available at fortifying-defence.pdf (europa.eu) - https://eda.europa.eu/docs/default-source/consultation-forum/studies/fortifying-defence.pdf

top exercise hosted in Sofia is a rare opportunity to encourage collaboration between European stakeholders in defence and civilian sectors. It helps deepen our shared understanding of how hybrid threats can impact critical energy infrastructure and subsequently compromise our armed forces' operational effectiveness". The TTX was planned and executed in collaboration with BHC Laboratory OU.

One of the key objectives of the TTX was to raise awareness and cultivate a culture of security and resilience in a multi-stakeholder model (including MoDs, energy businesses, academia, governmental institutions, and other civil stakeholders), which embraces a whole-of-society approach, encouraging collaboration between public and private sector actors to counter hybrid threats against defence relevant CEI. The importance of this collaboration was emphasised, and continues to be reiterated throughout this publication, as a result of the defence sector's significant reliance on civilian critical infrastructure, specifically with regards to, but not limited to, energy systems. The TTX focused on three key dimensions:

- Raising awareness on the protection of CEI against hybrid threats.
- Exploring MoDs' decision-making processes related to the protection of CEI and interrelated areas.
- Identifying areas for improvement in the protection of CEI from the perspectives of preparedness, prevention, and resilience.

The exercise generated lessons learned and recommendations to improve national processes and procedures, identifying areas where the EU can support and enhance national efforts while fostering collaboration at the EU level. The TTX scenario encouraged interaction among participants, promoting the sharing of information and best practices to develop situational awareness and management skills in a rapidly changing operational environment. The exercises also focused on how MoDs, armed forces, and relevant defence stakeholders should or could respond to, prevent, and manage hybrid threats against defence-related CEI while maintaining operational effectiveness and resilience.

6.4 TTX concept development and scenario design activities

The **Hybrid Threats Tabletop Exercise (TTX)** was designed to enhance decision-making and cross-sectoral preparedness by engaging defence, government, industry, and civil society stakeholders. Rather than scoring performance, the exercise aimed to facilitate discussions, highlight different perspectives, and identify areas for future improvements.

The TTX divided participants into four groups:

- **Blue Team (group A)**: Military (MoDs, armed forces).
- **Yellow Team (group B)**: Political/administrative decision-makers (e.g. ministries of energy, interior).
- **Orange Team (group C)**: Energy sector representatives (TSOs, DSOs, industry).
- **Brown Team (group D)**: Civil society (media, academia, NGOs, trade unions).

Facilitated by a **TTX management team**, the exercise simulated **hybrid threats** such as cyberattacks, physical sabotage, disinformation campaigns, and climate-related crises. The scenario was based in a **fictional geopolitical region (Rahulik Sea)**, representing competing national interests, energy dependencies, and vulnerabilities in critical energy infrastructure (CEI). To fully immerse participants in the scenario, the TTX included a **situational map** (Figure 39), depicting the Rahulik Sea region - **a hotspot of competing interests, resource rivalries, and geopolitical tensions**. The region featured an authoritarian power dominating its neighbours and several democratically leaning but fragile states struggling with energy security challenges. This setting enabled participants to navigate complex decision-making scenarios while assessing risks to CEI.

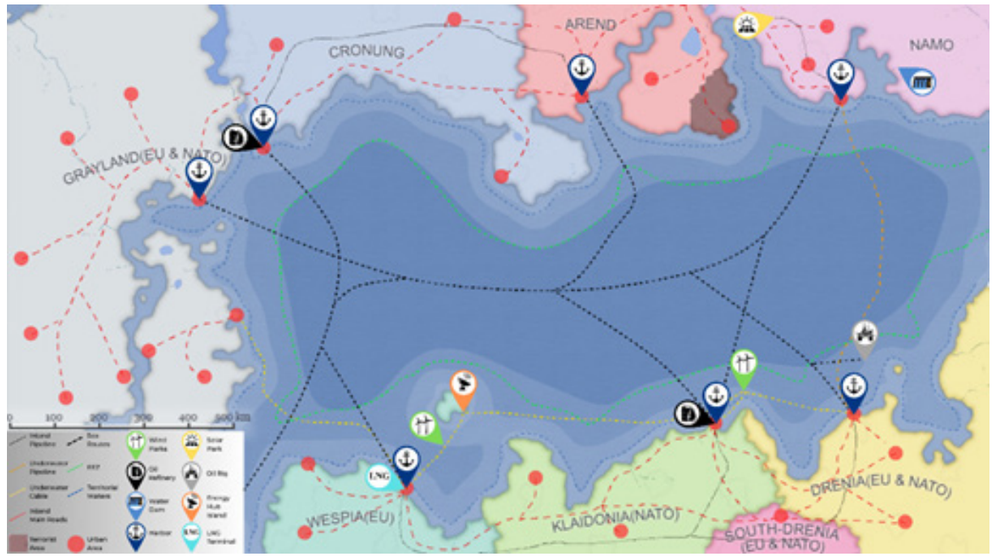


Figure 39 The image of the situational map of TTX scenario. Source: EDA

The exercise focused on four key areas:

1. **Hybrid Operations and Energy Production** - Addressing influence campaigns and offshore CEI vulnerabilities.
2. **Energy Transportation Infrastructure** - Examining sea-route risks and hybrid attacks on energy supply chains.
3. **Climate Change and Environmental Challenges** - Exploring cascading effects of extreme weather and adversarial exploitation.
4. **Military Capability Development** - Identifying how armed forces can enhance protection of CEI while navigating jurisdictional and operational complexities.

By fostering **situational awareness and collaboration**, the TTX provided valuable insights into defence-related energy resilience, civil-military cooperation, and strategic decision-making in the face of hybrid threats. Georgios Giannopoulos, Deputy Director of the Societal Resilience and Security Directorate of the Joint Research Centre of the European Commission, called the TTX "one of these moments when science, strategic thinking and operational capabilities are beautifully bundled together."

6.5 Execution of the tabletop exercise

The **Hybrid Threats TTX** gathered over 80 participants from 20 countries, including representatives from the European Commission, European External Action Service, industry, and the media. The exercise aimed to enhance coordination, assess hybrid threats, and test resilience strategies for CEI.

The TTX was structured around a simulated crisis in a fictional Sea region, where geopolitical tensions, hybrid threats, and energy disruptions threatened regional stability. The exercise tested decision-making, response coordination, and civil-military cooperation through scenario-based discussions, interactive incidents, and strategic assessments. It simulated a situation where a **hostile state, along with non-state actors, engaged in hybrid attacks targeting European energy security**.

These multi-domain threats included:

- **Cyberattacks on energy infrastructure**
- **Physical sabotage of critical assets**
- **Disinformation campaigns to manipulate public perception**
- **Disruptions to energy supply chains and defence logistics**

Participants had to **analyse threats, assess risks, and propose coordinated responses**. The digital exercise platform facilitated real-time collaboration, information-sharing, and strategic decision-making.

Key Scenarios and Insights

Part I: Energy Generation Network

- **Drone Attack on Wind Park** - A drone crashed into an under-construction wind park, leading to casualties, public panic, and operational disruptions. Participants evaluated threat severity, government-industry coordination, and strategic communication.
- **Underwater Cable Sabotage** - A power transmission cable was damaged, causing energy supply disruptions. The exercise tested resilience strategies, response coordination, and legal implications for securing offshore infrastructure.

Part II: Energy Transportation and Supply Chains

- **Naval Exercise Disruption** "(Figure 40) - A geopolitical rival launched an unannounced military exercise, disrupting key maritime routes and energy logistics.

Figure 40 Breaking news: Announcement of naval exercises. Source: EDA

Participants explored diplomatic, economic, and security responses to energy supply chain vulnerabilities.

- **Cyberattack on LNG Pipeline** (Figure 41) - A ransomware attack crippled a major gas pipeline, forcing stakeholders to decide whether to pay the ransom or mitigate the disruption through alternative means.

Figure 41 Breaking news: LNG pipeline under ransomware attack. Source: EDA

The discussion focused on cyber resilience, information-sharing mechanisms, and regulatory frameworks for crisis response.

Part III: Climate and Environmental Challenges

- **Dam Breach and SCADA System Hack** - A flooding disaster, coupled with a cyber intrusion targeting energy infrastructure, disrupted power supply and stressed emergency response capabilities.
- **Disinformation Campaign** - A coordinated propaganda effort spread false narratives, requiring participants to develop counter-disinformation strategies and public awareness measures.
- **Ammonia Leak in a Major Port** (Figure 42) - A terrorist attack on a chemical cargo vessel created a large-scale crisis, raising questions about civil-military cooperation, emergency preparedness, and rapid decision-making.

Figure 42 Breaking news: Leak in the harbour. Source: EDA

Part IV: Security and Defence Capability Development

Using the **DOTMLPFI framework, participants assessed capability gaps, policy recommendations, and response** effectiveness in:

- Doctrine and policy alignment
- Organizational coordination
- Training and preparedness
- Infrastructure security enhancements

Key Takeaways and Strategic Insights

1. **Cross-sector coordination is crucial** - Strengthening collaboration between military, government, and private sector stakeholders is essential for protecting CEI from hybrid threats.
2. **Hybrid threats require proactive resilience strategies** - The exercise reinforced the importance of cybersecurity, misinformation countermeasures, and infrastructure protection.
3. **Civil-military cooperation must be enhanced** - Effective communication, training, and joint crisis planning improve energy security and national resilience.
4. **Scenario-based exercises improve readiness** - Regular TTXs help identify policy gaps, streamline emergency protocols, and test real-world crisis responses.

The TTX provided valuable insights into hybrid threat management, CEI resilience, and defence-energy security interdependencies, emphasising the need for an integrated, multi-sectoral approach to crisis preparedness.

6.6 Lessons learned from the execution of the tabletop exercise

The **TTX management team and service provider** gathered extensive data and participant feedback, identifying key takeaways:

Enhancing information exchange
Stronger coordination between governmental entities (Group B) and media/social stakeholders (Group D) is needed to improve public awareness, counter disinformation, and ensure a more coherent situational picture for decision-making. Influence operations and hybrid threats underscore the need for better communication strategies to support authorities in crisis management.

Building shared situational awareness
In hybrid threat scenarios, information is often fragmented and originates from diverse sources. Effective data handling is critical, but more importantly, ensuring all stakeholders operate with a common understanding improves coordination and decision-making.

Strengthening multi-stakeholder involvement
The exercise reinforced the importance of input from MoDs, the private sector, and media in shaping response strategies. National decision-making processes must be more inclusive, reflecting the interdependence between defence, infrastructure operators, and public communication channels.

Defining clearer participant roles
Participants preferred representing a single state or actor rather than shifting roles. A more structured role assignment would allow for a deeper understanding of responsibilities, available resources, and international relationships, enhancing response coordination.

The role of civil society
The inclusion of media, academics, NGOs, and other citizen groups brought diverse perspectives. However, civil society does not function as a centralized entity in real-life crises, making their integration into decision-making complex. Future exercises should explore more realistic engagement models that reflect how civil society influences security responses.

Integrating civil society in decision-making
Group D should be involved in response planning, even if only as observers. Their expertise in communication, disinformation management, and public engagement can enhance crisis response efforts. However, trust, security culture, and institutional frameworks must be addressed to facilitate effective cooperation between defence actors and civil society.

6.7 Best practices, conclusions and recommendations

Participants identified several key principles for sharing best practices:

- Best practices should be shared at strategic, operational, and tactical levels.
- Civilian-military cooperation is essential.
- Academic involvement should be expanded to address new CEI protection challenges.
- Media strategies and counter-disinformation efforts must be prioritized.
- Tabletop exercises (TTXs) are effective for multi-stakeholder learning and cooperation.

Coordination and Response Models
Countries have different approaches to CEI protection—some have dedicated ministries, while others rely on a National Crisis Management Board integrating military, public, and private sectors. Early coordination and a national strategy enhance crisis response and mitigate communication failures.

The NIS and NIS 2 Directives were highlighted as key frameworks that facilitate information sharing and coordination across sectors. However, discussions revealed gaps in knowledge and collaboration, particularly regarding the role of non-operational and policy stakeholders in crisis events. Alternative strategies, such as strategic communication and mobilization of counter-narratives, were identified as areas for further development.

Key conclusions

- **Situational awareness varied across groups**, leading to different perspectives on threats and responses.
- **Standardized procedures** for public-private information sharing should be established.
- **Greater interaction between exercise groups** would improve shared awareness and stakeholder coordination.
- **Decision-making under uncertainty** remains a challenge, especially in civil-military cooperation where resources, expectations, and capabilities may be misaligned.
- **Strategic communication is vital** in hybrid threat scenarios, as adversaries aim to create prolonged uncertainty while staying below the threshold of armed response.

Managing uncertainty in hybrid threats
To navigate **high-uncertainty hybrid threats**, stakeholders should:

- Utilise AI and open-source data collection for better intelligence.
- Engage in cross-sectoral analysis (national-international, civilian-military) to leverage best practices.
- Consider multiple response strategies and decision-making frameworks.
- Prepare for cascading and escalating effects of incidents.

Offshore CEI protection and legal considerations
Participants raised concerns about **offshore CEI protection**, emphasizing:

- **Unclear roles and responsibilities** among stakeholders.
- **Legal uncertainties** regarding international law, liability, and proportional responses.

Additionally, **strategic communication** was identified as a key element in modern warfare and hybrid threats. Participants stressed the need for a coherent media strategy that connects national and EU-level communication efforts to counter misinformation and maintain public trust.

Civil-military cooperation and resilience strategies

- Civilian authorities must be fully aware of military capabilities and limitations in crisis response.
- National legislation should formalize civil-military cooperation to improve training and resource allocation.
- Armed forces recognize their reliance on privately-operated CEI, but concerns remain regarding uncertainty, overlapping jurisdictions, and multi-stakeholder coordination.
- National legal frameworks are crucial in guiding multinational civil-military responses to hybrid threats.

Strategic communication and countering disinformation
The **war in Ukraine** demonstrated that securing **public support** is crucial in both warfare and hybrid threats. However, participants noted a **lack of a unifying strategic narrative** that integrates media strategies into a broader crisis response framework. **Improved training and education** on disinformation tactics are needed at both national and EU levels.

Recommendations for future preparedness
Building on the **1st CF SEDSS III WG3 Hybrid Threats TTX**, the following **recommendations** were made:

- **Reduce information asymmetries** to improve resilience and crisis response.
- **Develop multidisciplinary teams** for crisis management, ensuring expertise in law, policy, and security.
- **Pre-establish crisis response networks** to avoid delays in mobilizing resources.
- **Strengthen EU-wide infrastructure** (e.g., CIWIN and ERNCIP networks) to improve transborder information sharing and resilience.
- **Enhance media and communication strategies** to explain crisis response measures to the public.
- **Expand TTX participation** across multiple stakeholder groups for more com-

prehensive training.

- **Establish continuous feedback loops** to ensure that lessons learned from exercises translate into improved resilience.

6.8 Overall evaluation of the TTX

The TTX successfully met its key objectives:

- **Investigating hybrid threats** and their impact on **critical energy infrastructure (CEI)**.
- **Bridging knowledge gaps** between stakeholders across defence, energy, and civilian sectors.
- **Providing resilience-enhancing recommendations** to strengthen responses against hybrid threats.
- **Promoting a 'whole-of-society' approach** to resilience-building through cooperation between public and private sectors.

In the words of Jiří Šedivý, Chief Executive of the European Defence Agency: "*The exercise allowed us to take advantage of diverse perspectives in developing comprehensive solutions to bolster defence energy resilience*".

It was **mutually agreed** that **EDA, JRC, DG ENER, EEAS, the European Centre of Excellence for Countering Hybrid Threats, and CF SEDSS PCEI WG3** will continue to analyse the insights gained from the exercise to **inform future TTX planning** and improve hybrid threat preparedness.

Parallel Study on Hybrid Threats
As mentioned in this chapter, parallel to the TTX, **EDA (CF SEDSS) and JRC** published an **in-depth study: Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats**[242]. The study aims to:

- **Enhance defence energy resilience** by proposing a **comprehensive suite of measures** at both EU and national levels.
- **Assess and mitigate vulnerabilities** in CEI through risk management, **policy streamlining, and technological advancements**.
- **Develop recommendations** for tailored risk management solutions, technology investments, intelligence reporting, training, and scenario-based exercises.

As hybrid threats continue to evolve, the study will be regularly updated to reflect European and national policy priorities, ensuring it remains a relevant and practical resource for decision-makers.

07

Critical Energy Infrastructure Protection in the Near Future - Topics for the Next Phase of CF SEDSS

***Alexandru Georgescu**, National Institute for Research and Development in Informatics ICI Bucharest*

7.1 Introduction

Alexandru Georgescu, *National Institute for Research and Development in Informatics ICI Bucharest*

As emphasised throughout this publication, CEI are faced with a challenging, complex and dynamic security environment. The wide array of stakeholders and the complexity of CEI, coupled with this environment, results in new risks, vulnerabilities and threats which undermine security and resilience, affecting defence actors but also business continuity in general, as well as trust on the part of citizens, partners and investors. We are faced not only with the prospect of greater frequency and impact of extreme weather phenomena and other disaster events, but also a greater diversity of deliberate threats from a wide array of threat actors engaged in hybrid warfare, such as systemic rivals, organized crime groups, lone wolves, ideological groups and more. In addition, we face the reality that complex systems experience "normal accidents", spontaneous malfunctions resulting from the interplay between different components and subsystems that can defy proper foresight and anticipation, as well as emerging behaviours that can cause disruptions. If they manifest at the same time as other crisis events, they can prolong a disruption, enhance its impact and delay the resumption of minimum acceptable levels of functioning. This is why resilience is so important, as the concept encapsulates different dimensions of a CEI's capacity to prevent negative events from occurring, to minimize damages should they occur and to return to a normal level of functioning having adapted through lessons learned in order to become stronger in the future.

WG3 of CF SEDSS brings together MoD participants and academics, private sector experts and representatives of other national and European institutions in order to allow their diverse backgrounds to produce new ideas for projects, new perspectives, new approaches and new arguments for European cooperation for ensuring the security and resilience of defence-related critical energy infrastructures.

7.2 A horizontal and a forward look upon the resilience of critical energy infrastructure

Georgios Kolliarakis*, German Council on Foreign Relations*

"Infrastructure," originally a French term adopted into English in the late 19th century, initially referred to the system of public works of a country or region. Its meaning expanded into the military domain following World Wars I and II, where it came to denote permanent installations required for military purposes[243]. Eventually, the term's usage broadened once more to include civilian contexts, now encompassing all foundational aspects of a system or organisation, both material and intangible[244]. Despite its various applications, infra-structure is traditionally understood as being "below" the surface - not always visible or immediately noticeable.

Contrary to that etymological claim, "infrastructure" has gained significant visibility in EU policy discourse in recent years. A series of strategic shocks in Europe since 2020 have exposed its vulnerabilities, including underinvestment, inadequate maintenance, and lack of fitness to meet evolving political and societal demands. These vulnerabilities include poor resilience to accidents, supply chain bottlenecks, and inadequate robustness against malicious foreign interference.

Since 2008, critical infrastructure categories in the EU have expanded from two (transport and energy) to eleven under Directive 2022/2557[245], which includes banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, and food sectors. By 17 October 2024, Member States are required to adopt national strategies, implement measures, and conduct regular risk assessments to identify critical vulnerabilities affecting society and the economy. Focusing on the cross-border nature of energy infrastructure, the Consultation Forum for Sustainable Energy in the Defence and Security Sector has been proactive since 2016 in emphasising the centrality of energy for defence and security, even before it became a prominent issue. This strong foundation is carried forward into the new Phase IV of the Forum (2024-2028) with a high level of ambition. As the EU's geopolitical landscape evolves and affects the threat environment, and with potential shifts in priority due to the changing European Commission, Parliament, and Council from 2025, the following recommendations aim to broaden the scope of strategic actions for the years ahead[246].

The geo-politicisation of energy infra-structure

The geopolitical significance of critical infrastructure, similar to research and innovation in advanced technologies, has sharply increased in recent years. Global geopolitical rivalries now frame infrastructure as a theatre of power competition, where dependencies can be weaponized. In this context, treating energy infrastructure within its traditional policy silo would be a strategic oversight.

The World Economic Forum's Strategic Intelligence work has mapped out an "Energy Transition" Transformation Map, highlighting correlations between core factors like energy system resilience and related drivers such as energy geopolitics, policy and governance, and innovation[247]. Notably, this map—though not defence-specific—links international security, infrastructure, cybersecurity, and the digital economy with social protection, illustrating the interconnectedness of these domains (Figure 43).

243 "Infrastructure." Merriam-Webster Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/infrastructure. Accessed 24 July 2024

244 Batt, H. W. 1984: Infrastructure: Etymology and Import. Journal of Professional Issues in Engineering, Volume 110, Issue 1

245 https://eur-lex.europa.eu/eli/dir/2022/2557/oj

246 The author has had the privilege to participate as invited expert in a number of workshops during the Phase III of the Forum. The thoughts in this brief are inspired by the interactions and valuable insights gained in that context

247 World Economic Forum – Strategic Intelligence: "Energy Transition: Building Energy System Resilience". Curation: Massachusetts Institute of Technology (MIT). Accessed 24 July 2024 under https://intelligence.weforum.org/topics/a1Gb00000038oN6EAI/key-issues/a1G0X000006DQC9UAO

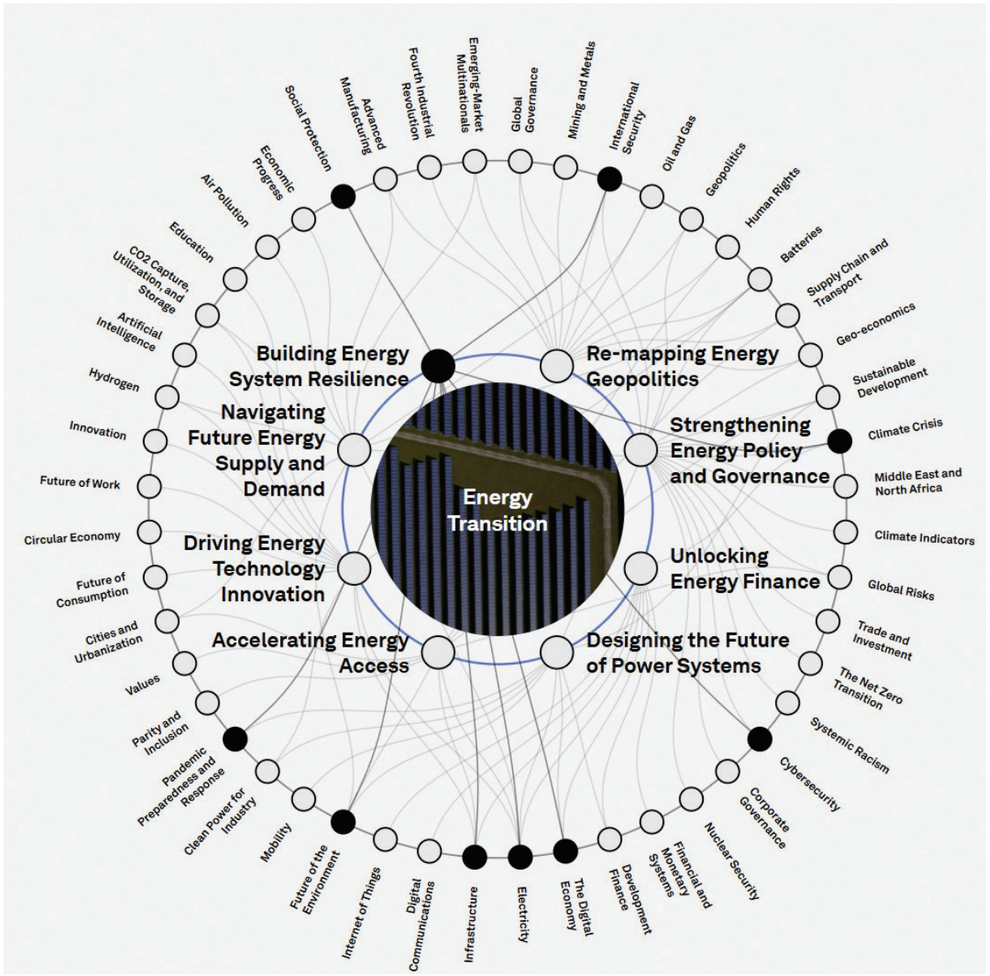


Figure 43 WEF Strategic Intelligence: Transformation Map "Energy Transition: Building Energy System Resilience"[247].

A decisive recast of that framing in the EU has recently taken place in the form of a European Union Economic Security Strategy, encompassing five initiatives to strengthen the EU's strategic autonomy while upholding the openness of trade, investment, and research[248]. The strategy prioritises four risk categories, among which the physical and cyber-security of critical infrastructure. Dual-use research and innovation uptake, as well as outbound and inbound foreign investment deserve dedicated attention as a matter of urgency from now on in matters related to critical energy infrastructure. Needless to say, the "Economic Security" paradigmatic shift will still need to pass over from paper to practice. In the author's view that entails the respective broadening of a "command and control" perspective in the consultations and analyses of the Forum the years to come. Practically speaking, the Consultation Forum ought to spell out how "de-risking" options, that is, mitigating risks and limiting strategic dependencies for energy infrastructure could or should look like, e.g. by conducting feasibility-desirability analyses.

248 https://ec.europa.eu/commission/presscorner/detail/en/IP_24_363

Risk assessment methodologies to get a grip on the double criticality

Energy infrastructure is a kind of "hyper"-critical asset, underpinning the functionality of most of the eleven essential plus seven important sectors designated by the NIS-2 directive. Its increasing susceptibility to cyber threats, especially due to the integration of digital components and heightened cross-border interdependence, creates what can be described as double criticality: firstly, in the sense that energy infrastructure is of vital importance to guarantee the continuity and security of most other societal functions; secondly, in the sense that it is vulnerable and subject to attack and weaponisation and needs itself to be secured. The salience of that double-faced criticality, given the number, frequency, sophistication, and impact of cyber-related incidents on networks and grids, cannot be overstated when accounting for the change in the security profiles of the NIS-2 directive's taxonomy of essential and important sectors.

Not least, the expansion of Grey Zone "hybrid" operations targeting energy infrastructure necessitates new methodologies to assess and mitigate risk, accounting for cyber-physical spillovers that can cause tangible societal disruption beyond traditional defence mandates. Leveraging the European Defence Agency's successful multi-stakeholder engagement during Phase III, future efforts should extend beyond national defence to include collaborations with bodies like the European Commission's JRC and the European Centre of Excellence for Countering Hybrid Threats.

A significant shift in the risk landscape involves the increasing influence of private corporations, from energy grid operators to digital platform and satellite companies. These entities often occupy a quasi-public–quasi-private domain, challenging conventional market competition and public accountability rules[249]. Consequently, issues of national sovereignty and security intersect with the contractual liabilities of public-private partnerships. Moreover, the insurance sector now plays a crucial role in defining acceptable risk levels for complex infrastructure, necessitating a deeper exploration of command and control rules in public-private partnerships to ensure public accountability.

An "all-hazards" capability-driven approach

While calls for technological innovation in infrastructure (e.g., AI or low Earth orbit satellites) are prevalent, it is essential to recognise that technological advances do not automatically equate to enhanced performance or security for energy infrastructure. If new technologies introduce vulnerabilities that necessitate further technological solutions, we risk a cycle of perpetual fixes, akin to the Red Queen's and Alice's race in Lewis Carroll's novel, where progress requires running ever faster just to stay in place[250]. To avoid this "hammer-nail" bias, it's crucial to focus on the contextual factors around technology adoption—organizational absorption, regulatory fitness, institutional mandates, stakeholder ecosystems, and human skills—rather than solely on the technologies themselves. Those "soft" factors around technology R&D seem instead to act as enabling (or constraining) for innovative technology to

249 Bridges, M. 2024: Infrastructure Is Remaking Geopolitics. How Power Flows from the Systems That Connect the World. In: Foreign Affairs, May 10, 2024

250 Carroll, L. 1871: Through the Looking-Glass and What Alice Found There, Chapter 2

turn into factual capability[251].

Future preparedness will hinge on innovation across organisational, institutional, regulatory, and human skill dimensions to manage emerging threats and complex emergencies with cross-sectoral impacts. This need was underscored by the scenario used in the 2023 tabletop simulation exercise in Sofia (see chapter 6), which highlighted the relevance of an "all-hazards" approach to include cyber and hybrid operations. Acknowledging the role of defence beyond territorial security, particularly in civil protection, points to the necessity of overcoming rigid divisions between civilian and military domains, potentially leading to more integrated "whole-of-government" or even "whole-of-society" approaches.

High-Impact/Low-Probability incidents foresight for capability planning

Building on the first and very productive tabletop decision game simulation in 2023, Phase IV should incorporate more hypothetic situational exercises, to foster, first, anticipatory forward-thinking and awareness of implications and impacts, and second, operational readiness and practical capacity of stakeholders across sectors. Ministries of Defence, among other governmental bodies, infrastructure operators, enterprise, and the civil society need to get trained to think outside of the conventional "box" if they are to prevent, respond, and prepare better against infrastructural disruption in the future. Scenario-building should cover a broad range of risk use cases, including but also going beyond the probable and improbable threats, and include HILP (High-Impact/Low-Probability) incidents, which are, as a rule, a major source of strategic surprise and shock.

Of particular focus should therefore be cross-sectoral spillover effects and the respective analysis of cascading and escalation dynamics, the preservation of business continuity, and the prevention of interstate conflict, or societal crisis/disruption. Methodologically speaking, risk use cases should be followed by road mapping exercises based upon capability gaps and requirements. The insights should elucidate future opportunities and constraints for action, and focus upon conditions for better situational awareness, the value-added of an EU-wide coordination, successful navigation within the multiple regulatory landscape, synergies or barriers to cross-stakeholder group cooperation, and modalities of public crisis communication.

Shift the strategic framing paradigm in the Phase IV: From protection to resilience

The choice of terms in policy and public discussions has repercussions of legal, political and technical character. In that respect "protection" of critical energy infrastructure signifies something different that critical energy infrastructure "resilience". Whereas the former is a more static term, seeking to maintain the status quo, the latter has a more dynamic connotation, pointing to equilibrium also with regard to future states. That difference between the protection and the resilience framings has already been an issue at the beginning of the respective EU CER directive 2022/2557"[252]

Almost simultaneously, at EU level, and as a result of the push toward more systematic foresight capabilities, better regulatory fitness and preparedness, the resilience dashboards have been introduced at EU level in 2021. The dashboards aim to provide a holistic assessment of resilience in the EU and its Member States, and they span four dimensions: social and economic, green, digital, and geopolitical. They feature a broad set of composite indicators, aiming to assess the relative strengths and weaknesses of Member States to help to identify areas for further policy action, and make Europe and its Member States shock-proof[253].

Specifically with regard to energy- or infrastructure-related indicators, the Green Dashboard includes indicators such as "energy productivity", "circular material use rate", or "renewable energy in final consumption". Suffice here, however, to feature only an excerpt from the Geopolitical Dashboard, containing the trends in key indicators such as "import dependence in energy materials", "supplier concentration in energy carriers", or "supplier diversification for energy carriers", among other, documenting the discrepant state of play in the EU Member States and the important "unfinished business" still to be accomplished (Table 5).

It would be of added value if the Forum in its future work contributed further evidence and insights to the drafting of Dashboards, rendering the view on energy infrastructure, more comprehensive and inclusive of potentially missing indicators. That would be an instrumental step forward, towards delivering both horizontal and forward-looking advice to European policymakers and stakeholders.

Concluding this brief, the author wishes to highlight a fragment from Enrico Letta's recent report on the future of the Single European Market, advocating the necessity to advance digital, energy or defence infrastructures and equipment to the status of European Public Goods[254].To build up European "muscle" would need to come hand-in-hand with building up such a mindset.

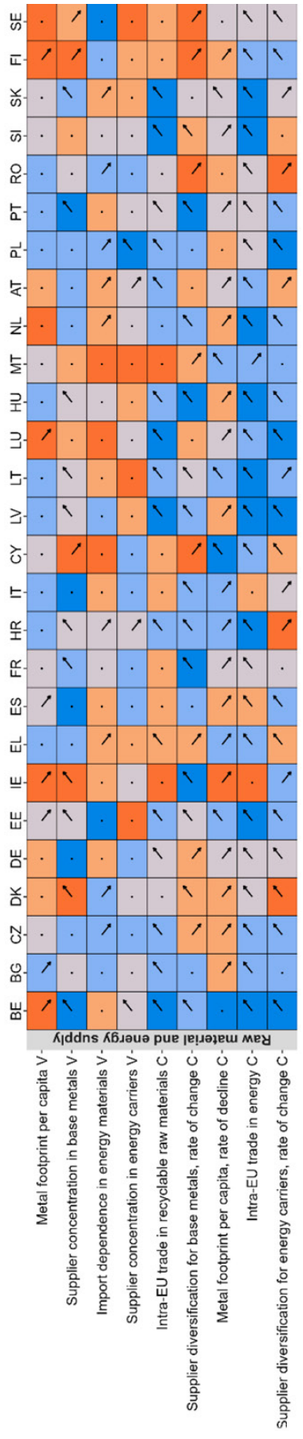
251 A compelling elaboration of how an "augmented" capability-driven approach looks like is delivered by the United Nations Institute for Disarmament Research on the domain of Cybersecurity, where capability is disaggregated into Policies and Regulations, Processes and Structures, Partnerships and Networks, People and Skills, and Technology. In: Dominioni, S. and Persi-Paoli, G. 2023: Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities. UNIDIR, Geneva. https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-i-mapping-the-foundational-cyber-capabilities/

252 "… due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted to enhance the resilience of critical entities. Critical entities should be able to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services." EU directive 2022/2557. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

253 https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report/resilience-dashboards_en. The dashboard includes a set of indicators that show the level of vulnerability and resilience capacities within a country, relative to other countries. Data typically refers to 2018-2022. Download from Eurostat as of 15 May 2024. The colours (Blue: Highest capacities/lowest vulnerabilities; Orange: Highest vulnerabilities/lowest capacities) indicate the position of a country in the distribution of all available values for EU countries in the 2007-2017 reference period (2015-2022 for indicators with an asterisk). An upward pointing arrow for a vulnerability indicates a substantial reduction (improvement)

254 Letta, E. 2024: Much more than a market, p. 36. https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

Table 5 EU Geopolitical Dashboard – Spring 2024 update (latest available year for each indicator up to 2022)[253], p. 9 (excerpt)



7.3 Artificial intelligence as an emerging threat vector, securing Europe's energy infrastructure

Luca Sambucci, *Gradient Intelligence and Italian Association of Artificial Intelligence*

7.3.1 The evolving landscape of AI threats and the heightened risks for critical infrastructure

As artificial intelligence (AI) systems become increasingly integrated into various sectors across the European Union, their potential to revolutionise operations and enhance efficiency is matched only by the emergence of new vulnerabilities that demand immediate attention from all industries and from policymakers at all levels. The rapid adoption of AI **has expanded the attack surface**, presenting significant challenges for cybersecurity.

While AI can offer advanced capabilities in threat detection and response, assisting and enhancing the defensive abilities of organizations, it can also be leveraged by malicious actors to develop highly targeted and adaptive attacks, and AI systems themselves can be vulnerable to exploitation, with attackers seeking to manipulate outcomes, compromise data integrity, or gain unauthorized access.

Some examples of adversarial attacks to AI systems include:

- **Dataset poisoning**: Introducing carefully crafted malicious data into training sets to manipulate model behaviour and undermine its integrity.
- **Evasion**: Modifying inputs to deceive AI systems, bypassing detection mechanisms and leading to incorrect or harmful outputs.
- **Model stealing**: Extracting the functionality or intellectual property of AI models, enabling attackers to replicate or misuse the technology.
- **LLM prompt injection**: Manipulating the outputs of language models through carefully crafted prompts, enabling the generation of targeted inappropriate or harmful content.
- **Backdoors**: Embedding hidden triggers within AI models during training, allowing attackers to control their behaviour when specific inputs are provided.
- **Supply chain compromise**: Targeting the AI development lifecycle and its dependencies, introducing vulnerabilities or malicious components at various stages.

Adversarial attacks on AI systems are not a new phenomenon, but as AI adoption accelerates and attackers become more sophisticated, we must anticipate and prepare for a significant increase in adversarial AI incidents. So far, the general incidence of AI-targeted attacks remained low due to their high costs in terms of resources, know-how and the relatively low footprint of AI in mission critical systems. Yet, in this context, **CEI face higher risks than other organisations**. Nation-state actors, motivated by geopolitical objectives rather than financial gain, have historically targeted these infrastructures to disrupt essential services, exert political pressure, or destabilize regions. The advanced capabilities and vast resources of nation-state actors enable them to exploit AI vulnerabilities, regardless of the complexity or expertise required. As AI becomes more integrated into the management and control of critical infrastructure, the potential impact of successful attacks grows exponentially.

7.3.2 CF SEDSS future focus

Recognising the urgent need to address the evolving landscape of AI-enabled threats in Europe and especially to critical energy

infrastructures, the Forum should pursue in phase IV tackling the multifaceted challenges posed by AI integration in the energy sector. It should focus on identifying vulnerabilities, exploring defence mechanisms, and formulating effective policies:

- **Identify and analyse AI-enabled attack techniques**: Conduct a thorough exploration of current and emerging AI-enabled attack vectors specific to the energy sector, evaluate their potential impact on various components of energy infrastructure, and analyse relevant case studies to gain insights into attacker methodologies and motivations.
- **Examine risks and vulnerabilities of AI integration**: Focus on assessing the vulnerabilities introduced by AI systems in control, monitoring, and decision-making processes within energy infrastructure, identifying potential points of compromise in AI models, and evaluating the cascading effects of successful attacks on AI systems.
- **Explore best practices and emerging technologies**: Investigate cutting-edge techniques in AI security, explore the effectiveness of AI-specific security measures, and determine the potential of emerging technologies in enhancing AI robustness in critical infrastructure.
- **Develop strategies to bridge the defence gap**: Identifying key areas where current defence mechanisms fall short, proposing collaborative frameworks for knowledge sharing between stakeholders, and developing guidelines for continuous assessment and improvement of AI security measures in response to evolving threats.
- **Formulate policy recommendations**: Propose policy measures to incentivise secure AI systems, recommend strategies for international cooperation, and develop guidelines for ethical AI development and deployment in the energy sector, with a focus on security and reliability.

To achieve these objectives, it requires exploring the activities below:

- Form a cross-disciplinary task force comprising experts in AI, energy systems, cybersecurity, and policy to identify and prioritise AI security challenges in the energy sector.
- Build strategic ties with relevant EU-level projects and initiatives focusing on AI and cybersecurity to leverage existing knowledge, avoid duplication of efforts, and ensure alignment with broader European strategies.
- Conduct a comprehensive study on the impact of AI-related threats on European energy security, including:
    - Analysis of potential attack vectors and their consequences.
    - Assessment of current defence capabilities and gaps.
    - Examination of regulatory frameworks and their effectiveness.
    - Exploration of international cooperation opportunities.
- Develop a set of guidelines and best practices for implementing AI systems in critical energy infrastructure securely.
- Publish and disseminate the findings and recommendations to relevant stakeholders.

7.4 Enhancing protection and building resilience for the European subsea critical energy infrastructure (SCEI) against hybrid threats

Roxana Andrei, *Centre for International Studies – University Institute of Lisbon*

7.4.1 Problem analysis and relevance

At present, the maritime areas of the European Union and of its neighbours are challenged to an unprecedented level by quickly multiplying hybrid warfare techniques and actors, with a constantly growing set of risks, threats and vulnerabilities to the European offshore critical energy infrastructure. **The subsea critical energy infrastructure (SCEI)** is the most vulnerable component of the offshore facilities, as a considerable part of the offshore infrastructure, such as pipelines, electricity and communication cables, is located under the sea and on the seabed, rendering the SCEI almost invisible to aerial and maritime means of conventional surveillance, and consequently more vulnerable to potential hybrid and cyber-attacks, terrorism, and acts of naval warfare.

As of 2023, the European Union has recorded several **attacks on its SCEI**, all in the Baltic Sea: the Balticconnector gas pipeline damage in October 2023, the Nord Stream gas pipelines explosions in September 2022 and the damage of the Estlink 2 submarine power cable between Finland and Estonia in December 2024. In addition to the existing subsea infrastructure, new offshore projects, dependent on their embedded subsea infrastructure are underway, such as the multi-purpose interconnector that will connect the Netherlands with the UK, **new offshore wind projects** in the Black Sea and the North-Sea Atlantic region, or the Georgia-Romania subsea electricity interconnector under the Black Sea.

7.4.2 Objectives

In this dynamic context, the fourth phase of the CF SEDSS should focus on building on the activity already undertaken by its WG3 in protection and resilience of offshore CEI, and to work in line with the **2023 EU Capability Development Priorities**, by focusing specifically on the most vulnerable of the offshore infrastructure: the **Subsea Critical Energy Infrastructure**. This requires extending and deepening the knowledge base formed through the two expert studies developed by the WG3 experts, "Protection of offshore critical energy infrastructure beyond national sovereignty: military rules of engagement and barriers" and "Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats", by working in the new phase on **enhancing the protection and building resilience of the European subsea critical energy infrastructure against hybrid threats. In this context, we recommend exploring the following objectives**:

- **Identify and analyse the most recent hybrid warfare techniques threatening the SCEI** under an all-hazard approach including cyber, conventional, and cognitive warfare, and superiority factors and actors, in the four maritime areas of the EU: the Baltic Sea, the Black Sea, the Mediterranean Sea and the North Sea-Atlantic Region.
- Identify and highlight the existing and prospective initiatives that can be used for the protection of SCEI and be replicated elsewhere in Europe.
- **Examine the risks and vulnerabilities posed by the extensive use of unmanned underwater vehicles (UUV)** - drones, due to their potential of being employed for malicious purposes in underwater warfare; bearing in mind their

ability to operate in an almost invisible mode, and to carry weapons and gather intelligence.

- **Analyse the synergies between the ongoing risks, threats and vulnerabilities to the maritime and offshore energy security outside of the EU borders**, in order to reveal the connections and implications to the European SCEI security in a possible spillover effect, as for example from the Red Sea to the Eastern Mediterranean.
- Develop **guidelines for the EU and the defence sector** offering concrete recommendations for enhancing the protection and resilience of the subsea infrastructure, as an integral part of the already proposed suggestions for an aggregated EU-level Offshore Energy Security Strategy.

7.4.3 Activities

To address these objectives, the Forum could:

- Organise a **workshop** with the participation of the EU policymakers, EDA, MoDs, industry and the academia.
- Establish a **working nucleus** of experts and policymakers in the field, under the auspices of the WG3.
- Publish an **expert study** on the topic of enhancing the protection and building resilience of the European subsea critical energy infrastructure against hybrid threats.

7.5 Safeguarding the renewable transition by cyber risk quantification technology that allows for balancing of security, climate, and economical politics

Jens Christian Vedersø, *Head of Cyber Risk Management Vestas*

The transition into renewable energy entails digitalising and distributing energy production, while energy supply becomes exposed to cyber risks. To be successful, the transition to renewable energy sources will require large investments and decisive political compromises. While geopolitical tension is growing, the uncertainty to investments and security requirements risks becoming a barrier for the renewable transition. When faced with uncertainty and technical complexity, it is easy to be perplexed, which, combined with the current cyber threats, means that an overreaction is likely. To address this problem, an open-source reference model for cyber risk quantification should be developed. This model will allow communication on factors of cyber risk across the complex value chain of the future electricity sector.

As the renewable transition requires a new combination of technologies, processes, and organisations, controlling the cyber risks associated with the transition requires collaboration; at the same time, attack methods of threat actors constantly evolve, making the challenge a bigger problem as incentives, capabilities, and knowledge all need to align to support the most efficient mitigation of risk. Hence, there is a need to structure collaboration on cyber risks across government security entities and the organisations driving the renewable transition. Currently the attackers and defenders are in an unequal race, where attackers maintain the element of surprise while defenders struggle to establish clear communication, responsibilities, and reactions.

The **renewable energy transition will require balancing three political ambitions**:

1. **Reduce carbon emissions** - to secure a sustainable environment for future generations.
2. **Support a competitive economy** - by having affordable energy to power future economies.
3. **Support security politics** - by providing energy independence and minimize the attack surface of our society.

Balancing these three ambitions we will require deep understanding of all areas and a framework to prioritise between these. There is a need for defining this framework, set metrics and develop a communication form that allows investors to forecast the return of investment while governments can prioritise resilience towards hostile attacks.

Addressing the quantification of cyber risk

When attempting to manage cyber risk, one is faced with the challenge of accurately determining it. Various sources claim various levels of risk, and the embedded factors of threats, weaknesses, and impacts. To understand these sources and utilise them there has to be a structured method for gathering threat data and analysing it. The concept of a cyber-attack implies deliberate action from a threat actor. To assess how often a specific digital environment will be attacked requires considering the capacity, motive, and knowledge of the threat actor. The concept of a cyber-attack implies the exploitation of a vulnerability or structural weakness to gain technical access to a digital system. To assess these, it is paramount to involve the manufacturers and structure their data. Consequently, the concept of cyber attacks implies losses. These losses can be measured in lost efficiency of achieving three ambitions:

- Reduce carbon emissions (CO_2 emitted)
- Efficient return of investment (Net-cash-flow)
- Secure and reliable energy supply (Energy not served to society)

7.6 Interdependencies of critical infrastructure

Rune Lausund, *Norwegian Defence Research Establishment FFI*

7.6.1 Problem analysis

Several studies[255,256,257] have documented the vulnerability modern societies face due to interdependencies of critical infrastructure. Critical infrastructure is described as complex adaptive systems that undergo constant interaction with their economic, social, and natural environments. In short, energy is crucial for all sectors, e.g. governance, finance, digital communication, health care and logistics, and likewise the energy sector depends on systems such as critical digital communication, logistics and numerous support systems. Building a robust and resilient society within available resources therefore requires a well-bal-

255 S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control System Magazine, vol. 21, pp. 11-25, 2001

256 E. J. Oughton, W. Usher, P. Tyler, and J. W. Hall, "Infrastructure as a Complex Adaptive System," Complexity, vol. 2018, p. 3427826, 2018

257 E. Chang, "Infrastructure resilience to disasters," The Bridge, vol. 39, pp. 36-41, 2009

anced system of robust infrastructure in all main sectors, CEI being one of the most important key stones.

Several Member States organise national readiness and defence in a total defence system meaning that the whole society must be prepared, and act coordinated to optimise the nation's ability to handle natural disasters, hybrid war and, if needed, armed conflicts; hence, governmental policy makers must identify vulnerability within all sectors and prioritise within limited resources cross-sectorial actions to optimise resilience. In a complex system of systems with accelerating technology development and rapidly growing cross-sectorial complexity, policymakers at European and national level increasingly need fact-based guidance. Stig Rune Sellevåg, in his article[258], has proposed a practical-in-use system-scale and cross-sector functional approach for modelling total defence systems that is grounded in theory for complex systems. The model is a simplified model that maps interdependencies between the sectors and estimates interdependency parameters for each sector. Sellevåg establishes his functional approach on the basis of an abstraction-decomposition space for critical infrastructure systems, taking into account NATO's seven baseline requirements.

Studies conclusively show that the robustness of the civilian readiness systems as well as nations defence systems depends on a well-balanced system of critical infrastructure whereby the energy system is crucial. To enable governments across Europe to establish and assess resilience within the individual nations and collectively for Europe, a model to study interdependencies and potential cascading consequences that follow disruptive events in a complex system should be enabled.

7.6.2 Objectives

Based on the identified need for a well-balanced and resilient cross-sectorial readiness the CF SEDSS in phase IV should continue building on the work already undertaken by its WG3 and focus specifically on the energy sector as a key stone in a critical infrastructure interdependency model. This can be achieved through the following goals:

- Develop a conceptual study to identify and analyse the need for a critical infrastructure interdependency model based on crucial input from policymakers across Europe.
- Propose a practical-in-use model that may be used by European policymakers.
- Examine the proposed model and establish methodology for identification and estimation of critical infrastructure interdependency parameters.

The effort may lead to a state of the art practical-in-use and evaluated model to be used by European policymakers when prioritising measures to increase robustness in critical infrastructure in general and more specifically critical energy infrastructure.

7.6.3 Activities

For these goals, the following activities are proposed:

- Organise a workshop to identify the need for critical infrastructure interdependency models and identify existing models.
- Establish a working nucleus of experts and policymakers in the field to identify key user requirements for an enhanced critical infrastructure interdependency model.
- Develop a study describing a model that fulfils the identified key user requirements.

258 Stig Rune Sellevåg, Modelling Total Defence Systems to Inform National Resilience Objectives – A Norwegian Case Study, STO-MP-SAS-OCS-ORA-2022

7.7 Enhancing protection and building resilience for European critical infrastructures against cascading risks

Christos Makropoulos, *School of Civil Engineering, National Technical University of Athens*

7.7.1 Problem analysis and relevance

The interconnectivity of critical infrastructures (CIs) in Europe is rapidly increasing, driven by advancements in (mostly digital) technology and the implementation of green and digital EU twin transition policies. This interconnectedness, while enhancing efficiency and integration across sectors, has simultaneously introduced a complex web of dependencies and potential vulnerabilities. Key infrastructures, such as energy, telecommunications, water, and transport, are now interwoven so tightly that a disruption in one can have significant cascading effects on several others. On the military side, this risk is further complicated by the level of integration of civilian and military infrastructures. As such, the challenges CI operators face in being able to identify attack vectors originating from interconnected CIs and assess related effects, including between these interconnected civilian CIs and military-relevant infrastructures, especially in the context of sustained warfare, remains an intricate challenge. The complexity of these systems-of-systems means that traditional risk assessment methods are no longer sufficient. A new, much deeper, understanding of these cascading risks is essential for enhancing the resilience of European CIs and of the military capabilities these civilian CIs support.

7.7.2 Objectives

In this context, it is recommended that the future work of the CF SEDSS includes advancing the understanding and management of cascading risks among European CIs. Building on the previous work, the focus could be on identifying and quantifying risks from CI cascades, with a particular emphasis on the interconnectedness of civilian and military infrastructures.

- **Objective 1**: Develop a comprehensive framework to identify and map interdependencies among key CIs, including energy, telecommunications and water.
- **Objective 2**: Create methodologies and metrics for quantifying the cascading effects of disruptions across interconnected CIs, incorporating both civilian and military infrastructures.
- **Objective 3**: Enhance the capability of CI operators to identify and mitigate attack vectors originating from interconnected CIs.
- **Objective 4**: Formulate guidelines and best practices for CI operators and policymakers to improve resilience against cascading risks.

7.7.3 Activities

To achieve these objectives, the following activities are proposed for future work as part of the CF SEDSS:

- **Activity 1**: Workshops: Organise a series of workshops with EU policymakers, CI operators, EDA, MoDs, industry leaders, and academia to discuss the current state of CI interdependencies and cascading risks. Facilitate knowledge exchange and collaborative problem-solving among stakeholders.
- **Activity 2**: Expert Working Groups: Establish expert working groups under the auspices of WG3 to focus on specific aspects of CI interdependencies and cascading risks. Include experts from various fields such as cyber security, in-

frastructure management, risk assessment, and military logistics.

- **Activity 3**: Research and Development Projects: Initiate R&D projects and studies aimed at developing tools and methodologies for mapping CI interdependencies and quantifying cascading effects. Projects will leverage advanced technologies such as AI, machine learning, and big data analytics to model complex interactions between CIs.
- **Activity 4**: Case Studies and Simulations: Conduct case studies and simulations of past incidents involving CI disruptions to understand the nature and impact of cascading effects. Use insights from these studies to refine risk assessment methodologies and enhance predictive capabilities.
- **Activity 5**: Guidelines and Best Practices: Develop and publish a set of guidelines for CI operators and policymakers based on findings and expert recommendations. Guidelines will focus on enhancing resilience through improved risk identification, mitigation strategies, and response protocols.
- **Activity 6**: Interdisciplinary Collaboration: Foster interdisciplinary collaboration between civilian and military sectors to ensure a holistic approach to managing CI risks. Promote joint training exercises and scenario planning to prepare for potential cascading disruptions.
- **Activity 7**: Publishing an expert study: Develop a study examining this new understanding and proposing a framework for management of cascading risks among European CIs highlighting their relevance for European Defence.

7.8 The space dimension of defence-related critical energy infrastructures

Alexandru Georgescu, *National Institute for Research and Development in Informatics ICI Bucharest*

Space systems are now indispensable to the resilience and security of defence-related CEI, providing essential services for navigation, communication, and grid synchronisation. We can even argue that some of these systems, alongside their ground stations, communication uplinks and downlinks and other components, are themselves critical infrastructures and critical components of defence-related CEI. Space assets provide critical services related to earth observation, telecommunications, navigation, positioning and timing, early warning and others. In the context of CEI, we can see the following contributions:

- Remote sensing for observation of the environment of operation for CEI, including disaster management, weather forecast, investment planning, civil preparedness and mapping environmental impact;
- Atomic clocks aboard global navigation satellites help synchronise European energy grids, ensuring stability despite fluctuating RES and an increasing number of prosumers;
- Telecommunications services, for emergency response and the management of complex distributed control systems and databases.

The role of space services is heightened by the twin digital and green transitions of the EU, as well as the gradual shifts in the CEI landscape due to economic, environmental, policy or technological factors. In the future, the consumption of space services will grow, not just in the field of CEI operation or protection, but also across many other domains, from food production to financial markets and banking or ICT. For this reason, the CER Directive and the NIS 2 Directive recognise space as a new domain where critical European entities (essential for NIS 2) may be identified and designated. The EU has consistently built up a framework for space governance and the pursuit of its interests as a space power, with moves such as:

- The development of the EU Space Programme Agency (EUSPA) with a mandate for cooperation with other member state agencies and partners abroad like the US;
- The development of an EU Space Strategy for Security and Defence in 2023;
- The development of DG DEFIS, the Directorate General for Defence Industry and Space;
- The 2024 decision of having an EU Commissioner for Defence and Space, whose mission also includes “the design and implementation of a European Air Shield and cyber defence common project”, the implementation of the EU Space Strategy for Security and Defence, the EU-NATO partnership covering “all threats, including those linked to cyber, hybrid or space”, further European Defence Fund investment in space capabilities and cyber, while overseeing the future space law and the Space Data Economy Strategy;
- The rising number of national space forces, following the establishment of the US Space Force and then that of France.

The EU has prioritised the development of critical space capabilities through projects such as the Copernicus Earth Observation constellation, the Galileo global navigation satellite system, EGNOS, the European Geostationary Navigation Overlay Service, or the future GOVSATCOM secure government communications network, recently renamed as IRIS^2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite).

From the perspective of Working Group 3 on PCEI, the subject of space is of growing interest. It has been approached through specialty presentations by European experts during the June 2022 fourth CF SEDSS III Conference and first Energy Technology Solutions Conference in Bordeaux, France, and during the April 2024 WG 3 and WG 1 Joint Ad-hoc at FORTH in Heraklion, Greece. Space was also a background element in the scenario of the Hybrid Threats to PCEI tabletop exercise organised in Sofia, in May 2023. However, the Working Group 3 has so far not approached the subject systematically, from the perspective of integration into its deliverables. Space is becoming more and more relevant to MoDs, which are interested not just in securing their affordable, accessible, sustainable and resilient access to critical space services for their missions, but also through the impact of disruption of space services now and in the future, on the critical infrastructures on which the MoDs are critically dependent, such as energy.

Some of the potential activities on space services and resilience in the context of PCEI within Working Group 3 include:

- Organisation of an ad-hoc event bringing together experts to explore the impact of space on PCEI in the context of European transformations on space and space governance;
- Conducting a contracted study on the impact of space on European PCEI

As space systems become increasingly vital for CEI resilience, defence stakeholders must urgently assess and mitigate the risks posed by space service disruptions. A coordinated approach—integrating defence, energy, and space policies—is essential to ensuring operational continuity and security in an era of emerging hybrid threats.

7.9 EDA HEDI's role in strengthening critical energy infrastructure resilience through innovation

Federica Valente, *Hub for EU Defence Innovation Manager, European Defence Agency*

The European Defence Agency's Hub for EU Defence Innovation (HEDI) plays a pivotal role in addressing defence innovation challenges in the defence sector by providing a platform for Member States and seed funding to industry to identify, mature and test solutions for future capabilities. As we look towards future phases of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), it becomes increasingly clear that innovation must sit at the heart of efforts to safeguard critical energy infrastructure (CEI). This section outlines how HEDI's activities could contribute to enhancing resilience through collaboration, innovation, and capability development, especially in the context of sustainable energy, climate change adaptation, technological advancement and addressing hybrid threats. HEDI's initial portfolio of services provides an array of capabilities that can support the resilience and protection of defence-related CEI against a rapidly evolving threat landscape.

Innovation as a cornerstone of resilience

In an era of hybrid threats and climate-driven disasters, the complexity of defending CEI necessitates a shift from traditional protection mechanisms to dynamic, adaptive, and innovative approaches. HEDI's mission aligns with this objective by fostering a comprehensive innovation ecosystem that encourages collaboration across Member States, private industry, and research institutions. Innovation in defence is not only about developing new technologies but also about creating resilient systems that can anticipate, absorb, and recover from disruptions — whether those disruptions come from cyberattacks, extreme weather events, or geopolitical tensions.

HEDI's innovation framework emphasizes:

- **Cross-sector collaboration**: Bringing together civilian and military actors, particularly in energy and defence, to jointly develop resilient infrastructure.
- **Dual-use technologies**: Investing in solutions that can protect both civilian energy systems and military operations.
- **Agile capability development**: Fostering rapid prototyping and operational experimentation (OPEX) campaigns to test and integrate innovative solutions within short timeframes.

The OPEX campaign spearheaded by HEDI is a core pillar of its strategy to foster innovation across defence sectors. These experiments focus on pushing technologies from technology readiness level (TRL) 5 and above, directly into military operational settings to assess their real-world application. In the context of CEI protection, HEDI's OPEX campaigns can be instrumental in testing and validating emerging technologies that aim to protect critical energy infrastructure. For instance, testing autonomous systems for **real-time monitoring** of energy networks can prevent physical attacks or malfunctions caused by environmental factors. Likewise, technologies that optimise **energy grid recovery** following a cyberattack or natural disaster can be refined through these experimentation platforms.

Through initiatives such as the HEDI-led OPEX campaigns, these innovation pathways are actively shaping how the EU's defence sector can better prepare for and respond to disruptions in energy infrastructure.

One of HEDI's most impactful services is its role in **innovation foresight and horizon scanning**. This service helps Member States and defence organisations anticipate and prepare for emerging threats to CEI by identifying key technological trends and breakthroughs.

Through foresight activities, HEDI enables stakeholders to gain an advanced understanding of potential **technological disruptors** that could both enhance or challenge CEI resilience. For example, advances in **artificial intelligence and machine learning** can be leveraged to predict and mitigate energy network failures before they happen. Simultaneously, foresight can identify new threat vectors, such as **adversarial AI** or **sophisticated ransomware**, ensuring that EU Member States are prepared for the next generation of cyber threats.

By continuously scanning the horizon, HEDI's foresight services offer crucial data to guide **investment in R&D** and ensure that EU defence sectors are strategically aligned with both energy security and resilience goals.

Building a common picture of innovation

One of HEDI's contributions is the definition of a **common picture of defence innovation**. By facilitating open dialogue, HEDI aims at enhancing transparency around emerging technologies and defence solutions, ensuring that EU Member States and their defence sectors can share and adopt best practices in defence innovation.

Synergies across the EU defence ecosystem

A central theme in HEDI's approach to innovation is the importance of fostering synergies across the EU defence ecosystem. CEI resilience is inherently multi-disciplinary, requiring cooperation between a wide range of sectors and actors. HEDI's collaboration with CF SEDSS, the European Commission, and private sector innovators aims to break down silos and build a united front against emerging threats to CEI.

Conclusion

As the EU advances into the next phase of CF SEDSS, HEDI can become an instrumental player in strengthening CEI resilience through innovation. By fostering a collaborative, forward-looking approach to CEI protection, HEDI can bridge the gap between defence needs and emerging technological solutions. In a rapidly evolving threat landscape, the ability to innovate quickly and effectively will be key to ensuring that the EU's critical energy infrastructure—and by extension, its defence sector—remains secure, resilient, and prepared for the challenges of the future.

HEDI's efforts align seamlessly with CF SEDSS objectives in advancing sustainable energy technologies and climate change adaptation. By promoting collaboration between armed forces, civilian energy operators, and private industry, HEDI ensures that advanced technologies like blockchain, big data analytics, and digitalisation enhance energy management and mitigate operational risks. Additionally, HEDI's foresight and horizon scanning capabilities help anticipate emerging threats such as adversarial AI and ransomware, enabling proactive measures against hybrid threats and addressing the interdependencies of critical infrastructure. By supporting the CF SEDSS Technology, Research, and Innovation Hub, HEDI helps promote best practices in smart energy technologies, making a strong contribution to the EU's energy security and defence resilience.

08

Recommendations and Concluding Reflections

Hadjisavvas Constantinos, *European Defence Agency*
Maja Kuzel, *European Defence Agency*
Elisabeth Krausmann, *European Commission Joint Research Centre*
Ioannis Chatzialexandris, *European Defence Agency*
Alexandru Georgescu, *National Institute for Research and Development in Informatics ICI Bucharest*
Nektarios Nasikas, *Hellenic Army Academy*
Alessandra Lazzari, *European Defence Agency*

8.1 Introduction

The effectiveness of European defence operations depends on the resilience of CEI, which faces increasing threats from hybrid warfare, cyberattacks, and climate change. Strengthening CEI protection is not just necessary—it is a strategic imperative. This concluding chapter synthesises the findings of this publication. It outlines **key recommendations** for enhancing CEI resilience across multiple levels:

i. **EU level** (for strengthening strategic frameworks and coordination).
ii. **Ministries of Defence (MoDs) and Armed Forces** (for integrating CEI resilience into defence planning).
iii. **Private sector/industry** (for enhancing cooperation and technological innovation in CEI protection).

These recommendations aim to ensure that CEI can withstand emerging challenges, safeguarding the energy supply that defence forces rely on for mission readiness, operational effectiveness, and sustainability. This concluding chapter also underlines that addressing these challenges is critical for maintaining operational effectiveness and ensuring the security of national and EU defence systems in the face of growing and evolving threats. It also underscores that the EU and the MoDs should not follow the developments but rather place themselves as the shapers and be proactive rather than reactive. Following these **key recommendations**, we also offer **concluding reflections**, synthesising insights from the TTX and preceding chapters.

8.2 Recommendations at the EU level

The EU is uniquely positioned to lead initiatives that enhance CEI resilience across Member States. The following key actions should be taken:

- **Strengthen EU-Wide Resilience Frameworks and Coordination**

  The EU must continue to foster a comprehensive, unified approach to CEI protection that aligns with broader EU resilience strategies, such as the Critical Entities Resilience Directive and the Joint Communication on the climate and security nexus. The EU should ensure that national efforts to protect CEI are harmonised and coordinated across Member States, with mechanisms for sharing best practices, intelligence, and resources. This would help mitigate the transnational impacts of CEI disruptions and hybrid threats that can cascade across borders.

- **Establish an EU Competence Centre on Climate Change, Security and Defence**

  Creating an EU-led Competence Centre on Climate Change, Security and Defence would support the coordination of research, policy development, and cross-sector collaboration. This Centre would serve as a knowledge hub, bringing together defence, energy, and climate experts to develop strategies for enhancing CEI resilience in the context of hybrid and climate-related threats. Establishing such a mechanism is essential in underpinning the MoDs policy and decision-making processes to increase energy efficiency and ensure the coherence of activities in implementing the EU's energy and climate objectives in defence. It would address the specific needs of the defence sector as the EU moves towards a resilient Energy Union and aims at achieving climate neutrality by 2050.

- **Promote Joint Defence-Energy Projects**

  The EU should actively promote and fund joint defence-energy projects that focus on enhancing the resilience of CEI against hybrid and climate threats. These projects could involve cross-border infrastructure protection exercises, technology innovation programmes (e.g., AI for cyber resilience), and renewable energy deployment for military use, reducing fossil fuel dependency while increasing energy security.

- **Expand the EU's Role in Cybersecurity for CEI**

  The growing reliance on digital infrastructure makes cybersecurity critical for CEI protection. The EU should expand its efforts to integrate cyber defence into CEI protection strategies, ensuring that cyber threats are addressed as part of the broader CEI resilience framework. This could include establishing common cybersecurity standards, fostering joint exercises, and enhancing information sharing on cyber incidents targeting energy infrastructure.

8.3 Recommendations for Ministries of Defence and Armed Forces

Ministries of Defence and Armed Forces are key stakeholders in ensuring CEI resilience, given the reliance of military operations on uninterrupted energy supply. The following recommendations focus on strengthening military preparedness and response to CEI disruptions:

- **Integrate CEI Resilience into Military Planning**

  Ministries of defence should integrate CEI protection and resilience into military operational planning, logistics, and procurement. This includes conducting risk assessments of military dependencies on civilian energy infrastructure and incorporating CEI vulnerabilities into military exercises and training programs. Resilience planning should also address the interdependencies between energy, transport, and telecommunications sectors, as disruptions in one sector can significantly affect defence operations.

- **Develop CEI-Specific Response and Recovery Plans**

  Defence forces must develop detailed response and recovery plans tailored to potential CEI disruptions, including scenarios involving cyberattacks, extreme weather events, and hybrid threats. These plans should be coordinated with national emergency response agencies, energy providers, and other critical infrastructure operators. Developing rapid response teams trained explicitly for CEI-related crises would enhance military readiness during energy supply disruptions.

- **Foster Civil-Military Collaboration**

  Given that the majority of CEI is privately owned or managed by civilian entities, it is crucial that MoDs establish strong partnerships with energy providers and regulators. These partnerships should focus on joint efforts to protect energy infrastructure, share threat intelligence, and collaborate on developing resilient energy systems. Regular coordination exercises and simulations would help ensure that both civil and military entities are prepared to manage and mitigate the impact of disruptions on defence operations. To institutionalise collaboration, MoDs should establish permanent working groups with energy providers, integrating energy security into national defence strategies and crisis response frameworks.

- **Prioritise Green Energy Transition for Defence**

  Ministries of Defence and Armed Forc-

es should accelerate the transition to renewable energy sources for their practices and operations. This will reduce reliance on fossil fuels and enhance energy autonomy. Initiatives such as deploying microgrids, solar power, and energy storage systems in military bases would increase the resilience of military installations while contributing to broader EU climate goals.

8.4 Recommendations for the private sector/industry

The private sector, particularly energy companies and critical infrastructure operators, plays a pivotal role in ensuring the resilience of CEI. These entities must collaborate closely with defence and government agencies to safeguard energy infrastructure against a range of threats. Key recommendations include:

- **Strengthen Collaboration with Defence and Government Agencies**

  Private sector operators must engage in ongoing dialogue with defence and government entities to align resilience strategies. This includes participating in national and EU-level CEI protection initiatives, sharing real-time information on potential threats, and contributing to joint exercises to test the resilience of energy systems under duress.

- **Invest in Resilient and Smart Energy Infrastructure**

  Energy companies should invest in modernising their infrastructure to withstand physical and cyber threats. This includes upgrading grids with smart technologies, such as AI-driven monitoring systems and automated response mechanisms that can detect and mitigate disruptions in real-time. In addition, adopting renewable energy technologies such as decentralised energy systems and microgrids can improve overall system resilience.

- **Enhance Cybersecurity Measures**

  The private sector must prioritise cybersecurity as a fundamental aspect of CEI protection. Energy companies should adopt industry-leading cybersecurity practices, including regular vulnerability assessments, advanced encryption protocols, and multi-layered security architectures to defend against increasingly sophisticated cyberattacks. Public-private partnerships for sharing cybersecurity intelligence will be essential in pre-empting and responding to potential threats. Cyber resilience strategies must include regular joint exercises between defence, government, and industry to simulate real-world attacks on CEI and test coordinated response capabilities. These exercises will enhance threat detection, response efficiency, and cross-sector coordination, ensuring a more resilient energy infrastructure.

- **Build Redundancies into Energy Systems**

  Energy operators should build redundancies into their systems to ensure that defence-related CEI can continue to function in the event of disruptions. This can include implementing backup power generation systems, increasing energy storage capacity, and diversifying energy supply sources to mitigate the risk of long-term outages.

8.5 Concluding reflections

The seven chapters of this groundbreaking publication, including the analysis of the TTX on hybrid threats, underscore several critical insights about the evolving threat landscape and the need for a more proactive, integrated approach to CEI resilience. The TTX exercise revealed several critical gaps in CEI resilience, including intelligence-sharing failures, civil-military coordination challenges, and the increasing complexity of hybrid threats. **The key takeaways include**:

i. **Hybrid threats are increasing in complexity**

   The TTX highlighted how hybrid threats are evolving beyond traditional security challenges, now incorporating digital threats, influence operations, and physical disruptions to CEI. The nature of these threats demands a whole-of-society approach, with close cooperation between defence, government, industry, and civil society to anticipate, detect, and respond to attacks effectively.

ii. **Situational awareness and information sharing must improve**

   A major challenge identified during the TTX was the lack of a common situational awareness framework across different actors. Better intelligence-sharing mechanisms at the national and EU levels will be necessary to bridge the gap between defence forces, energy providers, and policymakers.

iii. **Civil-Military coordination remains a challenge**

   While military forces are critical in crisis response, they often lack a formalised role in CEI protection, given that most infrastructure is civilian-owned and operated. The TTX demonstrated the need for stronger partnerships between Ministries of Defence, civilian authorities, and industry stakeholders to clarify roles, responsibilities, and response protocols.

iv. **Proactive risk management is more effective than reactive crisis response**

   Traditional crisis response models are not sufficient to address hybrid threats. Instead, proactive strategies—such as predictive risk modelling, AI-driven monitoring, and early intervention mechanisms—must be prioritised to detect and neutralise threats before they escalate.

v. **Strategic communication is a critical tool**

   The war in Ukraine and other geopolitical crises have reinforced the importance of strategic communication in countering disinformation and hybrid threats. Defence and civilian actors must work together to shape public narratives, ensuring that CEI-related crises are managed with clear, coordinated messaging that builds public trust and prevents misinformation.

vi. **Digitalisation and dual-use technologies are essential for CEI protection**

   Digitalisation is transforming CEI protection, but without a clear digital strategy, new technologies may also introduce vulnerabilities. To stay ahead, the Armed Forces must strategically adopt and secure these advancements. The accelerating digitalisation of CEI introduces both opportunities and vulnerabilities. While digital transformation enhances efficiency, it also exposes infrastructure to cyberattacks, AI-driven disinformation, and data breaches.

   a. To effectively protect defence-related CEI, the armed forces must adopt cutting-edge and dual-use technologies, including AI-driven analytics, quantum encryption, secure connectivity, 5G/6G, autonomous surveillance systems, and resilient energy storage solutions.

   b. The defence sector should leverage civilian technological advancements, ensuring that military capabilities remain at the forefront of cybersecurity, infrastructure resilience, and crisis response.

c. Public-private partnerships will be critical in accelerating the development and deployment of next-generation digital tools that enhance situational awareness, real-time threat detection, and rapid-response capabilities.

Ensuring the resilience of defence-related CEI is no longer optional—it is a strategic necessity for sustaining military operations and national security. The evolving threat landscape—from cyberattacks to climate-induced disruptions—demands a proactive, integrated response from the **EU, MoDs, armed forces, and the private sector**.

Rather than merely reacting to crises, the **EU and its Member States must lead the security and defence agenda**, shaping policies, investments, and frameworks that strengthen CEI protection at all levels. This means:

- **Shifting from reactive policies to proactive resilience-building**, prioritising cross-border infrastructure protection, digitalisation, cybersecurity, and renewable energy adoption.
- **Anticipating and countering hybrid threats before they materialise**, ensuring CEI security is embedded within defence and security strategies.

However, **policy alone is not enough**. Implementing these recommendations requires:

- **Sustained investment** in resilient energy and digital infrastructure.
- **Cross-sector collaboration** between defence, government, and private industry.
- **Clear governance mechanisms** to align CEI security with broader EU defence and energy policies.

Failure to act will leave European defence operations vulnerable to escalating hybrid threats and energy disruptions. **History has shown that those who fail to protect critical infrastructure become vulnerable to those who exploit its weaknesses**. The EU must **take the lead-driving a secure, resilient future rather than reacting to crises**.

List of Figures

List of Tables

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Publications Office
of the European Union