WHY IS CRITICAL UNDERWATER INFRASTRUCTURE THE TARGET?

By CDR H.Ceyhun TURE

2024

Introduction

Maritime Critical Energy Infrastructure has experienced significant growth and transformation in recent decades. One notable developments is the increasing utilization of the sea as a source of energy, as seen in the expansion of larger offshore wind farms incorporating various underwater elements such as offshore substations and related power cables. Additionally, underwater pipelines have become the most cost-effective, secure, and efficient method for transporting oil and gas, leading to a global increase in investments in this area.

Underwater Energy Infrastructure in Northern Europe
Source: European Atlas of the Seas website

Offshore Windfarms *Source: https://commercial.allianz.com/*

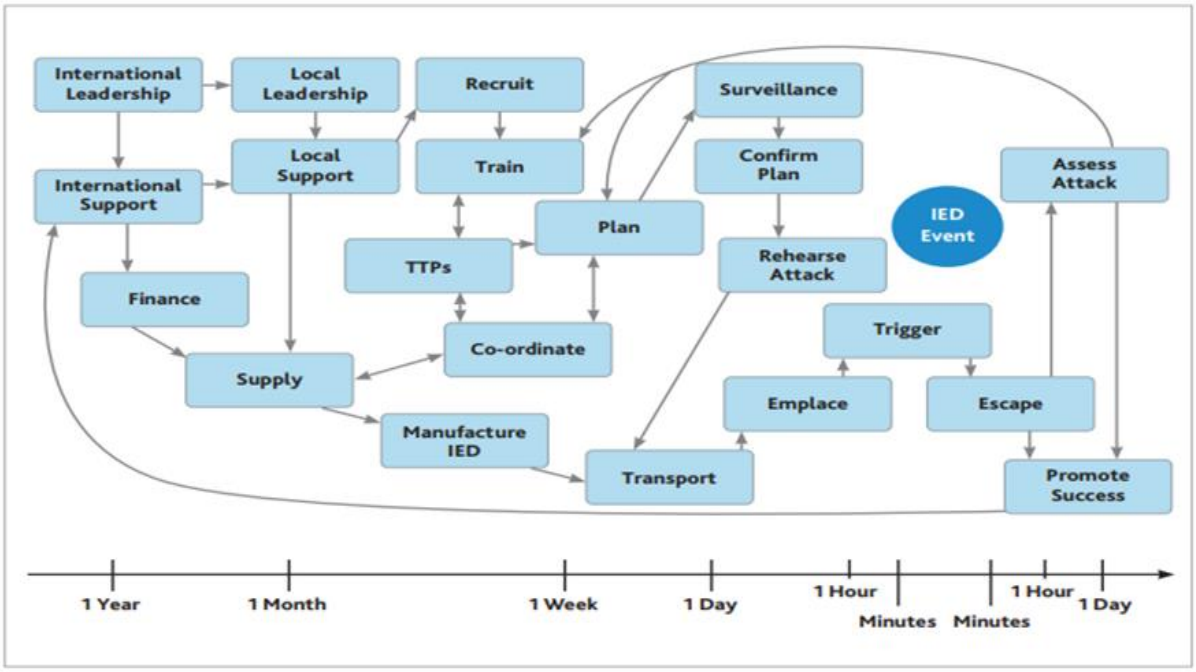
However, these advancements have also attracted the interest of adversaries who understand the strategic importance of targeting such valuable assets. Particularly, the Nord Stream pipeline explosions on September 26, 2022, captured all attention and offered valuable lessons regarding this new threat vector, centred on underwater energy infrastructure. Following these explosions, NATO has highlighted the vulnerability of Critical Underwater Infrastructures (CUI) and has taken substantial measures to protect them. On October 8, 2023, the Balticconnector gas pipeline incident once again underscored the susceptibility of underwater infrastructure. It is widely recognized that the issue is highly intricate, encompassing a diverse array of stakeholders, such as governments, armed forces, private companies, and academia, all operating within a complex and demanding maritime domain. Besides the collective efforts of NATO, individual nations have also undertaken diverse initiatives, investing in seabed warfare and innovative underwater surveillance technologies. In this short article, the aim is to **shed light on why CUI has become a target** and to examine the **challenges involved in its protection**.

SAAB AUV, *Source: https://www.saab.com/products/sabertooth*

Saildrone USV, *Source: https://www.saildrone.com/news*

Why Adversaries Target CUI and Challenges in Protection

Actually adversaries do not display irrational behaviour in their actions. They carefully assess vulnerabilities of CUIs and challenges of security forces, evaluate potential consequences, and aim to maximize impact while minimizing costs and risks. Moreover, attacks on maritime critical energy infrastructure could have significant strategic effects. They have the potential to influence global energy prices and even geopolitical dynamics. This factor alone can serve as **significant motivation** for adversaries to target such infrastructures with more sophisticated and creative methods. The illustrated graphic below is a good example, depicting all phases of adversary attack activities. It starts with a decision approximately one year before, followed by phases such as international support, finance, supply, manufacture, etc. Therefore, cutting off this line of support before the attack is paramount. Since the **challenges in protecting CUIs** are significant considerations for adversaries during their decision-making and attack-planning phases, these **challenges will be emphasized** in the subsequent paragraphs of this section.



Activities Take Place Before and After Attack, *Source: AJP-3.15*

The characteristics of maritime energy infrastructures, especially underwater ones, contribute to their attractiveness as targets for adversaries. The **restricted mobility**, **intense energy content**, and **expansive geographic footprint** of these CUIs render them vulnerable, making potential attacks easier to execute without detection and attribution. The vast area to be covered presents significant difficulties for security forces, necessitating effective patrolling strategies. Therefore, **deterring and attributing adversaries** requires enhanced Maritime Domain Awareness through integrated Intelligence, Surveillance, and Reconnaissance (ISR) technologies. This includes unmanned surface or underwater systems equipped with effective sonar systems, underwater smart cables, and enhanced AI-assisted

integrated ISR capabilities spanning from the seabed to space, as exemplified by NATO's Digital Ocean initiative.

ULAQ USV, *Source: CORE-23 Baltics TTX Academic Lecture* by METEKSAN

Source: https://www.nato.int/cps/en/natohq/news_219441.htm

Moreover, while the protection of critical infrastructure remains a **national responsibility**, the **defined role of Military Forces/NATO** in peacetime is insufficient. CUIs are often **owned and operated by private companies**, some of which may be part of consortiums and not necessarily inclined to collaborate with all nations or NATO. These private entities are primarily responsible for responding to incidents during peacetime. However, in a crisis situation, they may lack the capability to prioritize & respond or be unaware of emerging threats and intelligence. Therefore, this delicate issue necessitates cooperation among CUI private companies, related authorities and military forces.

Finally, as we are all aware CUIs extend beyond national territorial waters or even exclusive economic zones. Consequently, intervening in such scenarios is always complicated, with the **intricate legal framework in the maritime domain** (UNCLOS 1982 & SUA-2005 Protocol), particularly in international waters where the **principle of freedom of navigation** takes priority. This complexity adds further challenges to the protection of CUIs and requires cooperation with neighbouring countries and a common understanding of the legal framework.

Conclusions

The close interconnection between Energy Security and Maritime Security highlights the importance of a coordinated and comprehensive approach to effectively address shared concerns. Maritime Critical Energy Infrastructure has witnessed significant growth and transformation in recent decades. However, it is crucial to recognize that alongside maritime energy shipping, the expansion of CUIs such as underwater pipelines, offshore wind farms, and underwater electrical cables is progressively making them more susceptible to threats from adversaries.

Countering this threat in the maritime domain necessitates a fluid and comprehensive approach, taking into account the unique characteristics of the maritime environment. This approach requires three-dimensional planning that encompasses not only the surface and air but also the underwater

environment. Protecting CUI requires specialized equipment, surveillance technologies, research, innovation, intelligence sharing and most importantly coordination among all stakeholders. Furthermore, international collaboration among nations is vital to prevent duplication of efforts, maximize resource utilization, ensure effective strategic communication and crisis management, and establish a common legal framework. In this regard, NATO ENSEC COE's Tabletop Exercises, such as the **Coherent Resilience Baltics-23 TTX**[1] which focus on "Maritime Critical Energy Infrastructure Protection" providing excellent opportunities for close cooperation among **nations**, **ministries**, **private companies**, **military personnel**, and **academics**.

Tabletop Exercise "Coherent Resilience 2023 Baltic" took place in Riga - NATO ENSEC COE

Ensuring a reliable and stable energy supply is of utmost importance, and it is crucial to acknowledge and prioritize the responsibility of protecting critical energy infrastructure. There is no doubt that adversaries consistently strive to develop novel methods and technologies to execute attacks on maritime critical energy infrastructures including CUIs. As the threat of adversaries advances in complexity and lethality, collective NATO investments in innovative solutions and coordination between nations are needed to thwart or minimize the impacts of such attacks.

[1] The CORE-23 Baltics TTX was executed between November 13th and 17th, 2023, in Riga. It involved **120 registered participants** from **13 countries** (all Baltic Countries except Russia), 53 institutions and organizations.