Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26165-cd

The Cost of Doing Business: A Collaborative Approach to Hybrid Threats – a Regulatory Perspective

Linn Steensrud Øverland

Senior Engineer, Norwegian Ocean Industry Authority, Norway. E-mail: linn.steensrud@havtil.no

Truls Campe Pettersen

Advisor, Norwegian Ocean Industry Authority, Norway. E-mail: truls.pettersen@havtil.no

Kristian Solheim Teigen

Principal Engineer, Norwegian Ocean Industry Authority, Norway. E-mail: kristian.teigen@havtil.no

Hybrid threats have gained considerable traction over the past years as the current geopolitical landscape has shifted. The emerging risks that follow must be remediated; however, this comes with an increased organizational and financial cost.
As threat actors evolve methods combining traditional and emerging tactics, it is integral for risk management practitioners, across both industry and government sectors, to further develop capabilities, knowledge, and understanding of these risk vectors.
Over time, the cyber dimension has become an integral part of the risk and vulnerability management, across cyberspace and cyber-physical systems alike, as well as in the realm of physical security. In practice, this means that these disciplines are becoming increasingly intertangled. As such, risk management practitioners must pivot towards increased cross-disciplinary collaboration. In other words, it is time to pay the cost for resilience - it is time to move from well said to well done.
This paper explores the interface between cyber and physical security, the possibilities for synergetic processes, the need for an increased focus on cross-disciplinary collaboration, and the costs of doing so – or not.

Keywords: Cybersecurity, physical security, hybrid threats, collaboration, risk, safety, risk management

1. Introduction

Over the past decades, cybersecurity has become just as much about protecting people as about protecting data. This rings especially true for cyber-physical systems, which automate, control, and safeguard machinery and infrastructure. Cyber-physical systems integrate the cybersecurity and physical security domain, enforcing their interdependence and emphasizing the need for coordinated collaboration between the disciplines.

Due to technological advancements, many modern physical protection measures depend on cybersecurity components to achieve their security objectives (Lee, 2020). At the same time, the effectiveness of cyber defense also depends on physical and personnel security, as unauthorized access, insider actions, or physical disruptions to cybersecurity components may compromise otherwise robust digital safeguards.

While the topic and discussion of cross-disciplinary collaboration is far from a new one, it is integral to examine the security concept in a cross-disciplinary context to gain a holistic understanding of lasting resilience. However, cross-disciplinary collaboration carries certain costs – financial, organizational, and maybe even personal (Cummings & Kiesler, 2005). In other words, building resilience requires investment.

To complicate matters further, hybrid threats have become a key challenge for both national security and critical infrastructure amidst growing geopolitical unpredictability. Hybrid threats pose an advanced and persistent risk, ranging from utilizing tactics like disinformation, intelligence, sabotage, to data manipulation and cyberattacks (Llinàs, 2022). As such tactics develop, the interconnectivity between cyber- and physical security grows, the attack surface is expanding. This further emphasizes the need for collaboration between physical security and

cybersecurity professionals – both in academic environments side and in operations.

This paper provides a regulatory perspective on the intersection between physical security and cybersecurity, the need for cross-disciplinary collaboration when dealing with hybrid threats, and the potential costs of implementing – or not implementing – change.

This paper employs a conceptual and literature-driven analysis to explore the governance implications of hybrid threats and the need for integrated security approaches.

2. Context and Risk Landscape

When discussing the collaboration between cyber- and physical security, it is vital to understand the context in which these domains intersect. The increased integration between physical and technical assets introduces new vulnerabilities and risks. To effectively address these challenges, it is important to understand the risk landscape in which they exist.

2.1. *The contemporary security risk landscape*

The current security risk landscape is characterized by more complexity and interconnectivity than ever. This occurs at the same time as the geopolitical landscape is shifting, tensions are rising, and there is an ongoing convergence of cyber, cyber-physical, and physical threats (Goode, 2025).

Concurrently, the threat landscape is further complicated by the increasingly diffuse and opaque nature of threat actors, particularly in the cyber domain. Traditional boundaries between state-sponsored groups, criminal networks, and ideologically driven hacktivists are becoming blurred, as nation states increasingly rely on loosely affiliated proxies and intermediaries whose motives and alignments shift over time (CISA, 2025; DHS, 2025; ENISA, 2025). This fluidity reinforces the challenges of attribution and contributes to the unpredictability that characterizes today's hybrid threat environment.

The increase of hybrid threats signifies the tone and color of the contemporary security landscape (Treverton et al. 2018). Considering this, it is integral to stay vigilant when dealing with emerging risks in a shifting environment.

2.2. *Hybrid threats*

Hybrid threats pose a risk to both physical and cyber assets and have become a persistent security challenge for Western nations. These threats are characterized as being complex and they span from disinformation campaigns and surveillance to the use of proxy actors and cyberattacks (Treverton et al. 2018).

Hybrid CoE (2025) defines hybrid threats as

(i) Coordinated and synchronized actions that deliberately target democratic states' and institutions' systemic vulnerabilities; activities that exploit the thresholds of detection and attribution.

(ii) Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).

In practice, hybrid measures manifest as coordinated actions that blend physical, digital, and informational tactics to create cumulative effects. In a cyber-physical context, threat actors may exploit weaknesses, both on a technical and a human level, such as remote access pathways or control environments, or personnel security gaps, such as insiders with legitimate access or individuals susceptible to coercion or manipulation. While the result of accumulated tactics may not result in direct operational disruption, it may cause a gradual erosion of trust in the accuracy and safety of operations. The complexity and simultaneous utilization of tactics make hybrid activity difficult to detect and attribute in real time.

2.3. *From physical security to cybersecurity*

Effectively managing hybrid threats requires both resources and an in-depth understanding of how associated risks emerge in practice, across a technical and non-technical level alike. This reflects the multiplicity nature of security in practice.

What constitutes prudent security measures have consistently been dependent on what needs protection, from the size and location of the asset, to emerging threats and changing risks. As technology has advanced, the security thinking has evolved with it (Lee, 2020).

While physical security is often associated with the protection of physical assets, such as buildings, equipment, and people, cybersecurity is often

associated with the protection of more conceptual assets, such as data, networks, and systems (Riskhan et al. 2024). However, Lee (2025) posits that the role of technology in the security concept has broadened and evolved from physical assets to encompassing information assets. He argues that a multilayered approach to security is both comparative to and compatible with the holistic understanding of the intersection of physical security and cybersecurity (Lee, 2025).

However, there are limitations to what physical security measures can achieve in the cyber domain. While physical security measures can offer protection against attacks on infrastructure, equipment, and physical systems, they are unable to protect against cyber threats and provide limited visibility and monitoring in cyber- and cyber-physical systems (Lee, 2025; Riskhan et al. 2024).

Effective protection of digital assets requires that measures involve a combination of technical, organizational, and physical controls. These are all aspects that must be considered when addressing hybrid threats.

3. Relevance for the Norwegian Petroleum Sector (and Others)

As the national significance of industrial production assets and supporting infrastructures has become increasingly clear, they are becoming more exposed to potential threat actors. In these environments, hybrid threats now pose a substantial risk to digital infrastructure, supply chains, and operations (PST, 2025). The petroleum sector is no exception.

The petroleum industry is one of the largest industries in Norway, and there is continuous political focus on Norway's ability to ensure a secure and stable energy supply, while also ensuring that operations are carried out with the highest standards of HSE in the world (Havtil, 2018; Midtun, 2025a).

The Norwegian Prime Minister has stressed it is vital that workers on, and adjacent to, the Norwegian Continental Shelf (NCS) stays vigilant and report unusual activities – in systems, as well as physical occurrences on plants and installations (The Office of the Prime Minister & Havtil, 2025).

The sentiment of vigilance is also relevant to other sectors. The Norwegian Police Security Service (PST) stressed in their national threat assessment (NTV) that they assess hybrid threats to be characteristic for the coming year for companies and organizations that operate critical infrastructure (PST, 2025).

3.1. *Threat landscape in the sector*

The annual threat and risk assessments from the national security services indicate that the sector is facing an increasingly challenging threat landscape. In the petroleum sector, the Norwegian Ocean Industry Authority (Havtil) continue to observe a positive development in the industry's security work but notes that there is still room for improvement (Midttun, 2025b).

Additionally, the threat and risk assessments emphasize the importance of Norway as a stable and reliable supplier of oil and gas to Europe. PST highlighted in NTV 2025, that sabotage by the use of proxy-actors is likely to impact the threat landscape. Considering this, the petroleum industry may be potential targets for actions like espionage and sabotage on critical infrastructure that have the potential of significant consequences for both the industry and national security interests (Midttun, 2025b; PST, 2025).

3.2. *Investment in the NCS must come at a cost*

As a critical factor in the European energy market, the Norwegian petroleum sector must continue investing in safety and security. Havtil's main theme for 2026 is that "investment in the Norwegian Continental Shelf must come at a cost" (Havtil, 2025).

Analyses of global energy needs indicate that production on the NCS may continue for another 100 years (Anda, 2025). Upholding quality across the entire value chains is crucial for safe, secure, and reliable operations in both established and emerging NCS energy sectors.

Companies must invest in robust solutions and technology, prioritize maintenance, and ensure proper expertise. This also means it is vital to protect assets and people against deliberate attacks (Havtil, 2025). Investments in the NCS must be holistic and cover technology, infrastructure, and organizational measures and efforts.

4. Governance is Key

Both contemporary hybrid threats and the current risk landscape are complex and ambiguous in nature (Treverton et al, 2018; Goode, 2025).

To effectively address hybrid threats and emerging risks, governance is a key aspect. Without adequate governance, organizations risk becoming less resilient and more vulnerable to attacks. Technical security controls and barriers are simply not enough – the organization's continuous improvement of capabilities and governance are imperative to managing risks.

While discussions related to these topics are often emphasized, simply discussing these challenges will not suffice to manage these threats - decisive action is overdue. However, taking decisive action may be easier said than done.

4.1. *Governing cybersecurity as part of hybrid threats*

Technological developments introduce new vulnerabilities through systems, design, and focus (Khan, 2025). It provides new attack surfaces for threat actors and can be utilized in coordinated hybrid attacks (Kimbrel, 2024).

Cybersecurity is often focused on technological development, secure design, embedded secure measures, and other technical measures. However, cybersecurity is as much about governance as it is about technology (Kulkarni, 2022). Effective cybersecurity governance requires a systematic and integrated approach – it is no longer sufficient that cybersecurity professionals manage cybersecurity independently, it must be embedded into the entire organizational framework (Gòmez et al. 2025).

Considering the implications of cybersecurity on organizational resilience, it is necessary that all personnel working with, and adjacent to, cybersecurity risks receive adequate training to develop the necessary skills to manage and respond to emerging threats. In addition, it is integral that challenges are addressed through a holistic approach, including both technical and organizational measures (Kulkarni, 2022).

Furthermore, as the scope of cybersecurity grows, the need to include all relevant disciplines – technical and non-technical alike – becomes apparent (Jacobs et al. 2020).

4.2. *Governing physical security as part of hybrid threats*

Physical security remains a critical component in managing emerging risks and hybrid threats. Considering that physical security is a necessity when developing and improving organizational resilience.

Physical security is oftentimes associated with the protection of physical assets, such as buildings, equipment, and people (Riskhan et al. 2024). The available security measures are numerous, from doors, locks, ID check points, files, and safes to perimeter protection, gates, and walls (Lee, 2020). Even so, physical security measures have limitations, in particular their inability to protect against cyber-based threats (Riskhan et al. 2024).

This does, however, not imply that physical security is unnecessary for protection against cyber and hybrid threats - it is in fact indispensable.

Physical security has a long tradition, robust lessons learned, and has evolved over time. The multilayered nature of physical security can provide valuable insights when dealing with emerging risks (Lee, 2020). To effectively combat hybrid threats, the knowledge and expertise found in the physical security discipline must be included to gain a holistic understanding of relevant risks and threats. However, the successful utilization of this knowledge is dependent on widespread integration of knowledge between the security disciplines, proper implementation, and training for both security personnel, and those who work adjacent to physical risks.

4.3. *Necessary convergence of physical and cybersecurity*

As hybrid attacks target both physical and digital assets, and there is an ongoing convergence of cyber and cyber-physical systems, the lines between cybersecurity and physical security are becoming increasingly blurred (CISA, 2021). This, in combination with the rising risk of physical sabotage and surveillance, necessitates the need to facilitate better collaboration between the security disciplines.

Digital and physical assets represent a significant risk, both together and by themselves. A targeted attack on either, or both, simultaneously, may result in compromised infrastructure. At the same time, cybersecurity and physical security are most often viewed, and treated as separate entities (CISA, 2021). While there are good reasons for these disciplines to continue to be separate entities, there is a dire

need for information sharing and close collaboration between them.

Such collaborative efforts can support better preparedness, increased resilience, and ensure better response to threats and incidents (CISA, 2021).

Successful collaboration ensures a foundation on which expertise can provide valuable insight into the intersection between technology and physical security risks and develop a systematic approach to threat and risk management.

5. Challenges with Convergence and Collaboration

Despite clear benefits, achieving convergence and collaboration between the physical and cybersecurity domains remain difficult. Several structural and organizational barriers continue to hinder effective collaboration.

5.1. *Lack of alignment*

A key challenge is the absence of shared language, concepts and priorities across the security disciplines. Cybersecurity and physical security often place different meanings on core terms and concepts (Cains et. al. 2021).

Furthermore, they evaluate risks through incompatible lenses, which undermines risk communication and coordinated decision-making This complicates and undermines effective risk communication across disciplines. These misalignments contribute to miscommunications, inadequate risk evaluations, improper incident management, and tensions in collaborative efforts when attempting to identify and mitigate hybrid threats.

5.2. *Siloed functions*

Another challenge is the issue of siloed functions. Organizational separation between physical security and cybersecurity limits visibility into cross-domain risks. Despite this, security leaders often end up operating independently from one another, and there is often little collaboration between the disciplines outside enterprise-wide risks (CISA, 2021).

Siloed functions lead to blind spots, limit information sharing, and contribute to fragmented risk governance. A failure to situate risks, incidents, and threats within a broader risk context negatively influences the organization's resilience and diminishes the capability to respond to incidents or threats.

5.3. *Costs of fostering collaboration*

Developing cross-disciplinary collaboration requires investment in time, resources, and organizational commitment (Cummings & Kiesler, 2005). It requires the organizations to allow resources to prioritize time away from their daily tasks to collaborate in set and formalized forums. Such efforts may be constrained by time restrictions, deadlines, and resource deficiencies, thus introducing an organizational cost.

Furthermore, it requires organizations to establish and offer broader training, to ensure common understanding between the disciplines, which in turn can be costly in time, resources, and introduce issues related to ownership of risks (Lee, 2019).

5.4. *Insufficient standardization?*

Existing security frameworks typically reflect the historical separation of the two domains, resulting in guidance that is comprehensive within the individual area but insufficient for managing risks that span disciplinary boundaries.

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems offer one alternative for risk management across disciplines. The standard aims to cover all aspects of information security, which includes organizational, people, physical, and technological controls (ISO, 2022). While this standard includes measures related to the components of hybrid threats, it is not created to manage the complexities hybrid threats introduce. Most notably, it does not address the challenges related to cross-disciplinary collaboration, even if it requires it.

This raises a broader question of how organizations can be supported in improving cross-disciplinary cooperation without necessarily merging the domains into a single unified structure. The answer may not lie only in the development of additional standards, but also in standards that explicitly define interfaces, collaboration mechanisms, common terminology, and shared responsibilities across the two security domains.

6. Opportunities Emerging Through Collaboration

While cross-disciplinary collaboration introduces several complexities, it simultaneously creates important opportunities for strengthening integration between the physical and cybersecurity domains, thus offering a more holistic approach to risk management, better incident response capabilities, and increasing organizational resilience overall.

6.1. Alignment

Creating alignment between the security disciplines is an important aspect of fostering collaboration. While it may be challenging to implement training, forums, and collaborative platforms between the physical and cybersecurity teams, it has the potential to result in a more aligned security organization (Lee, 2019). This may enhance the organization's ability to anticipate, monitor, and respond to risks, alongside improving communication across disciplines. Furthermore, it makes it possible for organizations to gain a better understanding of the risks they face, and their potential impact on operations. It also provides the added advantage of eliminating siloed and fragmented functions. This further supports continuous improvement efforts and provides organizational resilience.

Gaining a broader perspective of the impacts and implications of, especially hybrid threats, can support decision-making through more thorough vulnerability analyses and risk assessments.

To effectively foster cross-disciplinary alignment, it is necessary to set collective goals, create a common understanding of risks, and establish common understanding of concepts. While most of the collaboration must occur between the security domains themselves, it is important to note that the successful implementation of such alignment requires management to prioritize, facilitate, and support such collaboration.

The objective is not to cultivate comprehensive expertise across disciplines at the individual level, but to strengthen threat response by leveraging the expertise and capabilities of each discipline.

6.2. *Resilience and capabilities*

A more aligned security organization, in combination with gaining a comprehensive understanding of risks and impacts, facilitates the strengthening of resilience and development of capabilities (CISA, 2021). When dealing with hybrid threats, the ability to develop such skills is essential.

Through increased collaboration, organizations can enhance their resilience and capabilities, while enabling insights from physical security and cybersecurity environments to be effectively shared, understood, and interpreted to the organizational context. Viewing risks and threats that impact both physical and cybersecurity holistically is essential for good risk governance. Additionally, this may accelerate the process of building trust and robust security organizations.

7. The Cost of Doing Nothing

The opportunities and advantages of cross-disciplinary collaboration are significant and contribute to continuous improvement and development of risk management and incident response capabilities. Yet, the challenges associated with collaboration may seem daunting. Even so, the cost of doing nothing is far greater. Inaction may lead to increased vulnerability and undermines the organizational ability to prepare for emerging risks.

7.1. *Degradation of trust*

Isolating physical security from cybersecurity is unfeasible, as security is a multilayered concept, thus needing a multilayered approach to achieve positive results (Lee, 2020). Moreover, there are numerous impasses where the two disciplines must collaborate to achieve a meaningful understanding of relevant risks. Without actively cultivating collaboration, neither discipline will be prepared for effective joint efforts.

Furthermore, the lack of alignment in both conceptual understanding and understanding of risk may result in a degradation of trust between the disciplines. This increases the probability of fragmented risk management, especially when dealing with hybrid threats. Managing such threats is already complex, and adding distrust may be detrimental to the effectiveness of both implemented measures and incident management.

7.2. *Unclear ownership*

One of the challenges of dealing with hybrid threats is the inherent complexity of such threats (Treverton et al. 2018). They are by nature difficult to manage, and when introducing both

digital and physical components to such threats, holistic management becomes a prerequisite. By allowing siloed security functions, organizations introduce complications in managing threats and emerging risks (CISA, 2021). One such is the unclear ownership of the risk at hand.

It can be nearly impossible to conclude where the cybersecurity aspects end, and the physical security aspects begin. This makes managing the risks nearly impossible. Failure to act may leave hybrid threats unidentified or improperly managed. It may also result in duplicated efforts as security disciplines remain siloed and overlook critical aspects related to the relevant risks and threats.

Holistic management is a cornerstone to managing hybrid threats, and cross-disciplinary collaboration is a necessity to avoid fragmented risk management.

7.3. *Eroding the resilience scheme*

Without the capability to manage hybrid threats, the result is the erosion of organizational resilience, thus making the organization vulnerable to attacks.

Fragmented divisions, poor communication, lack of collaboration, and unclear ownership may undermine effective risk management and threat response. Considering the implications of hybrid threats and their potential consequences, it is crucial that resilience is built and not eroded.

8. Conclusion

This paper highlights the governance mechanisms and cross-disciplinary structures required for organizations to build lasting resilience and manage hybrid threats effectively.

The growing complexity of hybrid threats emphasizes the need for integrated security practices that connect the physical and cyber security domains. As hybrid threats exploit systemic vulnerabilities across technological and organizational measures and regimes, the traditional distinction between physical security and cybersecurity is becoming increasingly untenable.

Effective management of hybrid threats requires coordinated efforts, structured collaboration, and investment in resilience. Increasing interconnectivity means that siloed approaches not only weaken efficiency but also create new vulnerabilities and fragmented risk management.

Building lasting resilience requires organizations to focus on strengthening competence, governance, collaboration mechanisms, and shared situational awareness. Security cannot rely on intentions alone - it requires deliberate continuous action.

While cross-disciplinary cooperation comes with financial, organizational, and cultural costs, the cost of inaction is far greater. Siloed functions, misaligned risk perceptions, and insufficient risk communication undermine the ability to handle complex threats and may erode trust between security disciplines. To address these challenges, organizations must develop mechanisms that support collaboration, define interfaces, establish common terminology, and define shared responsibilities. Creating forums for discussing collective goals and risk perspectives - through workshops, training, collaborative spaces, and developing standards - is essential.

Ultimately, holistic, cross-disciplinary security practices through organizational alignment and trust-based collaboration offer a path toward improved resilience and more effective risk governance in an increasingly complex threat landscape.

References

(Zech) Lee, S. (2020) A Basic Principle of Physical Security and its Link to Cybersecurity [online]

America's Cyber Defense Agency (CISA) (2021) Cybersecurity and Physical Security Convergence [online]

Anda, Inger. (2025) Build for the Future. In *Dialogue. A journal from the Norwegian Ocean Industry Authority no 2* (2025) pp. 6-8

Cains, M. G., Flora, L., Taber, D., King, Z., Henshel, Diane S. (2021) Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context Using Expert Elicitation. In *Risk Analysis – An International Journal* [online]

CISA (2025) Cybersecurity and Physical Security Convergence. *Cybersecurity and Infrastructure Security Agency* [online]

CISA (2025). Nation-State Threats: Cyber Actors and Activities. *Cybersecurity and Infrastructure Security Agency* [online]

Cummings, J. N., Kiesler, S. (2005) Collaborative Research Across Disciplinary and Organizational Boundaries. In *Social Studies of Science vol. 35, no. 5* [online]

DHS (2025). Homeland Threat Assessment 2025. U.S. *Department of Homeland Security, Office of Intelligence and Analysis* [online]

ENISA (2025). ENISA Threat Landscape 2025. *European Union Agency for Cybersecurity.* [online]

Gòmes, L., Peterson, C. V., Rojas, M., Pereira, A. (2025) A Risk-Based Approach to Cybersecurity Governance and Management: Strengthening Information Assurance Through Policy Development, Compliance Measures, and Technical Controls. In *Annual Review of Foundational and Emerging Scientific Methodologies, 15(6), pp. 1-14* [online]

Goode, E. (2025) Adapting leadership: Balancing Cyber and Physical Security [online]

Havtil (2018) Safety and responsibility. Understanding the Norwegian Regime. Pp. 7-13

Havtil (2025) Main Issue 2026. In *Dialogue. A journal from the Norwegian Ocean Industry Authority no 2* (2025) pp. 49

Hove, O. (2025) We Too, When Required. In *Dialogue. A journal from the Norwegian Ocean Industry Authority no 2* (2025) pp. 44-47

Hybrid CoE (2024). Hybrid threats as a concept. Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. [online]

International Organization for Standardization (2022) - ISO/IEC 27001:2022 Information Security Management Systems - Requirements. *Geneva: International Organization for Standardization*

Jacob, J., Peters, M., Yang, T. A. (2020) Cross-disciplinary Cybersecurity: Rethinking the Approach and the Process [online]

Khan, I. 2025. The Cybersecurity Paradox: Why More Technology Creates More Vulnerability. [online]

Kimbrel, J. (2024) Five Ways Hybrid Attackers Find Exposure Beyond the Endpoint [online]

Kulkarni, T. (2022) Cyber-Physical Convergence in Critical Infrastructure Security: A Comparative Review of Cybersecurity Strategies in the Water and Energy Sector. In *International Journal for Multidisciplinary Research, vol. 4, iss. 3* [online]

Lee, H. W. (2019) The Cost and Benefit of Interdepartmental Collaboration: An Evidence from the U.S. Federal

Midttun, Øyvind (2025a) On Solid Ground. In *Dialogue. A journal from the Norwegian Ocean Industry Authority no 1* (2025) pp. 5-7

Midttun, Øyvind (2025b) Urges Vigilance. In *Dialogue. A journal from the Norwegian Ocean Industry Authority no 1* (2025) pp. 12-15