Position paper Seabed Security Seminar

Seabed Security Seminar

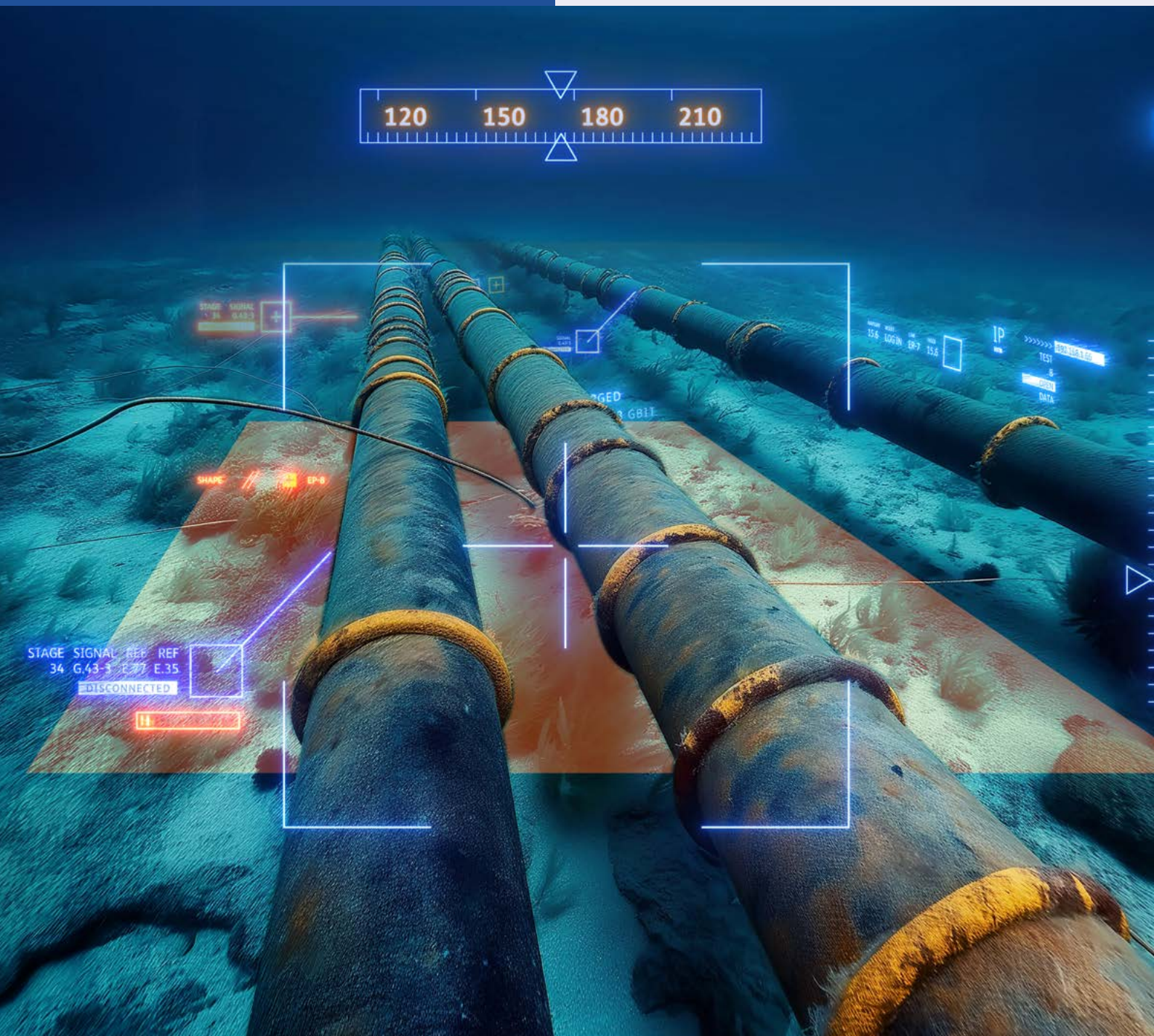
Protecting our Critical Undersea Infrastructure Together

TNO innovation for life

Authors
Jeroen de Jonge, Casper Bosschaart (TNO)

In collaboration with HCSS, Ministry of Infrastructure and Water Management and Ministry of Defence.

The Hague, March 27, 2025



The Strategic Importance of Seabed Security

The report *High Value of the North Sea*, issued already in 2020[1] highlighted both the economic significance and vulnerabilities of Critical Undersea Infrastructure (CUI). Recent incidents, particularly in the Baltic Sea, suggest a deliberate strategy by the Russian Federation to exploit these vulnerabilities. Sabotage operations have been used to undermine Western support for Ukraine, NATO membership of Finland and Sweden, and disrupt the energy independence efforts of the Baltic states. Sabotage of CUI with a more direct impact on energy security, or enhanced focus on targeting CUI beyond the Baltic Sea region should be regarded as conceivable options for further escalation of the hybrid conflict between the Russian Federation and Western nations.

These scenarios pose a significant threat to national security and hinder investments in offshore economic activities, such as the development of offshore wind farms, which are crucial for achieving energy transition goals. This situation has prompted NATO members to establish a robust deterrence posture and develop capabilities for defending against sabotage targeting CUI.

Key Challenges

This position paper will examine the establishment of a robust deterrence against sabotage threats, grounded in an analysis of three pivotal challenges and three strategic enablers:

- **Developing a Defence & Security Capability**
  - The spatial extent of CUI is wide and its nature is diverse; that raises the question: how to obtain an effective, efficient and affordable defence & security capability that allows for agile response to different levels of escalation and can be adapted to evolution of the threat and new infrastructure development;
  - How to overcome the technological shortfall in detecting and countering small underwater systems, which pose a significant threat to critical infrastructure.
- **Enhancing CUI Resilience**
  - How to maintain viable business cases for development of offshore assets, given the enhanced threat and associated cost for security & resilience measures;
- **Strengthening Societal Resilience**
  - How to mitigate societal disruptions from energy or data outages.

Key Enablers for Effective Action

This position paper will examine the establishment of a robust deterrence against sabotage threats, grounded in an analysis of three pivotal challenges and three strategic enablers:

1. **Governance Systems and Legal Frameworks**
   - Provide clarity about tasks and responsibilities of governments, its executive agencies such as the navy and the coast guard and asset owners.
   - Improve the legal frameworks to provide mandates for adequate responses in the national EEZ's.

2. **Industrial Development of Dual-Use Technology**
   - Create the right conditions to invest in dual-use technology for seabed security solutions.

3. **International Cooperation**
   - Enhance intelligence sharing, maritime situational awareness, and interoperability between systems, national security partners, neighbouring nations, and EU and NATO aiming to defend CUI in the national EEZ's and international waters.

1 https://hcss.nl/report/high-value-of-the-north-sea/

A Realistic Approach to Deterrence

Deterrence should be founded on a balance among solutions for these three key challenges and by leveraging the key enablers. Given resource constraints, it is unrealistic to be able to defend against all threats at all times and in all locations. Instead, a more realistic approach is to prioritize defence in high-risk areas to mitigate the risk of significant societal impact. Even in these prioritized areas, complete threat elimination is unlikely. Therefore, reinforcing CUI resilience and preparing society to handle disruptions are critical complementary strategies.

Paths to Addressing Key Challenges

Developing a Defence Capability

The primary objective of a defence capability for protecting CUI is to establish comprehensive maritime situational awareness and understanding of potential threats. This enables effective support for law enforcement efforts and facilitates successful criminal prosecutions. However, in cases where an imminent threat to CUI is expected to potentially lead to societal disruption, a robust defence capability must have at its disposal the resources and capabilities needed to effectively neutralize hostile operations.

An important constraint is the practical limitation of resources such as sensors for situational awareness and effectors to neutralize threats in an effective way.

A scenario- and data-driven risk-based approach is proposed to address effective use of these limited resources. The approach consists of the following elements:

- Understand vulnerabilities of CUI, threat capabilities, and develop threat scenarios from this understanding;
- Conduct geo-spatial risk assessments that consider both the likelihood and potential consequences of disruption;
- Prioritize protection of high impact – high risk CUI;
- Develop, procure and operate a sensor system of systems and maritime security centers that are able to detect, classify and track high risk threats in prioritized areas;
- Develop, procure and operate effectors in prioritized high-risk areas that are able to neutralize high risk threats.

Technology for CUI defence, undersea infrastructure, and threat scenarios and will evolve over time. Developing a defence capability to protect Critical Underwater Infrastructure is a complex, iterative process that requires ongoing effort and continuous improvement. The governance needs ownership and persistent attention and requires to maintain up to date knowledge on threats and vulnerabilities, as well the availability of performance models for sensors and effectors to make the necessary future adaptations of the defence capability.

An important technology shortfall is the lack of systems capable of detection and countering Uncrewed Underwater Vehicles (UUVs). Existing sensor and effector technologies are geared towards detection of either large moving targets like submarines or small stationary targets such as sea mines. This necessitates dedicated research and development for both detection and threat mitigation systems. Applications of these systems are not restricted to protection of CUI, but will also be valuable in protecting naval and civil platforms against the threat of UUV's.

A critical action lies in the accelerated development of defence capabilities to enable timely crisis responses, such as gathering evidence for criminal prosecution or neutralizing adversary operations. Adequate law enforcement and criminal prosecution require either speed or forward presence. To enable timely responses and persistent surveillance, defence operations should leverage autonomous and remote-operated platforms to address personnel constraints.

Maritime Situational Awareness can not be achieved by sensors alone. The data generated by these sensors needs to be fused into a recognized Maritime Picture (RMP). This RMP can serve as a basis for detection of anomalous behaviour. The vast quantity of data that will need to be processed requires a labour-extensive solution. The direction for this solution can be found in machine learning and artificial intelligence (AI) technologies. In order to reach true MSA the data should be analysed from multiple perspectives. This provides opportunities for SME's with relevant knowledge and technology.

Governments must adopt an agile approach combining both short-term improvements and a long-term capability roadmap aligned across NATO and EU members.

Enhancing CUI Resilience – security by design

The resilience of CUI is driven by its redundance, hardening and ability to recover after an incident. This has both a physical and a cyber or digital component, however these are intertwined.

Improving redundance requires to mitigate the impact of sabotage by eliminating single points of failure. Redundance can be pursued in two ways. Firstly, developing offshore energy grids instead of single shore connections is crucial for enhancing physical assets. Secondly, at a system level, it is essential to ensure that the failure of one asset does not jeopardize energy or data security across national or regional systems.

Infrastructure hardening seeks to reduce the impact of sabotage by engineering resilience into systems, allowing them to absorb potential damage. This includes practices like burying cables, improving protection at cable crossings, and installing barriers to protect high-value assets.

The ability to recover aims to improve resilience after an incident, e.g. by having the means, supplies and procedures to repair or replace damaged infrastructure.

The development of new infrastructure should be secure by design, implementing solutions to improve resilience, implement hardening and enable quick recovery. Naturally, measures to improve the resilience of CUI will have an impact on the return on investment, and ultimately on the viability of business

cases for offshore asset development. This is not just an economical concern, but also a political concern, as it may impede the transition to cleaner energy production. Therefore political priorities and governments taking up responsibilities are required. Strategic options for governments to improve the viability of offshore assets are the defence of high-risk / high-impact assets, sharing financial risk and subsidizing investments. These measures should be risk based to ensure effective spending.

Protection and resilience of CUI are for the reasons mentioned above a combined public – private effort. Sharing of critical private data, e.g. sonar surveys that locate CUI exposed on the seabed, between asset owners and governments enables an adequate response to crisis situations. Sharing data requires an investment in digital infrastructure, sharing the investment between partner nations while reducing cost and improve interoperability.

Strengthening Societal Resilience

The increased probability of a prolonged disruption of power, energy or communications demand a whole-of-society approach to resilience. A first priority is to raise public awareness about the impact of disruptions. Media coverage of the recent series of incidents and operations such as Baltic Sentry aids this cause. A broader public can be reached by leveraging more diverse media content, e.q. a film or documentary on the consequences of an enduring power disruption. Public awareness aids the propagation of public preparedness. The strengthening of resilience can be established raising public preparedness encompasses three levels.

At the household level, governments can inform the public about the necessity of preparing an emergency kit and provide clear instructions. Furthermore, governments and the energy sector can promote household energy security through stimulation of ownership of home batteries. Governments, car manufacturers and grid operators can work towards future facilitation of, or even mandatory bi-directional charging of electric vehicles. At the community level, local governments can encourage local initiatives, including community resilience hubs for coordination of local aid in times of crisis. At a national level, governments and industries in the critical infrastructure sectors should develop comprehensive emergency response plans to ensure that all stakeholders are prepared to act swiftly and effectively. These plans should include clear communication strategies.

Strengthening Governance Systems and Legal Frameworks

In recent times, nations have found themselves entangled in the intricate challenge of devising a coordinated approach that balances the enhancement of Critical Undersea Infrastructure (CUI) resilience, the development of robust defence capabilities, and the stimulation of societal resilience.

The process of delineating clear tasks and responsibilities between ministries and executive agencies such as coast guards, navies and safety authorities has proven to be a time-consuming endeavour. Each step towards clarity reveals the complex and overlapping nature of jurisdictions and mandates, leading to prolonged deliberations and slow progress.

Moreover, the UN Convention on the Law of the Seas, a cornerstone of international maritime law, falls short in providing a definitive mandate for the protection of CUI beyond a nation's territorial waters. This legal ambiguity places the principle of the right of free passage, and by extension, the international rule of law, in a precarious position, often at odds with the pressing need to safeguard critical infrastructure.

As nations grapple with these multifaceted issues, the quest for a coherent and effective strategy continues to be a challenge, reflecting the broader tension between maintaining open seas and protecting vital undersea assets.

Guidance for solutions can be drawn from Norway's Security Act which facilitates enhanced governmental coordination, promotes public-private partnerships for resilience, and ensures real-time situational awareness and information sharing between national governments, allies, and private stakeholders.

Furthermore, the 1884 subsea cable convention grants nations the power to stop civilian vessels under the flag of nations who have ratified the convention and are suspected of damaging subsea cables. An improvement can be made through a broader ratification of the convention. Finland, the Baltic States and Ireland are among the nations who have yet to ratify the convention.

Nations should review their national legislation to penalize sabotage to CUI to ensure that sabotage can be penalized to an adequate degree. In the EU, national legislation should be coordinated to standardize the legal situation in European waters. Within coalitions of the willing partnerships can be forged to address shortfalls and develop legal frameworks to act more effectively and quickly within the context of international law.

The use of effectors to neutralize hybrid sabotage operations will remain at odds with international law. Whether the stakes of stopping an impending attack on a high-impact target outweigh the stakes of maintaining the rule of law is a political decision. Governments can empower their navies, coast guards and police forces by providing a clear mandate and corresponding rules of engagement.

Data Driven Industrial Capability Development for Seabed Security

Industry plays a vital role in closing technology gaps. Development of specific capabilities for the protection of CUI can be accelerated by experimentation with relevant use cases, and by teaming between industrial parties that can provide a part of the solution. All solutions together lean on the use of data. The scope of this data ranges from digital twins of infrastructure, environmental and hydrographical data, data collected by service providers or dedicated sensors to situational understanding necessary for prevention or intervention through risk based deployment of effectors.

The Northern Naval Capability Cooperation (NNCC) nations have launched the Seabed Security Experimentation Centre (SeaSEC) initiative. SeaSEC offers a shallow water experimental environment to test existing technology in seabed security use cases under representative conditions for operations in shallow waters. SeaSEC acts as an accelerator, fostering collaboration among industrial parties, each contributing a piece of the puzzle to create a demonstrator of promising solutions.

The data produced during joint experimentation campaigns such as SeaSEC can drive unified, data-driven solutions. By pooling data on threats, creating a comprehensive digital twin of the North and Baltic Seas, and employing an evidence-based strategy, we can effectively counter maritime threats. NNCC countries should therefore embrace the joint SeaSEC approach within their own borders, instead of opting for individual national solutions.

Looking ahead, governments can contract civil parties with a continuous assignment to develop a digital twin of the seabed infrastructure. This digital representation would provide invaluable insights and enhance the ability to protect and manage maritime assets. There is a role for government agencies to guard and maintain these data in a government owned, government shared digital representation.

Investment in specific seabed security technologies remains limited due to uncertain business cases. Greater harmonization of procurement requirements across NATO and EU member countries is needed to drive efficiency and interoperability and will drive viable business cases for industry. The EU Permanent Structured Cooperation (PESCO) is a framework that can aid joint planning, development and investment in collaborative capability development.

Furthermore, governments must take a more proactive approach to procurement. The speed at which solutions are needed justifies an agile procurement approach to drive short cycle innovations in research, development and production of defence capabilities. This approach will stimulate industry to team up and integrate technologies into solutions.

Strengthening International Cooperation

International cooperation can be sought on a political, military, industrial and scientific level.

Political and administrative cooperation

Currently, the focus of PESCO Seabed Security is on safeguarding Critical Underwater Infrastructure (CUI) in deep waters. However, there is a pressing need to broaden this scope. It is essential to include the protection of CUI in shallow waters as well. This expansion will ensure a more comprehensive security strategy.

Furthermore, political cooperation can drive efforts to adapt to more robust legal frameworks and harmonization of law enforcement policies. At a regional level, the authors would like to call for the formation of a North Sea Security Council with representation at Prime Minister level to spearhead these efforts.

Military cooperation

In the realm of intelligence and situational awareness, NATO Allied Maritime Command (MARCOM) should be empowered to take the lead in coordinating a military response from NATO countries to threats against Critical Underwater Infrastructure.

Meanwhile, cooperation in surveillance and crisis response is being strengthened through NATO Standing Maritime Group 1, and the NATO Admirals Channel Committee (CHANCOM). This collaboration focuses on conducting exercises, implementing strategies, enhancing interoperability, and refining the Command and Control (C2) structure. These efforts are vital for maintaining readiness and cohesion among the forces. Military activities such as NATO's Baltic Sentry will enhance NATO's military presence in the Baltic Sea and improve Allies' ability to respond to destabilizing acts.

National Maritime Situational Awareness with respect to ships of interest moving from one EEZ to the other, can be improved from sharing data and intelligence between neighbouring countries and between civil and military sectors. The European Common Information Sharing Environment (CISE) is a network that enables structured and secure information sharing among maritime authorities. Maritime authorities are urged to improve their cooperation on sharing data and intelligence within the CISE framework. Data and information sharing between civil and military actors can be further facilitated by Privacy Enhancement Technologies (PETs).

Industrial cooperation

Cooperation in European Defence Fund (EDF) projects has become a cornerstone of industrial development. Cooperation in PESCO acts as a key enabler to formulate calls for EDF projects. Furthermore NNCC and SeaSEC are important facilitators and accelerators of industrial cooperation.

Scientific cooperation

Scientific cooperation between academia and research institutes should aim to synchronize modelling of threats, vulnerabilities and responses, as well as experimental development of sensor and effector technologies. Moreover, research institutes can play a vital role in supporting experimentation and accelerating short cycle innovation in facilities such as SeaSEC. Scientific cooperation can drive future interoperability standards by developing and testing and evaluating Experimental Tactics (EXTAC's).

Scientific cooperation is facilitated by the existing Memorandums of Understanding (MOU's) for bilateral and trilateral cooperation as well by joint experimentation in SeaSEC or the NATO Robotic Experimentation and Prototyping using Maritime Uncrewed Systems (REPMUS) exercise.

Conclusions and recommendations

This position paper highlights the need for immediate and long-term action to counter threats to CUI in order to provide guidance for political, governmental, and military decision-making.

Defending our seabed infrastructure requires three priorities:
Firstly, governments need to develop defence capabilities to protect CUI. The priority is to have a response capability to defend high-risk high-impact infrastructure. Governments need to take ownership of the process of continuous improvement to account for evolving infrastructure and technology. Research institutes and industry need to work together to develop technology to counter the threats from small underwater systems.

Secondly, resilience of critical infrastructure needs to be improved. The priority is to maintain viable business cases for the development of offshore assets by finding a balance between energy transition goals, security and the right conditions for investment. Governments must develop risk-based security requirements for the protection of infrastructure. If security of CUI leads to negative returns on investments, politicians must take responsibility and provide budgets for governments to maintain viable business cases.

Thirdly, we must improve our societal resilience. Here, our priority is to mitigate societal impact of energy or data disruption. National and local governments must raise awareness to improve and facilitate preparedness at household and community levels. National governments and energy sectors must jointly promote and facilitate solutions for household energy independence. Governments and industries in the critical infrastructure sectors should develop comprehensive emergency response plans to ensure that all stakeholders are prepared to act swiftly and effectively.

To meet these priorities, political, government, military and industry efforts must be aligned:
Navies and coast guards need clarity about their tasks and responsibilities. Therefore, politicians and governments should empower them by providing a clear mandate and corresponding rules of engagement to protect CUI in the current hybrid conflict phase. Furthermore, the different government agencies involved in CUI should aim for a clear demarcation of roles, tasks and responsibilities.

We must cooperate internationally to create a legal framework that mandates an adequate response in our national EEZs. Nations should review their national legislation to penalize sabotage to CUI to ensure that sabotage can be penalized to an adequate degree. In the EU, national legislation should be coordinated to standardize the legal situation in European waters. Within coalitions of the willing partnerships can be forged to address shortfalls and develop legal frameworks to act more effectively and quickly within the context of international law.

Closing of the technology gap requires industry to team up and invest in dual use seabed security technology. Governments must create the conditions to invest by alignment of their investment roadmaps and cooperation with national investments using the EU Permanent Structured Cooperation. Governments must adapt to agile procurement to enable accelerated industrial development of solutions.

Finally, cooperation between maritime authorities, both civil and military is needed to improve the maritime situational awareness of threats to CUI. A government owned, government shared digital representation of the sea area to be protected is paramount for this endeavour. European Maritime authorities are urged to improve their cooperation within the Common Information Sharing Environment (CISE).

TNO innovation for life

SeaSEC Seabed Security Experimentation Centre

Northern Naval Capability Cooperation NNCC

The Hague Centre for Strategic Studies

Ministerie van Defensie

Ministerie van Infrastructuur en Waterstaat