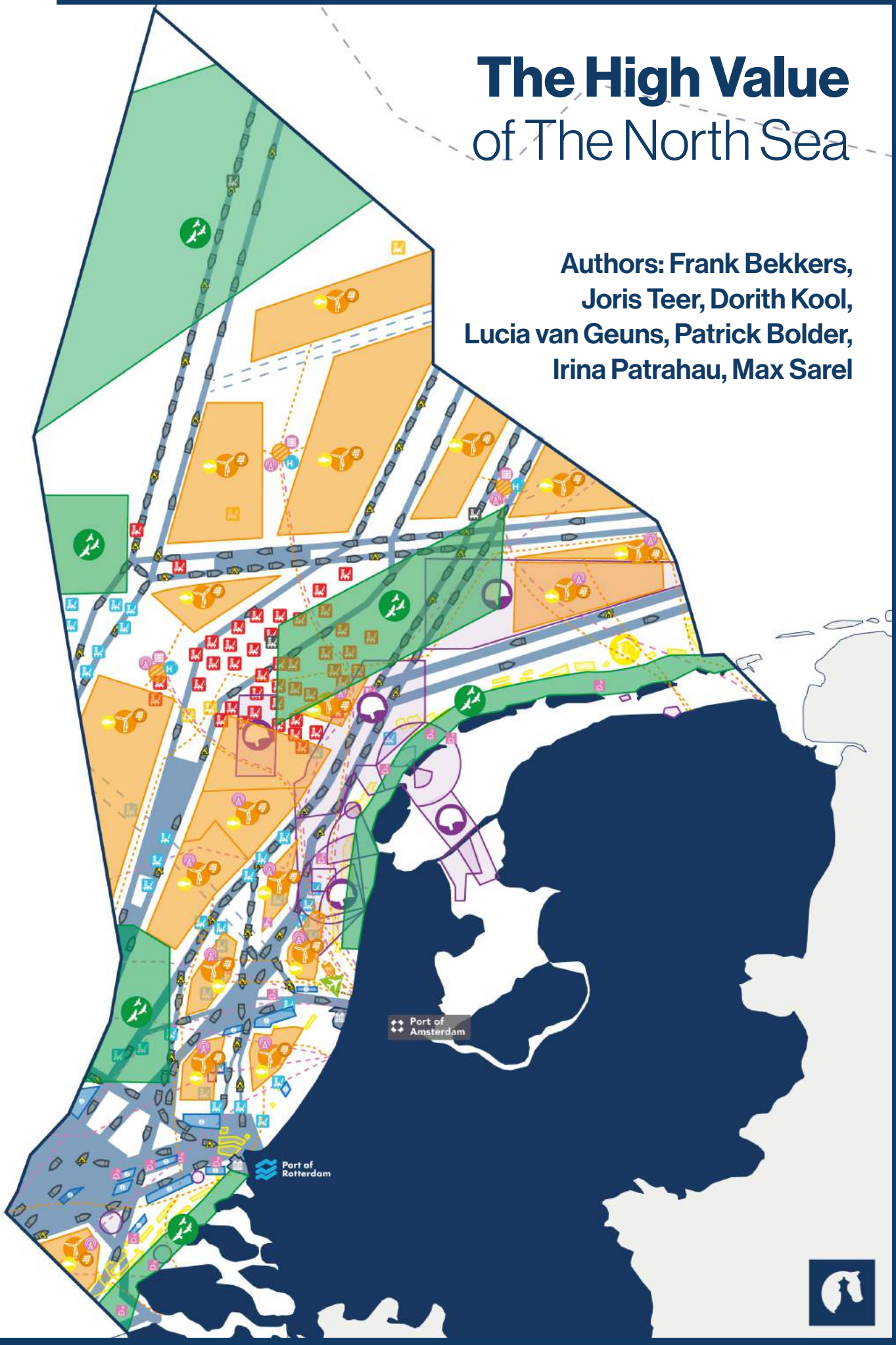
The Hague Centre
for Strategic Studies

The High Value of The North Sea

Authors: Frank Bekkers,
Joris Teer, Dorith Kool,
Lucia van Geuns, Patrick Bolder,
Irina Patrahau, Max Sarel



The Hague Centre
for Strategic Studies

The High Value of The North Sea

Authors:
Frank Bekkers, Joris Teer, Dorith Kool, Lucia van Geuns,
Patrick Bolder, Irina Patrahau, Max Sarel

Design:
Jelle van der Weerd (Online Dienstverlening) designed the
visualizations and graphs with the HCSS logo

ISBN/EAN: 9789492102881
September 2021

Table of Contents

Executive Summary

Study context and aim

Sea-based economic processes rapidly expand, both in size and complexity. Many of the expanding activities in the North Sea, such as the production of offshore energy, are vital to the Dutch economy: they are part of the critical processes defined in the Dutch National Security Strategy. Inside the territorial sea, the zone between the coast and 12 miles out where national legislation applies, protecting these critical processes against malicious actors is a national responsibility. As offshore economic value creation surges, the organization of security within the 12-mile zone should be critically reviewed. But as vital activities move further out to the Exclusive Economic Zone (EEZ), a fundamental dilemma arises. Under the Law of the Sea, outside the 12-mile zone, the national mandate for prevention, detection, protection and response in the face of security risks and threats is limited. So how and by whom is the integrity of the – increasingly critical and vulnerable – processes and associated infrastructure in the North Sea guaranteed? Current policy documents hardly address that crucial question.

Within this context, this study particularly looks at the future role of the Netherlands Coast Guard (NLCG) and of the Royal Netherlands Navy (RNLN) in providing security in the North Sea. The focus lies on deliberate security risks and threats, planned for and executed by malicious actors. In more detail, the study aims to:

1. Identify, describe, and analyze the trends and **developments in value-creating activities** in the Dutch part of the North Sea towards 2035, with some vistas for the period up to 2050.

2. Assess how new or enhanced vulnerabilities associated with these value-creating activities at sea offer **leverage for malicious actors** in the period up to 2035 and beyond.

3. Analyze and interpret what the developments identified in 1. and 2. may **imply for the NLCG and the RNLN**. These implications are discussed within the wider context of a range of stakeholders relevant for the security in and of the North Sea.

4. Draw **conclusions** for the NLCG and the RNLN in terms of possible policy development and engagement with other stakeholders.

Developments in offshore value creation

Even today, large parts of the North Sea are designated for specific, sometimes overlapping, users and usages, see Figure 1.

Spatial use of the Dutch part of the North Sea in 2015

Percentage of the Dutch continental shelf

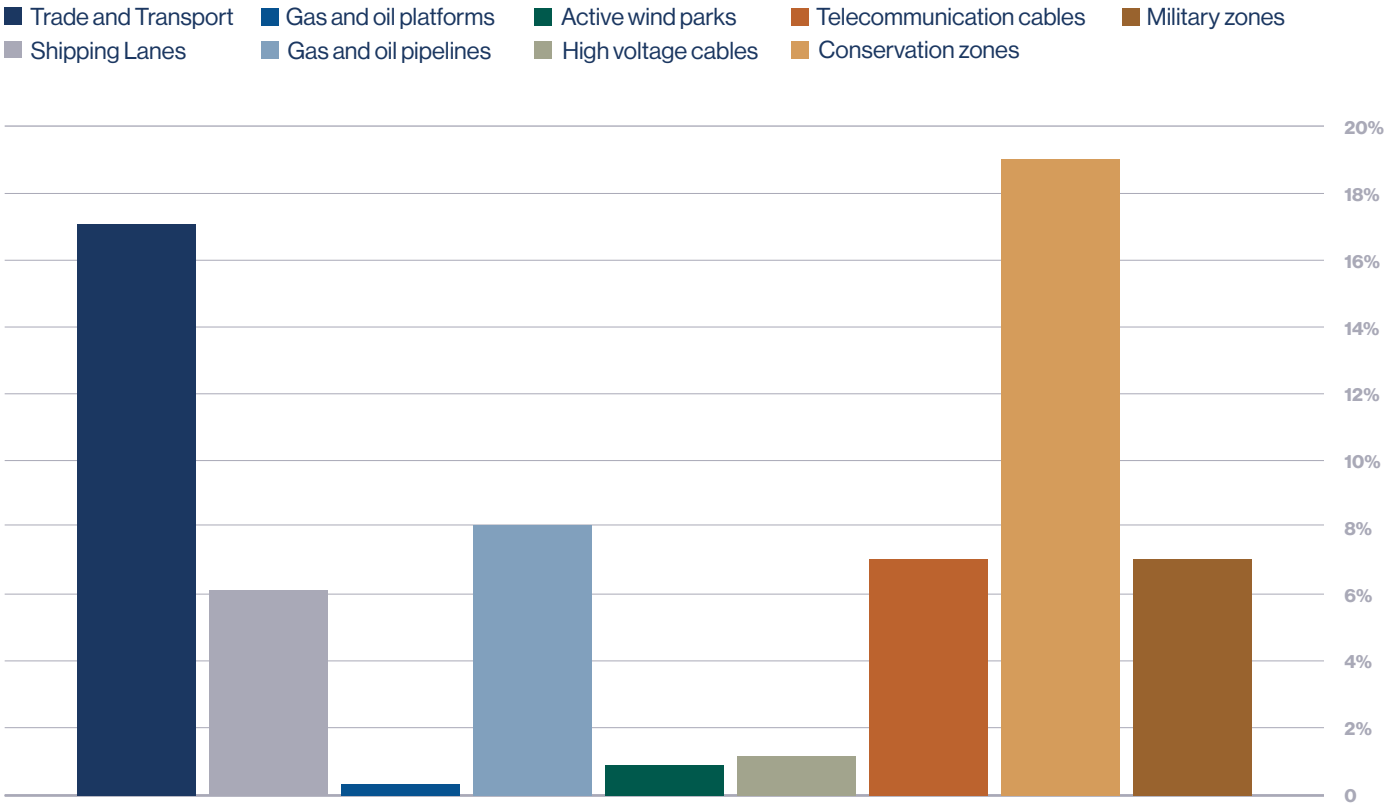


Figure 1. Spatial use of the Dutch part of the North Sea in 2015

Primarily due to the expansive growth of offshore wind energy, the pattern of North Sea usages becomes more covering and more complex in the decades to come, as visualized by the overview maps of Figure 2.

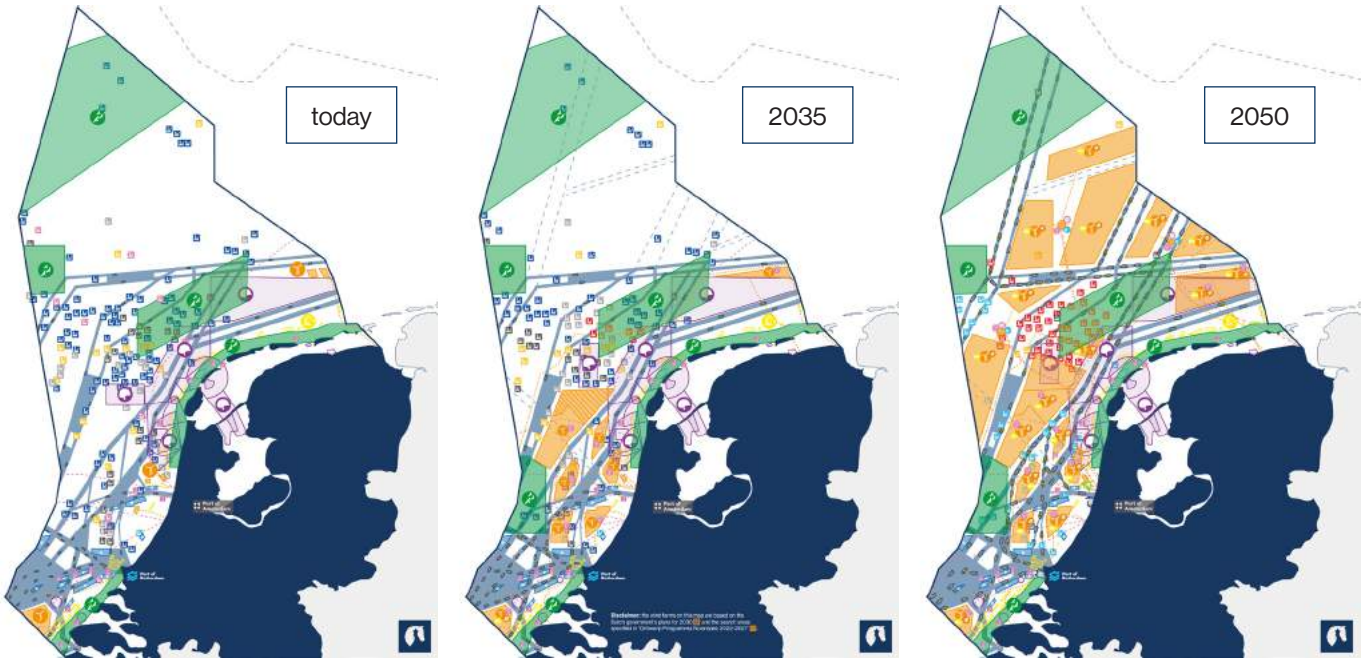


Figure 2. Projected development of users and usages in the North Sea (legend in Annex B)

Three parallel transitions will transform the use of the North Sea towards 2035 and beyond. The most prominent of the three is the energy transition. The National Climate Agreement (2019) states that greenhouse gas emissions, compared to 1990 levels, must decrease by 49% in 2030 and by 95% in 2050. The North Sea Agreement (2020) sets out how a wide range of stakeholders plan to realize the required energy transition. In addition, a nature transition and a sustainable food transition are necessary to ensure a healthy maritime environment in the North Sea. Table 1 summarizes the key developments.

Category	Key take-aways
Trade and transport	• Likely increases in traffic volumes will further aggravate already busy shipping lanes in the North Sea. Other activities will grow, exerting spatial pressures that will further restrain the freedom of movement for trade and transport. • LNG activities centered around the Port of Rotterdam have grown significantly recently and will continue that growth trajectory. • CCS-related CO_2-shipping will likely have commenced but on a limited scale. • Ship-propulsion will diversify as less-polluting methods are explored.
Energy	• Gas production will continue to decline. • Wind power production capacity will increase dramatically. • By 2035 hydrogen production will likely have surpassed the experimentation scale, with maybe the first major project just completed. Large scale application, however, is highly uncertain. • CCS projects are expected to commence soon. Large scale CO_2 sequestration projects are expected in the 2035-50 timeframe.
Communication and sensing	• With the Netherlands being a digital node for Europe, data telecommunications are expected to increase with new cable laying plans already concrete. • Sensors at sea will be moved from oil and gas platforms to transformer blocks in wind farms.
Industry at sea	• Sand drenching remains the primary industry at sea to support the increased sand demand for coastal defenses and onshore building activities. • Floating nuclear plants in the North Sea and Schiphol at sea remain very unlikely by 2035.
Fishing and aquaculture	• Large parts of the North Sea currently available for fishing will make way for other uses, such as wind farms and sustainable aquaculture. This may lead to (further) unrest in the sector. • Brexit is an added source of uncertainty for traditional fishing.
Living and recreational use	• Recreational use of the North Sea is modestly important to Dutch society but a minor factor in the grander scheme of the anticipated developments in the use of the North Sea.
Conservation	• To ensure conservation, additional restrictions on other activities are expected to be implemented.
Defense use	• Military exercise areas remain important and will likely incur limited alterations.

Table 1. Expected key developments towards-2035 in the usage of the North Sea

Table 2 provides an overview of the anticipated trends in the spatial use of the North Sea in the period 2015-2035. The last column of Table 2 lists some potentially impactful developments / projects that might take shape in the period 2035-2050, divided in three categories. *Probable* projects will likely be technically and economically feasible at a large scale between 2035 and 2050, building upon existing policy-plans and strategy documents. *Possible* projects might be technically and economically feasible at a large scale in the future, but not yet supported by policy and strategy plans. *Unlikely* projects currently lack a clear business case, are technically extremely challenging and/or depend on very uncertain drivers.

Activity		Scale[1] (2015)	Trend towards 2035	Potential key developments towards 2050
Trade and transport	Shipping lanes	3600km², 6%	slight increase	Possible: Arctic route opens up Probable: autonomous ships common Possible: Schiphol at Sea
	Anchorage sites, clearways, ports	6260km², 11%		
Energy	Gas and oil platforms	161, 126km², 0.2%	sharp decrease	
	Gas and oil pipelines (incl. 500m zones)	4500km², 8%	slight decrease	Probable: some pipelines repurposed for CCS/ hydrogen
	Wind farms	5 parks 471 km², 0.8%	sharp increase	Probable: further sharp increase
	Other renewables	0%	slight increase	Probable: hydrogen substantial in energy mix Probable: Tidal wave energy and other alternative energy (e.g. floating solar panels)
	High voltage cables (incl. 500m zones)	<1%	sharp increase	Probable: further sharp increase
	Carbon capture storage	0%	slight increase	Probable: CCS introduced on a large-scale
Communication	Telecom cables (incl. 750m zones)	20 (active) cables, 2000km; 7%	slight increase	
Industry at sea	Sand drenching	25 million m^3	slight increase	Probable: even larger scale sand drenching Possible: multi-purpose artificial islands created out of sea Unlikely: nuclear reactors at sea
Traditional fishing		EEZ except for prohibited areas	sharp decrease	
Aquaculture			slight increase	Probable: seaweed farms, mussel farms
Living and recreational use			approx. the same	Possible: artificial islands for living purposes
Conservation zones		6 zones 11.020km², 19%	slight increase	
Defense zones		5 zones, 4200 km², 7%	approx. the same	

Table 2. Spatial use of the Dutch part of the North Sea in 2015;[2] and trends towards 2035 and 2050

We may conclude that value creation in the North Sea is rapidly expanding over the next 10-15 years, a development that is likely to continue in the subsequent period up to 2050. Many of the developing offshore processes and associated infrastructure can be classified as critical for national security.

1 Percentages indicating the fraction of the Dutch continental shelf (58,000km²) used for the specific activity. See also Figure 1.

2 For the sake of comparison, the figures of 2015 were used as these were comprehensively available. Sources: Windenergie op zee – Noordzeeloket; Policy Document on the North Sea 2016-2021, p34; The Future of the North Sea, pp27,55,65; Ontwerp Programma Noordzee 2022-2027, pp77,82. Since 2015 many changes have occurred, as for instance additional wind farms have been constructed and gas and oil platforms have been decommissioned. The main text specifies more recent figures.

New and enhanced risks in a changing security environment

The upsurge of critical processes in the North Sea requires more attention to the security of these processes and the underlying infrastructure. This should be gauged against the backdrop of a rapidly evolving geopolitical and security environment. Over the past two decades, we have witnessed the return of geopolitical competition between major powers. At the same time, the role of non-state actors in the international system is growing, for better and for worse. Armed groups, insurgents, terrorist organizations, and criminal networks can instigate large-scale violence and threaten order and stability, either independently or in cooperation with state actors (as proxies). Conversely, non-governmental organizations, international corporations, and philanthropic institutions can promote resilience and stability in societies. Other non-state actors, such as social media platforms, play a dual role, fostering cohesion in society but also generating fragmentation.

The changing character of conflict is another factor driving rapid transformation in the international system. Although a conventional conflict between major powers cannot be ruled out, states tend to opt for options that fall below the threshold of (all-out) war. Often referred to as 'hybrid threats' or 'operations in the gray zone', this entails the deployment of various instruments of power in concert. These instruments range from disinformation campaigns and cyber operations, via supporting extreme groups and proxies, to sabotage and targeted killings. The orchestrated deployment of these tools is mostly covert or disguised. As a result, the nature of the threat is often unclear and diverse, and attribution can be difficult.

In the new security environment, threats and conflicts have come closer to home. With borders disappearing or taking different forms in the digital world, the Netherlands, with its open economy and society, has in many ways become a front-line state. Given the interconnectedness of domestic and international security, the Netherlands must consider not only conflicts far away, but also – and perhaps primarily – the security and resilience of its own society and territory against a range of risks and threats. At the same time, security challenges are becoming more complex. Vulnerabilities compound, for instance in the combination of functions – energy, communication, sensors, datacenters – on multi-purpose, offshore platforms or artificial islands which provide malicious actors high-value targets. On the threat side, we see the blending of crime and terrorism, state actors employing non-state proxies, and cyber and physical attacks linked together.

Based upon our desk research and expert consultation, HCSS assesses the following security issues the most pressing for the security in and of the North Sea towards 2035.

Diversity of risks and threats requires a comprehensive approach. Offshore processes and assets face a wide range of possible threats. We have categorized these threats as listed in Table 3. Our research indicates that all these types of threat are possible; and that all may cause substantial consequential damage. The whole threat palette is therefore relevant from a national security perspective. Furthermore, offshore processes and infrastructures tend to become more entangled, with threats also turning more complex and intertwined, as different types of malicious actors join forces. Overall, we project mounting probabilities that incidents in the North Sea generate cascading effects leading to severe disruptions of critical processes, offshore and onshore. As the range of high-consequence risks and threats expands, and risk and threats tend to overlap and merge, a comprehensive approach of security in and of the North Sea becomes imperative.

Criminal & terrorist threats
Piracy and hostage taking. Criminal or terrorist activities directed at vessels or maritime structures
Cybercrime. Criminal or (state backed) terrorist activities that attack or take control over ICT systems of vessels or maritime structures
Smuggling and trafficking. Criminal activities that are enabled using the seas, such as human trafficking and smuggling of drugs and arms.
Unauthorized entry. Criminal activities that violate a coast state's sovereignty, such as illegal fishing and unauthorized entrance of a state's internal waters
Environmental crimes. Criminal activities that violate international law, such as dumping and discharging of polluting materials
Hybrid threats
Sabotage. Hybrid actions to deliberately destroy, damage, or obstruct vessels or infrastructure at sea for political or military advantage in peace time
Cyber operations. Hybrid actions that are directed at covertly monitoring or interfering with ICT systems of vessels or maritime structures
Espionage and interference. Hybrid actions to gather intelligence in peace time, for instance by using civil vessels equipped with advanced sensors for military purposes or by tapping or compromising communication cables at sea
Incursions. Hybrid actions, often by military vessels, that violate a coast state's sovereignty, either openly or covertly, to probe defenses or to 'show the flag'
Military threats
Physical attacks. Military operations targeting critical maritime functions, vessels and structures, military or otherwise. Includes stand-off and direct attacks by military platforms aimed at follow-on forces transports from North America in case of a war in Europe involving NATO
Cyber electromagnetic activities. Military operations targeting to destroy, degrade, or take control of ICT systems of vessels or maritime structures, military or otherwise
Deny access and use. Military operations to disrupt or hinder the access to and use of the North Sea, including through the use mines or stand-off means
Military espionage. Military operations to gather intelligence, for example by tapping communication cables or deploying unmanned sensor platforms at sea
Raids and landings. Military operations to access the land from the sea, ranging from small scale and covert deliverance and extraction of units (e.g., SOF) to larger amphibious operations

Table 3: Various types of threat associated with three categories of threat actors

Countering cyber risks and threats top priority. Cyber threats combine a relatively high likelihood and impact. As the maritime domain becomes more digitized, cyber vulnerabilities are expected to increase. Clearly, cybersecurity constitutes a key issue in any North Sea security strategy. At the same time, whilst there are very specific characteristics involved in maritime cybersecurity, it is also part of the broader cyber challenge. A first step is to fully incorporate offshore critical infrastructure in national cybersecurity and critical infrastructure protection plans and practices, considering the specific characteristics such as jurisdiction, reduced physical accessibility, and the wide variety of international interests involved with assets in the North Sea, such as flag states, shipowners, and IT/OT-suppliers.

Sabotage and physical threats potentially have the most impact. Even if we judge cyber threats to score highest in overall likelihood X impact, incurring physical destruction may well have the most immediate consequential damage (note that a cyberattack can be a channel through which to achieve physical damage). However, these threat categories are considered less likely than cyber threats because they have, in general, a higher threshold for execution in terms of opportunity and costs and are typically more attributable, more defendable, and easier to retaliate. Paying more attention to cybersecurity should certainly not lead to the neglect of traditional physical protective measures.

Protect critical infrastructure hubs. Platforms that function as energy hubs are lucrative targets for sabotage. Malicious actors can take control over and occupy these platforms. Incapacitating electricity transformer stations, for instance, has the potential to cause power outages across the Netherlands, forcing critical socio-economic processes to a standstill. The combination of, for example, hydrogen production, CO_2 storage, sensing and data centers on artificial islands might be economically advantageous but dangerous from a security perspective. These future hubs could be targeted by state actors and terrorist groups not only to cause severe damage, but also to gather crucial intelligence. Despite its importance for national security, critical infrastructure is often left weakly protected because its design is primarily economically driven. Much more attention should be given to 'security by design' right from the inception of new infrastructure projects.

Monitor chokepoints in critical shipping lanes. The increasing congestion in the North Sea leads to more critical chokepoints. Narrow shipping lanes can be effectively closed using a relatively small amount of sea mines. Digitally or physically hijacking ships and letting them drift or sink in chokepoints is another possible modus operandi to severely hit the Dutch and European economy. Early warning and action must ensure adequate deterrence and response.

Counter industrial, political, and military espionage. The numerous offshore economic, industrial, and military activities projected in the North Sea make it a lucrative target for espionage and intelligence gathering. Various state actors are involved in espionage operations around the world, in the case of China and Russia known to be using look-alike commercial vessels. These may e.g. be equipped with unmanned underwater vehicles, targeting data cables on the seabed, which can be intercepted and tapped. State-Owned Enterprises that have acquired a solid foothold in harbor and offshore processes may act as a platform for espionage and political interference. With most data digitally stored and processed, espionage in the information age has considerable overlap with cyber threats. This, once again, re-enforces cybersecurity's top priority.

Pay attention to highly combustible and poisonous energy-related shipping. The changing energy mix in the ongoing energy transition brings new risks. As an increasing volume of combustible fuels such as LNG and hydrogen (stored in e.g., ammoniac) are transported at sea, the impact of hijacking a ship also increases. If hydrogen production seriously takes off after 2035, not only the transport but also infrastructural elements might become a target for malicious actors. Where oil can cause massive environmental damage and pollution, these new energy sources are explosive and/or spread poisonous gas, with the potential to cause harm to life far from the area of explosion. A digitally hijacked LNG tanker or even an LNG powered ship can thus be used for ransom by criminals or as a floating bomb by terrorists.

Smuggling and trafficking is a nuisance that requires an international and chain approach. Smuggling and trafficking is not a hypothetical scenario but an everyday fact. The consensus seems to be that drug trafficking is something we must have to live with; but not something we should accept. To contain the impact, enough effort must be put in discouraging the most profitable and distressing business cases.

Implications for Coast Guard and Navy

What do the above findings mean for the Netherlands Coast Guard and the Royal Netherlands Navy as these organizations prepare for 2035 and beyond? Below some of the most salient implications.

Legal and managerial framework

As security in and of the North Sea has many stakeholders, the functioning of the NLCG and the RNLN must be seen in light of the wider context in which these two organizations operate.

Territorial sea vs EEZ. A key issue is the separation between the territorial sea where, by and large, national legislation applies; and the EEZ, where room for national measures in the face of security risks and threats is limited.[3] National governance of the territorial sea must be critically reviewed and adjusted. For practical reasons, security at sea should as much as possible be aligned with existing onshore security structures and processes. Other than on land, the North Sea lacks a local framework for safety and security tasks and responsibilities. Security incidents are handled at the national level, with the NLCG as first responder. But the NLCG is a small network organization, neither equipped nor tasked to deal with the full spectrum of prevention, detection, protection and response in the face of security risks and threats. In addition, the NLCG lacks the authority, constituency and resources to act as the public custodian of security in and of the North Sea in the political and policy battles for attention and budget.

In the EEZ, the Law of the Sea offers limited room for national authorities to exercise security measures. Thus, as critical activities move further out to sea, guaranteeing security outside the territorial sea poses a crucial dilemma, with difficult political, judicial, administrative, economic, and technical ramifications. This dilemma is hardly addressed, if at all, in the current debates on the future of the North Sea. This study flags this as a serious omission, which hampers adequate responses to many of the key issues below.

A 'North Sea Authority' (NSA). Establishing a single Authority to take responsibility over the related issues of spatial planning and security in the Dutch part of the North Sea would be an important step in taking maritime security more seriously (note that the two have a clear relationship, as 'security by design' is a crucial element of responsible spatial planning). The mandates, and therefore tasks and responsibilities, of such a NSA are different for the territorial sea and the EEZ – where our advice would be to try and minimize or bridge these differences as much as possible. The NLCG would act as the operational arm of the NSA, broadening its executive responsibility and authority to prevent, detect, protect, and response in the face of security risks and threats considerably. Risk analysis and prevention, including regulation and supervision, would become an integral part of its task package. An NSA would make it easier to switch between local, national and international levels of action and response. This is important when it is unclear what the cause and consequential damage of an incident is; or whether the incident is a stand-alone event or connected to other incidents (e.g., as part of a hybrid campaign).

3 For the so-called contiguous zone, 12-24 miles from the coast, coastal states claim no territorial rights but may assert limited jurisdiction for one or more special purposes.

Security functions

Prevent. The NLCG and the RNLN can strengthen general awareness of security risks throughout the maritime sector by setting up regular consultations between relevant government bodies, the offshore energy industry, port operators, and shipping companies. Together they may claim a structural advisory role in the formulation of standards, legislation, and regulations for activities and infrastructures at sea, aimed at promoting resilience and enforcing security. And they can organize network events and joint exercises with industry and the intelligence community. Many of these activities are aimed at creating a North Sea security constituency, a body of stakeholders that know one another, and can easily contact one another when needed in the other security functions.

Detect. Currently, the NLCG has limited real-time awareness of security-related activities in the North Sea. More than today, information from a multitude of sources must be brought together and analyzed to create integral Maritime Situational Awareness & Situational Understanding (MSA/SU). The Maritime Information Hub (MIK) is set up for this purpose but lacks sufficient connectedness to a wide range of sources and processing and analytical capacity. Information sources that should be utilized structurally include:

- The future Maritime Operations Center (MOC), with which the MIK should be fully connected and interoperable. The future division of labor and/or integration of MIK and MOC is a clear focal point.
- Next to the RNLN and the network partners already represented in the MIK: national public organizations and bodies such as the National Coordinator for Security and Counterterrorism (NCTV), the Royal Netherlands Air Force, and the intelligence agencies AIVD and MIVD.
- International peers, Frontex and the coast guards of other North Sea states.
- Companies in the maritime sector, such as port authorities, ship owners, and off-shore energy producers and facilitators.
- Permanent sensors to monitor large sea areas. In particular surveillance drones are a flexible asset that may greatly enhance MSA/SU.

As important as rich data is the ability to process that data into meaningful information and intelligence. The MIK's analytical capacity must be greatly expanded, partly in-house and partly by using external services. Close cooperation between the MIK and the MOC is required to share analyses and not duplicate work. Analytical effort should not only be directed towards MSA/SU of the North Sea itself, but also to build and maintain an overview of developing risks and threats that could, in due course, affect security risks and threats on the North Sea. This concerns, for example, information about international criminal drug networks, international terrorism or the positions and intentions of (maritime) units of possible adversaries.

An extremely important point of concern is the legal ability to use and share information coming for a range of sources. Impeding legal restrictions on linking information sources and integral analysis in the MIK for the purpose of security at sea should be evaluated.

Protect and respond. For many of its activities the NLCG piggybacks on the executive powers and the resources of its network partners. In the 'North Sea Authority' construct sketched above, the NLCG develops from a coordinating body largely dependent on the mandate and, ultimately, goodwill of its partners for executive action, to an organization that may act as first responder in the case of security incidents under its own authority. In addition, the NLCG should be given more responsibility for formulating its own policy and executive

priorities within a given constitutional framework and in close consultation with its stakeholders. More executive power residing with the NLCG should facilitate dealing with structural security risks and challenges pro-actively, as well as responding timely and adequately to complex security incidents.

With hybrid threats likely to be a defining characteristic of the security environment towards 2035, the role of the RNLN must also be clarified and calibrated. Acting in the gray zone between peace and war is where the responsibilities of civil security agencies and the military meet, with potential overlaps and voids that might cause friction or insecurities if left unresolved. Naval assets deployed in the North Sea may act (1) under the NLCG's mandate; (2) under civil mandate as part of Defense's third main task, support to the civil authorities; or (3) under military mandate as part of Defense's first main task, collective defense. As highly violent threats with possible state actor involvement become more likely, (2) or (3) may befit naval deployment better than (1). Currently, there is no clarity on what scenario would warrant which framework and, consequently, what rules of engagement would apply sanctioned under whose authority. A single North Sea Authority would make it easier to establish escalation mechanisms in the case of violent threats, with clear complementary roles for the NLCG, the Special Interventions Service DSI and the RNLN.

(Additional) resources. More authority vested in the NLCG does not necessarily imply markedly more 'own' resources. More in-house capacity *is* required for creating MSA/SU and for oversight and possible direction over complex security incidents. For other assets, however, preferred access to resources of its network partners might well remain the favored model. That said, there is certainly a requirement for more response capabilities, such as:

- Capabilities for a permanent presence in the North Sea, for surveillance and monitoring purposes as well as to keep incident response times low for events further offshore.
- Capabilities to counter seabed warfare.
- Capabilities for monitoring and early threat detection with drones.
- Capabilities to be able to act in and counter highly violent incidents against armed malicious actors, in close cooperation with the RNLN and the DSI.

Cyber

Cybersecurity awareness at sea is currently marginal, with the maritime environment not a priority for onshore security agencies. Response capabilities specific for offshore cyber incidents and cyberattacks are practically non-existent. What capabilities are required for prevention, detection and response?

In the sphere of prevention, an advisory role of the NLCG to better incorporate offshore critical processes and infrastructure in cyber-related standards, legislation, and regulations can be envisaged. In joint exercises and knowledge sharing events with the stakeholders involved in North Sea security, the cyber domain should be fully incorporated.

In the realm of detection and early warning, cyberspace should be an integral part of a comprehensive MSA/SU. Information sharing with the National Cyber Security Centre and the Defense Cyber Command is essential. A broader cyber threat analysis is also essential as an anticipatory framework for specific cyber risks and threats aimed at North Sea traffic and infrastructure. This is where the MIK, the future MOC (which will feature cyber expertise), the NCSC, and the DCC should join forces.

In terms of protection and response, the way forward is to better incorporate vital offshore processes in existing arrangements for (cyber-related) critical infrastructure protection, with an advisory and auxiliary role of the NLCG to guard the particulars of the maritime environment.

Cooperation

Between NLCG and RNLN. Currently, there are no clear mechanisms for persistence and unity of command and effort in complex security incidents at sea. Broadening the executive responsibility and authority of the NLCG as the operational arm of the North Sea Authority and clarifying the role of RNLN in more complex scenarios could address this issue. We would advocate a layered arrangement for NLCG and RNLN cooperation. In relatively low-violence threats and incidents, the NLCG provides the framework for deployment of naval personnel and assets, very similar to the way special units from the Armed Forces are employed under the Police Law in the Special Interventions Service DSI, closely working together with special units from the police. Against highly violent threats and/or threats with (possible) state actor involvement, however, the RNLN may deploy fully naval teams and assets under national civil authority (as part of the third main defense task) or under military mandate (as part of the first main defense task). As in reality complex situations typically come with a lot of uncertainty, intimate cooperation between NLCG and RNLN is required to smooth over formal ambiguities in 'who does what under which mandate'.

Internationally. With the distinction between domestic and international security fading, cross-border security cooperation becomes essential. This is certainly the case for the North Sea: the EEZ is governed by international treaties rather than by national legislation; and sea trade as well as cables and pipelines cross EEZ borders as a routine matter. Therefore, the NLCG should cooperate as much as possible with European partners. Frontex, the European Border and Coast Guard Agency, is important in this regard. Other international initiatives, particularly in the realm of information and analysis sharing, should also be pursued.

Final thoughts

A key insight to be taken from this study is that the volume and diversity of activities in the North Sea will grow moving towards 2035 and beyond. Activities become more intertwined, by nature, by spatial pressure, and by design. This trend comes with amplified existing and novel vulnerabilities that might be exploited by criminal, terrorist, hybrid, and/or military actors. Security risks, threats and actual incidents also become more multifaceted and may increasingly affect critical processes. Yet, our research and the feedback from experts and practitioners clearly indicate that, in the context of national security, 'offshore' is given less formal and practical attention than 'onshore'.

Given the expanding risk palette, the division of maritime security responsibilities and mandates between the various public, private and public-private stakeholders must be fundamentally revisited. As the nature, origin and possible follow-on consequences of various foreseeable security incidents may remain unclear until late in the process, operational flexibility between the various responders is key. This is particularly true for hybrid threats, which may overlap with criminal and terrorist threats on the one hand, and with military threats by state actors on the other.

The networked Netherlands Coast Guard is well suited for a multidisciplinary approach to face these complexities. To fully capitalize on this, in essence four lines of development are required: (1) comprehensive security in and of the North Sea should be taken more seriously and integrated in existing national security processes, structures, and mindset; (2) more authority should be vested in the NLCG to execute security functions throughout the risk management cycle, in close coordination with and supported by its network partners; (3) the respective roles of NLCG and RNLN in a range of potentially highly violent scenarios should be clarified and calibrated; and (4) more (guaranteed access to) resources is needed for an adequate execution of the security tasks presented by these scenarios.

With many organizations involved in maintaining security in and of the North Sea, each with its own mandate and task profile, the intimate relationship between the Netherlands Coast Guard and the Royal Netherlands Navy is a key asset to guarantee operational solutions that smooth over institutional ambiguities and seamlessly align the required capabilities from various sources. We have advocated a construct that brings as much as possible clarity in the fruitful cooperation between the NLCG, the RNLN and other agencies. This construct gives the NLCG additional executive authority under the umbrella of the North Sea Authority, with the latter guaranteeing institutional embedding while the NLCG and its partners concentrate on operational security in and of the North Sea.

1 Introduction

1.1 Why this study?

The North Sea is home to some of the busiest shipping lanes in the world, connecting Northwestern Europe to its global trade partners. But outside these sea lanes, it is still possible to sail across large stretches of water seemingly devoid of human activity. Appearances can be deceptive, however. Beneath the surface, communication cables transport gigabytes of information to and from data hubs worldwide. Oil and gas flows through pipelines from production platforms just over the horizon to onshore users; the same pipes may well be repurposed for large scale hydrogen or CO_2 transport in the decades to come. It is quite likely that, in a few years' time, the ostensibly empty sea has been turned into a wind park construction site. It might even be that the water we sail on today will give way to land in the foreseeable future: artificial islands in the North Sea are a serious prospect.

The trend is clear. Sea-based economic processes rapidly expand, both in size and complexity. The next decades will see a sharp rise in the amount of critical infrastructure at sea: wind farms; communication, data, and power lines on the seabed; carbon capture and storage (CCS) in abandoned gas fields; and possibly sea food farms, energy production and other industrial activities at sea that the densely populated Dutch delta is no longer able or willing to accommodate. These new activities at sea will compete with more traditional activities such as sea transport, fishing, resource exploitation, recreation and military use (such as military exercise areas). The spatial pressures generated by these activities will be accompanied by other developments, such as advanced automation of barges, service vessels, and cargo ships.

Examples of security issues in the North Sea

Communication and power cables on the seabed, as well as under water oil and gas pipelines, are vulnerable, difficult to monitor continuously, and virtually impossible to protect completely. Disturbing the virtual and physical flows through these cables and pipes would result in significant problems in Northwestern Europe and the Netherlands.

Tensions with Russia in northeastern Europe could escalate to the extent that it would be necessary to ship additional US, Canadian, and UK troops, equipment, and supplies to mainland Europe for onward movement east. These shipments would likely travel via the North Sea and use Dutch ports. Attempted sabotage by Russia is to be expected. Alternatively, it cannot be excluded that ships from states involved in conflict – such as Iran, Israel, and Saudi-Arabia – would be targeted by their opponents while navigating the North Sea.

Sea mines constitute a cheap method for maritime area denial and their use is proliferating. They can be deployed by all kinds of state and non-state actors. Mine laying can be done covertly by commercial vessels. Even the potential presence of mines can bring commercial shipping to a halt. In the congested North Sea, with maneuvering space further reduced, for instance by offshore wind farms, deployment of sea mines would have dire economic consequences for the Netherlands and Northwestern Europe.

Activists, for example anti-globalists or environmentalists, have already targeted maritime assets such as oil rigs, ships carrying nuclear cargo, and cruise ships, both at sea and in ports. Most of these protests have been non-violent, but not all. In September 2020 in Indonesia, hundreds of environmentalists and fishermen bombarded the dredger *Queen of the Netherlands* with Molotov cocktails and stones, after which several fires broke out on board.

Cybersecurity is a key issue in the maritime environment. Critical infrastructure at sea as well as ships are prone to cyberattacks. An example would be criminals or (state sponsored) terrorists remotely taking control of a ship to hijack or capture the cargo and crew, or to create a dest-abilizing incident.

As the size, diversity and importance of sea-based assets and activities increase, so do the entry points for criminal and terrorist actions, and for disturbances and attacks by state actors. As 'sea' becomes more like 'land', guaranteeing the security of structures and processes in the North Sea warrants persistent attention – much more then currently is the case – and could potentially necessitate new approaches.

Figure 3. A more congested North Sea

Many of the expanding activities in the North Sea, such as the production of offshore wind energy, are vital to the Dutch economy: they are part of the critical processes defined within the framework of the Dutch National Security Strategy. Inside the territorial sea, the zone between the coast and 12 miles out where national legislation applies, protecting these critical processes against malicious actors is a national responsibility. As offshore economic value creation surges, the organization of security within the 12-mile zone should be critically reviewed. But as vital activities move further out to the Exclusive Economic Zone (EEZ), a fundamental dilemma arises. Under the Law of the Sea, outside the 12-mile zone, the national mandate for pro-action, protection and response in the face of security risks and threats is limited. So how and by whom is the integrity of the – increasingly critical and vulnerable – processes and associated infrastructure in the North Sea guaranteed? Current policy documents hardly address this crucial question.

1.2 Study aim

Within the context sketched above, this study particularly looks at the future role of the Netherlands Coast Guard (NLCG) and the Royal Netherlands Navy (RNLN) in providing security in the Dutch part of the North Sea. The focus lies on deliberate security risks and threats, planned for or executed by malicious actors. Accidents and disasters, as well as safety risks, are not our prime concern here. We also focus on the North Sea itself, and not the air space above it. In more detail, the study aims to:

1. Identify, describe, and analyze the trends and **developments in value-creating activities** in the Dutch part of the North Sea towards 2035, with some vistas for the period up to 2050.
2. Assess how new or enhanced vulnerabilities associated with these value-creating activities at sea offer **leverage for malicious actors** in the period up to 2035 and beyond. Three threat classes are considered: criminal and terrorist threats stemming from non-state actors; hybrid threats originating from Russia and other state actors, possibly acting through proxies; and the military threat from Russia.
3. Analyze and interpret what the developments identified in 1. and 2. may **imply for the NLCG and the RNLN**. How do they affect their security-related tasks and responsibilities, organizational structures, mutual relationship, modi operandi, and capabilities? These implications are discussed the wider context of a range of stakeholders relevant for the security in and of the North Sea, such as law enforcement agencies, private operators at sea, and the intelligence services.
4. Draw **conclusions** for the NLCG and the RNLN in terms of possible policy development and engagement with other stakeholders.

Approach. The study employs a combination of desktop research, interviews with stakeholders, and consultation sessions with experts from the customers, the NLCG and the RNLN. The list of interviewees and experts can be found in Annex A.

1.3 Reader's guide

This study has the following structure.

	Subject	Key Questions
Chapter 2: Setting the stage	Trends in activities on the North Sea	What are the high-level trends for the period up to 2035 in value-adding activities in the North Sea? (Further elaborated in Chapter 3)
	Trends in security	How could the evolving security environment, globally and in Europe, affect security in the North Sea? (Further elaborated in Chapter 4)
	Trends in governance	How is governance in the North Sea organized? What issues for maritime security responsibilities and tasks follow from the increased complexity of activities in the North Sea? (Further elaborated in Chapter 5)
Chapter 3: Value Creation	Key documents	What foresight, guiding and planning documents outline and drive developments in usage of the North Sea?
	Activities in the North Sea today	What activities are currently present in the North Sea, how are they conducted, and at what scale?
	Activities in the North Sea towards 2035	What are the trends in the usage of the North Sea towards 2035, what are the most relevant changes?
	Activities in the North Sea beyond 2035	What types of usage might only seriously take off beyond the 2035 timeframe, moving towards 2050?
Chapter 4: Threats	Key vulnerabilities	Given the trends and developments in the usage of the North Sea, how do current vulnerabilities develop and what new key vulnerabilities may arise?
	Criminal & terrorist threats	Looking towards 2035 (with some vistas beyond): what are 'business cases' for malicious actors to target these vulnerabilities? What would be the consequences if threat scenarios become reality?
	Hybrid threats	
	Military threats	
	Overall assessment	What are the most pressing overall security issues in the North Sea towards 2035?
Chapter 5: Implications	Legal and managerial framework	Given an increased need for security in and of the North Sea, how should authority of the North Sea and execution of security tasks be organized?
	Security functions	What do the changing and expanding security requirements imply for the security functions prevent, detect, protect and respond?
	Cyber	With cybersecurity increasingly critical, how should the security functions be shaped in the cyber domain?
	Cooperation	How should the relationship and cooperation between NLCG and RNLN develop? The same for coast guard cooperation in Europe?
	Final thoughts	What are the key messages to take home for the readers?

Table 4. Structure of the report

2 Setting the stage: the North Sea towards 2035 (and beyond)

This chapter sets the stage for more detailed discussions in the next chapters by providing an overview of trends and developments that are likely to affect the North Sea, with a focus on three aspects: value-creating activities, security, and governance.

2.1 Competing activities in an increasingly cluttered sea

The fundamental assumption behind this study (substantiated in Chapter 3) is that many maritime areas will be ever more filled with human activities, economic and otherwise, particularly in the coastal waters of densely populated delta's. The North Sea is a prominent example of this trend. The North Sea already is one of the busiest and most intensively used seas in the world. In addition, states in the North Sea region are looking for ways to alleviate growing spatial pressures on land by pushing activities to sea.

In 2018, the Netherlands Environmental Assessment Agency (*Planbureau voor de Leefomgeving*, or PBL), issued *The North Sea in 2030 and 2050: a scenario study*. Based upon a range of different policies that address various subtopics regarding the (future) use of North Sea, this study presents four scenarios. Two scenarios are based on *The Netherlands in 2030 and 2050*, which forecasts Welfare, Prosperity and Quality of the Living Environment in a low and a high dynamics variant. Both scenarios assume that government policy as it stood in 2015 will continue unchanged. Two sustainability scenarios were added, assuming that additional policy will be developed that contributes to the climate objectives in the Paris Agreement and the UN sustainable development goals. All four scenarios focus on three policy themes -- towards an energy transition, towards resilient ecosystems and towards a sustainable food supply -- and address other themes, such as defense and cultural heritage, in less detail (see Figure 4).

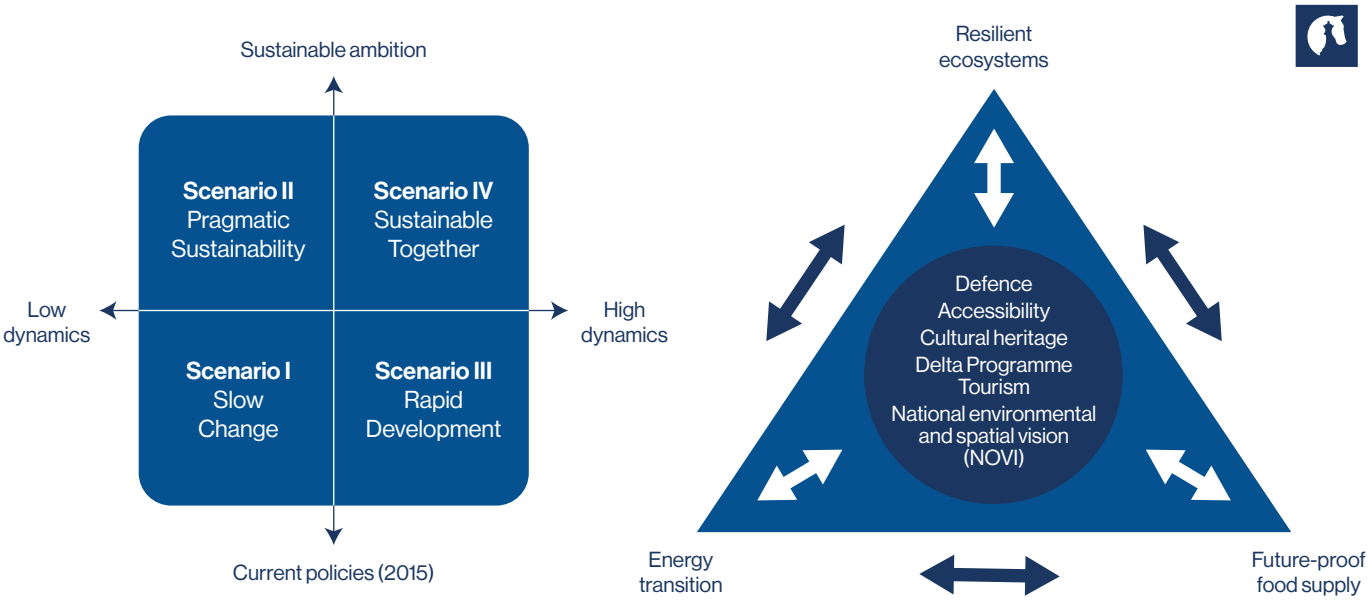


Figure 4. Four 'future of the North Sea' scenarios and key policy themes in PBL study[4]

The PBL study focuses on the question how combining various user functions can be implemented to make the most efficient and sustainable use of the limited space available on the Dutch continental shelf. It shows that, especially in the high dynamics scenarios, spatial pressures necessitate multiple use of space. Wind farms may have to be combined with other means of energy generation, nature reserves, fishing, and aquaculture. Fishing and recreational vessels will need to share space with increased ship movements, for instance for maintenance and supply of wind farms. Frictions between mobile and static users of the North Sea will increase. In areas with several spatial claims, the rules and conditions for each function must be clearly and comprehensively described. And even if various functions are combined in single spaces, priority setting might be required.[5]

Some new forms of activity at sea, such as the conversion of electricity from wind farms into hydrogen (power-to-gas) and the use of depleted natural gas fields for Carbon Capture and Storage (CCS), require new legislation and increased international cooperation to plan and coordinate investments in large-scale infrastructures. The timing of future changes in oil and natural gas production, offshore wind energy, CCS and the sub-surface storage of hydrogen is both critical and uncertain. There are substantial knowledge gaps. Although natural gas is important in the current energy supply and as an industrial resource, its role will be reduced in the transition to a sustainable energy supply. Is hydrogen produced by offshore wind energy a realistic alternative? Although a lot is known about CCS technology and costs, various governance questions concerning responsibilities for the capture, supply, transport, and storage of CO_2 will arise when we start using CCS. Finally, we do not know the long-term effects on the environment. Can these effects be reconciled with the need to conserve and sustainably use oceans, seas, and marine resources, one of the UN sustainable development goals?

4 Sources: PBL and www.noordzeeloket.nl

5 Note that more activities at sea may also increase spatial pressure on land. For instance, the growth of offshore wind energy requires new landing locations along the Dutch coast for power cables, as well as additional electrical grid infrastructure to deal with a more variable power supply.

2.2 Maritime trade remains important

2.2.1 The future of globalization

The North Sea plays a crucial economic role in linking Northwestern Europe to the global maritime trade routes. Maritime transport handles over 80% of global merchandise trade, thereby underpinning global supply chains and economic interdependency. Within the EU-28, the ratio of international trade in goods and services relative to GDP rose from 14.9 % in 2008 to 17.6 % by 2018, thereby confirming that trade in goods and services was growing at a faster pace than the overall EU economy.[6] Although the impact of Covid-19 in the second quarter of 2020 meant a decrease of the gross weight of goods handled in European ports of 17% vs Q2 2019,[7] according to UNCTAD international maritime trade is projected to recover and expand by 4.8% in 2021.

Yet there is no certainty that sea trade will continue to grow in the period up to 2035 and beyond. The golden age of globalization is over and has given way to a new era of sluggishness, what the Economist calls "slowbalisation". Activity is shifting towards services, which are harder to sell across borders. Multinational firms have found that it is increasingly difficult to compete with local rivals. 3D-printing impacts what is produced locally. The COVID-19 crisis has reinforced the tendency towards re-shoring and near-shoring to Western economies and their neighboring countries. Regionalization is gaining momentum. One of the major systemic trends for the next decade will likely be the decoupling of large economic blocs, particularly the US and China, in certain sectors. These tendencies have been amplified by the sudden increase in freight transport costs, which have made long-term transport costs less affordable.

Shifts in globalization patterns and supply-chain designs could transform the landscape of maritime transport. It could push shipping lines to rationalize services on the main east-west trade routes while strengthening intra-regional shipping networks.[8] Notably, China's Belt and Road Initiative (BRI) and its maritime branch, the Maritime Silk Road (MSR), could have a disproportionate impact on the geography of international shipping. For the time being, however, MSR does not appear to have substantially altered the main shipping routes between Asia and Europe**.** The main route is still from Suez towards the large ports in north-west Europe, with so-called vertical routes unravelling from the main artery still minimal. The importance of large ports and of large shipping companies are increasing. Still, the March 2021 blocking of the Suez Canal by the 20.000 TEU[9] *Ever Given* shook international trade for several days by causing high economic losses and significant supply problems.[10] The incident could lead to re-evaluations of global shipping routes, the cost-risk trade-off of ultra-large ships in the face of accidental or deliberate chokepoint blockades, and of land versus sea routes.

6 World trade in goods and services – an overview – Statistics Explained (europa.eu). In comparison, the average value of exports and imports for goods and services for Singapore represented 163.1 % of its GDP in 2018, for China 19.1 % and for the US 13.7 %.

7 Maritime transport of goods – quarterly data – Statistics Explained (europa.eu)

8 UNCTAD, *COVID-19 and Maritime Transport Impact and Responses*, 2021.

9 There are two common international standardized container types, twenty and forty feet long. A TEU or Twenty-foot Equivalent Unit is the unit used to measure cargo capacity for container ships and container terminals. See Figure 8. Evolution of container ships.

10 See e.g. The cost of the Suez Canal blockage – BBC News for an early discussion on the consequences.

Overall, the huge importance of trade routes through the North Sea is very likely to remain towards 2035, even if some of the characteristics and geographical patterns of global sea transport may change. The propensity for disturbances in an increasingly cluttered environment, however, is likely to grow.

2.2.2 Scales continue to increase

Economies of scale are the foundation of the containerized maritime transport model. Unit costs decrease when the ship's size increases. This trend is more important on longer routes, such as from China to Europe and vice versa. Therefore, European ports invest significant resources in their ability to accommodate large ships coming from Asia. The Port of Rotterdam has an advantage in this respect, with the Euro-Maasgeul allowing deep-water access. Typically, this makes Rotterdam the first and last port of call for large ships coming from and going to Asia that are not able to enter other ports fully loaded because of their draft.

Given these developments towards larger scales, combined with increasing environmental and societal pressures, we are witnessing a consolidation in both shipping companies and ports. More consolidation of port authorities will become inevitable in the coming years and decades. Land is a scarce commodity and competition for its use is high. Recent examples of such consolidation in the North Sea region are the announced merger of the ports of Antwerp and Zeebrugge and the recent creation of a cross-border 'fusion port' between Ghent, Vlissingen and Terneuzen. This coincides with a global consolidation in shipping companies. The three largest alliances in the global container shipping industry now account for about 80% of the global market. Furthermore, vertical integration is underway, with shipping companies also operating in terminals, logistics, and land transportation.

Such scale and scope enlargements affect security in two ways. When the need for increased risk mitigation measures is acknowledged, large(r) companies and conglomerates have more room for new investments in risk assessment, preparedness, and resilience measures.[11] The downside of consolidation is that the impact of incidents affecting single points of failure tends to increase. The blocking of the Suez Canal by the stranding of the *Ever Given* in March 2021, and the ceasing of all operations by shipping giant Maersk when it was struck by *NotPetya* ransomware in June 2017 serve as cases in point.

In the long run, the trend towards scale enlargement may be counterbalanced by end-to-end supply chain integration and strategic collaboration for smart and connected freight transportation, or re-shoring and near-shoring. Many companies are reducing the vulnerability of their long and often opaque supply chains to natural (pandemics, earthquakes, hurricanes) or geopolitical risk factors beyond their control. Smaller carbon footprints are another reason for scrutinizing transport routes and modalities. Mid-sized and smaller vessels may gain ground because their operational flexibility may become more important than the efficiency and lower slot costs of larger container ships.

2.2.3 Operations will further digitize and automate

Increasing size and cargo volumes, combined with the market pressure towards more efficiency, require ports and shipping companies to become more digital, sustainable and connected. This will further transform operations at sea and in ports. Digitization will increase efficiency in vessel route and arrival planning and loading/discharge productivity.

11 UNCTAD, *COVID-19 and Maritime Transport Impact and Responses*, 2021, p73-74.

Many of these changes are already underway. The construction of the sophisticated APM Terminals facility at the newly created Tweede Maasvlakte offers a glimpse of things to come, but fully automating existing operational sites located near port city centers will take much longer. In the longer run, we may reach a point where automation and real-time data handling between port players converge with the application of artificial intelligence and predictive forecasting using big data collated from devices throughout the port. The speed of development will depend on the willingness of all stakeholders to share sensitive data.

The Port of Rotterdam serves as a reference point in the field of technological innovation. With the help of IoT technology, Rotterdam's port has equipped itself with its own digital twin. This exact virtual copy of the port includes real-time data on all its infrastructure, ship and rail movements, weather conditions, and sea currents. The system will keep an eye on the assets' technical condition and conduct digital inspections. Furthermore, by 2030 it will be able to automatically guide ships, even unmanned ones, to their berths, reducing waiting times. The Port of Rotterdam Authority estimates that this platform can save operators up to $80,000 every time they dock. Another example is the use of a blockchain application that allows parties to track their containers at any point in the shipment, which becomes paper-free.

The International Maritime Organization (IMO) intends to begin incorporating autonomous vessels into its regulatory framework, with elaborate pilots already underway. The IMO distinguish between four main classes: (1) conventional ships with automated decision support systems, such as collision avoidance systems; (2) periodically autonomous ships, that is, autonomous functions are activated at night, on high seas, and in fair weather; (3) fully autonomous ships with facilities for crew to take ships into or out of ports; and (4) fully autonomous ships with no crew facilities on board. Classes (2) and (3) can be combined with remote operations of critical functions from a manned shore control center (SCC) on land. The technical feasibility of fully autonomous ships has been established, as have potential business models.[12] However, most experts believe that the arrival of commercial solutions at levels (3) and (4) will not happen in the timeframe up to 2035. Technology is not the limiting factor. Instead, regulation, acceptance, and operational risks of cyberattacks are the main hurdles. Multiple successful proofs of concept have shown remotely operated vessels to be an important step towards partial or full autonomy.

Remote operation is relevant in relation to cybersecurity. With the digitization of operations at sea and in the seaports, maritime security risks and issues also become more digital. Risk and threats against activities and infrastructure at sea will increasingly have a substantial cyber component or may even become predominantly geared towards virtual targets.

2.2.4 Opening up of the Northern route affects sea trade niches

The receding Arctic Sea ice may slowly turn the centuries-old idea of the northern passage into an economically viable reality. The Northern Sea Route (NSR) makes the route from Rotterdam to Yokohama up to 37% shorter compared to the Suez Canal route. In August 2018, the first commercial container vessel navigated the NSR, partly with the help of icebreakers. But, as the Dutch Polar Strategy concludes, "[h]ow soon this route becomes permanently navigable and commercially viable depends on many factors and is difficult to predict." [13] There are several challenges. First, the just-in-time principle of global supply chains is at odds with the unpredictability of the Northeast Passage, with extreme and highly unpredictable weather and ice conditions. Second, the Suez Canal allows for the passage of bigger

12 Z.H. Munim, *Autonomous ships: a review, innovative applications and future maritime business models*, 2019.

13 Ministry of Foreign Affairs, *The Netherlands' Polar Strategy 2021-2025. Prepared for Change*, March 2021, p32.

ships than the coastal part of the NSR due to its shallowness. The optimal route for bigger ships, the Transpolar Sea Route, lies further to the north, but it is unknown whether this route will ever be navigable. Scientists estimate that it will at any rate be well after 2050, and only in summer. The third challenge is the lack of intermediate ports. Container ships rarely sail from one port to another; the Suez Canal route from Rotterdam to the Far East passes many large ports on the way, where cargo can be dropped off and picked up and where maintenance and support is possible. Fourth, ships need to be made Arctic-ready, in terms of equipment and crew. Currently, Russian icebreakers and Russian pilots are for hire to navigate ships through the NSR, incurring additional costs for shipping companies. The economic feasibility thus depends on NSR navigation time, Russian fees, and fuel prices.[14]

Nevertheless, several countries, including Russia, China and Iceland, are investing in new ships, icebreakers, and ports to facilitate a growing use of the NSR. Russia is investing heavily in infrastructure, nuclear-powered icebreakers, and the modernization of ports. The Netherlands Bureau for Economic Policy Analysis (CPB) forecasts that if the NSR becomes commercially viable in the longer term, two-thirds of goods now transported via the Suez Canal will instead travel via this route. This would increase trade flows between Northwestern Europe and northeast Asia by approximately 10%.[15] The Netherlands Institute for Transport Policy Analysis expects that the NSR may eventually become an alternative route for high-quality, time-sensitive products.[16]

In conclusion, the opening of the northern passage will slowly take shape, for the foreseeable future mostly servicing only specific product groups. It is unlikely to become a major game changer towards 2035, while projections after that period remain uncertain. The NSR has historically been seen by Russia as an internal waterway and in a practical sense could be considered as one for at least the next decade.

2.3 Security in an era of major power rivalry

More sizable and diverse value-creating activities and associated infrastructures in the North Sea generate vulnerabilities that may be exploited by malicious actors. With the North Sea becoming a more integral part of economic, societal and environmental processes, the potential impact of security incidents also mounts. This must be gauged against the background of developments in the security environment. In the following pages, we highlight three: the increased geopolitical rivalry between major powers, possibly leading to hot conflicts; more power and influence for non-state actors (NSAs); and pursuing strategic objectives through hybrid actions in the 'gray zone'.

2.3.1 Major power conflict

The global geopolitical and security environment is evolving rapidly. Over the past two decades, we have witnessed the return of geopolitical competition between major powers. This rivalry is eroding the post-World War II multilateral order that has been a pillar of Dutch security and prosperity. At the same time, the role of non-state actors in the international system is growing, for better and for worse. Armed groups, insurgents, terrorist organizations,

14 Liu and Kronbak, *The Potential Economic Viability of Using the Northern Sea Route (NSR) as an Alternative Route between Asia and Europe*, 2010.

15 CPB, *Melting Ice Caps and the Economic Impact of Opening the Northern Sea Route*, 2015.

16 Kennisinstituut voor Mobiliteitsbeleid, *Trends en de Nederlandse zeevaart*, 2020.

and criminal networks can instigate large-scale violence and threaten order and stability, either independently or in cooperation with state actors (as proxies). Conversely, non-governmental organizations, international corporations, and philanthropic institutions can promote resilience and stability in societies. Other non-state actors, such as social media platforms, play a dual role, fostering cohesion in society but also generating fragmentation and protest.

After the '9/11' terrorist attacks on New York and Washington DC in 2001, US-led Western political and military strategy focused on counter terrorism, counter insurgency, and stabilization operations in fragile states. But over the course of the last decade, attention has shifted to interstate strategic competition. With states vying for political and economic influence, hopes of integrating revisionist powers into the international order have been fading. China's global rise, Russia's resurgence, Iran's destabilizing activities in the Middle East, North Korea's nuclear weapons testing, and the America First strategy under US President Donald Trump have unsettled an already shaky international order. Over the course of the 2010s, these changes have transformed a relatively uncontested status quo into a multipolar order. States have increased their military expenditures, stepped up efforts to modernize their armed forces, and strengthened their capabilities to fight conventional wars. Great power conflict is not imminent, but it is more likely. In concrete terms, tensions between China and the US in the Indo-Pacific region and between Russia and NATO over Eastern-Europe and the Middle East could escalate. Flow security is a crucial notion in the context of this study.

From a military perspective, an assertive Russia signifies the most immediate concern for Europe. The probability of relations between Russia and NATO crossing the threshold to a direct military conflict is currently low. Although military planners contemplate scenarios in which Russia intentionally initiates a conflict, these are extreme cases. More likely are the risks of an inadvertent outbreak of conflict. As each side harbors fears about the other side's intentions, misreading or misjudging the other side's behavior during a crisis are a real possibility. How would war with Russia affect the North Sea? While the force balance between NATO and Russia makes it impossible for Russia to establish control over the North Sea, it could hamper the use of the North Sea by others. (The threat of) sea mines or the sinking of a few ships could bring sea trade to a standstill. The cutting of a few seabed cables could gravely obstruct overseas internet traffic. And military maneuvers at sea, for instance the transfer of military reinforcements from North America to the European theatre, could be hindered by concealed sabotage actions (during a build-up to a 'hot' conflict) or outright attacks, for example with long-range, high-precision missiles or submarines (in a war situation).

China is a different matter. As one Asia-based analyst argues, "The big strategic game in Asia isn't military but economic."[17] Although Chinese warships have regularly taken part in Russian naval exercises in the Mediterranean and the Baltic Sea, a military confrontation with China in the seas around Europe is highly unlikely in the period up to 2035. Even so, if Europe becomes involved in an armed confrontation between China and the US in the Indo-Pacific, the repercussions could be severe. The massive amount of trade between China and Europe, much of which is channeled through the North Sea, could be decimated; and retaliatory cyberattacks may severely impede critical processes in the Netherlands.

In any conflict that involves NATO or the EU, or even individual Member States, repercussions in cyberspace must be considered. Cyberattacks by state actors or proxies could affect large parts of the European economy and European society. As infrastructures and processes at sea increasingly become vital to the Dutch economy and society, they too should be (cyber)secured.

17 Kishore Mahbubani, *Why Attempts to Build a New Anti-China Alliance Will Fail*, Foreign Policy, 27 January 2021.

2.3.2 The power and influence of non-state actors

Non-state actors (NSAs) have strengthened their position vis-à-vis state actors. In broad terms, NSAs come in two kinds. NSAs such as non-governmental organizations, multinational corporations, philanthropists and grassroots movements organized primarily via social media are "increasingly assuming functions traditionally executed by states".[18] These groups and organizations have objectives that tend to overlap with societal development goals and often play a constructive role in societies and in multilateral arrangements. In many cases – though not all – states willingly partner with these NSAs in pursuit of their interests and values. Pernicious NSAs, such as terrorist or organized crime groups, pursue agendas that are at odds with and undermine the societal or international order. Organizations like Hamas or Hezbollah, assume state-like functions *and* act as criminals and terrorists.

In the context of this study, both kinds of NSA are important. Criminal and terrorist groups pose a threat to secure operations on the North Sea. Looking toward the future, two trends are important to consider when assessing this threat. First, more diverse value-creating activities on the North Sea translate into more opportunities for criminals and terrorists. Second, in hybrid confrontations (see §2.3.3), we discern a tendency for state actors to empower malicious NSAs.

As many of the value-creating activities involve private actors, NSAs are also important in the governance of the North Sea. Currently, the allocation of security tasks and responsibilities amongst public and private stakeholders is not always clear or covered (see §2.4). With the growth in size and diversity of activities in the North Sea towards 2035 and beyond, this is an important issue.

2.3.3 Hybrid threats and operations in the gray zone

While investments in conventional forces may effectively signal states' readiness to engage in military confrontation (see §2.3.1), actual action is likely to occur at the lower end of the force spectrum. For a variety of reasons, interstate competition has been pushed into the gray zone between peace and overt war. To remain below the threshold of an armed attack, states are employing a mixture of clandestine, covert, and ambiguous military and non-military activities to attain their political objectives. Through these hybrid activities states seek to coerce, hamper, slow, drain, disrupt, or overthrow the adversary without engaging in open hostilities. States act and respond below major response thresholds, often using proxies to carry out hostile activities on their behalf, as already indicated in §2.3.2.

In the new security environment, threats and conflicts have come closer to home. With borders disappearing or taking different forms in the digital world, the Netherlands, with its open economy and society, has in many ways become a front-line state. Although still isolated, there have been cases of cyberattacks against critical processes in Dutch society,[19] and attempts to influence the public debate by foreign powers.[20] Given the interconnectedness of domestic and international security, the Netherlands must consider not only conflicts far

18 HCSS and Clingendael, *Strategic Monitor 2020-2021. Geopolitical Genesis. Dutch Foreign and Security Policy in a Post-COVID World*, 2021.

19 The *Cybersecuritybeeld 2021* notes (p9): "In the past year, vital processes in the electricity, water, oil & gas, chemical, food, transport and healthcare sectors have again been targeted worldwide by digital attacks by criminal groups", "[a]lthough targeted attacks on vital processes have not yet been observed in the Netherlands". Translated with www.DeepL.com/Translator (free version)

20 With the Russian manipulation surrounding the MH17 dossier as a prime example.

away, but also – and perhaps primarily – the security and resilience of its own society and territory against a range of risks and threats.

The European Centre of Excellence for Countering Hybrid Threats concludes that "Threats in the maritime domain tend to be progressively hybrid in nature".[21] Many of the ten maritime hybrid scenarios the Centre of Excellence has explored pertain to a maritime terrain that lies between the opposing parties. In the case of the North Sea, this is an unlikely situation. Nevertheless, some of the scenarios considered are also relevant to the North Sea. These include protection of an underwater gas pipeline, cyberattacks against shipping, clandestine use of underwater weapons, and non-state actors.

2.4 Governance of the North Sea is more crucial than ever

The North Sea has many users and stakeholders. The coastal states – Norway, the UK, Denmark, Germany, the Netherlands, Belgium, and France – all have their specific demands and needs for the area. Furthermore, many of the activities in the North Sea involve private actors or public-private partnerships. With critical offshore processes mounting, the question of governance over the North Sea is crucial, not least when it comes to security issues. With offshore infrastructure for a substantial part in private hands, the government will need to work closely with industry to guarantee protection against natural, accidental, and deliberate disturbances.

2.4.1 Territorial rights and jurisdiction

The foundation for the governance of the seas, the United Nations Convention on the Law of the Sea (UNCLOS), was adopted in 1982. UNCLOS encompasses the legal framework for marine and maritime activities. It has been ratified by 167 states, with three additional states – Egypt, Sudan, and the US – having signed but not ratified the agreement.

21 European CoE for Countering Hybrid Threats, *Handbook on Maritime Hybrid Threats — 10 Scenarios and Legal Scans*, 2019.

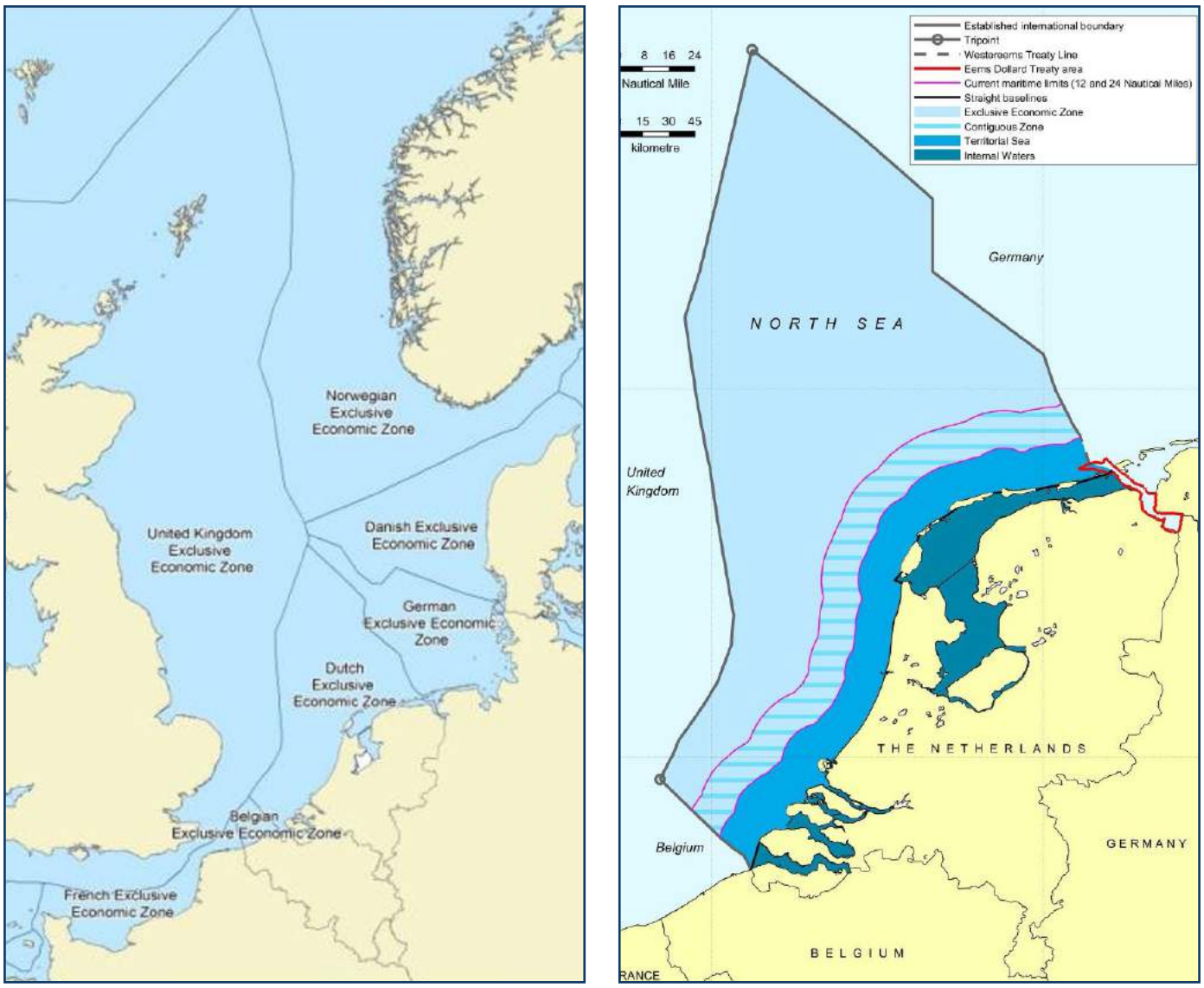


Figure 5. EEZs in the North Sea (left) and maritime zones in the Dutch part of the North Sea (right)

UNCLOS distinguishes between sea inside and outside the jurisdiction of coastal states. For the North Sea, the following maritime zones are important: the territorial sea, the contiguous zone and the exclusive economic zone.[22] The **baseline** is "the low-water line along the coast as marked on large-scale charts officially recognized by the coastal State" (UNCLOS, article 5). The area from the baseline to 12nm[23] out constitutes the **territorial sea**. Within this area, all Dutch laws are in force. The area up to 1km from the baseline is municipally divided. In this zone, in addition to the national government, the provinces and municipalities located on the coast have certain powers. Outside the 1km zone, only the national government has responsibilities.

The **contiguous zone** lies between 12-24nm from the baseline. In this zone, supervision can be exercised in compliance with rules on customs, taxes, immigration or public health that are in force within the Dutch territory or territorial sea. In addition, the Netherlands can also exercise certain powers in this zone regarding archaeological and historical artifacts.

22 The following is based upon Juridische Grenzen en Zones op de Noordzee – Noordzeeloket UK.

23 A sea mile or nautical mile (nm) is equivalent to 1852m.

The **Exclusive Economic Zone (EEZ)** extends from 12nm to a maximum of 200nm from the baseline. Where EEZs overlap, an imaginary boundary is drawn, as is the case in the North Sea. The boundaries of the Dutch EEZ were set out in a treaty with Belgium, Germany, and the United Kingdom in 1958. The Dutch EEZ also includes the Dutch part of the continental shelf under the North Sea (the seabed and subsoil). Outside the 12-mile zone, only the laws and regulations apply that were declared in force for the area. The Netherlands, in accordance with UNCLOS, exercises certain sovereign rights in the EEZ. First, this includes the exploration, exploitation, conservation, and management of the living and non-living natural resources of the waters above the seabed and on and below the seabed. Second, it also encompasses other forms of economic exploitation and exploration, such as the generation of energy from the water, currents and winds. Finally, the Netherlands claims jurisdiction with respect to the construction and use of artificial islands, installations and facilities, marine scientific research and the protection and preservation of the marine environment. The Water Act, the Mining Act, and the Earth Removal Act apply in the Dutch EEZ. The Flora and Fauna Act and the Nature Conservation Act will eventually also enter into force within the EEZ.

For ships sailing in Dutch waters, a shared jurisdiction applies, which includes the jurisdiction of the flag state. Within the 12-mile zone, in most cases Dutch law prevails. Outside the 12-mile zone, the Netherlands only has jurisdiction on specifically designated grounds (the EEZ regime).

2.4.2 EU regulation and international treaties

EU maritime legislation is mainly focused on the quality of the water and the marine environment, on the preservation of ecological values, and on the regulation of fisheries. The fisheries policies of the European Member States are determined almost entirely at the European level.[24] For environmental protection, the European Marine Strategy Framework Directive (MSFD) is important. Its aim is to protect and restore the European seas and oceans and promote sustainable usage. Member States must take the necessary measures in their waters to protect, preserve, and restore the marine environment and guarantee the sustainable use of the North Sea. To do this, they must work together as EU Member States as well as with other countries in their marine region.

Usage of the North Sea is not restricted by the territorial borders within the North Sea, nor by the extent of the North Sea as a whole. Therefore, the MSFD obliges the EU Member States to take a regional approach, with an explicit coordinating role for the existing regional marine conventions, such as OSPAR. The OSPAR Commission consists of 15 countries in the North-East Atlantic area and the EU, focuses on marine spatial management, and is mostly concerned with environmental issues. The Netherlands is also a member of the International Maritime Organization (IMO). IMO is a specialized agency of the United Nations with 174 member states. In the IMO, worldwide agreements are made with respect to safety, efficiency, and environmental measures related to shipping.

On a practical level, cooperation between states is more important than international treaties or EU legislation. For instance, decisions on wind farms and access to ports are usually taken by the states involved. However, with increasing spatial pressure and competing interests at play in the North Sea, the need for and influence of EU legislation superseding current national legislation may grow.

24 European legislation North Sea – Noordzeeloket UK

2.4.3 Maritime security

The North Sea is fully covered by EEZs. As no single nation has the sovereignty or capacity to effectively deal with transnational threats to maritime security, the North Sea states share a common interest in joint approaches to maritime security. Furthermore, a range of private or public-private actors operate in the North Sea, several of whom provide important functions for the North Sea states. The alignment of security responsibilities and tasks at the international, national, and corporate level is essential.

What kind of security responsibilities and tasks are we considering here? The UN acknowledges no settled definition of maritime security, but defines the concept in terms of threats and illicit activities that pose a risk to peace and order.[25] The U.S. Navy defines maritime security as "tasks and operations conducted to protect U.S. sovereignty and maritime resources, support free and open seaborne commerce, and to counter maritime-related terrorism, weapons proliferation, transnational crime, piracy, environmental destruction, and illegal seaborne immigration."[26] This definition lacks explicit reference to the protection of critical infrastructure at sea, which in this study is highlighted as an essential complementary element in maritime security of the North Sea.

Figure 6. Intertwining components of safety and security risk management

Furthermore, the management of security risks is much broader than incident response. Figure 6 portrays four components of safety and security risk management. Although these components are often represented as a chain, and thus a series system, they more closely resemble a parallel system. In such a system, the idea of a chain being as weak as its weakest link is a false one. Trade-offs can be made between investments in the various components, and weaknesses in one component may be compensated for by strengths in other components.

International level

As a result of Brexit, the border between the Dutch and British EEZ is now an EU external border. This means that the tasks and responsibilities of Frontex, the European Border and Coast Guard Agency, have direct bearing upon the Netherlands' part of the North Sea. Frontex promotes, coordinates, and develops European border management in line with the EU concept of Integrated Border Management. It focuses on preventing smuggling, human trafficking, and terrorism as well as many other cross-border crimes. Frontex analyses data and identifies trends and patterns related to the situation at and beyond the EU's external borders. It monitors the situation at the borders and shares intelligence with relevant national authorities and Europol. The agency also carries out vulnerability assessments to evaluate the capacity and readiness of each Member State to face challenges at its external borders and coordinates and organizes joint operations and rapid border interventions to assist Member States. The agency deploys European Border and Coast Guard teams, including a pool of at least 1,500 border guards and other relevant staff to be deployed in rapid interventions. The members of the rapid reaction pool must be provided by Member States upon request by the agency. Frontex also deploys vessels, aircraft, vehicles, and other technical equipment provided by Member States in its operations. Frontex supports the cooperation between law enforcement authorities, EU agencies and customs at sea borders. Finally, the agency is also a center of expertise for border control. It develops training curricula and specialized courses in a variety of areas to guarantee the highest levels of professional knowledge among border guards across Europe.

Many of the security threats facing the North Sea are transnational in nature, while many effective security solutions require international cooperation. Therefore, the role of Frontex – in present practice focused on the Mediterranean – is likely to expand in the North Sea,

25 Natalie Klein (ed), *Maritime security and the law of the sea*, 2012.

26 US Government, *Naval Operations Concept 2010*, 2010, p35.

leveraging the cloud and operational power of the NLCG. Frontex can, for instance, provide input for legal frameworks at the EU level; harmonize security-related classifications, reports and notifications in all European seas; facilitate and stimulate information exchange between European Coast Guards; act as a knowledge and training center; arrange handovers between countries in monitoring shipping and transnational infrastructure; facilitate and stimulate information exchange between European Coast Guards; act as a knowledge and training center; initiate personnel exchange and equipment cooperation; promote operational cooperation; and make its own resources available for use in the North Sea.

National level

The overarching governing body is the Interdepartmental Directors North Sea Consultative Body (IDON). IDON brings together several ministries and the executive organizations *Rijkswaterstaat* and the Netherlands Coast Guard. IDON's coordinating role is intended to ensure that policy making and execution by the various ministries proceeds based upon a shared vision of the condition, use, and further development of the North Sea area. However, IDON has no power to enforce cross-sectoral alignment, and comprehensive plans linking various types of activities in the North Sea are largely non-binding. In practice, management of the North Sea is executed within the sectoral stovepipes of the ministries involved.

Furthermore, where safety *is* a concern, security is barely addressed in North Sea plans and policy. The *Incident Response Plan North Sea* (IRP-NS) determines the organization and coordination of incident responses in the North Sea, based upon the statutory and regulatory tasks and responsibilities of the various government parties involved. The types of incident (scenarios) discussed in the IRP-NS are related to safety incidents and infringements of legislation. They hardly cover security risks with malicious actors threatening vital national interests. In the wider context of critical infrastructure protection (CIP), a range of so-called critical processes notionally have an offshore component, see Table 5. In practice, however, threats to offshore critical processes are largely neglected. Very few of the scenario or training exercises pertaining to CIP have a bearing on North Sea infrastructure. The *2019 National Risk Assessment* only refers to the 'sea' in conjunction with possible flooding.

Critical processes	Cat.	Critical processes	Cat.
National transport and distribution of electricity	A	Large-scale production/processing and/or storage of chemicals and petrochemicals	B
Regional distribution of electricity	B	Storage, production and processing of nuclear materials	A
Gas production, national transport and distribution	A	Retail transactions	B
Regional distribution of gas	B	Consumer financial transactions	B
Oil supply	A	High-value transactions between banks	B
Internet and data services	B	Securities trading	B
Internet access and data traffic	B	Communication with and between emergency services	B
Voice services and text messaging	B	Police deployment	B
Geolocation and time information by GPS	B	Personal and organizational record databases	B
Drinking water supply	A	Interconnectivity between record databases	B
Flood defenses and water management	A	Electronic messaging and information disclosure to citizens	B
Air traffic control	B	Identification of citizens and organizations	B
Vessel traffic service	B	Military deployment	B

Table 5. Critical processes in the Netherlands.[27] Critical processes with a clear offshore component are indicated in blue

27 Critical processes are processes that could result in severe social disruption in the event of their failure or disruption. The failure of category A critical processes has greater potential effects than the failure of category B critical processes. See Critical Infrastructure (protection) | National Coordinator for Security and Counterterrorism (nctv.nl)

The upsurge of critical processes in the North Sea requires much more attention to the security and protection of these processes and underlying infrastructure. Furthermore, security challenges are becoming more complex. This includes the blending of crime and terrorism, state actors employing non-state proxies, and cyber as well as physical attacks. To address this trend, security responses should also be more comprehensive: they should be both cross-sectoral and encompass the components portrayed in Figure 6. Further note that national authority is restricted to the territorial sea. National security and critical infrastructure protecting have very little bearing outside the territorial sea. As more critical processes move out further to sea, this is a crucial dilemma – flagged repeatedly throughout this document – that needs much more attention and scrutiny than is currently the case.

Coast Guard and Navy

Only the NLCG has a cross-sectoral role providing services, enforcement, and coordination across multiple policy areas pertaining to the North Sea.[28] The NLCG's three main goals are: (1) A responsible use of the North Sea; (2) to provide services that contribute to safety and security at sea; and (3) Upholding (inter)national laws and duties.

The NLCG is an interdepartmental network organization that brings together all kinds of government bodies and services. Six ministries are jointly responsible for the adequate functioning of the NLCG, namely the ministries of Infrastructure and Water Management; Justice and Security; Finance; Economic Affairs and Climate Policy; Agriculture, Nature and Food Quality; and Defense. Infrastructure and Water Management is the coordinating ministry for the NLCG; Justice and Security is the coordinating ministry for law enforcement within the NLCG; and Defense (in effect, the RNLN) is the responsible ministry for the business management of the NLCG.

The RNLN tasks applicable to the North Sea partly overlap with the NLCG's tasks, and are indeed sometimes executed within the Coast Guard construct:

1. protect and defend Dutch territory;
2. facilitate the Coast Guard;
3. combat terrorism on and under water;
4. clear unexploded explosives at sea and in port areas;
5. provide diving expertise and diving medical assistance;
6. perform hydrographic measurements for the creation of sea charts; and
7. support the civil authorities in, among other things, natural disaster management and search & rescue.

Next to the RNLN, the following services work together in the execution of the tasks of the NLCG: Directorate-General Rijkswaterstaat, Human Environment and Transport Inspectorate, Royal Netherlands Marechaussee, Police, Customs, Fiscal Intelligence and Investigation Service, the Dutch State Supervision of Mines, and The Netherlands Food and Consumer Product Safety Authority. Each service conducts its own task. The NLCG is not overall responsible for the conducted activities, it is the coordinating body. The services themselves are responsible for their own activities, even if these activities are conducted under auspices of the NLCG.

The NLCG's service task includes nautical management and emergency response. The Coast Guard Centre functions as a 24/7 Communication and Coordination Centre for incidents at sea and all NLCG operations. The enforcement task includes general enforcement, enforcement of environmental legislation, traffic safety, and fisheries. An increasingly important

28 See Regeling organisatie Kustwacht Nederland.

element of the NLCG's coordinating task is to build and share a comprehensive 'maritime situational picture'. Such maritime situation awareness (MSA) is the core product of the Maritime Information Hub (*Maritiem Informatie Knooppunt* or MIK), located in the Coast Guard Centre. Better MSA allows for more effective and efficient tasking of the NLCG's assets. It also underpins better risk management. The MIK currently has only limited capacity to anticipate future risks by developing, among other things, trend analyses and risk profiling. As intensified competing static and dynamic usages of the North Sea create more, and more complex, risks, the need for more analytical and foresight capacity in the MIK is rapidly increasing.

Coast Guard's assets

Because of is its networked nature, it is somewhat complicated to exactly gauge the size of the NLCG in terms of personnel, materiel, and budget. The NLCG itself has some 90 people employed (administered by the ministry of Defense). In addition, some 60 people from the network partners work directly for the NLCG, e.g. as operational team members or as analysts in the MIK. The NLCG has no platforms of its own but has four vessels from the governmental shipping company permanently assigned**,** three patrol vessels and one Emergency Towing Vessel.[29] These vessels can also be used for security tasks, but neither personnel nor platforms carry weapons. The largest auxiliary force in case of violent security incidents is supplied by the RNLN. The NLCG can permanently call upon a mine clearing vessel and, if necessary, all other available ships of the RNLN, including frigates. Two NLCG aircrafts are managed by the Royal Air Force. Two police surveillance helicopters are available for regular patrol flights and Defense helicopters can be called upon when needed.

Table 6 exhibits the NLCG's exploitation budget over time. The NLCG's 'own' budget is remarkably constant. However, the costs associated with the deployment of partner assets in the context of NLCG tasks has grown significantly over a period ten years. The rise in costs in 2020 and 2021 is caused by a substantial additional contribution of the ministry of Infrastructure and Water Management for risk mitigation measures associated with the rollout of offshore wind energy, including new staff positions and the hiring of an ETV for the Borssele wind farm.

	2011	2016	2019	2020	2021
Expenses[30]	23.897	25.506	27.181	26.821	26.634
Costs[31]	7.941	23.258	24.543	29.436	38.058
Total exploitation	31.838	48.764	51.724	56.257	64.692

Table 6. Exploitation budget of the NLCG

The budget of the NLCG – spend on a host of tasks, with security tasks being only a minor part of the whole package – is approximately 1% of the yearly budget for the Dutch police organisation; while the territorial sea and adjacent EEZ constitute a sea area of some 65,000 km², more than 1.5 times the land area of the Netherlands. Even though the comparison is seriously flawed, it does give a flavour of how few assets are available for security in this vast stretch of sea area that, increasingly, constitutes a vital part of our economy and well-being.

29 A tender has been issued for the lease of two additional ships in addition to the current ETS Guardian.

30 Expenses refers to the expenditure budget managed by the Coast Guard, included in the budget of the ministry of Defense.

31 Costs refers to operating expenses included in the budgets of the contributing ministries, linked to the deployment of people and resources falling under that ministry, such as the deployment of the customs (Finance), police (Justice and Security), air surveillance (Infrastructure and Water Management), and Marechaussee (Defense).

Private companies

Private companies have a big stake in offshore vital processes. Wind farm operators are responsible for the connection to the national grid. Within the framework of the *Energy Agreement*, it has been agreed that a grid will be created at sea wherever this is more efficient than connecting wind farms directly to the national high-voltage grid. The national grid operator TenneT has been assigned responsibility for this. This puts the grid in public hands.[32]

Pipelines and communication cables are owned by private actors. While telecom cables usually rest upon the sea floor, power cables are buried below the seabed for protection against accidental damage, for example by ship's anchors, fishing nets, or dropped objects. Specific protection against deliberate damage (or tapping in the case of communication cables) is minimal. One common protective measure is that the precise locations of pipelines and cables are not made public. Due to the relatively high costs of subsea cables and pipelines, redundancy tends to be much lower than for onshore connectors.

Of increasing concern are cyberattacks on critical infrastructure. Although energy companies are aware of the risks, "security remains largely optional and the recent downturn in profits in the petrochemical industry led to large budget cuts, and security was no stranger to the budget cuts. What does not get cut is budgets to fulfil regulatory requirements."[33] The EU Directive on security of network and information systems (*NIS Directive*), which was adopted in August 2019, with Member States having 21 months to transpose into their national law, goes some way to ensure oil and gas operators in the EU implement cybersecurity mitigation measures. This NIS Directive is currently being updated, with the NIS 2.0 setting higher standards and more stringent rules.

32 Policy Document on the North Sea 2016-2021, p38.

33 Fighting cybercrime in the offshore oil and gas industry (offshore-technology.com)

3 The Evolving Value of the North Sea: Present, Future and Beyond

This chapter examines the developments that will increase the economic, environmental, societal and (therefore) political value of the North Sea – with a focus on the Dutch part – towards 2035 and beyond. First, we discuss the main agreements that are leading to a transition in usage of the North Sea. Second, we detail the current use of the North Sea in various usage categories. This provides a baseline for future developments. Third, using the same categorization, we map the anticipated usage of the North Sea in 2035, gauging the likeliness of potential changes. Fourth, we take a leap to 2050, drawing a sketch of what the North Sea might look like then. We do so by highlighting tendencies that, based on today's policy decisions, may become dominant towards 2050. Finally, we highlight the most important vulnerabilities that accompany the increase of value-creating activities in the North Sea.

3.1 Agreements that guide the North Sea transition

Two policy documents guide the major changes that are reshaping use of the Dutch part of the North Sea. The National Climate Agreement (2019) states that greenhouse gas emissions, compared to 1990 levels, must decrease by 49% in 2030 and by 95% in 2050 to reach the reduction targets for the Netherlands prescribed by the Paris Agreement. The North Sea Agreement (2020) sets out how a wide range of stakeholders plan to realize the energy transition in line with The National Climate Agreement. In addition, a nature transition and a sustainable food transition are necessary to ensure a healthy maritime environment in the North Sea. With the energy transition as the most prominent, these three transitions in parallel will transform the use of the North Sea towards 2035 and 2050.

The North Sea Agreement was brokered by a broad spectrum of parties participating in The North Sea Consultation (*Noordzeeoverleg*), including the ministry of Infrastructure and Water Management (the consultation coordinator), the ministry of Agriculture, Nature and Food Quality, the ministry of Economic Affairs and Climate, representatives from the energy sector, the main ports, environmental NGOs and fishermen. The North Sea Consultation is "focused on reaching consensus between national government and stakeholders" and remains the leading policy-making group for North Sea spatial planning for the foreseeable future. The participating government ministries are expected to run key decisions by the North Sea

Consultation prior to presenting them to the legislature.[34] As a result, current and future agreements reached by the North Sea Consultation are somewhere between legally binding and open-ended.

The North Sea Agreement serves as the foundation on which plans such as the upcoming *North Sea 2030 Agenda*, *the North Sea Program 2022-2027*, *the Roadmap for Offshore Wind Energy 2030,* and additional policy documents are based (see Table 7).[35] Measures introduced for shaping the energy transition – such as the introduction of Carbon Capture and Storage (CCS), hydrogen production, and more – are specified in the *North Sea Energy Outlook*. The North Sea Agreement is hence the linchpin for many other relevant policy documents. In short, the North Sea Agreement and the North Sea Consultation format will, to a large extent, determine the spatial design of the Dutch part of the North Sea towards 2035 and beyond.

Policies affecting the use of the North Sea also originate in Brussels. The European Commission has proposed a revision to the original European Green Deal completed in late 2019 that calls for a more ambitious greenhouse gas emissions reduction – moving from a 40% to 55% reduction target by 2030, compared to 1990 levels. The Dutch government supports the EU's more ambitious proposal.[36] The study-Group Climate Challenge Green Deal (*Commissie Van Geest*) outlines what additional actions the Netherlands should take to meet the revised 2030 target of 55% and how to achieve carbon neutrality thereafter[37].

Policy Document	Participating Parties	Date	Importance
North Sea Agreement	Multiple ministries, the energy sector, port representatives, environmental NGOs, (a slim majority) of fishermen	June 2020	Leading
National Climate Agreement	The Dutch government in consultation with 100 parties	June 2019	Leading
European Green Deal	Presented by the EU Commission	2019; under revision	Leading
Roadmap for Offshore Wind Energy 2030	The Dutch government	March 2018	Specific
North Sea Program 2022-2027	The Dutch government (as part of the National Water Plan)	March 2021	Specific
The Study-Group Climate Challenge Green Deal	*Commissie Van Geest*	January 2021	Specific
North Sea Energy Outlook	EBN, Gasunie, TenneT, Netherlands Organization for Applied Scientific Research TNO, Netherlands Environmental Assessment Agency PBL, Top Sector Energy and the DG for Public Works and Water Management	September 2020	Specific

Table 7. Published policy documents for the North Sea

34 North Sea Agreement, pp34-35.

35 North Sea Agreement, p5.

36 Dutch Goals within the EU; National Climate Agreement, p6.

37 Bestemming Parijs: Wegwijzer voor klimaatkeuzes 2030, 2050, pp10,11,46.

3.2 Today's Value Creation in the North Sea

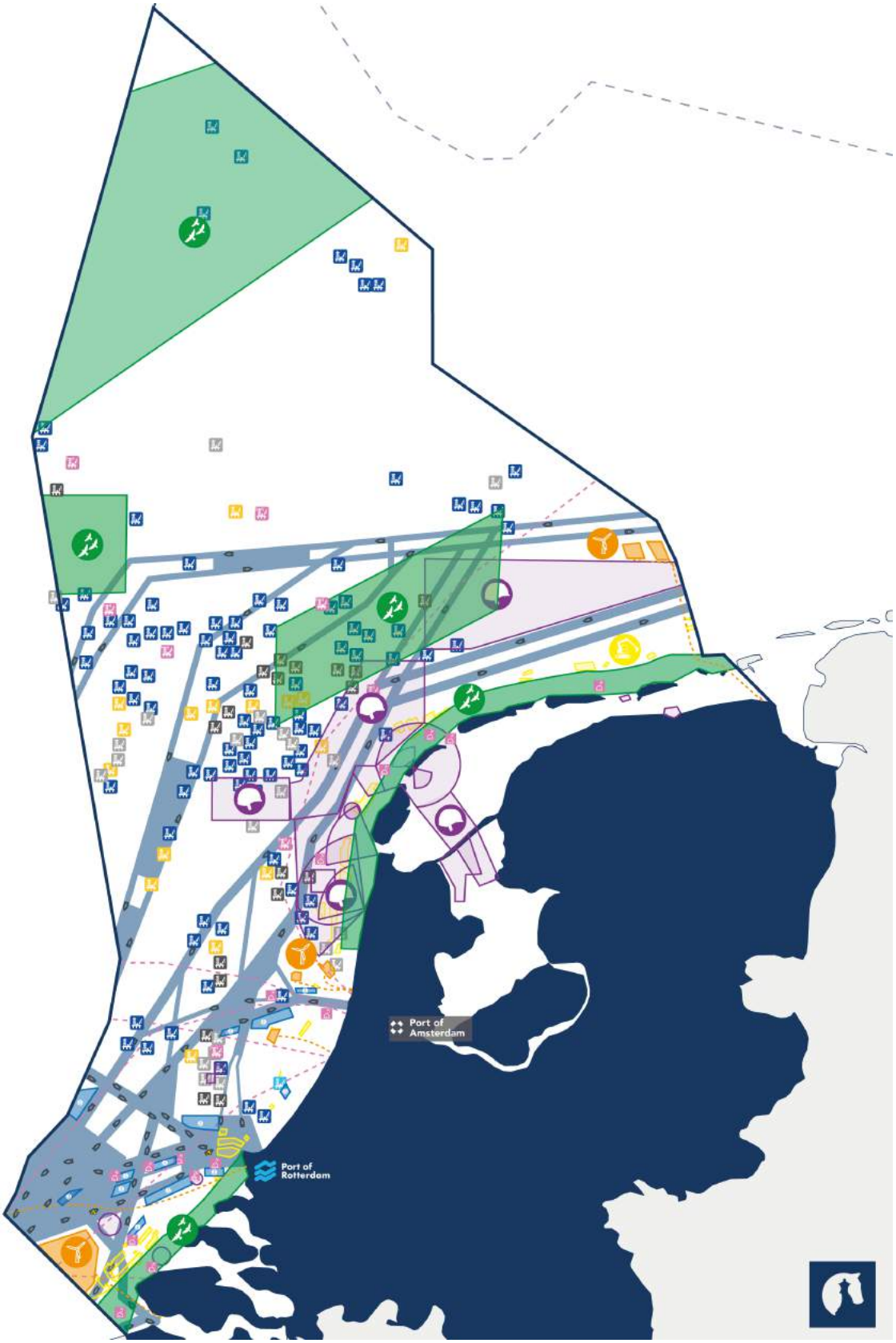


Figure 7. Many competing users and usages of the North Sea today (legend in Annex B)

3.2.1 Trade and transport

Trade and transport in the North Sea is a vital lifeline for the economy of not only Northwestern Europe, but the EU as a whole. Approximately half of EU trade goes by sea. Its three biggest cargo ports, Rotterdam, Antwerp and Hamburg, thoroughly depend on the North Sea.[38] The North Sea is especially important to the Netherlands. Some 240,000 ship movements cross the Dutch section of the North Sea each year, of which some 75,000 are directly linked to Dutch ports.[39] The latter amounted to a total value of €378 billion and €215 billion in 2019 for imported and exported goods, respectively.[40] In 2019, Dutch ports generated an added value of more than €8.6 billion, of which €2.2 billion was indirect added value.[41] Maintaining sufficient space for shipping lanes has therefore been defined as an issue of national interest in the most recent (2020) *Nationale Omgevingsvisie*.[42]

Space designated for shipping lanes and waterways currently takes up a substantial portion of the North Sea. The shipping routes themselves comprise 3,600km^2, or around 6% of the entire Dutch continental shelf.[43] Main waterways have an additional 500m exclusion zone in which other activities, such as the construction of platforms and wind farms, are prohibited.[44] The complete shipping system, with anchorage sites and ports included, covers 17% of the Dutch continental shelf.[45]

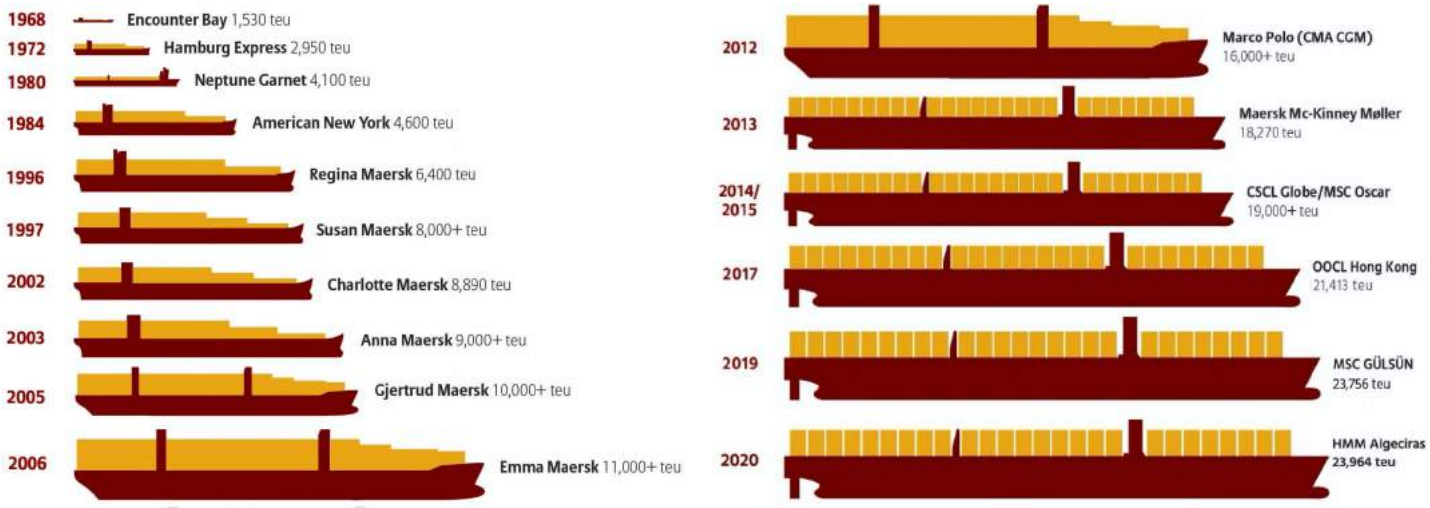


Figure 8. Evolution of container ships

Trade and transport in the North Sea is growing both in number of ships and in ship size. An analysis of the Port of Rotterdam shows that, in 2019, as compared to 2015, an extra 300 seagoing vessels docked, and an extra 1 million containers were transported annually.[46] Furthermore, shipping capacity and size has also grown globally year on year for at least the

38 Half of EU Trade in Goods Is Carried by Sea Rotterdam, Antwerp and Hamburg Busiest Cargo Ports; Good Practices for Cybersecurity in the Maritime Sector, p54.

39 Ontwerp Programma Noordzee 2022-2027, p67.

40 StatLine – Internationale handel en doorvoer; waarde, gewicht, goederen, vervoerwijze (cbs.nl)

41 Maritieme monitor 2020, p51.

42 Nationale Omgevingsvisie, p8.

43 Policy Document on the North Sea 2016-2021, p34.

44 Policy Document on the North Sea 2016-2021, p98.

45 The Future of the North Sea, p65.

46 Annual Port of Rotterdam report highlights 2019, pp10,16; Annual Port of Rotterdam report highlights 2015, pp6,7,12.

last 15 years (see Figure 8).[47] The coronavirus crisis caused a temporary dip for 2020 and 2021, but is unlikely to interrupt the overall trend.[48] These developments coincide with the North Sea's operating space being increasingly in demand for the installation of wind farms. One of the last sections that allowed for relatively free movement for shipping was occupied when the Dutch and Belgian governments in 2017 allocated space for the Borssele wind farms. Fixed lanes and altered anchorage sites and precautionary areas created the final piece of a designated shipping route now connecting France with Germany.[49]

With Amsterdam serving as the world's largest gasoline port and Rotterdam playing a large role in the market for crude oil, the shipping of flammable substances to Dutch ports is routine business. With more than 100 million tons annually, the Netherlands is the biggest crude oil importer in the EU.[50] Liquefied Natural Gas (LNG) imports increased five-fold from 2017 to 2020. Rotterdam is a key hub for LNG throughput, with 7.1 million tons in 2019, an increase of 36.6% compared to 2018.[51]

Trade and transport in the North Sea also includes helicopter and ferry services. Helicopters must navigate areas restricted for gas and oil production or natural parks. Helicopter flight routes influence spatial planning because (oil and gas) platforms with a helipad require a 5nm obstacle-free zone.[52] Ferry services also create additional spatial pressure, given their need for clearways.[53]

The first trial with automated shipping in the North Sea took place in March 2019 as part of a two-year research project. The ship was fully autonomous with no onboard crew or remote-control mechanisms. May 2019 saw the first crossing of the North Sea by an autonomous vessel, as the 12m-long *SEA-KIT Maxlimer* sailed from Belgium to the UK. The IMO imposes regulatory hurdles to the large-scale introduction of semi-automated shipping and the introduction of fully-automated shipping; but it plans to allow autonomous trials under secure safety standards and to begin the process of incorporating such technologies into its regulatory framework.

Key take-aways

- Trade and transport in the North Sea is a vital lifeline for the European economy. For the Netherlands, economic use of the North Sea is a critical national interest.
- Trade and transport in the North Sea is expanding whilst navigation space is becoming scarcer, mainly because of the construction of wind farms.
- The shipping of flammable substances takes place on a large-scale and LNG-transports are rapidly becoming routine business.
- Flight paths for helicopters and clearways for ferry services create additional spatial pressure.
- Pilots with (semi-)automated shipping have been successful, but rules and regulations imposed by the IMO to prevent the large-scale introduction of automated and autonomous shipping remain.

47 Ongoing Challenges to Ports: The Increasing Size of Container Ships, p2.
48 2020 Jaarverslag Port of Rotterdam, pp8,17.
49 Nieuwe Scheepvaartroutes Langs De Belgische – Nederlandse Noordzeekust, pp2,3.
50 2020 Jaarverslag Port of Rotterdam, p60; Annual Port of Rotterdam report highlights 2019, p15; Eurostat.
51 Annual Port of Rotterdam report highlights 2019, p15
52 Policy Document on the North Sea 2016-2021, p85.
53 Ontwerp Programma Noordzee 2022-2027, p101.

3.2.2 Energy

The landscape for energy-related activities in the North Sea has undergone incremental changes in recent years but is expected to experience more radical alterations in the future. Natural gas has long represented the lion's share of energy production in the North Sea. However, gas and oil activities have started to make way for what will be the dominant activity: renewable energy production. The large-scale installation of wind farms is the cornerstone of the energy transition for the immediate and mid-term future. The Climate Agreement stipulates that wind energy has the potential to be the "most significant green power source" and will be crucial in the attempt to reach the Dutch climate goals, as a result.[54] The North Sea Agreement further states that current plans to expand wind power should be seen as non-negotiable and that the focus should be on providing more wind power offshore.[55]

Fossil. Natural gas is the most important energy source in the Netherlands. In 2018, natural gas was responsible for 76.2% of domestic energy production, 42.1% of TPES (total primary energy supply) and 51.0% of electricity generation. Moreover, gas dependency is shared by a broad range of actors, with the three major sources of the Dutch demand for gas being heating and electricity 30.9%, industry 24.0%, and residential 22.3%.[56] Most natural gas produced in the Netherlands is produced in the North Sea. In 2019, gas produced in the North Sea was approximately 10 billion Nm^3 (normal cubic meters), 2.5 times larger than onshore gas production.[57] Its continued importance is reflected in the production of gas offshore being designated as an issue of national interest,[58] with the North Sea Agreement also stressing the importance of domestic energy supply.[59]

Gas activities in the North Sea are also prominent in spatial terms. In 2015, approximately 160 platforms – 93% for gas, 7% for oil – took up 126km^2 of space. The total length of all pipelines in the North Sea is 4500km. Due to their 500-1000m restricted maintenance and protection zone, the effective space in use for both pipelines and platforms is 4626km^2, or nearly 8% of the Dutch continental shelf.[60] These pipeline networks are also connected to international pipelines heading for Germany and Denmark, landing respectively in Den Helder and Eemshaven.[61] In short, offshore gas production takes up significant space on the North Sea and connects the Dutch energy network internally as well as internationally.

Offshore gas production has steadily decreased in line with the objectives of the energy transition, despite its centrality in the Dutch energy mix, see Figure 9. Article 3.8 of the North Sea Agreement states that the drilling for fossil fuels in the North Sea should be reduced in line with the Paris targets.[62] There has been an annual average decline in offshore gas production of roughly 7% in the last decade, with decreases of 15-22% in recent years. Production rates in 2019 were approximately half of that in the peak years of the early 2000s.[63] The decommissioning of platforms has coincided with the decrease in production and is accelerating: the approximately 20 offshore wells decommissioned in 2020 are double the number of wells

54 National Climate Agreement, p167.
55 North Sea Agreement, pp18,19.
56 IEA The Netherlands 2020 Energy Policy Review, p167.
57 Natural Resources and Geothermal Energy in the Netherlands Annual Review 2019, pp26,27,30.
58 TPolicy Document on the North Sea 2016-2021, p8.
59 North Sea Agreement, p15,27.
60 Policy Document on the North Sea 2016-2021, pp34,46,50.
61 .Noordgastransport (NGT); NOGAT
62 North Sea Agreement, p15,27,28.
63 Natural Resources and Geothermal Energy in the Netherlands Annual Review 2019, pp26,27.

decommissioned in 2019, and the largest amount in five years.[64] Oil production is relatively small, with outputs decreasing steadily since the 1990s and 2019 production levels being 12.4% less than those in the previous year.[65]

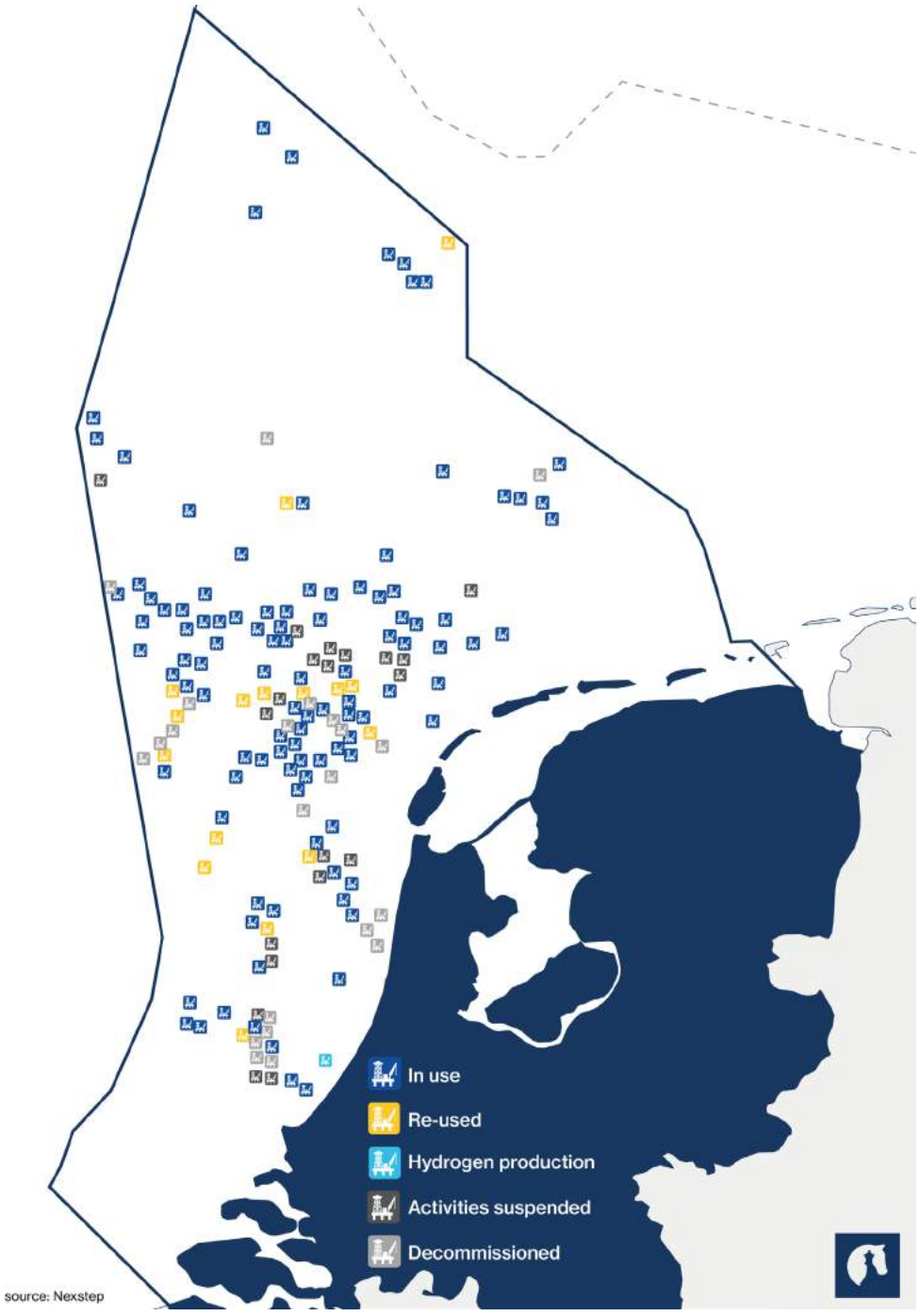


Figure 9. Gas and oil platforms are gradually being decommissioned[66]

64 Re-use & Decommissioning report, p23.

65 Natural Resources and Geothermal Energy in the Netherlands Annual Review 2019, pp8,103.

66 NexStep p8.

Wind and solar power. Wind energy is booming. The five existing offshore wind farms in 2020 (Figure 14) produced around 2.5 GW of electricity in total that year.[67] Many additional areas have been designated for the expansion of wind farms, including the Borssele 1&2 park opened in late 2020. As can be clearly distinguished from the disposition of the windfarm areas, both current and planned, a considerable restriction of the use of the North Sea is induced, channeling cargo vessels and naval ships. It creates sea lanes, or almost highways at the North Sea for ships which will make it an easy predictable course for criminals, pirates, even opposing navies and other spoilers for security. Recently, a trail has been conducted with a floating solar park in the Dutch North Sea. The placement of the windfarm areas, both current and planned, has led to considerable restrictions in the use of the North Sea. The result has been a channeling effect for cargo vessels and naval ships, creating lanes in the North Sea for ships. This will make it easier for malicious actors to block shipping routes.

High voltage cables. To connect these new wind farms, increased investments in high voltage cabling is underway, both nationally and internationally. TenneT, appointed in 2016 as lead administrator for the Dutch offshore electricity network, is in the process of executing 15 cabling projects.[68] The Netherlands has also seen a recent proliferation of international high voltage cables, which are intended to increase the flexibility of the national grid. One example is the 2019 COBRA cable connecting the Netherlands to Denmark, with cables laid to both the UK (BritNed) and Norway (NorNed) in the decade before.[69]

To meet the surge in offshore wind electricity production, TenneT has also begun adding landing sites, such as the Maasvlakte landing point. In addition, transformer blocks (3650-ton offshore platforms; otherwise known as '*stopcontacten*') have been installed in the North Sea to prepare for electricity transport to shore. Many more of these landing sites and transformer blocks will be introduced, as the plans for large-scale wind farm installation come to fruition. Undersea congregated high-voltage cables and landing points rely on relatively few points coming ashore in comparison to a relatively dispersed gas and oil production system of pipelines, see Figure 10.

67 CBS Hernieuwbare elektriciteit

68 Informatievoorziening op zee handig verankerd; Dutch offshore grid; Kabels en leidingen – Elektra, telecom kabels op de Noordzee.

69 Ontwerp Programma Noordzee 2022-2027, p51.

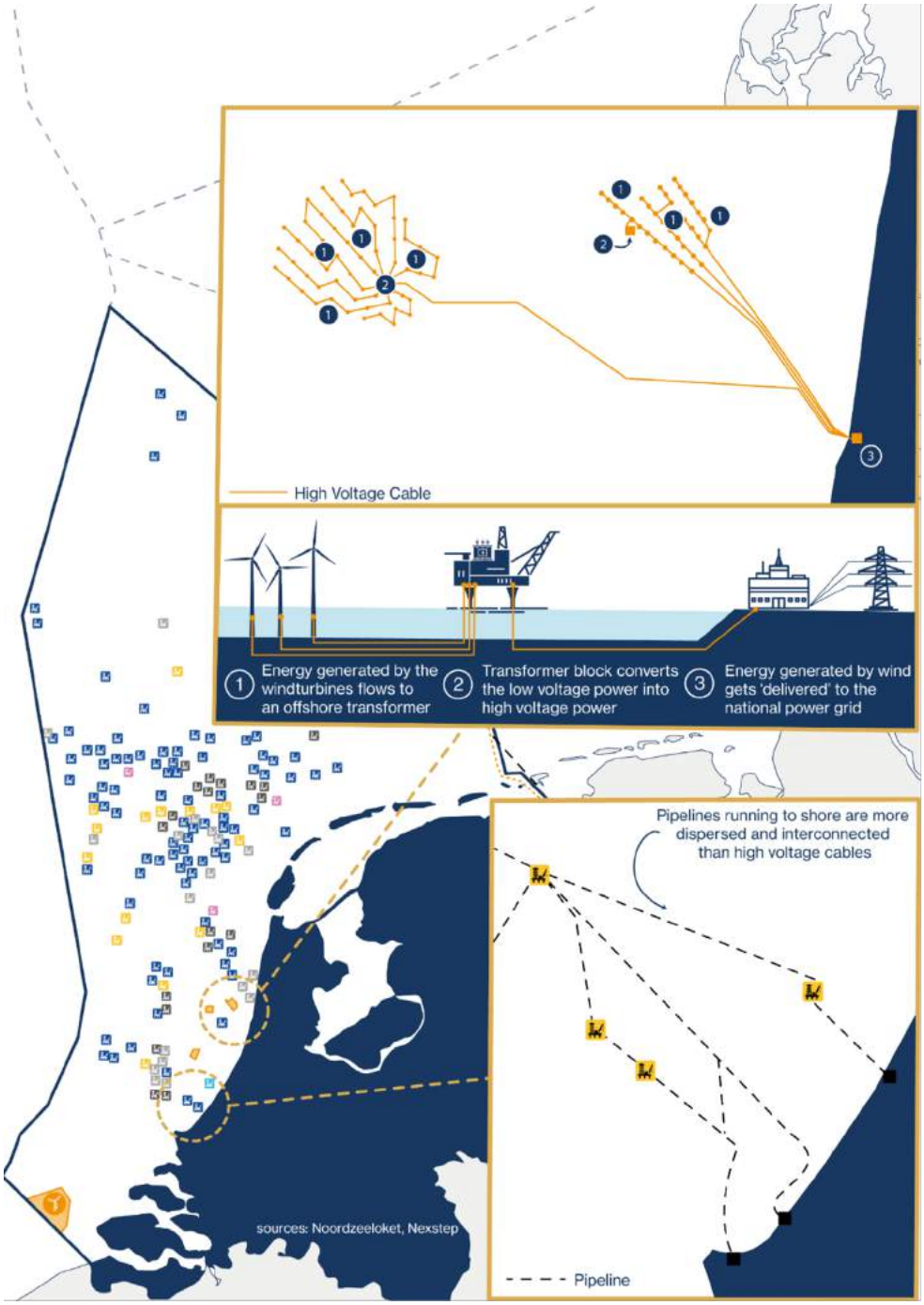


Figure 10. Undersea congregated high-voltage cables and landing points[70]

Key take-aways

- Energy activities in the North Sea are large-scale and a national interest. Natural gas activities remain indispensable to meet national energy demands, even though platforms are being decommissioned.
- The offshore transition to sustainable energy production, almost exclusively wind power, is underway.
- Wind farms, underwater high-voltage electricity cables, landing points and transformer blocks are constructed on a large scale and will radically alter the spatial design of the North Sea

70 Noordzeeloket. For an overview of planned wind farm zones see Offshore Wind Energy

3.2.3 Communication and sensing

Telecommunication cables have long been present in the North Sea. The Dutch continental shelf is also home to telecommunication cables connecting neighboring states. The North Sea is a hub for national, regional and international communication cabling, with one of the major landing spots near IJmuiden. The Netherlands serves as the Digital Gateway to Europe with a huge node in the international cabling and communication system located near Amsterdam. Amsterdam surpassed London in 2019 and now houses the largest data center hub of any European country. Increased data traffic requires more communication cables. To meet the increased demands of modern data traffic, new fiberglass cables have been installed. The Netherlands currently has around 20, or 2000km worth of, active telecommunication cables in the Dutch continental shelf.[71] The majority of these cables connect to European states, but the Netherlands is also connected to transatlantic telecommunications, directly via the AC-1 and indirectly via other European states through the TGN-Atlantic.

The continued laying of high-capacity telecommunication cables, with their large maintenance zones, presents significant space sharing issues. These cables – active and abandoned – take up nearly 7% of the Dutch continental shelf compared to less than 1% for high voltage cables and 8% for oil and gas pipelines (2015 figures). This relatively large spatial demand is partially a result of the larger 750m maintenance zone around the cable (as pipelines and high-voltage cables only demand a 500m zone).[72]

The NLCG, Netherlands Air Traffic Control LVNL, Rijkswaterstaat and the Meteorological Office KNMI, among others, have sensing sites at sea.[73] The KNMI has fourteen weather sensor stations spread across the North Sea. As oil and gas platforms are being decommissioned, the number of sensing locations is falling,[74] leading to a transfer of sensing stations to wind farms. Moreover, further digitalization at sea is being implemented. New sensors at sea will foster the advancement of maritime AIS technology and install new radar stations to monitor birds and bats. The biggest innovation towards digitalization of the North Sea came in mid-May 2021, when the Dutch government conducted an auction for the rights to provide 5G at sea, which was won by T-Mobile and Tampnet. The 5G network will be used by platforms, ships and wind farms; and will, for example, facilitate the operation of drones above the North Sea.

71 Ontwerp Programma Noordzee 2022-2027, p77.

72 Mathijssen, Dammers, and Elzenga, *The Future of the North Sea*, p55.

73 Ontwerp Programma Noordzee 2022-2027, p83.

74 Ontwerp Programma Noordzee 2022-2027, p83.

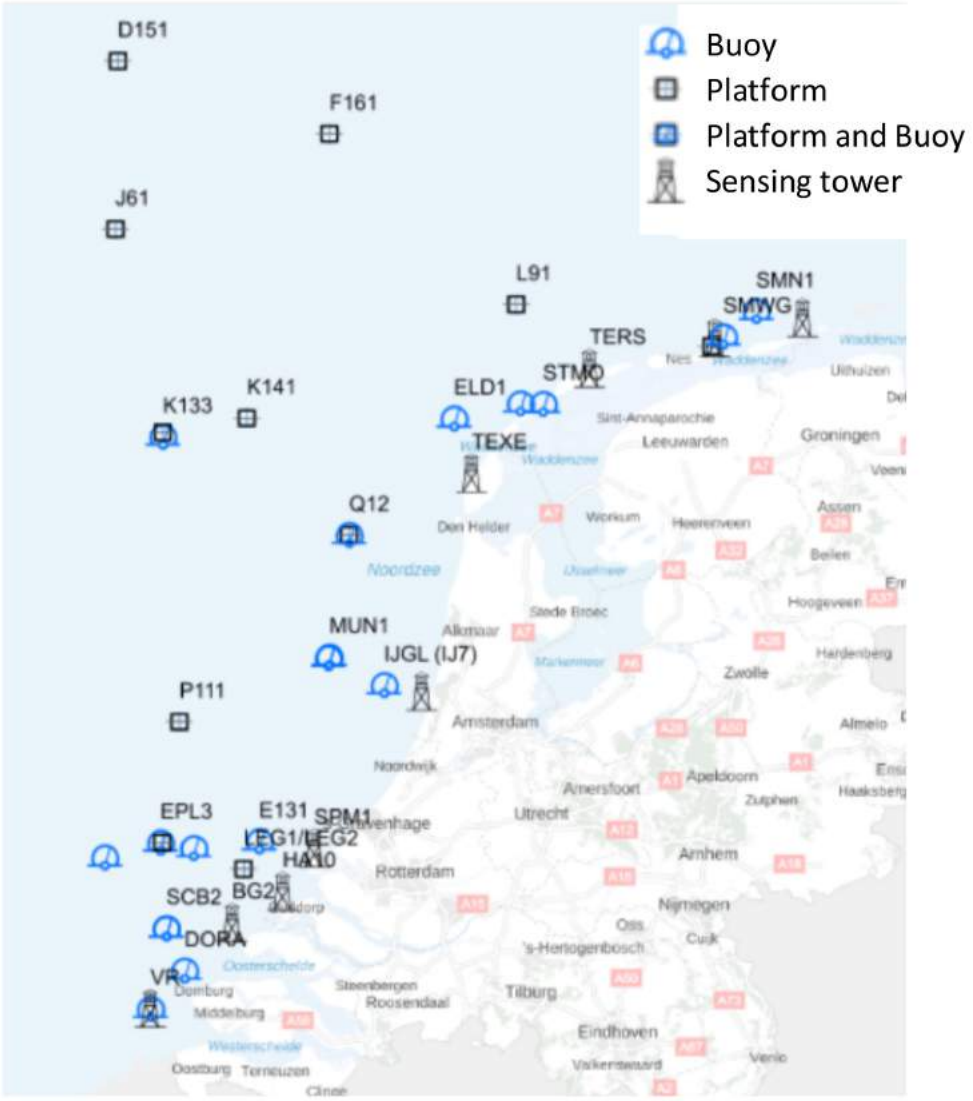


Figure 11. Sensing stations in the North Sea[75]

Key take-aways

- Telecommunication cables have long been present in the North Sea, with increases in data traffic resulting in the expansion of telecommunication cables.
- The continued laying of high-capacity telecommunication cables, with their large maintenance zones, contributes to congestion of in the North Sea.
- Sensing at sea has remained relatively stable as a large share of the sensing functions are done on shore.

75 Rijkswaterstaat data register

3.2.4 Industrial activities

Industrial activities at sea predominantly concern sand dredging. The Dutch government has identified sand dredging as an activity of national interest. The Netherlands dredges more sand in its territorial sea than any neighboring state.[76] Half of the sand taken from the sea is used for infrastructure works and onshore construction, while the other half is used for the replenishment of coastal defenses. In 2015, it was estimated that the Netherlands extracted 25 million m^3 of sand annually.[77] This figure fluctuates significantly with large expansion projects; Maasvlakte2, for instance, used 213 million m^3 of sand.[78]

Key take-away

- Industrial activities at sea – except for sand dredging – are minimal.[79]

3.2.5 Fishing and aquaculture

Traditional fishing techniques prevail when it comes to obtaining food resources from the North Sea. Fishing activities are being constrained due to environmental issues and, recently, Brexit.[80] The fishing industry on the Dutch continental shelf is seeing their operating capabilities decline. A 2015 analysis of the Dutch fishing fleet reported some 600 active Dutch vessels employing an industry of nearly 28,000 people. [81] The 2019 data shows a reduction of the fishing fleet to about 365 vessels, with 76% of the vessels being more than 20 years old, compared to 63% in 2015, indicating a possible lack of investment.

Sea-based farming is in the developmental phase, with pilots currently being undertaken, such as shell fishing in the Voordelta, seaweed near Scheveningen, and crustaceans in the Princess Amalia wind farm.[82]

Key take-aways

- Fishing is being constrained. Brexit is an added source of uncertainty for (traditional) fishing.
- Sea-based farming in developmental phase.

76 Policy Document on the North Sea 2016-2021, p44.
77 The Future of the North Sea, pp27,29.
78 Policy Document on the North Sea 2016-2021, p44.
79 The only exception is Carbon Capture and Storage (CCS) that will become a key activity. This activity is captured under the heading of Energy.
80 North Sea Agreement, p14-15.
81 Policy Document on the North Sea 2016-2021, p55.
82 Ontwerp Programma Noordzee 2022-2027, p43.

3.2.6 Living and recreational use

Recreational use of the North Sea is important to Dutch society and provides a modest contribution to the economy, even though the coronavirus crisis led to a temporary reduction.[83] The economic value of coastal tourism is twofold: it provides a limited contribution in direct revenues, and it contributes to employment. 25% of total hotel bookings in the Netherlands are at the coast, some 2.6 million people visit the coast, and activities such as recreational fishing account for approximately €165 million annually.[84]

Key take-away

- Recreational use of the North Sea is modestly important to Dutch society.

3.2.7 Conservation

Natura 2000 sites lie along the coast (North Sea Coastal Zone, Voordelta, Vlakte van de Raan, Delta Waters) and inside the EEZ (Dogger Bank, Cleaver Bank, Frisian Front).[85] Conservation is of increasing importance, with the designation of (limited) protected zones, restrictions on sea floor fishing,[86] on oil and gas production in nature reserves,[87] and the allocation of funds for research.[88] These developments are a result of the fact that the nature transition is one of the major transitions stipulated in the North Sea Agreement. The transition means that other activities, predominantly fishing, have had to give way to conservation efforts.

Key take-away

- Conservation is of growing importance at the expense of other uses, predominantly fishing.

83 StatLine – Hotels; gasten, overnachtingen, woonland, regio (cbs.nl)

84 Policy Document on the North Sea 2016-2021, p59.

85 Nature and biodiversity – Noordzeeloket UK. These 6 zones are not exclusively used for conservation with for example gas production in such conservation zones still being allowed according to the North Sea Agreement, p23.

86 North Sea Agreement, p23.

87 North Sea Agreement, p22.

88 North Sea Agreement, p7.

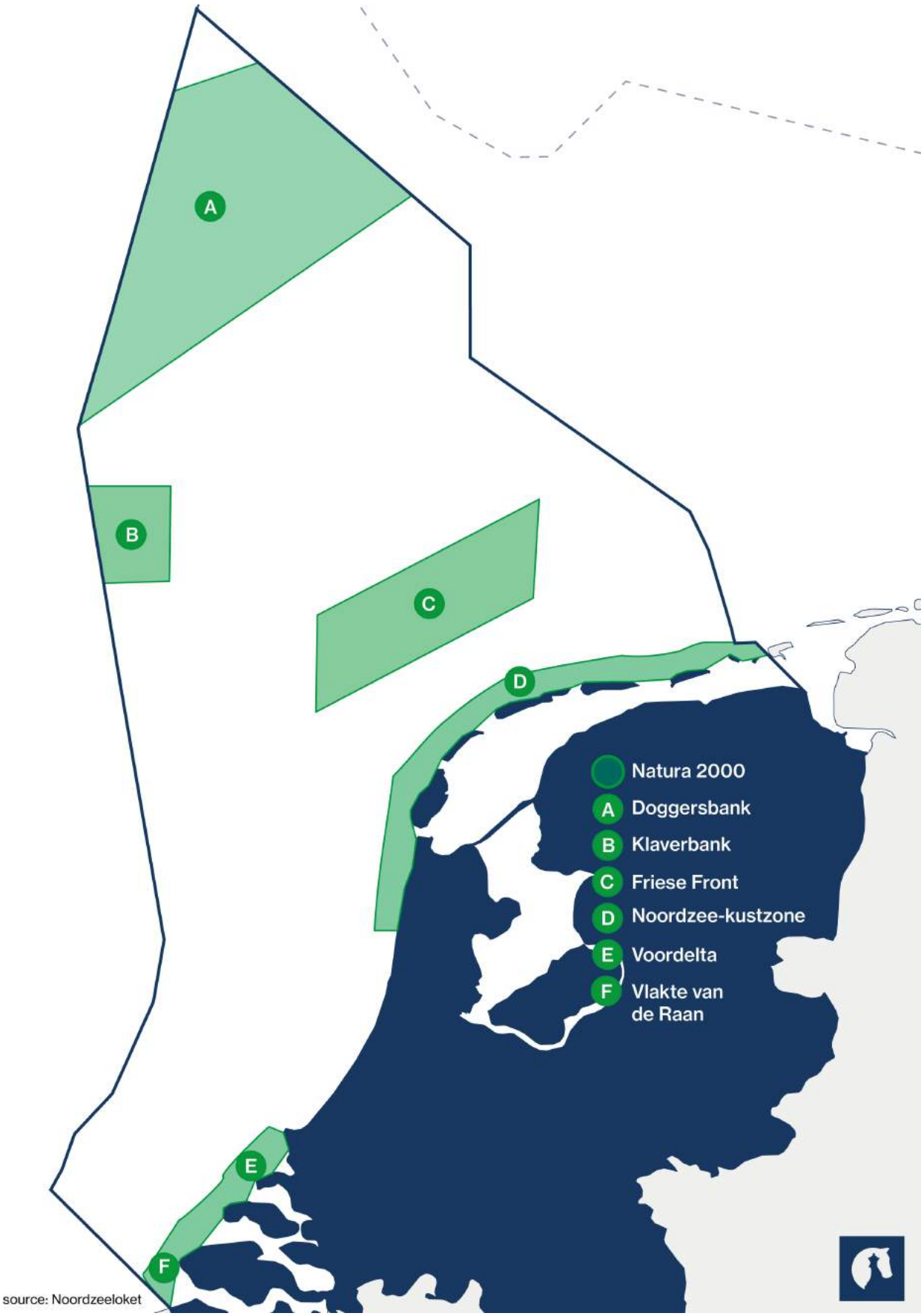


Figure 12. Conservation and fishing restrictions in the North Sea[89]

89 Policy Document on the North Sea 2016-2021, p70.

3.2.8 **Defense use**

The North Sea also serves as a military exercise area in which both naval maneuvers and live firing exercises in restricted zones take place. A military flying area, north of the Waddenzee, is reserved for the operation of jetfighters. Although the bottom of this exercise area is well above sea level, flying in that area may have consequences for activities at and below the surface. Military areas comprise about 4200km^2 or about 7.5% of the Dutch continental shelf.[90] Nonetheless, changes have been introduced that include increased space sharing and restrictions imposed for the sake of conservation limiting the use of live ammunitions.

Moreover, the Dutch ports and seaways function as a logistic artery for NATO troop movements to and from the UK and North-America. The ability to reinforce US military presence in Europe in the case of increased tensions or military conflict is a crucial element in NATO's deterrence strategy. In the past, large scale exercises have been conducted. In late 2017, for example, US military equipment on route to Germany was processed by the Port of Rotterdam that designated a section of the harbor as a temporary militarized zone with around the clock armed protection.

Key take-away

- Pressure on military exercise areas has grown as space sharing and environmental restrictions become more common.

90 Policy Document on the North Sea 2016-2021, p34.

3.3 Future value creation in the North Sea

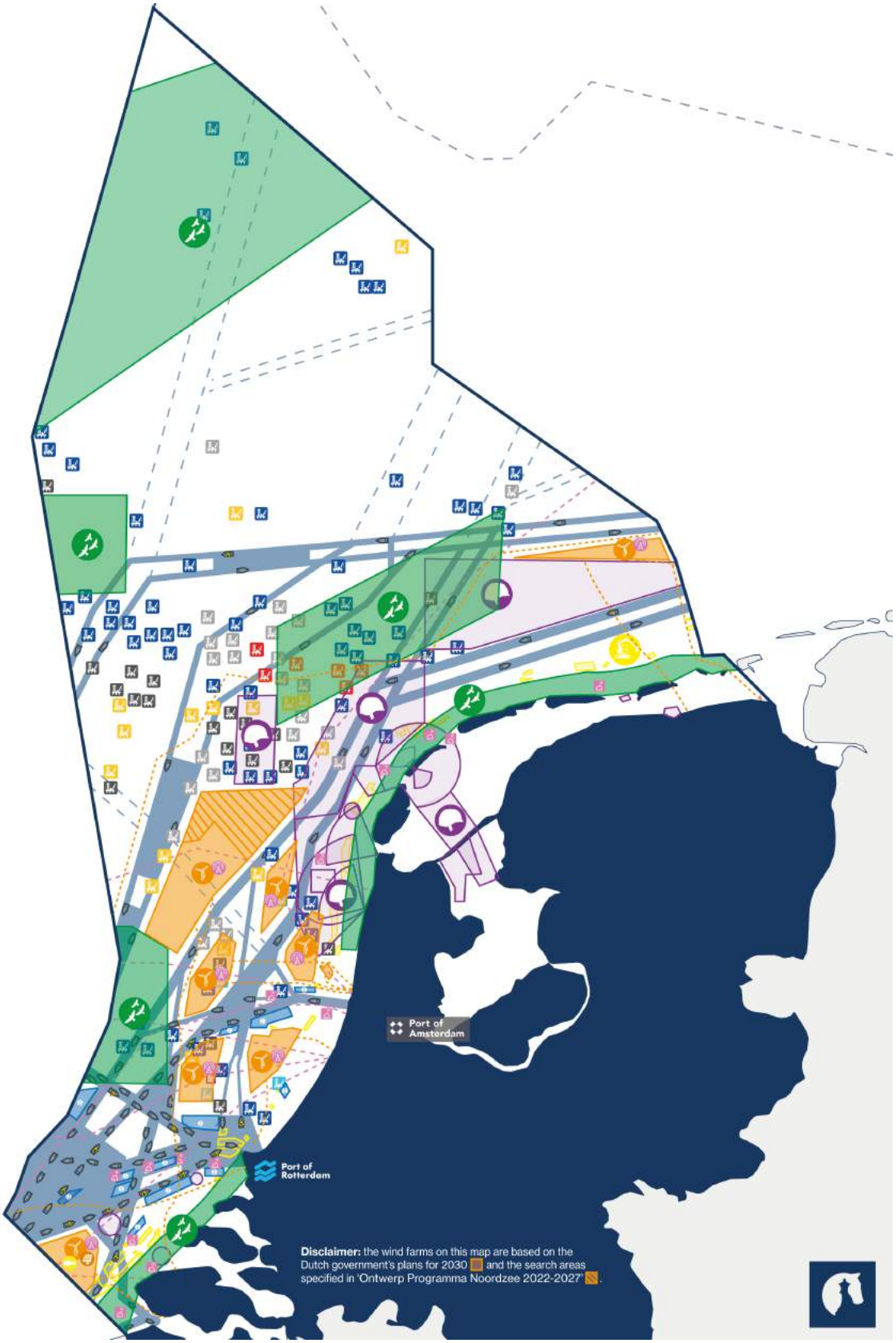


Figure 13. Large parts of the North fully allocated in 2035 (legend in Annex B)

By 2035, large parts of the North Sea will have been allocated to various, partly overlapping, usages. The three transitions that have a substantial impact on value creation in the North Sea, namely the energy, nature, and food transition, are well underway. CO_2 emissions will have to be reduced by 49% in 2030 according to the National Climate Agreement; or by 55% according to the updated CO_2 reduction target for the European Commission's revised European Green Deal, which is supported by the Dutch government. This requires far-reaching measures, reflected in the use of the North Sea.

3.3.1 Trade and transport

In 2035, increases in ship sizes and traffic volumes will put more strain on already busy shipping lanes in the North Sea. Although estimates vary, most forecasts project at least a gradual increase in global trade.[91] As there is little doubt that other offshore activities will grow, spatial pressures will further restrain the freedom of movement for trade and transport.[92] The busiest shipping lanes in the southern North Sea are also the most desirable locations for sand drenching, wind farms and fishery.[93] The recent IMO approved alteration in shipping activities to accommodate for the expanding Borssele wind farm for the Belgian and Dutch coast is a case in point.[94] Moreover, more infrastructure at sea will increase the amount of ship movements made by construction and maintenance vessels. These vessels are expected to cause significant – although not clearly defined – changes in maritime traffic.[95]

The PBL forecast predicts an expansion of shipping activities in the northern part of the North Sea in three out of its four scenarios.[96] The expected increase in traffic has resulted in the planned revising of two northern shipping routes: the Northern Sea Route and the Kattegat route.[97] The North Sea Agreement advises to start looking further north for areas suitable for non-shipping activities such as wind farms.[98] In other words, spatial pressure on shipping, already very much present in the south, is likely to expand to the north.

Energy-related shipping in the North Sea will diversify as it moves towards larger scale LNG imports, early carbon storage shipping and several hydrogen pilots. This changing energy mix influences risk profiles. As platforms continue to be decommissioned, offshore production of oil and gas will cover an even smaller part of energy demand in the Netherlands by 2030 leading to an increase in fossil fuel imports.[99] LNG activities in Dutch ports are expected to diversify with LNG bunkering, meaning the transferring of large amounts of LNG from large vessels to smaller vessels that are able to take this substance to refuel ships in the port, becoming increasingly important.[100] Eemshaven has started bunkering ships. Rotterdam has welcomed *Gas Agility*, the world's largest bunkering ship.

Around 2035, CCS-related CO_2-shipping will likely have commenced, albeit on a limited scale. The driving force for this is twofold. First, CCS is regarded as a crucial activity to

91 See for instance European Strategy and Policy Analysis System (ESPAS), *Global Trends to 2030: Challenges and Choices for Europe*, April 2019, pp23–24.

92 The Future of the North Sea, p58.

93 North Sea Agreement, p17.

94 Nieuwe Scheepvaartroutes Langs De Belgische – Nederlandse Noordzeekust, pp2,3

95 Ontwerp Programma Noordzee 2022-2027, p69.

96 The Future of the North Sea, p36.

97 Ontwerp Programma Noordzee 2022-2027, p99.

98 North Sea Agreement, pp17-18.

99 North Sea Energy Outlook, p31.

100 Ontwerp Havennota 2020-2030, pp13,35; Ontwerp Programma Noordzee 2022-2027, pp67-71.

reach the climate goals.[101] Second, CCS experimental projects such as the Northern Lights project in Norway are designed to be supplied with CO_2 from other countries by ship. In the Netherlands, H2M, currently a natural gas to hydrogen power plant, is expected to transport the CO_2 it produces to the Northern Lights project for storage.[102] The Netherlands based CO_2 transport company Carbon Collectors, may come to play a relevant role as it is expected to launch its first CO_2 storage ship by 2023 and store 6 million tons per year in North Sea wells – also to those outside the Dutch continental shelf – before 2030.[103]

Sustainability goals drive the diversification of propulsion methods used by commercial ships, with "almost all major shipping companies" having already launched LNG-propelled ships vessels. A more diverse mix is likely to also include methanol and ammonia. As research and development efforts in this field are dynamic and ongoing, the exact field of play, energy mix, and timing of tipping points are highly uncertain.

Key take-aways

- Likely increases in traffic volumes will further aggravate already busy shipping lanes in the North Sea. Other activities will grow, exerting spatial pressures that will further restrain the freedom of movement for trade and transport.
- LNG activities centered around the Port of Rotterdam have grown significantly recently and will continue that growth trajectory.
- CCS-related CO_2 -shipping will likely have commenced but on a limited scale.
- Ship-propulsion will diversify as less-polluting methods are explored.

3.3.2 **Energy**

Gas and oil activities will make way for renewable energy production. In fact, the transition to wind power is fully underway. This leads to a gradual decrease in the infrastructure needed to drill and transport fossil fuels and a substantial increase in the infrastructure needed for renewable energy at sea: high voltage cables, landing points and transformer hubs. Carbon Capture and Storage (CCS) is a crucial part of the energy transition. The pilots and plans needed for future CCS are in the making (see §3.2.4).

Fossil. Gas production rates are expected to decrease by 10% annually for the next decade, consistent with the National Climate Agreement.[104] Indeed, very few new gas fields have been identified in the previous decade.[105] The import of LNG is expected to continue to grow substantially, in line with the five-fold increase from 2017 to 2020. In all PBL scenarios, "oil and natural gas activities on the Dutch continental shelf stop between 2030 and 2050."[106] The PBL report stipulates that by 2030, in all scenarios, there are no more than 67 oil and gas platforms on the Dutch continental shelf, compared to approximately 160 in 2015.[107] Thus, the decommissioning of platforms is expected to be a major focus point towards 2035 with an estimated 60% of the platforms need to be decommissioned by 2030.

101 National Climate Agreement, p112.
102 North Sea Energy Outlook, p81.
103 New company Carbon Collectors launched | News | gasworld
104 Re-use & Decommissioning report, p9.
105 StatLine – Aardgas- en aardoliereserves; nationale rekeningen (cbs.nl)
106 The Future of the North Sea, p11.
107 The Future of the North Sea, p55.

This may nonetheless be an overestimation as it does not account for the repurposing of platforms.[108] Possible repurposing for gas and oil platforms includes CO_2 storage[109] and the installation of hydrogen production plants. It is also possible that platforms will be decommissioned long before these platforms can be employed for alternative uses. Overcoming this time lag requires long-term planning coordination between different parties.

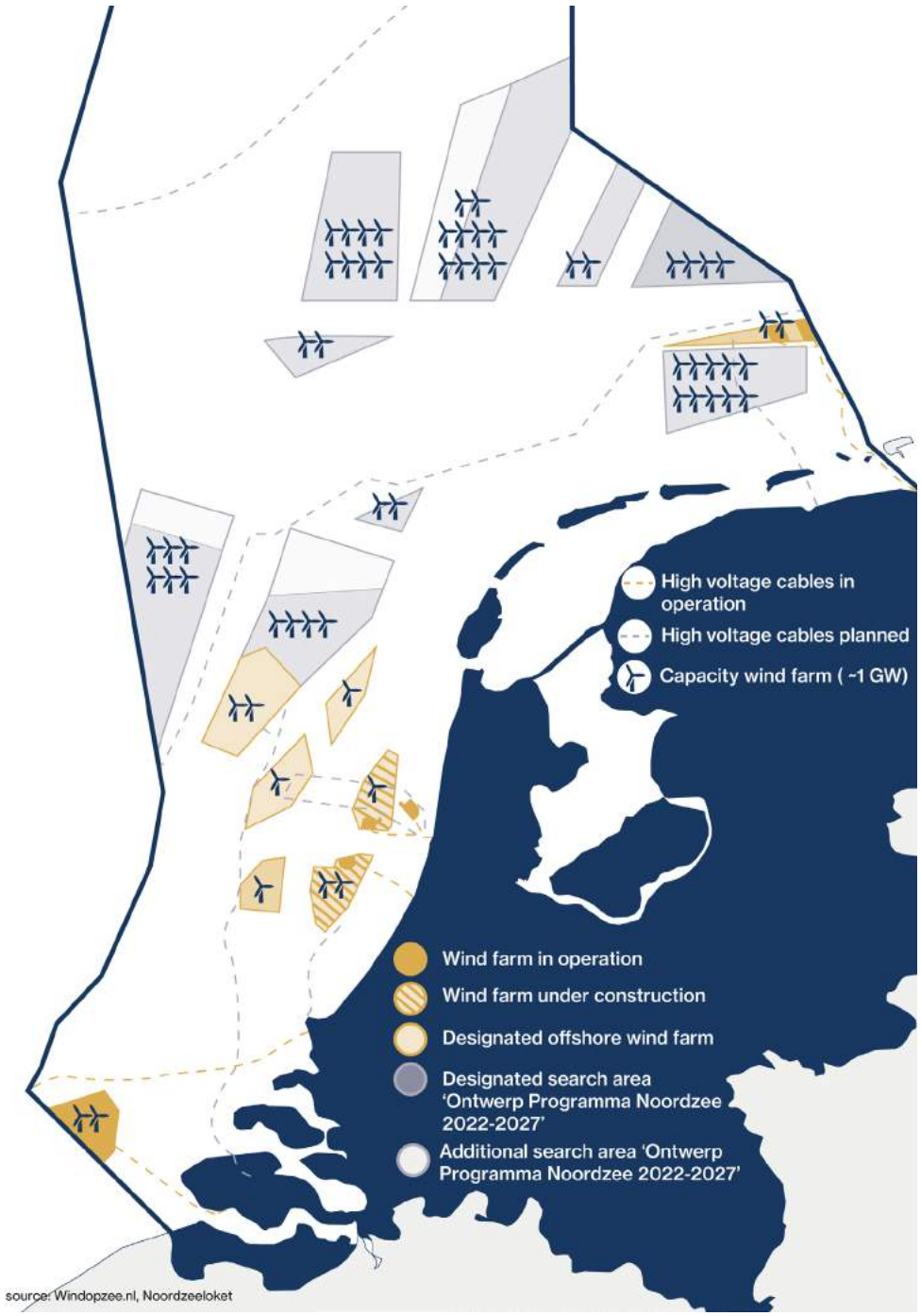


Figure 14. Existing, under construction and planned wind farms

108 Re-use & Decommissioning report, p10.

109 Ontwerp Programma Noordzee 2022-2027, pp63,106.

Wind. The North Sea of 2035 will be characterized by large scale wind power production. By 2035 the additional wind farms *Hollandse Kust Zuid* (1.52 GW), *Hollandse Kust Noord* (0.759 GW), *Hollandse Kust West* (1.4 GW), *IJmuiden Ver* (4 GW) and *Ten Noorden van de Waddeneilanden* (0.7 GW) are expected to be operational. Still, additional wind power may be necessary to achieve the revised European Green Deal CO_2 reduction target.[110] The North Sea Agreement states that it expects a continued increase post-2030 of 20-40GW worth of off-shore wind energy.[111] In spatial terms, with a 4MW/km^2 average, generating 60GW takes up 26% of the Dutch continental shelf.[112]

Hydrogen. By 2035 hydrogen production will likely have surpassed the experimentation scale, with maybe the first major project just completed. Large scale application, however, is highly uncertain. There currently is no active policy-making to support offshore electrolysis on a large scale by 2035.[113] Moreover, the PBL study into the future of the North Sea reaffirms that any plans for power-to-gas storage are still in early stages and that even when the post-2030 electricity grid will need to adopt such innovative solutions, hydrogen is only stated as a *possible* solution.[114]

Green hydrogen production[115] as a power-to-gas electricity storage solution and offshore electrolysis is still in its infancy. TenneT and Gasunie are currently evaluating the potential for green power-to-gas hydrogen islands in the North Sea.[116] Moreover, pilots focusing on the large-scale introduction of offshore electrolysis will also have been undertaken by 2035.[117] The PosHYdon project, an offshore green hydrogen pilot, will start still in 2021 and intends to evaluate the challenges associated with integrating three energy systems, namely offshore wind, offshore gas and offshore hydrogen. The NorthH2 project, which aims to produce onshore hydrogen with 4GW of offshore wind power by 2030, aims to start producing hydrogen in 2027.[118]

In 2035, the majority of hydrogen related activities will therefore still be onshore hydrogen production for industrial use. This industry is expected to grow with blue hydrogen making headway until green hydrogen becomes more likely after 2035 and towards 2050[119]. Plans that make this transition more likely include the building of Europe's largest green electrolysis unit led by AkzoNobel in the Netherlands and an additional green electrolysis center on the Maasvlakte.

Type	Specifics	Likelihood of industrial use scale by 2035
Gray	Hydrogen produced with fossil fuels	Almost certain
Blue	Hydrogen produced with fossil fuels. 80-90% of the emitted CO_2 is captured and stored	Probable
Green	Hydrogen produced with renewables	Unlikely, pilots under way

Table 8. In-use types of hydrogen by 2035

110 Bestemming Parijs: Wegwijzer voor klimaatkeuzes 2030, 2050, pp34,47.
111 North Sea Agreement, p19.
112 The Future of the North Sea, pp52-53.
113 North Sea Energy Outlook, p79.
114 The Future of the North Sea, p12.
115 There are three ways to produce hydrogen: with renewables (green), with fossil fuels (gray) and with fossil fuels and CCS (blue).
116 The Future of the North Sea, p12.
117 Ontwerp Programma Noordzee 2022-2027, pp61,62.
118 Ontwerp Programma Noordzee 2022-2027, pp61,62.
119 North Sea Energy, *Energy transport and energy carriers*, pp18-19; Ontwerp Programma Noordzee 2022-2027, pp61,62.

Other renewables are not expected to make significant headway in the Dutch North Sea before 2035.[120] That is not to say that they are not being developed and experimented with in pilot projects. Synergies between wind farms and other alternative energy sources possibly include floating solar parks (1MW to every turbine, building on an existing pilot), Airborne Wind Energy,[121] tidal systems and aquatic biomass (seaweed).[122]

Cabling and Pipelines. By 2035, the number of under-sea high voltage cables will have vastly increased.[123] TenneT has calculated that in 2029 a total of 9,600 MW of wind energy will be connected. Onshore, the electricity grid will have to be upgraded as the added supply of wind energy might cause overflows, given its fluctuations in output. This includes the additional construction of landing points where congregated high voltage cables come onshore.[124] The connecting of grids internationally is also expected to have increased by 2035.

By 2035, the network of gas pipelines will be used less as offshore gas production will have decreased. This leaves a large number of abandoned pipelines on the sea floor. These will either be removed or repurposed for large scale CCS and hydrogen transport. Both uses are expected to be introduced on a large scale towards 2050.

Carbon Capture and Storage (CCS). By 2035, CCS is very likely to have made its debut in the North Sea. By 2030, two of the four PBL scenarios feature CO_2 storage in the North Sea reaching 15-20Mt (metric tons) per year.[125] Previous pilots provide reasons for doubt as to how realistic this is. The ROAD CCS project in Rotterdam was cancelled. However, as the price of CO_2 rises so do the prospects for CCS and the Porthos and Athos projects that are expected to be operational by 2023 and 2027, respectively.[126] Porthos is a 2.5Mt project that would see CO_2 pumped and stored from the Port of Rotterdam, with Athos applying the same model for the Port of Amsterdam.[127] In addition, further expansion of CCS activities may take place in the L10-A/B/E areas of the North Sea where the oldest gas and oil production sites are located. The extent to which this will take place will depend in large part on the feasibility study that is currently being undertaken by Neptune Energy NL. All in all, the scene for 2035 is one that will see a large increase in CCS activities preparing for massive storage capacity in the 2035-50 timeframe.

Key take-aways

- Gas production will continue to decline.
- Wind power production capacity will increase dramatically.
- By 2035 hydrogen production will likely have surpassed the experimentation scale, with maybe the first major project just completed. Large scale application, however, is highly uncertain. Green hydrogen will still be in its infancy.
- CCS projects are expected to commence soon. Large scale CO_2 sequestration projects are expected in the 2035-50 timeframe.

120 Kamerbrief Routekaart Windenergie op Zee, p2-3
121 North Sea Energy Outlook, p57.
122 North Sea Energy Outlook, p31.
123 Programme 2030 – TenneT; Kabels en leidingen – Elektra, telecom kabels op de Noordzee
124 The Future of the North Sea, p11-12.
125 The Future of the North Sea, p18.
126 North Sea Energy Outlook, p81.
127 Ontwerp Programma Noordzee 2022-2027, p62.

3.3.3 Communication and sensing

A further increase in telecommunication cables in the North Sea by 2035 is highly likely. At least three new cables connect the Netherlands and the UK with additional expansion plans currently being refined.[128] Larger numbers of cables are needed with increased internet traffic and the introduction of 5G enables many new applications requiring network capacity.

The platforms (or, in the long term, artificial islands, see §3.4) created to house the transformer blocks to connect wind turbines offshore, will house a range of sensors. One soon to be realized example is the Netherlands Air Traffic Control radar in the *Borssele* wind farm, but by 2035 many more are expected to be placed on the 10 new transformer blocks.

Key take-aways

- With the Netherlands being a digital node for Europe, data telecommunications are expected to increase with new cable laying plans already concrete.
- Sensors at sea will be moved from oil and gas platforms to transformer blocks in wind farms.

3.3.4 Industry at sea

In 2035, the primary industrial activity at sea is still expected to be sand drenching. Sand drenching is expected to grow as coastal defenses require additional strengthening and large-scale construction of new houses in the Netherlands is required to alleviate housing shortage.

High-profile projects to create industry or mobility hubs at sea have been suggested but implementation is doubtful. "Schiphol at Sea", referring to the relocation of the Netherlands primary airport from near Amsterdam to the North Sea, is mentioned in the North Sea Agreement but without concrete proposals.[129] Therefore it is unlikely to materialize before 2035, considering the time required to execute plans. Floating nuclear power plants at sea are already a reality. In 2019, Russia's state nuclear company Rosatom completed the first commercial floating nuclear plant and has successfully towed it to its ultimate location in the Russian Far East where access to power is difficult. The floating power plant, named *Akademik Lomonosov*, houses two 35 MW reactors. By comparison, a typical on-land nuclear station in the USA or Europe is 1,000 MW.[130] It is unlikely that this concept will be seriously contemplated in the Dutch context, even as nuclear energy could support the Netherlands in reaching its goal of carbon neutrality by 2050.[131]

Key take-aways

- Sand drenching remains the primary industry at sea to support the increased sand demand for coastal defenses and onshore building activities.
- Floating nuclear plants in the North Sea and Schiphol at Sea remain extremely unlikely by 2035.

128 Ontwerp Programma Noordzee 2022-2027, p77.
129 North Sea Agreement, p35.
130 F.William Engdahl, *Could Russia Floating Nuclear Plants Change World Economy?*, November 2019.
131 Bestemming Parijs: Wegwijzer voor klimaatkeuzes 2030, 2050, pp34,35.

3.3.5 Fishing and aquaculture

The North Sea agreement will lead to a further reduction of traditional fishing activities.[132] The uncertainty for fishermen is compounded by the gradual decrease in access to the UK's EEZ until 2026 as a result of Brexit, with future negotiations set to take place thereafter to determine future access agreements. The long-term trajectory envisioned in current agreements point to sustainable fishing techniques that are currently undergoing early development. Sustainable, innovative fishing practices – aqua and mariculture – are seen as the only path for maintaining a vital economic fishing sector.

Key take-aways

- Fishing will continue the shift towards sustainability as traditional fishing makes way for wind farms, nature conservation and sustainable aquaculture.
- Brexit is an added source of uncertainty for traditional fishing.

3.3.6 Living and recreational use

No major changes are expected in the living and recreational use of the North Sea, except for a rebound of the tourism industry post-COVID-19. Recreational sailors will have to navigate increasingly congested waters.[133] Although long-term cruise ships providing semi-permanent residency are already in use, with more being constructed, it is very unlikely that the North Sea will be the preferred dwelling location for such ships.

Key take-away

- Living and recreational use at sea is not expected to undergo significant change. In the grander scheme of the anticipated developments in the use of the North Sea, it is a minor factor.

3.3.7 Conservation

In addition to the energy transition, the North Sea Agreement calls for a nature transition and a sustainable food transition. A gradual increase of protective measures is likely to be implemented towards 2035. The North Sea Agreement specifically calls for the continued increase in sea-floor fishing free zones, and for allocated funds to conduct research for nature conservation.[134]

Key take-away

- To ensure conservation, additional restrictions on other activities are expected to be implemented.

132 North Sea Agreement, p23.
133 Ontwerp Programma Noordzee 2022-2027, p110.
134 North Sea Agreement, p24.

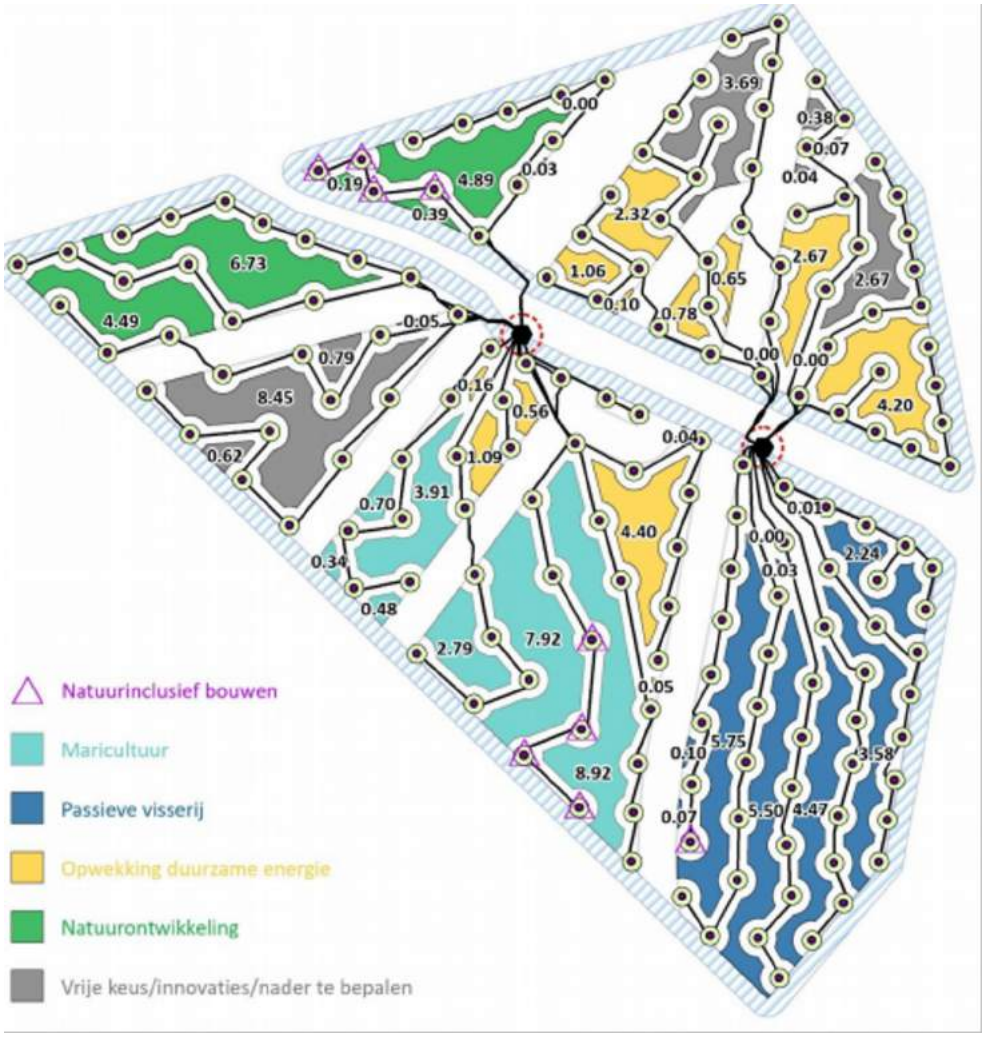


Figure 15. Borssele wind farm's space sharing program[135]

3.3.8 **Defense use**

Limited change in defense use of the North Sea is foreseen. Regulations for less live ammunition usage and additional reduction of environmental impact are to be expected. In a more intensively used and congested North Sea, increased pressure on military exercise areas is likely and spaces will need to be shared.[136] It seems unlikely that space designated for military use will be shared with platforms and wind farm installations.[137] However, current exercise areas (such as EDH-42) may have to be reduced or moved in favor of wind farms.[138]

Key take-away

- Military exercise areas remain important and will likely incur limited alterations.

135 Windenergiegebied Borssele – Noordzeeloket
136 Ontwerp Programma Noordzee 2022-2027, p79.
137 Policy Document on the North Sea 2016-2021, p54.
138 North Sea Agreement, p20.

3.4 Long-term trends in value creation in the North Sea

Figure 16. North Sea fully allocated for various usages towards 2050 (legend in Annex B). All 'probable' or 'possible' developments in §3.4 are included in the map

Developments in the use of the North Sea between 2035 and 2050 are difficult to predict. The ability to forecast on such a long-range is limited, as many technological, economic and political developments remain uncertain. Some potentially impactful developments / projects are highlighted in this section, divided in three categories. *Probable* projects will likely be technically and economically feasible at a large scale between 2035 and 2050, building upon existing policy-plans and strategy documents. *Possible* projects might be technically and economically feasible at a large scale in the future, but not yet supported by policy and strategy plans. *Unlikely* projects currently lack a clear business case, are technically extremely challenging and/or depend on very uncertain drivers.

Probable: Ships with a high degree of autonomy become common. This may vary from ships with a skeleton crew where an onshore Control Center takes control of the ship once it approaches the harbor to autonomous ships that intensively communicate with the authorities but basically navigate themselves. However, a proliferation of cyber threats might cause the IMO not to relax regulation further or to even impose more restrictions on autonomous shipping (§2.2.3).

Probable: Hydrogen becomes a substantial part of the Dutch energy landscape. To maintain industrial processes in the post-fossil fuel-era, hydrogen may have to be introduced on a large scale towards 2050. The H-Vision document of the Port of Rotterdam foresees the large-scale introduction of hydrogen power to not just the Netherlands but also for Northwestern Europe, with Rotterdam as the hydrogen hub. Stated specifically, by 2050 hydrogen is produced en masse by using (mostly) renewable energy in power-to-gas production plants onshore and offshore. A recent TNO report cited literature reporting that Dutch demand for hydrogen will fall between 10 to 50 billion m3 by 2050. If expansion into the production of synthetic bunker fuels and products in the chemical industry are included, the estimate reaches more than 100 billion m3.[139]

By 2050, hydrogen may be used at a large scale as a renewable energy carrier to overcome long distance electricity transportation losses and discrepancies between renewable energy supply and electricity demand.[140] Hydrogen will hence function as a storage medium for excess green renewable electricity production. With the current production of pure hydrogen based on natural gas reported by TNO to total 10 billion m^3, 2050 could therefore see a five to upwards of a tenfold increase in hydrogen demand.[141] Hydrogen produced offshore will likely be delivered via pipelines (repurposed from initial gas and oil production)[142] and via ships in both its direct- and converted form. Examples of the former have already been introduced, as the Suiso Frontier, representing the world's first hydrogen tanker, was launched in 2019. Examples of the latter are 'hydrogen carriers', carrying the hydrogen in the form of methanol and ammonia.

Probable: Carbon storage (CS) – via ship and via pipeline – introduced on a large-scale. CCS is essential for the Netherlands to achieve its 2050 net-zero target. Large-scale CO_2 storage in depleted gas fields, with CO_2 transported through pipelines (making use of the current gas pipeline network) and by ship to among others the vastly expanded Northern

139 TNO, *The Dutch hydrogen balance, and the current and future representation of hydrogen in the energy statistics*, 2020, pp19-20.

140 TNO, *The Dutch hydrogen balance, and the current and future representation of hydrogen in the energy statistics*, 2020, pp31-33.

141 TNO, *The Dutch hydrogen balance, and the current and future representation of hydrogen in the energy statistics*, 2020, pp19-20.

142 Ontwerp Programma Noordzee 2022-2027, p98.

Lights project in Norway, is likely to become routine business.[143] These projects compensate for the remainder of activities still emitting CO_2 in the Netherlands.

Probable: Sand drenching on an even larger scale. The demand for sand will rise dramatically because of the necessity to strengthen coastal defenses against rising sea levels and the construction of new infrastructure at sea and housebuilding onshore.[144] If artificial islands in the North Sea become a reality (see below), this demand is further exacerbated.

Possible: Arctic Route opens up. The new route between Europe and the Far East, along Russia's north coast becomes the preferable transport option for certain goods.[145] The traffic through the Northern Route to the North Sea increases.

Possible: Multi-purpose artificial islands created out of sea. The Netherlands Environmental Assessment Agency's (PBL) predictions for the North Sea in 2050 include energy hub islands. The islands would be installed near the furthest offshore wind farms and serve as efficient locations for power-to-gas (electrolysis) conversion.[146] Island-building for power-to-gas hydrogen hubs is already in an advanced planning stage in Denmark. The Danish energy island-hub[147] may even see first operations before 2035. The plan is for multiple wind farms to be connected to a few large islands that prepare the electricity for transport through high voltage cables, pipelines (preferably using existing gas pipelines transporting hydrogen), or hydrogen tankers. Neighboring states' grids in turn are expected to be connected to the power island and use excess energy generated in Denmark for domestic consumption. In other words, neighboring states are developing their offshore capacity and ability to transport electricity internationally. PBL outlines two scenarios in which by 2050 such islands exist in the Netherlands, showing these plans do not have to be unique to Denmark.[148]

In addition, such islands might also host data centers demanding a large amount of electricity. The Netherlands is the 'Digital Gateway to Europe', with Amsterdam housing Europe's largest datacenter hub. Combined with the government's determination to minimize CO_2 output, offshore data centers located on energy hub islands can make direct use of offshore wind energy. Microsoft has experimented with an underwater data center and found that these are "reliable, practical and use energy sustainably", enabling more opportunities for data centers on *and* near artificial islands. The Danish consultancy company Ramboll is currently conducting a feasibility study into placing such datacenters on the future Danish Green Lights energy islands.

Possible: Schiphol at Sea. Even if unlikely in 2035, the Dutch government might move (parts of) Schiphol, the national airport, to sea between 2035 and 2050, as spatial pressure on land and demands for a cleaner environment and noise reduction.

Possible: Artificial islands for living purposes. In addition to the development plans and pilots (e.g. the Danish energy island) for artificial island construction to house energy production facilities, towards 2050 additional islands for living purposes might be created. In Denmark,

143 North Sea Energy Outlook, pp23,41,81.
144 Ontwerp Programma Noordzee 2022-2027, pp74-75.
145 Ontwerp Programma Noordzee 2022-2027, pp70,99.
146 The Future of the North Sea, pp46,50,56.
147 See also: *Denmark Greenlights North Sea Energy Island Hub*
148 The Future of the North Sea, pp12,36.

plans to create an artificial island housing 35.000 people to "protect the port of Copenhagen from rising sea levels" have been approved in June 2021.

Unlikely: Nuclear reactors at sea. The discussion on nuclear energy in the Netherlands will reach a critical juncture somewhere in the upcoming 10 years. Nuclear energy will play no part in achieving the climate targets for 2030 but may be in the mix for the 2050 targets. The largest party, VVD, is in favor of nuclear energy to reach the net-zero target by 2050. Since the availability of cooling water is essential, a location by the sea, or indeed at sea, is most likely. A recent study by consulting firm KPMG concluded that the most likely location for a possible new nuclear power plant would be the province of Zeeland, with Noord-Brabant as a possible alternative. In that study, a new nuclear plant at sea is not considered at all.

3.5 Key vulnerabilities of the North Sea in the 2035 timeframe

As the value creating activities in the North Sea and associated infrastructure expand, so do the vulnerabilities for incidental and deliberate distortions – with the latter being the focus of this study. The overarching vulnerability theme is that the substantially expanded future use of the North Sea requires additional security measures and coordination between agencies. Vulnerabilities compound, for instance in the combination of functions – energy, communication, sensors, datacenters – on multi-purpose, offshore platforms or artificial islands which provide malicious actors high-value targets. This section highlights specific key increased areas of vulnerability.

3.5.1 Trade and transport

Increasingly congested sea lanes. Trade and transport on the North Sea will be more vulnerable to disturbances by 2035, as already congested sea lanes will be in even higher use and maneuvering room is further reduced by the growth of other space-consuming offshore activities. A high level of congestion increases the risks of boat-to-boat and boat-to-obstacle collisions. In worst case scenarios – that include accidents as well as deliberate events caused by terrorists – this may cause narrow sea lanes to be blocked. Even today, when ships, especially the largest ships (known as 'marginal ships' because they have very little leeway in terms of maneuvering), get stuck or sink in the Rotterdam approach routes Eurogeul and Maasmond, this may disrupt the port's activities for at least weeks and most likely months. A case in point is the 2012 sinking of the Baltic Ace off the coast of Rotterdam which caused safety risks for shipping traffic for multiple years and required a €83 million investment to salvage it. Moreover, with a gross tonnage (GT) of approximately 23,500, the Dutch Parliament's inquiry stipulated that the Baltic Ace was by no means a large ship.

Increase in and diversification to highly-combustible and poisonous energy-related shipping. Large amounts of combustible and environmentally polluting substances – currently mostly crude oil – are being transported over the North Sea. Crude oil spillage may lead to severe environmental pollution, but the dangers to human lives and human security are relative limited. The decrease in crude oil imports around 2035 will reduce the risk of environmental pollution because of tanker damage or terrorist attacks.[149] However, the number of

149 National Climate Agreement, pp102.

mid-sized LNG tankers will steadily rise towards 2035. Between 2035 and 2050 large scale hydrogen transport, likely carried in the shape of ammonia, methanol or formic acid,[150] and high-pressure CO_2 shipping[151] may become routine business. Exploding LNG and hydrogen tankers have limited consequences for the environment but may impact human lives and health severely. Ammonia represents a prime example of a toxic substance as documented cases of truck explosions leading to multiple deaths and hundreds of injuries have been recorded.[152] LNG tankers, already widely in use Today, are triple-walled to greatly reduce the risk of explosions.

Cargo	Transport volumes	Combustibility	Pollution if destroyed	Release of toxic materials	Average ship size
Crude-Oil	Stable/slight decrease until 2035, decrease towards 2050	Medium	High	Moderately toxic	Large
LNG	Increase towards 2035	High	Low	No	Medium
Hydrogen	Pilots until 2035, sharp increase towards 2050	High	Medium	Highly toxic when shipped as ammonia / methanol	Medium
CO_2 / CCS	Pilots until 2035, sharp increase towards 2050	Medium	Low	No	Medium

Table 9. Energy-related transport on the North Sea; today, tomorrow and beyond

Increasingly higher levels of ship autonomy and automated traffic systems. The presence and use of autonomous shipping and automated shipping guidance systems will likely increase towards 2035, pending relaxation of the IMO regulations. Ships and shipping systems thereby become more prone to exploitation of cyber vulnerabilities.

3.5.2 Energy

Established fossil fuel production is gradually replaced by untested, relatively vulnerable renewable energy production. Table 10 details the projections of key developments in the Dutch energy transition.

Offshore energy-related activity	Contribution to the Dutch energy system		
	2015-2021	2035	2050
Offshore gas production	high	medium	low
Crude oil imports	high	medium	low
LNG	medium	high	low
Wind power	low	high	high
Hydrogen	low	low/medium	medium/high
CO_2 Transport and Storage	low	medium	medium/high
Solar power	low	low/medium	low/medium
Nuclear power	none	none	none/low/medium/high

Table 10. Likely developments of Dutch offshore energy use per source

150 National Climate Agreement, pp179-183; North Sea Energy Outlook, p79; Drift, *Hydrogen for the Port of Rotterdam in an International Context – a Plea for Leadership*, 2020, pp16,17,23. Shipping Renewable Hydrogen Carriers | TU Delft Repositories

151 National Climate Agreement, pp112-113.

152 LLoyds Register, *Hydrogen and Ammonia Infrastructure*, 2020, p11.

Offshore wind power production relies on a few single points of failure. The currently dominant system of gas pipelines is relatively dispersed, except for a few specific high concentration points within the infrastructure. The large-scale installation of wind farms towards 2035 and beyond relies on congregated offshore transformer blocks that deliver electricity – via congregated cables under the sea – to a few landing points on the coast. Greater single-point of failure dependency means a greater share of grid neutralization when a transformer block, a congregated cable, or a landing spot is sabotaged.[153] Problems with undersea high-voltage cables are fairly common today. Fixing these cables is a time-consuming process involving many stakeholders.[154] In addition, storage possibilities for electricity are limited, whereas oil and gas can be easily stored to create reserves for immediate mitigation of supply interruptions. Once wind power is introduced on a large-scale towards 2035, and on an even larger-scale towards 2050, the interruption of supply caused by congregated high voltage cables being cut, transformer blocks malfunctioning or landing points disrupted will likely result in more blackouts.

	Gas and oil pipelines	High voltage cables
Current trends	Being gradually decommissioned and/or repurposed	Vastly expanding
Effects of unit sabotage	Low: only short-term losses / inconveniences that can be compensated	High: direct impact on electricity supply to both industry and residences
Critical junctures (single-points of failure)	Few, except for the congregation centers offshore where multiple pipelines converge	Many, undersea congregated cables, offshore transformer blocks, the onshore landing spots
Level of vulnerability	Low	High
Environmental risks	Limited due to safety valves	Negligible

Table 11. Vulnerability of pipelines vs. cables

The offshore energy grid becomes more vulnerable to cyberattacks. Already today, a cyberattack can infiltrate the entire or large parts of the network of gas and oil platforms, whereas a physical attack on a platform only disables the gas or oil production locally.[155] Cyberattacks are expected to grow from a nuisance today to attacks that need to be countered constantly in the period up to 2035.[156] High-impact incidents such as the recent hacking of a major US pipeline is likely to become more common as virtually all critical infrastructure becomes digitized. In fact, in ongoing conflicts such as between Iran and Israel or India and China, countries are known to attack each other's critical infrastructure – not to destroy but infiltrate or impede it.

Unmanned and abandoned gas platforms can be easily entered. The number of unprotected offshore places for threat actors to operate from will proliferate with the large-scale decommissioning of gas platforms likely to take place between 2021 and 2040. Unmanned or abandoned platforms can be used as a potential operating site or a safe haven for organized crime.[157] Repurposing of these platforms for undersea CO_2 storage and hydrogen production could negate this development, provided that these platforms operate with crews onboard.

153 Ontwerp Programma Noordzee 2022-2027, pp53-54.

154 Expert interview

155 Expert interview

156 Feike Hacquebord and Cedric Pernet, *Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry*, 2019, pp3–4.

157 Expert interview

Use of highly volatile hydrogen on energy islands and platforms. The use of offshore platforms towards 2050 for electricity-to-molecule conversion goes hand in hand with the production of highly combustible substances.

Our economy and society increasingly depend on underwater communication cables. The number of telecommunication cables connecting the Netherlands to the UK and across the Atlantic Ocean will only increase, as will the data traffic and the dependency of our economy on it. Three specific new cables will be laid before 2035 connecting the Netherlands and the UK. Even so, due to the relatively high costs of subsea cables and pipelines, there is a high reliance on a relatively low number of cables as compared to more plentiful, cheaper on land cables. With seabed warfare a distinct focal point of Russia's naval military strategy, protection of undersea cables becomes important. Where high voltage cables are generally buried below the seabed for protection against accidental damage by e.g. ship's anchors, fishing nets, and dropped objects, telecom cables usually merely rest on the sea floor. Specific protection against deliberate damage and/or tapping is currently minimal, but solutions exist.

3.5.3 Fishing and aquaculture

Uncertainty over fishing arrangements as part of broader emerging tensions with the UK. Brexit created a new regulatory reality between EU and the UK, as customs and hard borders returned. Until 2026, an arrangement regulates access to each other's waters, including yearly decreasing fishing quota for the EU in UK waters, a quota that was already reduced by 15% in 2021. After 2026, new arrangements will be achieved through annual and likely contentious renegotiation efforts. Considering fishing was "one of the final sticking points in the post-Brexit trade talks", it is not unlikely that individual fishing ships ignore the agreements and demarcations at sea. Lower fishing quota for EU ships in UK waters and vice-versa might lead to trespassing, for instance by turning off AIS-transmitters. In other parts of the world – such as the East China Sea and the South China Sea – escalating conflicts over fishing are routine business. The Cod Wars between Iceland and the UK underline that tensions over fish between states can also increase substantially in Europe.

4 The Evolving Threats Facing the North Sea

The previous chapter gives substance to the growing value-creating activities in the North Sea, and to the vulnerabilities for disruption of these activities and the associated infrastructure. In this chapter, we consider these vulnerabilities as possible entry points for malicious exploitation by state or non-state actors, thereby threatening one or more national vital interests as listed in Table 12. We will not explicitly consider natural causes or human errors causing incidents or accidents. However, many deliberately created incidents resemble accidental calamities, with no difference in terms of damage and follow-on consequences. Whether two ships collide and block a main shipping artery by accident or by terrorist intent, the impact is much the same. The effort to prevent or avoid the one or the other differs, although again some commonality is likely.

Vital interests	Definition and application to the North Sea
Territorial security	The undisturbed functioning of the Netherlands and its EU and NATO allies as independent states in the broad sense, or territorial security in the narrow sense. This includes the sovereign use of North Sea as laid down in the Law of the Sea. It says that a country may claim an area extending 12nm from its coast as its own territorial sea; and can exploit 200nm of the water column beyond its coast as its exclusive economic zone.
Physical security	The undisturbed functioning of people in the Netherlands and its surroundings. Projected on the North Sea, this includes absence of attacks by state and non-state actors that threaten death, illness and injuries and damage to surroundings, including ports and offshore infrastructures.
Economic security	The undisturbed functioning of the Netherlands as an effective and efficient economy. For the North Sea, this includes the undisturbed passage of vessels and goods into to and from ports and offshore infrastructures.
Ecological security	The undisturbed survival of the natural living environment in and near the Netherlands. This includes absence of threats that can lead to environmental disasters in the North Sea caused by leaks or explosions of fuels and equipment. For example, crashes of vessels, attacks on vessels or by a (purposeful) disregard of safety standards regarding transport and storage of harmful petrochemical substances offshore or in ports.
Social and political stability	The undisturbed survival of a social climate in which individuals can function undisturbed and groups of people can live together according to the Dutch democratic constitutional state and its shared values. This includes protection from activities such as drug and human trafficking, or attacks that can undermine the ability for persons to function undisturbed.
International Law & Order	The functioning of the international system of standards and agreements aimed at international peace and security. This requires that persons and vessels in the North Sea respect laws and regulations on conduct at sea, including maritime borders and boundaries, and relations between vessels and persons, as stipulated in national and international laws.

Table 12. Vital interests from the National Security Strategy 2019 *as applied to the North Sea*

This chapter distinguishes between three threat classes: (1) criminal and terrorist threats stemming from non-state actors; (2) hybrid threats ultimately stemming from a state actor, but typically acting through so-called proxies; and (3) military threats that arise in escalating crises. For each of these three threat classes, we categorize typical threat actions.

Each category is illustrated by a short 'story line', nominally placed in the 2035 timeframe (although many could also apply to today), linking back to the analysis of value creation in the North Sea and associated vulnerabilities in chapter 3. Below, a qualitative assessment is given of the likelihood of each threat category materializing in the period up to 2035, and of the possible impact this may have. *Likelihood* refers to the expected rate of occurrence of incidents that may lead to consequential damage (i.e., beyond the organization / object / agency directly affected). *Impact* refers to the volume and scope of that consequential damage, potentially affecting vital national interests. [158]

Note that the distinction between the three threat classes is far from absolute: the various threat actors take aim at similar targets, have overlapping ways and means, and their actions may have comparable effects. Even if their ultimate motives can be quite different, they can also pragmatically work together, generating considerable overlap between criminal & terrorist and hybrid threats on the one hand, and hybrid and military threats on the other. Criminal & terrorist activities can be part of a hybrid campaign, with the perpetrator acting as proxy forces or supported by a hybrid state actor.[159] In turn, Russian and Chinese hybrid activities are part of a comprehensive strategy that covers the entire spectrum of conflict, including the military high-end of that spectrum, based on the ability to "credibly threaten to inflict, at any level of escalation, a 'prescribed dosage of damage' sufficient to persuade an enemy to de-escalate but not so large as to create new stake and resolve for the enemy."[160] What this means for the current study is that the sections on physical violence for each of the three threat classes (§4.1.1, §4.2.1, and §4.3.1) are closely linked. The same holds for the three sections on cyber threats (§4.1.2, §4.2.2, and §4.3.2). To avoid duplication, the related sections have a distinctive focus, in line with the illustrative story line for that threat category. This focus, however, can – mutatis mutandis – to a large extent be applied to the other threat classes as well.

4.1 Criminal & terrorist threats

Criminals and terrorists tend to function in loose networks based on reputation, experience, and trust; in groups with an established hierarchical structure; or, occasionally, as individuals. Organized crime / groups (OCGs) tend to be opportunistic actors often involved in multiple criminal activities simultaneously and primarily motivated by financial gains and not by the desire to destabilize the political governance systems or countries' economic activities (although this may indirectly be the result of their actions). Terrorism / terrorist groups (TGs) on the other hand, seek to attain political objectives and often have a political agenda. Today, in contrast to some 20 years ago, the two are not always easily separated, as terrorists often rely on criminal activities for funds. There are several links between OCGs and TGs, with the connections giving rise to hybrid organizations. While the links between OCGs and TGs are a matter of serious concern for the international community, a far greater problem is that political power holders are involved as third parties, whereby state facilities (e.g. diplomatic channels) are used as vehicles and cover for violent and predatory crimes across international

158 The combination of the two, Likelihood X Impact, corresponds to a standard way of risk assessment. This approach is for instance used in the Dutch *National Risk Assessment* as part of the *National Security Strategy*. This chapter provides a qualitative Likelihood X Impact assessment for the threat categories facing the North Sea.

159 As made explicit in Frank Hoffman's definition of a hybrid threat: "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives." Frank Hoffman, *Hybrid vs. Compound War*, 2009.

160 Brad Roberts, *Toward New Thinking About Our Changed and Changing World*, 2020, p6.

borders.[161] OCGs/TGs tend to depend in large part on corruption, bribery, and threats as entry points into target systems. They can have contacts in port and security operations, enabling them to infiltrate and manipulate security systems. Depending on their structure and size, they may also have their own equipment including smaller vessels, weapons, explosive devices, and surveillance technology enabling them to carry out threats and attacks.[162]

	Criminal & terrorist threats	Illustrative story lines of possible threat manifestations
	**Piracy and hostage taking**. Criminal or terrorist activities directed at vessels or maritime structures	Terrorists have raided a ferry boat and have taken personnel and passengers as hostages. They have threatened to successively kill the hostages if their financial and political demands are not met (blackmail).
	**Cybercrime**. Criminal or (state backed) terrorist activities that attack or take control over ICT systems of vessels or maritime structures	A 160-ton cargo ship with autonomy level 3 (remotely controlled without seafarers on board) is digitally hijacked. The onshore command center in Rotterdam has lost control of the autonomous ship, with apparently all safety measures failing. If 10 million euros worth of bitcoins is not transferred within 24 hours, the hackers collective threatens to ram it into an offshore hydrogen production platform.
	**Smuggling and trafficking**. Criminal activities that use the seas, such as human trafficking and smuggling of drugs and arms	Fully submersible narco-submarines are now also involved in arms trafficking, being very difficult to detect through existing surveillance systems. They threaten the safety of coast states' citizens as well as economic security by facilitating a shadow economy.
	**Unauthorized entry**. Criminal activities that violate a coast state's sovereignty, such as illegal fishing and unauthorized entrance of a state's internal waters	A Dutch fishing vessel has rammed a British fish trawler operating in violation of post-2026 fisheries agreements between the UK and the EU. The fishing war between Dutch, French and British fishermen thus reached a new low. Fishermen demand that the rules are enforced and that escort vessels guarantee their safety.
	**Environmental crimes**. Criminal activities that violate international law, such as dumping and discharging of polluting materials	An international criminal network defies strong international environmental regulations by large scale clandestine dumping of polluted and toxic materials in the North Sea near Natura 2000 protected areas, making large profits.

Table 13. Categories of criminal & terrorist threats and illustrative story lines

4.1.1 Piracy and hostage taking

Piracy and hostage taking are serious security risks for offshore energy companies. Oil and gas rigs have some of the most expensive and complicated pieces of machinery on the planet, which leaves them prone to attacks. A *Chronology of Attacks on and Unlawful Interferences with Offshore Oil and Gas Installations, 1975 – 2010* lists some 60 events. Incident scenarios include abduction of workers, armed intrusion, hostage-taking, bombing and use of explosives, military strikes, and unauthorized boarding. The most common scenario is armed intrusion and abduction of offshore workers.

Although piracy and terrorism at sea remains centered in hotspots like of the Somalian or West-African coast, Western waters are not immune. In response to several false alarms and attempted attacks, states have conducted anti-piracy and anti-terrorist exercises at North Sea rigs since the early 1960s and 70s. Congestion at sea can lead to a complex environment which OCGs and TGs can exploit. Commercial vessels are tightly controlled, registered, and monitored in the North Sea, but recreational boats face relatively few and more lenient regulations and can be easily used by malicious actors. Vessels transporting CO_2 could become attractive physical targets for TGs, given their small size and high maneuverability on North Sea's narrow shipping lanes.

161 Alex Schmid, *Revisiting the Relationship between International Terrorism and Transnational Organised Crime 22 Years Later*, 2018.

162 *Security Threats and Challenges to Maritime Supply Chains*, 2010, p6.

OCG/TG actions can have dire economic consequences. Entire networks could be put offline if critical offshore nodes are targeted physically and/or digitally, potentially with cascading effects. For manned offshore platforms, human lives could be lost in hostage-taking situations. If oil rigs or tankers are hijacked, terrorists could threaten to cause environmental damage.

4.1.2 Cybercrime

Moving forward, secure ICT systems will be key to control and monitor navigation systems. While 'smart shipping' contributes to the competitiveness, safety, and sustainability of the maritime industry, it also introduces additional vulnerabilities. The safety and security of onboard and ship-to-shore systems are at risk, including traffic and cargo management, propulsion and power control, and onboard communication. These concerns are compounded by the risks of cybercrime affecting static critical infrastructure at sea (which is looked at in §4.2.2).

Cyberattacks on the maritime industry's systems have increased by 900% between 2017 and 2020, not accounting for the likely high number of unreported incidents.[163] The COVID-19 pandemic has had notable impact on this trend: since February 2020, the Naval Dome company specialized in cybersecurity of vessels has reported a 400% increase in attempted cyberattacks. While large-scale cyberattacks are minimally observed in the North Sea today, the increasing digitalization of systems observed vulnerabilities make this threat highly relevant. Vulnerabilities include outdated and unsupported operating systems, software, and inadequately trained staff. Absent, insufficient, or untested contingency plans and procedures also make ships and onshore systems more vulnerable to cybercrime.[164]

When a vessel is digitally hijacked, it may be held until the perpetrator's demands are met. More impactful is setting the vessel's course to purposively crash into other ships or facilities, especially those carrying highly combustible LNG or ammonia. Vessels that are controlled remotely can thus become massive weapons with the potential to disrupt all sea traffic in the vicinity. Malicious actors can deliberately insert false signals (spoofing) or deny reception through competing signals (jamming) that can confuse state-of-the-art Global Navigation Satellite Systems. Spoofing a vessel's navigation system can have geopolitical consequences. For instance, in 2016, spoofing may have played a role in misdirecting two US Navy patrol boats in the Persian Gulf by manipulating their GPS system. [165] In more subtle ways, a large vessel receiving false coordinates could also be directed to shift course and enter the wrong shipping lane in the North Sea, causing a grounding or a collision. Shallow waters require large ships to take a specific course to prevent them from getting stuck and causing a blockade at chokepoints such as Eurogeul and Maasmond.

As technology progresses, OCGs and TGs may hence become increasingly able to carry out cyberattacks against the maritime industry. Compared to conventional attacks, cyberattacks do not require much human or financial capital. The attribution and especially the prosecution of an attack originating from a rival state remains difficult. The economic impact can be severe. The NotPetya ransomware attack in 2017 forced shipping giant Maersk to interrupt operations worldwide, was expected to cost the company up to $300 million.[166] If a shipping company's systems are hacked, the disruptions in supply chains can lead to large financial

163 Andrej Androjna et al., *Assessing Cyber Challenges of Maritime Navigation*, 2020, p1.

164 BIMCO, *The Guidelines on Cyber Security Onboard Ships version 4*, 2020, p17.

165 Why vessels passing near Iran may have trouble staying on course | The Economist.

166 Note that the NotPetya malware did not specifically targeted Maersk, but rather accountancy software with Ukraine as its main target. It then spiraled out of control, with the Maersk incident a 'side-effect'.

losses for many companies in those chains. In worst-case scenarios, this can even threaten social stability. Loss of confidence in security systems can spur social unrest and undermine government legitimacy. Cybercrime is already a major threat with the potential of "paralyzing a society."[167]

Much of the maritime transportation and energy sectors consist of separate subsystems that are fully or partly controlled by private actors. The first line of defense is thus the private sector, not the government. The Dutch government provides some support for private companies in becoming resilient to cybersecurity threats through advice and information sharing. It also has (some) powers to intervene in the processes of vital suppliers – with this role likely to expand through new initiatives and laws.[168]

A final remark concerns IP theft. As the North Sea houses very high-tech companies, this certainly is an area of concern within the context of offshore cybercrime.

4.1.3 Smuggling and trafficking

The North Sea crowded and complex shipping lanes offer a rich breeding ground for trans-national crime, including drug, weapons, and human trafficking. A substantial amount of drugs from South and Central America enters Europe through the maritime domain.[169] The discovery of the bodies of 39 Vietnamese in Essex who had travelled in an unreported container via the Port of Zeebrugge in Belgium, showcase the extent of human trafficking issues. Migrants cross the Dover Strait, with boats chartered by middlemen. Chances are that refugees may begin to use more northern routes to reach the UK via the Netherlands.

Most containers that enter or transit ports remain unchecked or are subject to a quick scan that often fails to detect illegal goods. In the Port of Rotterdam, yearly only 40.000 containers out of 7-8 million are checked with x-ray scanners, based on a risk assessment of the location, destination and contents of the container. Smugglers employ numerous indigenous methods including concealing drugs in walls, ceilings or floors of containers, hollowed out fruits and vegetables, engines, inspection hatches of the engine compartment of refrigerated containers; underneath the waterline in torpedoes attached to vessels; by dropping drug packages off at sea after hiding on board of large sea-vessels; or pack drugs in carryalls placed near the doors of containers, which are then taken out of the container and driven off the terminal, the so called 'rip-off' method.[170] Fishing boats have become targets of the 'drop off' method due to the relatively little surveillance on their activity. Instead of bringing a large container ship with drugs to the shore, criminals throw bags filled with drugs and a transmitter into the water, where it is picked up by fishing boats. If the operation fails, cocaine often ends up as waste on the beach as happened in Noordwijk in 2015, when hundreds of kilos of drugs washed up ashore.

As surveillance becomes more robust, smugglers invent new indigenous ways of trafficking including the use of narco-submarines to reach the Spanish coast. These submarines are becoming increasing sophisticated in terms of size, speed and stealth. Newer prototypes

167 NCTV, *Cyber Security Assessment Netherlands*, 2020, p7.

168 See *Outcomes of exploration of legal powers for digital resilience and policy responses WODC reports* (Letter to Parliament), February 2021.

169 European Monitoring Centre for Drugs and Drug Addiction, *European Drug Report: Trends & Developments*, 2019, p26.

170 Robby Roks, Lieselot Bisschop, and Richard Staring, *Getting a Foot in the Door. Spaces of Cocaine Trafficking in the Port of Rotterdam*, 2020, p7.

are fully submersible, while first types are only semi-submersible. In March 2021, Europol seized the first narco-submarine made in Europe off the Spanish coast. To neutralize security checks, lowering the risk of being caught, criminals direct their attention to employees and customs officers to pressure staff to provide criminals with critical information, access to port areas or to physically transport drugs on their behalf. An estimated one in seven employees at the port of Rotterdam have been approached by a criminal at least once. Criminals exploit social, political, and financial grievances among staff and often offer large sums of money for cooperation. Criminals working together with hackers have managed to transport drugs by infiltrating computer systems at ports that track and control the movement of shipping containers. Hacks can occur without immediate notice. For over two years, hackers infiltrated the cargo tracking system in the port of Antwerp to identify the containers in which drug smugglers had hidden drugs and drove the identified containers from the port to sell the drugs elsewhere.

Trafficking leads to economic and security consequences for the countries involved. The value of illicit drug trade in the EU is estimated at a minimum of €30 billion yearly.[171] The sheer financial volume of the drug trade guarantees that it will remain the main challenge towards 2035 and beyond. Although drug trafficking has limited impact on the continued operation of vessels, it undermines international law & order at sea and risks undermining the security of persons in private vessels, personnel at ports and fishers.[172] Drugs trafficking also has negative implications on social and political stability. The automation of logistical processes towards a 'fully fenced and high-tech environment' using automation, artificial intelligence, big data, internet of things and blockchain offers opportunities to improve the resilience and security against traffickers.

4.1.4 Unauthorized entry

States have agreements on who has what kind of access to resources at sea. Denial or access to fishing grounds, excessive fishing in international waters and disagreements about fishing quotas can cause clashes between fishermen of different flag states.[173] Sixty years ago, fishermen from the UK and Iceland clashed over access to fishing grounds off the coast of Iceland; a dispute that lasted over 20 years. Conflict again erupted between the UK, EU, Norway, Iceland and the Faroe Islands over mackerel quotas; and between the UK and the French over access to scallops. The possibility of hostile and violent clashes erupting between fishermen in the following decades remains on the horizon. Fishing rights stood central in the discussions on Brexit. While the question of fisheries "was economic peanuts," at the same time it was "a political dynamite" that could become a key point of contestation between fishers and their flag states. As the EU/UK deal slowly transfers the greater share of fish from UK waters away from EU Member States, fishers may try to enforce states to meet their demands in violent ways. This could result in the involvement of escort vessels or patrol ships of the respective navies to protect their fishermen; which, in turn, could further escalate the situation and result in state-on-state conflict at diplomatic, economic, and in the worst case, military levels. In addition, social instability could result from fishermen manifesting their frustrations in the form of protests or refusal to obey with new rules

Next to bona-fide fishers clashing, illegal, unreported, and unregulated (IUU) fishing is another problem caused by weak monitoring of commercial vessels, leading to environmental issues.

171 European Commission, *EU Agenda and Action Plan on Drugs 2021-2025*, 2020, p1.

172 UNODC, *Global Report on Trafficking in Persons 2020*, 2021, p49.

173 Christian Bueger and Timothy Edmunds, '*Blue Crime: Conceptualising Transnational Organised Crime at Sea*', 2020, p5.

IUU might target fish protected species or use prohibited hazardous techniques such as cyanide or dynamite fishing.

From an economic point of view, a (temporary) disruption in fishing activities would impact global supply chains and lead to substantial – but not huge – financial losses.

4.1.5 Environmental crimes

Illegal discharging of polluting materials remains a pertinent problem in the maritime domain. Criminal organizations engage in discharging for financial purposes, by blending hazardous substances with fuel oil and selling it illegally, while terrorists seek to undermine the legitimacy of their opponents, by causing purposeful oil or chemical spills.[174]

In ocean shipping, heating oil is mainly used as fuel that is formed by residues from petroleum refineries. These residues are a thick slurry that needs to be mixed with other liquids or "blend components" to create a consistency that can be used to power vehicles.[175] What substances are used for this and whether these are legal, is not always clear. Companies often fail to properly register residual flows and fail to obey European substances regulations making it difficult, if not impossible, to determine what is in the fuel mixtures. The need for companies to get rid of this waste, and ability to turn it into a profitable good is an attractive business model that enables criminals to make profits of otherwise waste products, and to propel their vessels at much lower prices. Blended fuels can cause engine failure, leading vessels to drift and endanger other vessels and infrastructures in the vicinity. This is not a new problem in the North Sea. It is especially relevant in the Netherlands since the Port of Rotterdam is the largest bunkering port for fuel oil in Europe. Criminal actors can also hold the environment ransom as a weapon to threaten states or undermine their legitimacy. The Israeli-Iranian dispute over an alleged purposeful oil spill by Iran in Israel's waters, causing great environmental damage, shows the potential of using illegal discharging as a weapon.

While the shipping industry is subject to increasingly rigid regulations, the limited monitoring in the ship fuel chain and the low chance of being caught provide the incentive to mix hazardous (waste) substances into fuel oil. The transition toward more environmentally friendly fuels such as LPG, LNG, methanol, Ammonia or biofuels and shift away from heavy fuel oils will decrease the market for illegal fuel oil into 2035, making cases easier to detect.

4.2 Hybrid threats

While maritime hybrid warfare is not new, the diversity, frequency, and intensity of hybrid threats at sea has increased and is likely to increase further into 2035. Hybrid actors deploy means with low risk of detection and attribution, such as unmanned underwater vehicles and commercial vessels (or look-alikes) that have military sensors or weapons built into them. These vessels can also act as mother ships for air, sea and undersea unmanned vehicles. Non-military hybrid means such as media propaganda, deception, and sabotage are also employed by state actors in a maritime context.

174 UK Department of Transport, *Maritime 2050: Navigating the Future*, 2019, p170.

175 Ab de Buck and Jasper Faber, *Een Analyse van Bunkerolieketen*, May 2011, p11.

Hybrid actions are typically carried out in three stages. The first phase is characterized by surveillance and intelligence gathering to pinpoint the opponent's vulnerabilities. The intention is both to subtly influence the situation and to establish presence. In the second phase, subtle and covert threats are introduced that enable the attacker to avoid attribution or retribution when carrying out the threat. Once the actor has established presence, it follows with overt threats that are direct and can be clearly attributed to the attacker. The impacted state can respond with economic sanctions or by directing the attention of its special forces toward the territory of the attacker. Escalation to military conflict is the final, most serious consequence.

The expanding economic, political, and strategic value of the North Sea makes it a lucrative target for hybrid actors, with an abundance of targets: private and commercial transport, shipping, oil and gas rigs, pipelines, wind energy infrastructures, buoys, coastline clutter, small islands, and vast underwater infrastructures.

	Hybrid threats[176]	Illustrative story lines of possible threat manifestations
	**Sabotage**. Hybrid actions to deliberately destroy, damage, or obstruct vessels or infrastructure at sea for political or military advantage in peace time	A Russian coastal vessel has collided with a cargo ship in the approach route from the North Sea to the Nieuwe Waterweg, causing both ships to sink. The Maasgeul is effectively blocked for large container ships. The captain of the Russian vessel claims that his ship was hijacked. However, it is believed that the collision may be deliberately caused, as part of an ongoing Russian campaign to undermine the social and political stability in the Netherlands.
	**Cyber operations**. Hybrid actions that are directed at covertly monitoring or interfering with ICT systems of vessels or maritime structures	Wind-based electricity generation in the North Sea has been interrupted. A long-term cyberoperation appears to have caused system failure, as hackers have infiltrated several transformer blocks simultaneously. Neither the companies nor government agencies were aware of the cybersecurity breach, currently believed to come from a group connected to the Russian government (Russia relies heavily on gas/oil export and has a strategic gain in undermining the trust in wind-based energy). The massive shortage of electricity needs to be addressed rapidly.
	**Espionage and interference**. Hybrid actions to gather intelligence in peace time, for instance by using civil vessels equipped with advanced sensors for military purposes or by tapping or compromising communication cables at sea	Belgian, German, and Dutch security officials have expressed grave concerns over Chinese cargo ship fitted with advanced sensory systems – including stealthy UAVs with sensor payloads – that are presumably used for surveillance and espionage activities on the North Sea, in the harbors of Antwerp, Rotterdam and Hamburg, and in coastal areas. It is yet unclear whether such alleged spying activities are aimed at industrial or military targets, or both.
	**Incursions**. Hybrid actions, often by military vessels, that violate a coast state's sovereignty, either openly or covertly, to probe defenses or to 'show the flag'	Over the past years, Russian naval exercises in the North Sea have dramatically increased. The passage of Russian war ships through the North Sea on their way to and from the Mediterranean has become an almost monthly routine. Fears exist that these passages are also used to launch and dock unmanned underwater vehicles (UUVs) that operate in coastal waters and harbors along the North Sea coast. The legality of these activities is disputed. In a joint statement, the EU, Norway, and the UK have condemned this regularly display of Russian maritime military muzzle in the North Sea as "undermining the international peace and security" of the EEZs concerned and therefore a violation of international law.

Table 14. Categories of hybrid threat actions and illustrative story lines

4.2.1 Sabotage

Wind farms including platforms that house transformer blocks are rapidly expanding and becoming a key part of the Netherlands national energy grid, in addition to early-stage pilots in offshore hydrogen production. If malicious actors gain access to critical infrastructure, the possibilities to cause damage are substantial. Even false alarms can result in substantial costs.[177] Abandoned platforms, where surveillance tends to be lower, are particularly vulnerable to attack. The activities around wind turbines are also vulnerable. Small service boats

176 Note that some of the criminal & terrorist activities above can also be used as part of a hybrid campaign.

177 RAND Corporation, *Potential Threats to Offshore Platforms*, 1988, p4.

roam around wind farms daily, with staff that often lacks security clearance and is not subject to tight surveillance. These actors may be put under pressure by outside actors or may naively allow others to embark.

Possibilities for sabotage are not limited to static critical infrastructures but may also target moving vessels. Despite advances in technology and navigation systems, inadvertent collisions still occur at sea, resulting in the loss of tens of vessels a year globally.[178] Human error remains a key factor contributing to collisions, suggesting that such activities could also be carried out deliberately but covertly, as part of a hybrid campaign to undermine social and political stability. Adversaries may hack the targeted vessels' GPS system to falsify its location, remaining undetected until it is too late. In a worst-case scenario, vessels collide and sink at a strategic location, blocking vital routes. Large vessels are unable to stop immediately and are often difficult to maneuver quickly, meaning lack of an early response likely leads to a collision. The salvage and re-floating of a vessel is a complex, costly and time-intensive operation, requiring a flotilla of dredgers, diggers, and tugboats.[179]

The sinking of the ship and release of fuel and other chemicals may cause tremendous ecological damage to the seabed and coastal areas with potentially long-term effects. It is also likely to have immediate economic impact. The blockage of the Suez Canal by the *Ever Given* resulted in an estimated loss of the Canal's revenues between $14m-$15m (£10.2m-£10.9m) for each day of the blockage.

While the conditions at the North Sea would allow a pre-empted collision to have grave impact, the likelihood that adversaries such as Russia would carry out such an action seems limited. It would be a costly operation, resulting in the damage or destruction of expensive cargo vessels, and potentially crew members. The negative impact on social and political stability also appears limited, with other tactics such as disinformation campaigns and cyber-attacks seemingly better means to an end.

4.2.2 Cyber operations

The cyber realm allows hybrid actors to (simultaneously) monitor activity, interfere with surveillance systems, and gather intelligence. The aim might be to strengthen the opposing state's information position and with it geopolitical or strategic advantage, sabotage and destruction of an adversary's digital and physical assets.[180] Threat actors can infiltrate their adversaries' cybersecurity systems with the purpose of attacking at a later stage rather than taking immediate action.[181]

Cybersecurity is a growing issue in the oil and gas sector, since critical network segments in production sites, which used to be kept isolated, are now increasingly connected to outside networks or partly online. In doing so, there is a need to update outdated systems from the 70s and 80s. As the oil and gas industry continues its march towards greater digitalization, remotely operated platforms represent the future of offshore drilling. In February 2019, Norwegian energy giant Equinor launched the world's first fully automated oil and gas platform. With no living quarters, the North Sea rig is entirely unmanned and requires only one or two maintenance visits a year. Remote operations introduce new vulnerabilities for

178 European Maritime Safety Agency, *Annual overview of marine casualties and incidents 2019*, 2019, p61.

179 https://theconversation.com/suez-canal-container-ship-accident-is-a-worst-case-scenario-for-global-trade-157802

180 *Perspectives on Cyber Security for Offshore Oil and Gas Assets*, 2021, p4.

181 *Responding to the Evolving Cyber Threat Landscape in the Oil & Gas Sector*, 2018, p5.

cyberattacks and the lack of on-site personnel may impede a timely response to security threats. Decommissioned and abandoned platforms present likewise security challenges, as do wind farms.

Hybrid actors targeting energy grids to undermine the adversary's internal stability has a historic precedent in the cyberattack on Ukraine's power grid in 2015.[182] As energy production moves offshore, the North Sea may also become a target for such attacks. Renewable production platforms are vulnerable for various reasons. Remote monitoring and control create new entry points for cyberattacks, as do weak cybersecurity controls. Security systems are often outdated, complex or poorly integrated, with considerable disparity in maturity levels between information technology (IT) and operational technology (OT) systems.[183] Malicious actors could infiltrate into the electricity production and transmission system to assume control over the functioning of each component of the system. Detection systems can also be targeted, as hybrid actors would manipulate data to avoid the detection of a physical security threat or espionage.[184] The offshore oil infrastructure also remains vulnerable to cyber-induced damage in production systems by shutting down production, alarms and causing explosions through heightening the pressurization of oil in the pipeline.[185] For instance, in 2012 Saudi Aramco suffered a security breach in their network, leading to the wiping of 35,000 computers and severely affecting their operations.[186]

The impact of cyberattacks depends on its target. Targeting individual wind turbines may have minimal impact.[187] But energy relies on a few critical nodes – such as the transformer blocks in wind farms – that can be identified and targeted, especially if systems are designed for efficiency rather than security. Cyberattacks on critical nodes could cause huge power outages across the country with economic, and follow-on political and social impact. Such attacks may incite conflict between states (e.g., Russia and Ukraine). Digital sabotage of critical infrastructure is already considered to be one of the biggest cybersecurity threats in the Netherlands.[188] As critical infrastructure in the North Sea expands, offshore structures become lucrative targets for adversaries seeking political or economic gains.

4.2.3 Espionage and interference

By using civilian vessels equipped with advanced military equipment, hybrid actors may gather intelligence on North Sea states while avoiding detection. Espionage can be paired with foreign interference activities, through which a country's economic, social, or political decision-making is indirectly steered towards the foreign actor's interest.

Critical infrastructure in the North Sea makes a lucrative target for espionage and interference operations. The North Sea has already become a potential target for Russian forces, which are taking significant interest in subsea cable networks. These are often poorly protected and can be damaged or cut, leading to disruptions in communications as well as long and costly repair times.[189] Reconnaissance vessels are fully equipped with first class surveillance

182 *How Cyber-Attacks in Ukraine Show the Vulnerability of the US Power Grid*, 2017, p31.

183 Accenture, *Building Greater Cyber Resilience in Renewables*, 2020, p5.

184 Lauren R. Shapiro et al., *Trojan Horse Risks in the Maritime Transportation Systems Sector*, 2018, p73.

185 Iosif Progoulakis et al., *Perspectives on Cyber Security for Offshore Oil and Gas Assets*, 2021, p4.

186 Jamie Crandal, *Cybersecurity and Offshore Oil: The Next Big Threat*, 2019, p711.

187 Unless if there is a horizontal ICT architecture, which is the main issue with energy networks. A lack of hierarchical segmentation means once you are in, you have access to the entire network.

188 National Coordinator for Security and Counterterrorism, *Cyber Security Assessment Netherlands*, 2020, 15.

189 CCDCOE, *Strategic Importance of, and Dependence on, Undersea Cables*, 2019, p2.

technologies and cable tampering capabilities, posing as commercial vessels to avoid detection while gathering intelligence. If the idea of data centers located in the North Sea takes off, this is another potential target.

Technological advancement is the key determinant of how hybrid actors operate. High-tech espionage equipment is becoming increasingly compact and more difficult to detect. As systems become more automated, data cables and centers will become important targets for malicious actors when gathering intelligence. The threat is already present, with actors such as Russia or China constantly improving their capabilities to act while remaining in the gray zone. Increasing automation of the maritime sector, offshore industry and critical infrastructure, means that information advantage over adversaries will become an even greater asset in hybrid warfare. The impact of espionage is not necessarily evident on a short-term, but the more leverage a foreign actor gains, the more severe a future attack can be.

An emerging concern relates to the increasing activities of foreign state-owned enterprises (SOEs) in the European maritime industry. Both Russia and China use SOEs to further their geopolitical agendas. For Chinese SOEs, the distinction between commercial goals and political objectives is blurry, as both are pursued simultaneously.[190] Especially its central level SOEs, like COSCO shipping, are considered enormously important assets and are legally obliged to have a Chinese Communist Party (CCP) committees, which are "at the center of power in running SOEs". Chinese SOEs entering the European maritime industry means that the Chinese government simultaneously builds influence in the region. This economic influence could then be used to interfere in (geo)political issues when deemed necessary. Chinese SOEs in the shipping or dredging industries have for a long time been supported through state-backed loans and subsidies.[191] COSCO has a majority stake of 85% in the Port of Zeebrugge. CK Hutchinson Holdings, registered in the Cayman Islands and headquartered in Hong Kong, is the largest terminal operator in Rotterdam. While their operations are commercial on the short term, SOEs influence over European (and Dutch) port facilities and maritime trade is expected to become greater and politically oriented on the long term as EU-China relations become more contentious.[192] Chinese SOEs have also been trying to gain a larger share of the European and global dredging market. Cargo ships of Chinese SEOs may be equipped with advanced sensory systems to conduct covert surveillance and espionage activities aimed at industrial or military targets, or both. The Chinese vessel suspected to monitor Australian warships in 2018 indicates that such a scenario could become reality.

The ability of foreign states to interfere in Dutch and European affairs can increase gradually. The long-term geopolitical implications of foreign interference can be significant. If Chinese SOEs control a large share of cargo traffic to and from the Port of Rotterdam and relations become increasingly contentious, the Chinese government might leverage this control to impact domestic affairs or Dutch foreign policy.

190 The CCP has also increased its influence over private sector enterprises in recent years. See The CCP's New Directives for United Front Work in Private Enterprises – Jamestown

191 CSIS, *Hidden Harbors*, 2020, p1.

192 Clingendael, *European Seaports and Chinese Strategic Influence. The Relevance of the Maritime Silk Road for the Netherlands*, 2019, pp7,23.

4.2.4 Incursions

The direct objective of incursions is to weaken and undermine a coast state's sovereignty. Open incursions by Russian forces through military exercises or surveillance activities are common in the North Sea and they are likely to continue. These military exercises are permitted under international law, and function as a show of power to instill fear in adversary states and may interfere with NATO military activities. Russian naval presence in the North Sea suggests the country's willingness and ability for rapid response should a crisis erupt. A recent naval exercise in St Petersburg led to warships from, for example, Iran, China, Egypt, and Vietnam to sail past our coast. In one incident, machine guns were aimed at a NLCG Vessel.[193]

Open and covert incursions align with the Russian doctrine of strategic deterrence, a comprehensive approach to multi- and cross-domain coercion, one that combines all instruments of power in a single concept. It involves proactive measures including disinformation campaigns, cyberattacks and the prepositioning of illegals and covert units. In a speech in 2019, General Gerasimov, Russia's highest ranking military officer, argued that military force is still important, but that the role of non-military activities has become more important. In a maritime environment, this may include covert and clandestine attacks performed by merchant vessels or other small commercial vessels (e.g., fishing boats, tramp steamers, light coastal tankers). These vessels may have built-in hidden compartments to transport weapons such as explosive devices, tear gas, dispensers, light or heavy caliber arms. Bigger commercial vessels can be used as mother ships for smaller boats or UAVs that can, in turn, function as hybrid warfare weapons. They can deploy mines or other types of explosive devices against military targets. Attack could also be carried out against maritime infrastructure such as ports or offshore energy infrastructure. When commercial vessels are used for incursions, an increasing number of such vessels in the North Sea can cause uncertainty as to each of their objectives.

While the North Sea is unlikely to become a military target for Chinese forces, a Chinese hybrid threat remain a remote possibility. European countries may become involved in a possible future 'hot' conflict between the US and China over, say, Taiwan or freedom of navigation in the South China Sea. This may trigger China, like Russia, to use seemingly peaceful vessels, both military and commercial, to create opportunities for clandestine attacks from the North Sea. The involvement of Chinese SOEs, also serving state interests, in the North Sea's energy industry could provide an avenue for future incursions. CNOOC is one of the largest oil producers in the British part of the North Sea, meaning that commercial vessels and offshore platforms in the North Sea are operated by a Chinese SOE. In the short term the Chinese government prioritizes other regions such as the Indian Ocean, but incursions in the North Sea in the long term remain a remote possibility.

193 Expert interview

4.3 Military threats

All seven North Sea states are NATO Member States, five are also EU Member States. This fact alone renders military threats to or in the North Sea limited. But being one of the busiest maritime areas with considerable economic value, and with great power competition back on the geopolitical agenda, the North Sea also constitutes an interesting military target for possible opponents. From its proximity and strategic geographic orientation, Russia is the main military threat in the North Sea region. China also exerts influence in the North Sea through its commercial presence and its Maritime Silk Road initiative. As China's influence and the political and economic importance of the North Sea expands, China might in the future consider protecting its assets by posturing its rapidly expanding and advancing naval force, even though today it is unlikely that China can even sustain power projection efforts in the Indian Ocean, a region much more central to Chinese interests and closer to the homeland. Chinese military deployment in the North Sea is very unlikely in the period up to 2035, as a result. In this section, we therefore concentrate on the Russian military threat.

For the Russian Federation and its military, the North Sea has great strategic value. The sea is located between three critical sea lane choke points: the Danish Straits, the English Channel, and the Norwegian Sea. Both Russia's Baltic Fleet and Northern Fleet find their theatre of operations in and close to the North Sea. The Baltic Fleet has its headquarters at Kaliningrad and St. Petersburg. Its main tasks rest in sea denial and blockades. Russia is dependent on unopposed passage through the North Sea to deploy its Baltic Fleet elsewhere. Russia's Northern Fleet, with its main base in Severomorsk, must pass the Greenland-Iceland-UK Gap (GIUK) to sail the Atlantic.

The confined nature of the North Sea means that the transit of Russian naval assets immediately implies a show of force, whether intended or unintended, putting pressure on the North Sea states. All seven being NATO members, this complicates Russia's ability to maneuver freely for access to the high seas. As not usual for issues concerning the use of the open seas, the tension between law and politics here clearly surfaces.[194] The North Sea poses a challenge and an opportunity to Russia. On the one hand it can act as a NATO stronghold, jeopardizing Russia's access to the world seas. On the other hand, Russian presence is a sign of its increasing military strength, dauntlessness, and potentially threatening nature. The Russian navy might engage militarily in the North Sea primarily to project power and display its military capabilities. Its presence in the middle of the NATO and EU sphere of influence would assert its position as a strong military actor. Naval power projection can be used through attacks on Sea Lines of Communication (trade routes), attacks on offshore and onshore targets, kinetic and cyberattacks and all forms of unconventional maritime warfare. Power can be projected by carrying out military exercises in other countries' EEZ. Through power projection, a state actor can disrupt the adversary, damage or destroy its assets or take control of an area to support a campaign.[195]

194 William J Aceves, *The Freedom of Navigation Program: A Study of the Relationship between Law and Politics*, p69.

195 U.S. Marine Corps, U.S. Navy, U.S. Coast Guard, *A Cooperative Strategy for 21st Century Seapower*, 2015, p24.

	Military threats	Illustrative story lines of possible threat manifestations
	**Physical attacks**. Military operations targeting critical maritime functions, vessels and structures, military or otherwise. Includes stand-off and direct attacks by military platforms aimed at follow-on forces transports from North America in case of a war in Europe involving NATO	In the escalating dispute between Russia and the EU over the Russian military presence in Belarus, concerns grow that Russia may have compromised several of the over a hundred decommissioned oil and gas rigs in the North Sea, to be possibly used as an attack base if the dispute turns highly violent. Experts believe Russia may have installed (possibly partly remotely controlled) rocket installations as well as electronic warfare systems on these platforms. They could be also used as launch bases for coastal raids by Russian special forces, possibly disguised as technical personnel – and to launch an attack on underwater communication cables, cutting off essential telephone and internet access in NATO states in a time of crisis.
	**Cyber electromagnetic activities**. Military operations targeting to destroy, degrade, or take control of ICT systems of vessels or maritime structures, military or otherwise	In the escalating dispute between Russia and the EU over the Russian military presence in Belarus, maritime traffic control systems have been targeted, presumably by Russian hackers. Disturbance of the electronic systems has compromised the reliability and thus the safety of sea traffic in the area. A large number of highly combustible energy-related shipping in the form of LNG and ammonia carriers sailing around without navigation quickly degrades the security environment.
	**Deny access and use**. Military operations to disrupt or hinder the access to and use of the North Sea, including through the use mines or stand-off means	In the escalating dispute between Russia and the EU over the Russian military presence in Belarus, Russia has warned that it has deployed sea mines in the North Sea. These advanced mines are currently buried in the seabed of the North Sea – near both communication and high voltage cables – and inactive but may be activated at any time if the EU does not back down.
	**Military espionage.** Military operations to gather intelligence, for example by tapping communication cables or deploying unmanned sensor platforms at sea	In the escalating dispute between Russia and the EU over the Russian military presence in Belarus, intelligence agencies have warned that it is likely that Russian UUVs are tapping undersea data cables at various locations in the North Sea.
	**Raids and landings**. Military operations to access the land from the sea, ranging from small scale and covert deliverance and extraction of units (e.g., SOF) to larger amphibious operations	In the escalating dispute between Russia and the EU over the Russian military presence in Belarus, it is believed that Russia may secretly inject (or has already put) agents in Dutch society through covert landings with small submersibles launched from civilian vessels for the coast or abandoned platforms in the North Sea. These agents may act as spies, provocateurs, saboteurs and assassins.

Table 15. Categories of military threat actions and illustrative story lines

4.3.1 Physical attacks

Traditional force-on-force military attacks have been surmounted by hybrid and covert operations but remain a key security threat. Russia frequently deploys its fleets in the North Sea, conducting replenishment-at-sea, surface warfare, air defense, and anti-submarine warfare as part of exercises or on its way to support allies (e.g. Syria). They maintain presence in the North Sea for longer periods of time and are occasionally accompanied by spy ships. These deployments send a clear signal to the Baltic states and European powers that the Russian Navy can maintain its surface ships at sea and potentially interfere with NATO activities in this region.

NATO naval forces remain militarily superior vis-à-vis Russian naval forces, also in the 2035 timeframe. In case of escalation and force-on-force confrontation between Russia and NATO, Russian forces would not have the upper hand.[196] While this asymmetry is relevant, NATO's military advantage does not necessarily deter the weaker actor from seeking to make an impact. For instance, an attack on a naval vessel, disguised as an out-of-control accident or attack launched from a decommissioned rig under disguise, could still occur. Russia has the capacities to carry out these attacks and has become more advanced in its ability to achieve its objectives while remaining under the radar. It has access to the North Sea and knows where and how to conduct such attacks. Decommissioned oil and gas rigs in the North Sea remain relatively unprotected between the time of decommissioning and repurposing. In covert actions, Russia may install equipment including rocket installations and electronic

196 Even if the contribution of the US Navy is minimal in scenarios where it is engaged the Indo-Pacific.

warfare systems to carry out an attack. These installations are small, hard to detect and can be fitted onto platforms by military special forces personnel disguised as technical personnel. Once installed, attacks can be launched from a distance. Another possibility is to launch coastal raids from these platforms, using small vessels disguised as leisure boats.

First and foremost, such attacks result in physical damage to vessels and infrastructure(s) with associated economic costs. Impact can be more severe if the attack targets critical infrastructure. As an example, a coordinated attack on transformer nodes at sea may cause massive, longer-term power outages with potentially substantial socio-political implications next to large economic damage.

In spite of a continued advantage in total capabilities, American – and therefore NATO – military presence in Europe may decline towards 2035. The United States Navy shoulders an increasingly heavy burden in the Indo-Pacific to balance against China's rapidly modernizing navy. Towards 2035, Chinese capabilities will have grown significantly, drawing American resources away from the European continent, and leaving Europe's defense more-and-more in European hands.

4.3.2 Cyber electromagnetic activities (CEMA)[197]

CEMA threats emanating from state actors are expected to increase as a way of impacting adversaries' economic, political, and strategic positions. Offshore critical infrastructure, maritime navigation or military systems are targets which, if degraded, disrupted or destroyed, can severely impact a country's autonomy. Russia is perceived as the main challenger of the cybersecurity of Europe, employing cyber threats as part of its doctrine of strategic deterrence. Several of the most dangerous groups actively involved in cyberattacks on oil and gas infrastructure either have Russian connections or have been identified to act in accordance with Russian state interests.[198] In short, "whether the targets are ships, humans or logistics chains, the maritime environment continues to be vastly underappreciated for its cybersecurity risks and, ultimately, represents a major and underserved economic Achilles' heel of the [American] nation." [199]

Potential cyber operations – or, broader, cyber electromagnetic activities – on offshore energy infrastructure can have the following effects, as per defined by NATO:[200]

- Manipulate: to control, change, or compromise the integrity of adversary's information, systems and/or networks in a manner that supports the commander's objectives.
- Exfiltrate: to gather, download, disclose or gain possession of information through unauthorized access.
- Degrade: to deny access to, or operation of, an asset to a reduced level of its capacity and/or performance. A desired reduction level is normally specified.
- Disrupt: to completely deny access to, or operation of, an asset for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special

197 In a military context, cyberattacks and electronic warfare are closely connected. CEMA is defined as: the synchronization and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace.

198 Dragos, *Global Oil and Gas Cyber Threat Perspective: Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry*, 2019, p7-8.

199 *The Cyber Maritime Environment: A Shared Critical Infrastructure and Trump's Maritime Cyber Security Plan*

200 NATO, *Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations*, 2020.

case of degradation where the degradation level selected is 100 percent for a period of time.
- Destroy: to completely and irreparably deny access to, or operation of, an asset. The asset is affected to the maximum extent, both in terms of outage time and damage caused.

The increased automation of traffic control and navigation systems offer new opportunities to seriously disrupt operations. During the 2018 NATO exercise Trident Juncture along the Norwegian coast and in the high north of Norway, a major disturbance of GPS signals was encountered. According to Norway's defense organization, these interferences stemmed from the Russian Kola peninsula. This was not the first occurrence of such activities as was displayed during Russia's exercise Zapad in September 2017 and UK's *Clockwork* exercise in Norway's extreme north in early 2019.

If military cyber systems are attacked, the consequences for European interests and capabilities could be substantial. Military databases could be hacked to gather information on plans or location of navy vessels and troops. Defense operations by the Navy or Air force could be disabled through cyberattacks targeting electronic weapons systems, as happened in Crimea in 2014. The computers of political and military leaders can be compromised, releasing sensitive information to the public, weakening the position of a country and its citizens' trust.

Cyber threats thus are a serious and mounting concern. Growing awareness of the need to invest in cyber and electromagnetic security to protect critical infrastructure is rising and the EU has been working on developing strategies and frameworks to tackle new challenges associated with the EU energy sector. The Netherlands has also developed a strategy for protecting critical infrastructure. With its growing importance for the Dutch economy and society, significant parts of the offshore infrastructure should also be classified as critical infrastructure.

4.3.3 Prohibit access and use

Anti-access and area denial (A2/AD) has gained renewed attention in the 21st century. Anti-access refers to actions and capabilities to prevent opposing forces from entering an area while area denial refers to actions and capabilities to limit opposing forces freedom of maneuver within an area of operations. Russian A2/AD means in a maritime environment include sea mines; precision strike cruise and ballistic missiles that can be launched from air, naval and land-based platforms; long-range artillery; submarines armed with supersonic anti-ship cruise missiles and advanced torpedoes; and electronic warfare capabilities.[201] In the 2035 timeframe, coordinated attacks by swarms of drones (air- and sea-based) are also feasible. Swarm technology facilitates complex missions to be carried out simultaneously against strategic targets, in a rapid and cost-effective way. Navies can use drone swarms either to destroy enemy vessels or to confuse and overwhelm the opponent's air defenses.

Sea mines are attractive because they are "low in tech, high in effectiveness". These bulks of packed explosives can cause substantial destruction, automatic or through a remote trigger mechanism, either by physical contact or by the proximity of a magnetic field (such as the hull of a naval or cargo vessel). In confined maritime spaces, they can effectively stop all ship movements. The proliferation of sea mines is gigantic with more than 300 types and more than 60 navies employing them. Russia possesses a large arsenal of naval mines and the

201 Dr Aziz Erdogan, *'Russian A2AD Strategy and Its Implications for NATO'*, Beyond the Horizon, 6 December 2018.

capacity to lay these mines both overtly and covertly including a versatile range of launch platforms, from full-sized frigates to small fishing boats and small submersibles. In times of crisis and conflict, Russia may opt to deny EU or NATO allies access to the North Sea by deploying sea mines at harbor exits and choke points. Advanced mines may be laid in advance, remaining inactive and buried in the seabed, only to be activated by Russia at any time, for instance when the EU or NATO do not back down in a conflict in Eastern Europe.

The amount of mine counter-measure vessels has decreased over years in Western navies. The Netherlands and Belgium navies are jointly investing in modernizing their mine counter measure capabilities, and from 2024 onwards a total of twelve new ships, with a new counter-mine concept using unmanned sea- and airborne assets, will enter service. The Singaporean Navy already has such a capacity, and this modus operandi will be the future of maritime mine countering strategies.

4.3.4 Military espionage

The North Sea is an important hub for data including telecommunication and internet cables that are the arteries of the modern internet and information exchange. These undersea cables are here to stay because there is no viable alternative. They are vulnerable to cable tapping for intelligence penetration and espionage and cutting to disrupt and break communications. The shallow waters of the North Sea make this relatively easy and fast, requiring widely available tools. If cable tapping is carefully conducted, the target may not realize it operates on an exposed network. Russia possesses remotely operated submersibles that can roam over the sea floor for inspection and intelligence gathering. These are small enough to be covertly launched from other vessels, including merchant vessels, and may soon be equipped with manipulator arms, increasing their threat to undersea cables. Russia has also shown unwavering commitment to develop and maintain its submarine capabilities to intercept and tap into undersea cables or destroy seafloor infrastructures.[202]

Recently, the Chinese navy has also been strengthening its underwater capabilities. Chinese unmanned drones, equipped with sensors and long-range transmitters are believed to be used for espionage; they were found in strategic sea lines of communication off the Indonesian and Australian coasts. Since Chinese attempts at (economic) espionage in Europe and in the United States – primarily using cyber means[203] – have been abundant, the deployment of Chinese drones for military intelligence tasks in the North Sea is conceivable.

Undersea cables are not adequately protected under international law in conflict. Outside the territorial sea and the contiguous zone, UNCLOS does not give states the right to board suspect vessels nor provides jurisdiction over offenders (with, inevitably, ample historic examples where states have taken matters into their own hands). The placement and repair of cables is considered a commercial responsibility and not a public security concern. Currently, European states do little to secure the undersea cable network, given the lack of legislative mandate to act outside territorial sea and the ambiguity as to ownership, surveillance and protection roles between states and companies. This leaves states with limited capacities to counter the undersea warfare challenge, and lack the required coordination of platforms, sensors, and personnel to protect networks.[204]

202 CSIS, *Undersea Warfare in Northern Europe*, 2016, p v.

203 William C. Hannas, James C. Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, 2013.

204 CSIS, *Undersea Warfare in Northern Europe*, 2016, p v.

Although the threat is real for the period up to 2035, and the impact of data tampering or cutting cables potentially enormous and immediate, several factors mitigate this vulnerability, making actual attacks more difficult and possibly less effective. The congested North Sea makes detection and attribution of attacks likely. While damaging or cutting cables may be relatively easy, tampering with cables is more difficult. Data tapping without disrupting communication traffic and alerting the cable owners while the process is underway requires substantial expertise and sophisticated equipment. Appropriate countermeasures are relatively easy to apply (even if the actual implementation thereof leaves something to be desired). In addition, the amounts of data passing through the cables make it of limited immediate use unless the attacker can meaningfully manipulate the data or turn data into useful intelligence (albeit the sophistication of big data techniques is rapidly growing). The rise of encryption further mitigates the potential for surveillance of sensitive data.[205]

4.3.5 Raids and landings

Through amphibious operations, state actors project ground forces and air power from the sea onto their adversary's territory.[206] These are complex, high risk, and costly operations. Technological advancements in anti-access and area-denial systems, monitoring and stand-off precision firepower have substantially decreased the risk of such operations.[207] Navies around the world are moving toward smaller raiding parties with enhanced and specialized capabilities. Rather than engaging in conventional beach landings, amphibious forces have been carrying out lower scale interventions to reduce the risk of detection. A notable exception is a limited Russian amphibious assault in Georgia in 2008.[208]

The objective of a potential future amphibious operation in the North Sea is not to seize terrain or assault the enemy, but to achieve political goals beyond the maritime realm. By means of raids of platforms or landings on the coast, small scale offensive actions might be conducted. A state actor such as Russia may secretly inject agents in Dutch society with agents acting as spies, provocateurs, saboteurs, and assassins. Covert landings could be launched from civilian vessels for the coast or from abandoned platforms.

The confined nature of the Netherlands and the density of population make amphibious operations at sea more difficult, and less likely. The hack at the OPCW in 2018 showed how easily foreign agents can enter the Netherlands through its airport. Even if less concealed, such a method is much easier and remains the most probable way to insert foreign agents in the Netherlands. Yet covert landings at sea, by submersibles or small (inflatable) craft launched from commercial vessels, remain a possibility. Landings could be conducted as the shores have no permanent guarding by cameras and sensors. Unattended platforms offer opportunities for state actors to infiltrate. These can be used as staging areas for physical attacks, as bases for rocket systems or to conduct cyberattacks against the radar and sensor systems guarding the security of the North Sea.

205 Doug Brake, *Submarine Cables: Critical Infrastructure for Global Communications*, 2019, p6.
206 IISS, *The Future of Amphibious Operations*, 2020, p iv.
207 Brad Roberts, *Toward New Thinking About Our Changed and Changing World*, 2020, p43.
208 IISS, *The Future of Amphibious Operations*, 2020, p iv.

4.4 Overall assessment

4.4.1 Analysis combined with expert judgment

The increased usage of the North Sea comes with amplified existing and novel vulnerabilities that might be exploited by criminal, terrorist, hybrid, and/or military actors. Vulnerabilities may turn into clear and present threats if malicious actors perceive valid 'business cases' to exploit these vulnerabilities, i.e., they consider the anticipated rewards to surpass the likely costs; where both costs and rewards may have material as well as immaterial elements. Counter measures aim to undermine these business cases by lowering the (perceived) rewards and/or raising the (again, perceived) costs for the attacker, through adequate prevention and deterrence, effective protection, and timely and decisive response.

In the final section of this chapter, we abstract from the individual threat categories to provide a high-level assessment of crucial security issues associated with the evolution of value creation in the North Sea towards 2035 and beyond. We realize that the oft-used quote from physicist Niels Bohr, "Prediction is very difficult, especially if it's about the future", also applies here. It is virtually impossible to numerically assess likelihood and impact of the risks and threats that may face the North Sea in a well-founded, analytical way. This is why in the previous sections, a qualitative rather than a quantitative assessment is given to the fourteen threat categories we have discerned, based upon a literature review and expert interviews.

Expert judgment can be an important component in forecasting as a (partial) lack of objective data and immediate changes in the forecasting environment add uncertainties to the forecasts. We have therefore asked a group of seven subject matter experts of the Netherlands Coast Guard and the Royal Netherlands Navy to judge the threat categories in terms of likelihood and impact. This was a limited exercise, but it did serve as a valuable cross-check for the analysis in the previous sections in this Chapter.

4.4.2 Major security issues towards 2035

Based upon our desk research, corroborated with the insights from the conducted interviews and the expert judgment exercise, HCSS assesses the following security issues – the combination of high likelihood X impact risks and potential counter measures – the most pressing for the security in and of the North Sea towards 2035.

Diversity of conceivable risks and threats requires a comprehensive approach. Value creating activities in the North Sea grow and diversify substantially towards 2035. The former accentuates existing vulnerabilities, the latter gives rise to new ones. Both our research and the expert consultations suggest that the whole threat palette we have discussed in this Chapter is relevant from a national security perspective. Furthermore, offshore processes and infrastructures tend to become more entangled, with threats also turning more complex and intertwined, as different types of malicious actors join forces. Overall, we project mounting probabilities that incidents in the North Sea generate cascading effects leading to severe disruptions of critical processes, offshore and onshore. As the range of high-consequence risks and threats expands, and risk and threats tend to overlap and merge, a comprehensive approach of security in and of the North Sea becomes imperative.

Countering cyber risks and threats top priority. The three variations of cyber threats coming from criminal/terrorist, hybrid, and state actors combine a high likelihood and a high

impact, even if a few other threat categories score higher on either likelihood or impact. Many consulted experts underlined the cyber risks. As the maritime domain becomes more digitized, cyber vulnerabilities are expected to increase. Malicious actors can breach these remote connections, disrupting control over individual ships and/or over maritime traffic management. Furthermore, remote operations not only apply to maritime traffic, but also to offshore infrastructure. Clearly, cybersecurity constitutes a key issue in any North Sea security strategy. At the same time, whilst there are very specific characteristics involved in maritime cybersecurity, it is also part of the broader cyber challenge. A first step is to fully incorporate offshore critical infrastructure in national cybersecurity and critical infrastructure protection plans and practices, considering the specific characteristics such as jurisdiction, reduced physical accessibility, and the wide variety of international interests involved with assets in the North Sea, such as flag states, shipowners, and IT/OT-suppliers.

Sabotage and physical threats potentially have the most impact. Even if we judge cyber threats to score highest in overall likelihood X impact, incurring physical destruction – the threat categories sabotage and physical threats – may well have the most immediate consequential damage (note that a cyberattack can be a channel through which to achieve physical damage). However, these threat categories are considered less likely than cyber threats because they have, in general, a higher threshold for execution in terms of opportunity and costs and are typically more attributable, more defendable, and easier to retaliate. However, paying more attention to cybersecurity should certainly not lead to the neglect of traditional physical protective measures.

Protect critical infrastructure hubs. Platforms that function as hubs for wind energy are lucrative targets for sabotage. Malicious actors can take control over and occupy these platforms. Incapacitating electricity transformer stations, for instance, has the potential to cause power outages across the Netherlands, forcing critical socio-economic processes to a standstill. Attacks on such platforms can also inhibit maritime situational awareness, as these structures house sensors. Infrastructure platforms can further be used by malicious actors as forward operating posts from which to stage physical and cyberattacks. The combination of, for example, hydrogen production, CO_2 storage, sensing and data centers on artificial islands might be economically advantageous but dangerous from a security perspective. These future hubs could be targeted by state actors and terrorist groups not only to cause severe damage, but also to gather crucial intelligence. Despite its importance for national security, critical infrastructure at sea is often left weakly protected because its design is primarily economically driven. Much more attention should be given to 'security by design' right from the inception of new infrastructure projects.

Monitor chokepoints in critical shipping lanes. The increasing congestion in the North Sea leads to more critical chokepoints. Narrow shipping lanes can be effectively closed using a relatively small amount of sea mines (or even the threat thereof). States have deployed mines in warfare for decades and are developing increasingly advanced systems to lay mines on the seabed overtly and covertly using a versatile range of launch platforms. These mines may remain inactive until tensions escalate. Digitally or physically hijacking ships and letting them drift or sink in chokepoints (think of the Ever Given-incident in the Suez Canal) is another possible modus operandi to severely hit the Dutch and European economy. Early warning and action must ensure adequate deterrence and response.

Counter industrial, political, and military espionage. The numerous offshore economic, industrial, and military activities projected on the North Sea make it a lucrative target for espionage and intelligence gathering. Sensitive information could be gathered by malicious

actors and used to their advantage, either to plan further incursions or to influence political decision-making. Various state actors are involved in espionage operations around the world, in the case of China and Russia known to be using novel technologies attached to commercial vessels. Cargo ships fitted with advanced sensory systems – including stealthy unmanned aerial vehicles with sensor payloads – could be used for surveillance and espionage activities on the North Sea, in harbors and in coastal areas. Look-alike commercial vessels equipped with unmanned underwater vehicles may target data cables on the seabed, which can be intercepted and tapped. State-Owned Enterprises that have acquired a solid foothold in harbor and offshore processes may act as a platform for espionage and political interference. With most data digitally stored and processed, espionage in the information age has considerable overlap with cyber threats. This, once again, re-enforces cybersecurity's top priority.

Pay attention to highly combustible and poisonous energy-related shipping. The changing energy mix in the ongoing energy transition brings new risks. As an increasing volume of combustible fuels such as LNG and hydrogen (stored in e.g., ammoniac) are transported at sea, the impact of hijacking a ship also increases. If hydrogen production seriously takes off after 2035, not only the transport but also infrastructural elements might become a target for malicious actors. Where oil can cause massive environmental damage and pollution, these new energy sources are explosive and/or spread poisonous gas, with the potential to cause harm to life far from the area of explosion. A digitally hijacked LNG tanker (or even an LNG powered ship) can thus be used for ransom by criminals or as a floating bomb by terrorists.

Smuggling and trafficking is a nuisance that requires an international and chain approach. Smuggling and trafficking is not a hypothetical scenario but an everyday fact. The consensus seems to be that drug trafficking is something we must have to live with; but not something we should accept. To contain the impact, enough effort must be put in discouraging the most profitable and distressing business cases. "The dilemmas posed by security policies, the scale of the drug trade, and the potential dangers of organized crime to society as a whole require that governments, law enforcement agencies, and private companies continually work to find better solutions. The transnational nature of drug trafficking also calls for countermeasures of a similarly transnational character."[209]

209 WODC, *Justitiële Verkenningen 5|19. Criminaliteit en veiligheid in mainports*, November 2019, p45.

5 Implications for Coast Guard and Navy

This final chapter addresses the consequences of the analysis in the previous chapters for the Netherlands Coast Guard and the Royal Netherlands Navy as these organizations prepare for 2035 and beyond. The tasks, responsibilities and capabilities of the two organizations must be considered in the wider context of national security and the range of stakeholders that have a bearing on the security in and of the North Sea. The first section thus considers the wider legal and managerial framework in which the NLCG and the RNLN operate. The subsequent sections look at the various security functions in the cycle depicted in Figure 6; at these functions specifically for the cyber domain; and at future corporation between NLCG and RNLN, and internationally. We close off with some final thoughts.

5.1 Legal and managerial framework

Our research and the feedback from experts and practitioners clearly indicate that, in the context of national security, 'offshore' is given less formal and practical attention than 'onshore'. In theory, procedures and regimes for critical infrastructure protection apply to both onshore and offshore infrastructure. In practice, however, the focus is very much on onshore infrastructure. Indeed, various interviewees were in doubt whether, for instance, electricity production at sea is formally considered a critical process (see Table 5) or not.

Why is offshore infrastructure the poor relation in our security policy? The answer may partially lie in the assumption that there is little to protect in the North Sea. As we hope to have substantiated above, this sentiment is no longer valid: value creation in the North Sea is increasingly an integrated constituent of Dutch economy and society; and in this era of permanent interstate competition, chances that critical offshore processes and infrastructures are targeted by criminal, terrorist, hybrid, or military actors are real. A key issue here, as already flagged in the Introduction, is the clear separation between the territorial sea and the EEZ outside the 12-mile zone. In the former, by and large, national legislation applies. In the latter, room for national measures in the face of security risks and threats is limited.

Territorial sea. National governance of the territorial sea must be critically reviewed and adjusted. For practical reasons, security at sea should as much as possible be aligned with existing onshore security structures and processes. In the Netherlands, local or regional safety and security incidents are dealt with by the authorities and organizations operating at the local level – the municipalities – or regional level – the security regions.[210] The national

210 The Dutch *veiligheidsregio* is translated in English both as safety region and as security region. We use the latter translation.

government can, depending on the course of events, fulfil three roles: facilitate, guide and (take over) command. The North Sea, however, has no municipalities or security regions, thus lacking a local framework for safety and security tasks and responsibilities. Security incidents are handled at the national level, with the NLCG as first responder. But the NLCG is a small interdepartmental network organization with limited assets and little autonomous executive power: "Because individual ministries remain responsible for their own policies and legislation, the emphasis is on joint decision-making." [211] The organization is neither equipped nor tasked to deal with the full spectrum of the prevent, detect, protect, and response phases in the safety and security cycle of Figure 6. In addition, the NLCG lacks the authority, constituency and resources to act as the public custodian of security in and of the North Sea in the political and policy battles for attention and budget.

EEZ. In the EEZ, additional issues arise. International treaties hold that outside the 12-mile zone room for national authorities to exercise security measures is limited.[212] As critical processes move further out to sea, under spatial pressure and guided by economic considerations, this poses a crucial dilemma. The political dimension of this dilemma is how to balance the government-backed plans to create critical processes and associated infrastructure in the EEZ with the lack of security guidance and measures that same government can legally provide outside the 12-mile zone. The judicial dimension is how to balance UNCLOS – which is, after all, a largely Western invention, built upon the *mare liberum* principle that serves us well – with the wish for mandates to promote and enforce security in UNCLOS governed spaces. The administrative dimension is to how to assign responsibilities for action, within the legal boundaries, in the face of security threats.[213] And the economical (and technical) dimension is how to make intrinsically secure processes ('security by design') part and parcel of the business cases for the exploitation of the North Sea.

A 'North Sea Authority'. The lack of a clear national governance framework for the Dutch part of the North Sea should be alleviated by appointing a specific 'North Sea Authority' (NSA).[214] Because of the distinct regimes under UNCLOS (see §2.4.1), the NSA's mandates, and therefore tasks and responsibilities, are different for the territorial sea and the EEZ – where our advice would be to try and minimize or bridge these differences as much as possible. Principal tasks of the NSA include spatial planning in the North Sea, as well as policymaking, planning for and execution of security, and to a lesser extent safety, tasks in all aspects (note that the two have a clear relationship, as 'security by design' is a crucial element of responsible spatial planning). The NLCG would act as the operational arm of the NSA, in a construct that resembles how the police and the fire brigade operate within the security regions. The NSA chairs the 'North Sea Security Board' (*Noordzee Veiligheidsberaad*), which replaces the current Coast Guard Directorate (*kustwachtviermanschap* or KW4).

In this construct, the executive responsibility and authority of the NLCG would broaden considerably. Notably, security risk analysis and prevention, including regulation and

211 Regeling organisatie Kustwacht Nederland, *5: Inhoud van deze regeling*.

212 UNCLOS is the basis, making it for instance possible to enforce safety zones for wind farms in the EEZ. Other treaties providing some room for specific action. For example, the Nairobi Convention, which has been implemented in the Maritime Accident Response Act, provides room for wreck clearance; counter-terrorism/piracy treaties have been implemented in the Criminal Code. All in all, however, national manoeuvring space remain small.

213 If, for example, a Liberian tanker drifts towards a main transformer platform, UNCLOS does not preclude acting. Currently unclear, however, is which who decides this.

214 In 2003, Belgium established the function of minister of the North Sea, responsible for Maritime Mobility and Marine Environment, including the policy on authorizations for the operation of renewable energy infrastructure in the North Sea.

supervision, would become an integral part of its task package. Operationally, the NLCG may move towards a model that resembles the way the Special Interventions Service (*Dienst Speciale Interventies*, DSI) oversees the deployment on Dutch soil of special units of both the police and the armed forces. This combination allows the DSI to act flexibly under various command & control structures and legal regimes. Likewise, the NLCG could oversee the deployment of its own resources and those of its contributing partners, taking strength from the diversity while providing unity of command and effort. In fact, the DSI itself could act under the auspices of the NLCG. In the 2018 edition of the exercise Port Defender, part of the scenario was for the DSI to storm a hijacked cruise ship 5 miles of the coast.

With hybrid threats likely to be a defining characteristic of the security environment towards 2035 (see §2.3.3), the role of the RNLN must also be clarified and calibrated. Acting in the gray zone between peace and war is where the responsibilities of civil security agencies and the military meet, with potential overlaps and voids that might cause friction or insecurities if left unresolved. Naval assets deployed in the North Sea may act (1) under the NLCG's mandate; (2) under civil mandate as part of Defense's third main task, support to the civil authorities; or (3) under military mandate as part of Defense's first main task, collective defense. As highly violent threats with possible state actor involvement become more likely, (2) or (3) may befit naval deployment better than (1). Currently, there is no clarity on what scenario would warrant which framework and, consequently, what rules of engagement would apply sanctioned under whose authority. A single North Sea Authority would make it easier to establish escalation mechanisms in the case of violent threats, with clear complementary roles for the NLCG, the DSI and the RNLN.

Obviously, establishing something like an NSA requires further studying. However, it is quite clear that such an Authority would make it easier to switch between local, national and international levels of action and response. This is important, amongst others, when it is unclear what the cause of an incident is (accidental or deliberate; and in the latter case stemming from a criminal, terrorist, hybrid, or state actor); what the scope of an incident is (extent of the consequential damage); or whether the incident is a stand-alone event or connected to other incidents (e.g., as part of a hybrid campaign).

5.2 Security functions

5.2.1 Prevent

Acting together, the NLCG and the RNLN can contribute to resilience building in the North Sea, for instance through the following activities:

- Strengthen general awareness of the geopolitical security risks throughout the maritime sector. Regular consultations between relevant government bodies, including the intelligence services, the offshore energy industry, port operators and shipping companies can be an important tool for this, as is the case in Norway and the UK.
- Claim a structural advisory role in the formulation of standards, legislation, and regulations for activities and infrastructures at sea, aimed at promoting and enforcing security.
- Organize joint exercises/wargaming with industry and the intelligence community; Port Defender is an example.
- Organize network events with government partners and the maritime sector.

Many of these activities are aimed at creating a North Sea security constituency, a body of stakeholders that know one another, and can easily contact one another when needed. This is a step towards the Norwegian setup, where industry and security agencies are much more intertwined. This bottom-up model probably suits the Netherlands better than the British top-down model, where the national Centre for the Protection of National Infrastructure (CPNI) also brings together industry, security agencies and intelligence services.

5.2.2 Detect

Currently, the NLCG has limited real-time awareness of security-related activities in the North Sea. More than today, information from a multitude of sources must be brought together and analyzed to create an integral Maritime Situational Awareness & Situational Understanding (MSA/SU). The Maritime Information Hub (MIK) is set up for this purpose.

Sources for maritime situational awareness

MSA at the MIK aims for complete transparency not only of the North Sea, but of all European waters and indeed world-wide. To build MSA, the MIK collects, combines, and analyzes information from a variety of sources. These sources include the Automatic Identification System (AIS), Vessel Monitoring System (VMS), camera and alarm systems, radar and satellite systems and observations by aircraft and ships of the NLCG; as well as information from port authorities, traffic centers, weather services and other maritime and coast guard organizations at home and abroad. All this information is combined with information from the police, Customs, Fiscal Intelligence and Investigation Service (FIOD), Dutch Food and Consumer Product Safety Authority (NVWA), Rijkswaterstaat, Royal Netherlands Navy and Royal Netherlands Marechaussee. All these agencies are represented within the MIK; currently mostly in a part-time capacity.

The MIK is very much under development. The textbox above sketches the sources that are being used by the MIK. Towards 2035, the current connections should be strengthened and a range of additional sources should be added. Information sources that should be utilized structurally include:

- The future Maritime Operations Center (MOC), with which the MIK should be fully connected and interoperable.[215] The future division of labor and/or integration of MIK and MOC is a clear focal point.
- Next to the RNLN and the network partners already represented in the MIK: national public organizations and bodies such as the National Coordinator for Security and Counterterrorism (NCTV), the Royal Netherlands Air Force, and the intelligence agencies AIVD and MIVD.
- International peers, Frontex and the coast guards of other North Sea states.[216]
- Companies in the maritime sector, such as port authorities, ship owners, and off-shore energy producers and facilitators (such as TenneT).[217]

215 The MOC project will improve MSA/SU considerably but will take years to implement and will certainly not constitute a comprehensive solution. Further note that the MIK may be become fully integrated in the MOC sometime in the future.

216 For instance building upon the Common Information Sharing Environment (CISE) of the European Maritime Security Agency (EMSA), focusing on maritime security.

217 As much of the information handled within the MIK-NL is confidential, private companies should take part in the information and analytical processes in a layered structure.

Permanent surveillance should be intensified. Existing sensors used for other purposes (safety, environment, etc.) can be – and partly already are – connected to the Coast Guard Centre. For example, offshore platforms are typically equipped with various sensors for day-to-day operations and many electricity and telecom cables have sensors that report disruptions. Some of these sensors can also provide structural data for e.g. pattern recognition and anomaly detection in the MIK as a feed-in to the operational front-end of the Coast Guard Centre. Active presence in and above the North Sea should be enhanced. In particular surveillance drones are a flexible asset that may greatly enhance MSA.

As important as rich data is the ability to process that data into meaningful information and intelligence. The MIK currently lacks sufficient analytical capacity. This capacity must be greatly expanded, partly in-house and partly by using external services. The MIK should be able to perform trend and risk analyses and future projections, using state-of-the art analysis models, techniques and tools. Close cooperation between the MIK and the MOC is required to share analyses and not duplicate work. Analytical effort should not only be directed towards MSA/SU of the North Sea itself, but also to build and maintain an overview of developing risks and threats that could, in due course, affect security risks and threats on the North Sea. This concerns, for example, information about international criminal drug networks, international terrorism or the positions and intentions of (maritime) units of possible adversaries.

An extremely important point of concern is the legal ability to use and share information coming for a range of sources. Impeding legal restrictions on linking information sources and integral analysis in the MIK for the purpose of security at sea should be evaluated.

5.2.3 Protect and respond

For many of its activities the NLCG currently piggybacks on the executive powers and the resources of its network partners. Currently, in case of security incidents, response is usually left to others, with the NLCG performing tasks in the periphery, such as keeping ships away from the incident zone. In the 'North Sea Authority' construct sketched in §5.1, the NLCG develops from a coordinating body largely dependent on the mandate and, ultimately, goodwill of its partners for executive action, to an organization that may act as first responder in the case of security incidents under its own authority[218].[219] In the same vein, the prioritization of deployment of services coordinated by the NLCG is mainly a bottom-up consensus process. In our view, the NLCG should be given more responsibility for formulating its own policy and executive priorities within a given constitutional framework and in close consultation with its stakeholders. More executive power residing with the NLCG should facilitate dealing with structural security risks and challenges pro-actively, as well as responding timely and adequately to complex security incidents.

Scenarios with increasingly violent actions in and from the North Sea are not unthinkable. In the context of hybrid threats, these actions typically have an unclear origin, and uncertain scope and impact. To respond to highly violent threats, the role of the RNLN must be calibrated, making it more transparent and easier to switch between various frameworks in order to be able to execute the appropriate levels of action and response, tailored to the evolving situation.

218 The NLCG already has both coordinating and executive power when performing Search and Rescue and some other core tasks.

219 The legal authorities of the US Coast Guard may serve as a reference. Note, however, that the USCG is a separate branch of the US Armed Forces. This is not our suggestion for the Netherlands Coast Guard.

Of course, authority is a hollow concept without the resources to execute that authority. Still, considerably more authority vested in the NLCG does not necessarily imply markedly more 'own' resources. More in-house capacity *is* required for creating MSA/SU, as discussed in §5.2.2, and for oversight and possible direction over complex security incidents. For other assets, however, the current situation in which the NLCG has preferred access to resources of its network partners might well remain the favored model.

That said, there is certainly a requirement for more capabilities (both qualitative and quantitative) to protect and respond, regardless of whether that capacity resides with the NLCG, the RNLN or the network partners; or in a mix. Some of the more obvious capability requirements are:

- Capabilities for a permanent presence in the North Sea, for surveillance and monitoring purposes as well as to keep incident response times low for events further offshore. In the longer term, operating bases on future artificial islands are also conceivable.
- Capabilities to counter seabed warfare.
- Capabilities for monitoring and early threat detection with drones.
- Capabilities to be able to act in and counter highly violent incidents against armed malicious actors, in close cooperation with the RNLN and the DSI.

5.3 **Cyber**

Cybersecurity awareness at sea is currently marginal, with the maritime environment not a priority for onshore cybersecurity agencies. As a result, response capabilities specific for offshore cyber incidents and cyberattacks are practically non-existent. What would be necessary on the national level to set up a response capability? What capabilities are required for prevention, detection, protection and response in the cyber realm?

Most of the considerations in §5.2 also apply, mutatis mutantis, to the cyber domain. In the sphere of prevention, cyber awareness and cybersecurity should be further promoted and enforced. An advisory role of the NLCG to better incorporate offshore critical processes and infrastructure in cyber-related standards, legislation, and regulations can certainly be envisaged. In joint exercises and knowledge sharing events with the stakeholders involved in North Sea security, the cyber domain should be fully incorporated.

In the realm of detection and early warning, cyberspace should be an integral part of a comprehensive MSA/SU. Information sharing with the National Cyber Security Centre (NCSC) and the Defense Cyber Command (DCC) is essential. The shipping industry has a centralized point of coordination to share cyber threat information between trusted stakeholders, the Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), which could be a valuable asset to connect to. A broader cyber threat analysis is also essential as an anticipatory framework for specific cyber risks and threats aimed at North Sea traffic and infrastructure. This is where the MIK, the future MOC (which will feature cyber expertise), the NCSC, and the DCC should join forces.

In terms of protection and response, first responder capabilities to cyber incidents in the North Sea should be strengthened. The way forward is to better incorporate vital offshore processes in existing arrangements for (cyber-related) critical infrastructure protection, with an advisory and auxiliary role of the NLCG to guard the particulars of the maritime environment.

5.4 Cooperation

5.4.1 Between NLCG and RNLN

Currently, there are no clear mechanisms for persistence and unity of command and effort in complex security incidents at sea. In the following example, responsibilities are relatively clear cut. The NLCG receives information on the location of a sea mine obstructing maritime traffic. It relays this information to the Mine Counter Measures vessel which the RNLN keeps available as part of its standing orders. The NLCG executes operational control over the deployed RNLN unit, while the ultimate responsibility of the operations remains with the Director Operations at the Armed Forces level, who usually mandates this responsibility to the Director Operations at the RNLN level.

Things become more entangled when a naval asset is used for law enforcement at sea. In that case, a prosecutor is responsible for the enforcement action as such, while the nautical aspect of the action is a RNLN responsibility. The use of naval vessels for law enforcement is not just hypothetical. Spanish customs, for example, are sometimes 'outgunned' by drug traffickers caught in the act and have to back off. Similar scenarios could enroll in the North Sea. The NLCG only has unarmed ships at its disposal and might thus require naval 'fire power' to effectively deal with armed criminals or terrorists. However, the commander of a Dutch naval vessel has no investigative powers. If the NLCG would indeed require the assistance of a naval vessel, what is the commander allowed to do? May he send a boarding team along with the customs officers? May he fire a warning shot if a suspicious ship ignores stopping orders? Note that, other than in the North Sea, counter-drug operations in the seas surrounding the isles of the Caribbean part of the Kingdom of the Netherlands *are* conducted using naval assets (ships and helicopters) on a regular basis (under de authority of the Coast Guard CARIB, the U.S. Coast Guard and the San José Treaty).

Broadening the executive responsibility and authority of the NLCG as the operational arm of the North Sea Authority and clarifying the role of RNLN in more complex scenarios could address this issue of unity of command and effort. As argued in §5.1, we would advocate a layered arrangement for NLCG and RNLN cooperation. In relatively low-violence threats and incidents, the NLCG provides the framework for deployment of naval personnel and assets, very similar to the DSI model (see §5.1). Against highly violent threats and/or threats with (possible) state actor involvement, however, the RNLN may deploy fully military teams and assets under national civil authority (as part of the third main defense task) or under military mandate (as part of the first main defense task).

In reality, complex situations typically come with a lot of uncertainty over ultimate causes and potential consequences. Intimate cooperation between NLCG and RNLN may than smooth over formal ambiguities in 'who does what under which mandate'. An alternative option might be to fully integrate the NLCG in the defense organization. The US Coast Guard, for example, is a separate branch of the US Armed Forces. In Dutch proportions, a separate service is overkill, but the NLCG may well become a distinct part of the RNLN. This would greatly benefit the security orientation of the NLCG and would also anchor the important relationship between the NLCG and the Navy even more firmly. The disadvantage is that embedding a public service with mainly civilian tasks and many contributing civilian partners in a military organization is unusual in the Netherlands, and different from the common practice onshore.

5.4.2 Internationally

With the distinction between domestic and international security fading, cross-border security cooperation becomes essential. This is certainly the case for the North Sea, with the EEZ governed by international treaties rather than by national legislation; and sea trade as well as cables and pipelines crossing EEZ borders as a routine matter. Therefore, the NLCG should cooperate as much as possible with European partners. Frontex, the European Border and Coast Guard Agency, is important in this regard. Frontex can formulate legal frameworks at the EU level; harmonize classifications, reports and notifications in all European seas; facilitate and stimulate information exchange; act as a knowledge and training center; arrange handovers between countries in monitoring shipping; initiate personnel exchange and equipment cooperation; promote operational cooperation; and make its own resources available. Other international initiatives, particularly in the realm of information and analysis sharing, should also be pursued, such as the Common Information Sharing Environment (CISE) of EMSA mentioned earlier.

As navies of European NATO member states have a history of cooperation and promoting interoperability, and given the fact that there is a general tendency to involve navies and naval assets more in 'civil' blue border security issues, the RNLN can be instrumental in closer European cooperation for blue border control and maritime security in the North Sea.

5.5 Final thoughts

More activities mean more security issues. A key insight to be taken from this study is that the volume and diversity of activities in the North Sea will grow moving towards 2035 and beyond. Activities become more intertwined, by nature, by spatial pressure, and by design. This trend comes with amplified existing and novel vulnerabilities that might be exploited by criminal, terrorist, hybrid, and/or military actors. Security risks, threats and actual incidents also become more multifaceted and may increasingly affect critical processes. Yet, our research and the feedback from experts and practitioners clearly indicate that, in the context of national security, 'offshore' is given less formal and practical attention than 'onshore'.

The networked Netherlands Coast Guard is well suited for a multidisciplinary approach to face these complexities. To fully capitalize on this, in essence four lines of development are required: (1) comprehensive security in and of the North Sea should be taken more seriously and integrated in existing national security processes, structures, and mindset; (2) more authority should be vested in the NLCG to execute security functions throughout the risk management cycle, in close coordination with and supported by its network partners; (3) the respective roles of NLCG and RNLN in a range of potentially highly violent scenarios should be clarified and calibrated; and (4) more (guaranteed access to) resources is needed for an adequate execution of the security tasks presented by these scenarios.

Security outside the territorial sea poses a crucial dilemma. Within the territorial sea, all four challenges above can be addressed within a national context. Outside this zone, the Law of the Sea offers limited room for measures to prevent, detect, protect against and respond to security risks and threats. Thus, as critical activities move further out to sea, guaranteeing security outside the territorial sea poses a crucial dilemma, with difficult political, judicial, administrative, economic, and technical ramifications. This crucial dilemma is hardly addressed, if at all, in the current debates on the future of the North Sea. This study flags this as a serious omission, which hampers adequate responses to many of the key issues below.

Prepare for violent threats. The growing value-creation in the North Sea inevitably leads to greater security risks. And as the proliferation of arms continues, violent incidents are no longer a remote possibility. The NLCG itself is hardly prepared to deal with violent threats. One option is to equip Coast Guard ships with means to face limited violent scenarios (such as, for example, the German and American coast guards). As both an alternative and a supplement to this, the Special Interventions Service DSI (that includes a maritime special unit) could fill the gap for medium violent scenarios, preferably acting under the auspices of the NLCG. For highly violent scenarios featuring military-style arms and state actor involvement, the RNLN should step in. Currently, it is unclear under what kind of circumstances which organization should take the lead to deal with violent threats, what the legal framework is or how to scale up if the level of violence increases. In particular, it should be determined when and where the RNLN could act (1) under the NLCG's mandate; (2) under civil mandate as part of Defense's third main task, support to the civil authorities; or (3) under military mandate as part of Defense's first main task, collective defense.

Establish a 'North Sea Authority' (NSA). Although in itself not the silver bullet to tackle the various challenges, establishing a single Authority to take responsibility over the related issues of spatial planning and security in the Dutch part of the North Sea would be an important step in taking maritime security more seriously. The NLCG would act as the operational arm of the NSA, broadening its executive responsibility and authority throughout the prevent, detect, protect, and response phases considerably. A single Authority also makes it easier to establish escalation mechanisms in the case of violent threats, with clear complementary roles for the NLCG, the DSI and the RNLN.

Real time oversight and insight is key. Creating better maritime situational awareness and situational understanding (MSA/SU) is key for pro-action and prevention, as well as for timely and effective incident response. The NLCG is the ultimate network organization, coordinating and pooling the activities of a palette of actors covering the full range of areas of interest pertaining to security in and of the North Sea. It is thus uniquely positioned to build a comprehensive overview of all that is happening in the North Sea. This fundament allows for extensive risk analysis, using e.g. pattern recognition techniques to distinguish between normal and anomalous behavior; the latter serving as an early warning signal for potentially emerging security issues. For the NLCG to be able to build and maintain a comprehensive MSA/SU, however, the connectedness of the Coast Guard Center with a range of sources must be enhanced. This is a function of the willingness for data sharing amongst the stakeholders, the technical arrangements to do so, and the legal possibilities to indeed collect, use and share data from a range of sources. Furthermore, the MIK should significantly expand its capacity and capability to process and analyze the data. Close cooperation with other data and analysis cells is required, such as the navy's future Maritime Operations Center and the monitoring and risk analysis center(s) of Frontex.

The importance of cyberspace. MSA/SU is not restricted to the physical dimension, as threats in cyberspace are rapidly gaining prominence as a key security challenge. Capabilities to promote cybersecurity and counter cyberattacks are as important in the maritime sector as elsewhere, as remote operations for both shipping and infrastructure at sea become commonplace. Certainly in this area, but also for Critical Infrastructure Protection in general, offshore infrastructure should be considered an integral part of vital national processes – which it currently is not. Seabed warfare is another novel area that warrants close attention, requiring capabilities to detect and counter manipulation of undersea communication cables in particular.

As the functioning of the NLCG increasingly depends on real time information and intelligence sharing, connectedness between the Coast Guard Center, the MOC, sensors at sea (including future surveillance drones), and the operational units is a prerequisite. Indeed, the guaranteed availability of these connections should be seen as a critical process, as are the connections between auxiliary services onshore.

The area of interest expands. As economic activities in the North Sea move further offshore, assets to monitor security and respond rapidly to mounting threats and actual incidents over large maritime areas are needed. Given the current size of the NLCG and the RNLN, as well as a possible trend towards more high-end war ships rather than patrol ship type of naval vessels, it is necessary to analyze the required capacity for permanent presence over large swaths of the North Sea. This might require more sensors and platforms (ships as well as airborne platforms, both manned and unmanned) for permanent monitoring and rapid response over large and relatively distant sea areas.

The relationship between Coast Guard and Navy remains crucial. Given the expanding risk palette, the division of maritime security responsibilities and mandates between the various public, private and public-private stakeholders must be fundamentally revisited. As the nature, origin and possible follow-on consequences of various foreseeable security incidents may remain unclear until late in the process, operational flexibility between the various responders is key. This is particularly true for hybrid threats, which may overlap with criminal and terrorist threats on the one hand, and with military threats by state actors on the other.

With many organizations involved in maintaining security in and of the North Sea, each with its own mandate and task profile, the intimate relationship between the Netherlands Coast Guard and the Royal Netherlands Navy is a key asset to guarantee operational solutions that smooth over institutional ambiguities and seamlessly align the required capabilities from various sources. We have advocated a construct that brings as much as possible clarity in the fruitful cooperation between the NLCG, the RNLN and other agencies. This construct gives the NLCG additional executive authority under the umbrella of the North Sea Authority, with the latter guaranteeing institutional embedding while the NLCG and its partners concentrate on operational security in and of the North Sea.

Annex A:
Consulted experts

Expert interviews were conducted with the following persons.

Neptune Energy

- Lex de Groot, Managing Director, Neptune Energy Netherlands B.V.
- Phil Jones, Chief Security Officer, Neptune Energy
- Tim Dop, Security & Emergency Response Coordinator, Neptune Energy

Port of Rotterdam

- Alan Dirks, Program Manager Policy & Planning, Port of Rotterdam
- Douwe van der Stroom, Business Manager, Energy Transition & Digitalisation, Port of Rotterdam
- Three other interviewees prefer to remain anonymous

TNO

- René Peters, Business Director Gas Technology

Coast Guard

- Astrid Driesprong, Human Environment and Transport Inspectorate
- Norwin Kraaij, Human Environment and Transport Inspectorate
- Mick Lastdrager, Team Maritime Police
- Bastiaan Maltha, Coast Guard (seconded from Ministry of Infrastructure and Water Management)
- Hans Witte, Ministry of Infrastructure and Water Management
- Herman Schooljan, Coast Guard
- A representative of The Royal Netherlands Marechaussee

Members of the **sounding board** for the project also provided valuable feedback

- Ivo Moerman, RNLN
- Herman Schooljan, Coast Guard
- Rouby Smit, Coast Guard
- Bastiaan Maltha, Coast Guard (seconded from Ministry of Infrastructure and Water Management)
- Wouter van der Hilst, Coast Guard
- Roy de Ruiter, RNLN
- Pieterbas Peters, RNLN

Annex B:
Legend overview maps

Legend

Trade and Transport

- Shipping lane with infrastructure
- Shipping lane/corridor
- Anchorage
- Ship
- Highly combustable

Energy

- Offshore wind farm
- Solar energy
- High voltage cable
- Energy island (2050)
- Power-to-gas hydrogen hub
- Gas & oil platform*
- Re-used gas & oil platform*
- Hydrogen platform
- Carbon storage platform
- Inactive platform
- Decommissioned platform
- Gas / oil platform with sensing equipment

Communication and Sensing

- Telecommunication cable
- Sensing buoy
- Sensing platform
- Sensing tower
- Data center

* vast majority are gas platforms

Industrial Activities

- Sand dredging

Fishing

- Mariculture

Conservation

- Natura 2000

Military Activities

- Military exercise area (e.g., live fire area, mine clearance area & low flying area)

Other

- Dutch EEZ border
- Land reclamation for housing
- Schiphol at sea

Sources

"Militair gebruik." n.d. Noordzeeloket. https://www.noordzeeloket.nl/functies-gebruik/militair-gebruik/.
Ministerie van Economische Zaken en Klimaat "Windenergie op zee - Duurzame energie." August 11, 2016. https://www.rijksoverheid.nl/onderwerpen/duurzame-energie/windenergie-op-zee.
Nexstep. 2021. "Re-Use & Decommissiong Report 2021." https://www.nexstep.nl/re-use-decommissioning-report-2021/.
"Noordzee Natura 2000." n.d. Noordzeeloket. https://www.noordzeeloket.nl/beleid/noordzee-natura-2000/.
"Oppervlaktedelfstoffenwinning." n.d. Noordzeeloket. https://www.noordzeeloket.nl/functies-gebruik/artikel-baseline/.
Rijkswaterstaat. n.d. "Dataregister Rijkswaterstaat." https://maps.rijkswaterstaat.nl/dataregister/srv/dut/catalog.search#/map.
"Scheepvaart." n.d. Noordzeeloket. https://www.noordzeeloket.nl/functies-gebruik/scheepvaart/.
TeleGeography. n.d. "Submarine Cable Map." https://Www.Submarinecablemap.Com/. Accessed August 4, 2021. https://www.submarinecablemap.com/.
"Wind op zee tot en met 2030." n.d. Rijksoverheid. https://windopzee.nl/onderwerpen/wind-zee/wanneer-hoeveel/wind-zee-2030/.
"Windenergie op zee." n.d. Noordzeeloket. https://www.noordzeeloket.nl/functies-gebruik/windenergie/.

Disclaimers

The locations of platforms, shipping lanes, buoys and other designated areas are not 100% accurate due to practical constraints.

As projects currently remain undefined and the future is surrounded with a great deal of uncertainty, liberties were taken when designating future wind farms, energy islands, land reclamation areas and other areas.

The total construction of wind parks in 2050 is based on the complete use of all the search areas and additional search areas specified in the 2022-2027 program. The 2035 map is based on the construction plans for wind farms until 2030 and on additional sustainable energy production targets for 2035.

On the 2035 and 2050 maps mutually exclusive uses of the North Sea - such as wind power production and military training zones - overlap. This is the case because final decisions on priority of one use over another have not been made.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl