CHAPTER 12

Prevention and Detection of Adversarial Threats to Vital Infrastructure at Sea: An Operational Analysis Approach

Martijn van Ee, René Janssen, Relinde Jurrius, Hans Melissen, Herman Monsuur, and Alexander van Oers

Abstract

Climate change has given impetus to the task of reducing the fossil footprint. This has led to major investments in offshore wind farms. Sabotaging this vital infrastructure, including the cables connecting them to the mainland, can cause significant damage with immense consequences. It has resulted in a new homeland defense task for the Netherlands Coast Guard: maritime security. The recent acknowledgment by NATO and the EU that enemy states can use deliberate attacks on vital (military) infrastructure has sparked new interest in the analysis of these kinds of security threats. By using the quantitative operational analysis approach presented and promoted in this article, insight can be gained into the structure of optimal surveillance patrols of vital (military) infrastructure. These patrols by Coast Guard platforms, unmanned and manned, contribute to operational climate security strategies with regard to prevention and detection. The analysis can also support procurement and development policies. To identify optimal surveillance patrols (given the cable networks, limited security resources, intelligent and adaptive behaviour of the adversary, etc.), we focus on maximising the protection time (the amount of time the attacker needs to execute its task successfully) and minimising the detection time (required time for the defender to detect that the infrastructure is compromised and degraded). In our models we use network science (the topology of the cable network), game theory and optimisation theory (the strategic interaction between Coast Guard maritime patrols and its adversaries, and optimal allocation of limited security resources), and probability theory and machine learning (detection of anomalous behaviour). We illustrate our approach using two illustrative examples, which also underpin the added value of including the reaction of adversaries into our models.

Keywords: critical infrastructure security and resilience, maritime security, rural postman problem, game theory, climate change

12.1 Introduction

The main consequence of climate change is global warming, causing irreversible disruption to global weather systems and the entire water cycle. As a result, more extreme weather types will exacerbate water-related hazards such as extreme droughts and major floods. The first main consequence of climate change therefore is the scarcity of drinking water, food, and a safe living environment. Subsequently, this results in a scarcity of energy and raw materials that are necessary to adapt to these changing preconditions. Secondly, scarcity leads to further weakening of fragile states, but also to opportunities for powers seeking expansion or disruption, which will ultimately result in conflict and strife (Houben, 2017).

Society's response to climate change is twofold. First, strengthening resilience to cope with the far-reaching consequences of climate change and the resulting scarcity and safety issues (for example through the involvement of the Royal Netherlands Navy at St. Maarten after the hurricane Irma in 2017), i.e., making society shock-resistant. Second, tackling the causes of climate change for instance, by accelerating the energy transition. The construction of large offshore wind farms is an example of how this policy of generating energy security can be put into practice.

One aspect that is often overlooked is that the energy transition is occurring amidst increasing conflicts and strife. For instance, between 1970 and 2018, there were nearly 2,000 terrorist incidents targeting gas or oil facilities (Lee, 2022). The economic globalisation of recent decades has primarily been driven by cost considerations, causing aspects such as security and autonomy to gradually receive less attention. The latter is reinforced by the fact that there is often not one authority responsible for setting up facilities at sea (Bekker et al., 2021). It has become evident that not all participants in the field are as reliable as assumed or hoped. The recent conflict in Ukraine has served as a stark reminder of how economic interdependence with malicious powers can significantly disrupt the world order in terms of energy and food supplies. The sabotage of the Nord Stream 1 and 2 gas pipelines exposed the vulnerability of both energy and information infrastructure in a resounding manner. Power cables connecting offshore wind turbines to the mainland, global information networks, and pipelines are susceptible to sabotage by terrorist groups or hostile powers. Alternative approaches, such as converting wind energy into liquefied ammonia for easier transportation and storage, bring about potential safety and environmental risks for the transport network.

Disruption of these networks can have significant consequences for both energy and information supply. Climate change acts as a threat multiplier, impacting security, critical infrastructure, and military operations. NATO's role in energy security was defined at the Bucharest Summit in 2008, recognising that disruptions in energy supplies have a substantial impact on the safety of NATO members and

can affect military operations (Olech, 2022). More recently, in January 2023, NATO and the EU agreed to establish a joint task force on resilience and critical infrastructure. The task force aims to enhance the resilience of critical infrastructure, technology, and supply chains against potential threats, and take action to mitigate vulnerabilities (European Commission, 2023).

In the North Sea, sea-based economic activities are rapidly expanding in size and complexity. These activities offer opportunities for malicious actors, as highlighted by The Hague Centre for Strategic Studies (Bekker et al., 2021). Their report analysed the associated consequences for the Netherlands Coast Guard (NLCG) and the Royal Netherlands Navy (RNLN). The report emphasised the need to integrate information from various sources to establish comprehensive maritime situational awareness and understanding. Permanent sensors to monitor large sea areas, including surveillance drones, are valuable assets for enhancing situational awareness. The NLCG is leading efforts to protect wind farms, pipelines, and communication cables at sea within the context of maritime security. Ensuring the security of these cables and wind farms remains a critical concern.

Our article serves as a plea to approach maritime security and the challenges posed by climate change in the context of adversaries or opponents, utilising a quantitative operational analysis approach. The ultimate goal is to create a safer living environment. Designing solutions to the multifaceted challenges of climate change involves numerous considerations that often conflict with each other, such as efficiency, effectiveness, cost, scarcity, security, risk management, and hostile interventions. Quantitative risk-informed decision-support models derived from operational analysis offer a natural framework to substantiate these efforts. They can assist in prioritising infrastructure investments based on quantitative risk assessments.

The general methodology of quantitative operational analysis is as follows. First, all relevant aspects, including desired objectives and imposed limitations of the problem, are incorporated into a mathematical model. The model, along with the experiences of the user, forms a system. In other words, the model functions as a link or moderator between observed reality and the model's designer/user/client (De Regt, 2017). By applying the model to the field of protection, calculations can provide insights into optimal inspection routines for wind farms and cabling, maximising protection time while minimising detection time. The model can also help determine the required military capabilities and doctrines. Theoretical concepts can be applied within the model to gain insights, which then serve as a platform for discussions with military experts. It is important to note that the model is not an endpoint but rather a starting point for discussion. Through this iterative process, one can identify the relevant parameters of the system and refine the model (also see Jacobs and Meester, 2023).

Although legal experts, maritime safety- and security professionals, government policy makers and the private sector alike, should expedite their efforts to deal with the increasing demand for maritime security, we focus on surveillance patrols only. To identify optimal surveillance patrols (given the cable networks, limited security resources, intelligent and adaptive behaviour of the adversary, etc.), we focus on maximising the protection time (the amount of time the attacker needs to execute its task successfully) and minimising the detection time (required time for the defender to detect that the infrastructure is compromised and degraded). Catching an adversary red-handed contributes to securing evidence, while pre-positioning other assets improves the time to recreate a safe system state. This means that surveillance of the network also contributes to minimising the reaction time (the time to recreate a safe system state and/or secure evidence); we will not elaborate on that in our contribution. The results are used for quantitative risk management and risk-informed decision-making, ultimately contributing to a safer, stable, and resilient (economic, social, and environmental) living environment.

In the next section, we introduce the protection, detection and reaction time in a general framework of Time-Based Security. In Section 3, using a few illustrative examples, we discuss models that focus on optimising the protection time. As adversaries introduce uncertainty regarding when and where they will attack a network of cables, we show the necessity and profitability of introducing randomness into our modus operandi. It shows how to manage adversarial risk. Section 4 summarises our approach and results.

12.2 Relevant Parameters in Critical Infrastructure Security and Resilience

Our aim is to model the security situations involved with offshore windmill parks with a model of Time-Based Security, (following Farhang & Grossklags, 2017). We will not elaborate on the details of the game-theoretical description of this model, but emphasise the three important parameters the model is based on: protection time, detection time, and reaction time (also called response time). Applied to our situation, they can be explained as follows.

12.2.1 Protection time

In general, the *protection time* represents the amount of time the attacker needs to execute its attack. For an offshore wind farm, this is a combination of the time needed to physically get to the desired location, added to the time needed for sabotage. Naturally, the aim is to design a system such that this time is as long as possible. This can be done by building resilience into the system. In case of an

offshore wind farm, one can think of placing the transformation station in a secure place: hiding its location, or guarding it with a lock. The cables can be protected by placing them in pipes, ensuring also protection against natural influences like sea life and corrosion. Note that there is a trade-off between these security measures and how easy it is to do maintenance on the system.

An interesting way to increase the protection time is by patrolling the wind farm. If an attacker needs to hide from time to time to stay out of sight of the patrol, it will take longer to finalise an attack.

12.2.2 Detection time

It can take a long time before an attack is noticed in practice: think for example about infiltrating a secure cyber environment. And the longer it takes to detect an attack, the more harm can be done. Therefore, the goal of the designer of a system will be to decrease the *detection time*. Detecting an attack on an offshore wind farm consists of two phases: first, one detects that there has been an attack. Since the goal of an attack can be assumed to be a loss of power from the park, the detection of an attack is almost immediate. On the other hand, it is much harder to detect where in the park the problem exactly is and what this problem is (is one of the mills out of order, is it the transformation station, is it a cable?). One of the directions to tackle this problem is to use many sensors in the area. Power can be measured at multiple places in the park and this data can be monitored constantly. Video surveillance from the park itself can be captured, and there might be ships nearby whose location data can indicate suspicious behaviour.

However, this direction is expensive (many sensors needed), not failure proof (communication between sensors and observers can be attacked as well) and has several privacy issues (video surveillance, ship location data). This is why we argue that until this way of detecting is implemented, another way to decrease detection time is needed. Again, patrolling can be a very effective way to determine the exact location of an attack.

12.2.3 Reaction time

The *reaction time* is the time between the detection of the attack and the moment that the system is operational again. It is not necessary that the system is fully operational and in its original state: it can be that a backup is running, allowing for more time to repair the system in total. This time includes the time needed for repairs, but also travelling to the location of the attack. The first type of time can be shortened by the design of the system. In the case of a windmill park, there can be several cables connecting it to the coast. Inside the park, redundancy can be

built in. This is closely related to the improvement of protection time, as discussed before: redundancy will both improve the resilience of a park against attacks, as well as improve the reaction time once an attack has occurred. Optimising the time needed to get to the place where repairs need to happen, in this case the wind farm, can be done for example by placing repair teams at strategic places.

12.2.4 Improving the protection and detection time using patrols

We have discussed the three parameters from the general Time-Based Security model, and illustrated their meaning for the security of an offshore wind farm: protection time, detection time, and reaction time. The NLCG traditionally focuses on shortening the reaction time: if a distress call from the sea comes in, they are well prepared to get there as fast as possible. Dealing with protection and detection of attacks on wind farms is a new task for the NLCG. As seen, effective patrolling can be used to improve both these parameters. In the following section we will discuss several techniques to optimise surveillance, by means of examples.

12.3 Maritime Security: Wind Farms and Seabed Warfare

In this section, we introduce our two illustrative cases in the first subsection. In the second subsection, we show how to determine and improve the maximum time between two surveillance visits along the network, which will be called the inter-arrival time. It shows that maintaining acceptable inter-arrival times necessitates a large fleet of UUvs (unmanned/autonomous underwater vehicles), which may not be available. In addition to that, another challenge arises as adversaries may observe the defensive surveillance patterns to estimate the inter-arrival time, allowing them to plan their attacks accordingly. A way out, tackling both scarcity of resources and the issue of an intelligent and adaptive adversary, is to introduce randomness in the modus operandi in an optimal way: game-theoretic risk management. This is discussed in the third subsection.

12.3.1 Description of the two cases

In this section, we illustrate the application of operational analysis to optimise the surveillance of underwater cables of wind farms and oil or gas pipelines using two examples. The first case resembles part of a network of oil pipelines near the isle of Ameland in the Netherlands, containing 98.5 NM pipelines connecting (underwater) platforms 1, 2, 6, 7, 8, and 9 with a through pipeline 3-2-4-5 (Figure 12.1). The second case is a network of underwater cables from the Luchterduinen wind

farm in the Netherlands, containing 15 NM cables connecting 43 wind turbines to the transformation station (Figure 12.2). We assume we can use unmanned/autonomous underwater vehicles (UUVs/AUVs) that can detect anomalies while travelling along a cable or pipeline. For our computations, we assume a cruising speed of 2 knots. To impede sabotage of our network, our goal will be to design surveillance routes that cover every cable or pipeline, while minimising the maximum time between two surveillance visits (inter-arrival time) along the network.

Minimising the maximum time between two surveillance visits contributes to the task of improving the protection time (and detection time as well). If the inter-arrival time along the cables is small, an attacker is faced with the problem of executing its malicious task within that small time-frame. If the time needed to interrupt the operation of the network is larger than this inter-arrival time, the action surely will be detected, and also possibly prevented. We will consider this protection time given the technical parameters of the UUV and the number of UUVs available for the surveillance. This problem of minimising the inter-arrival time is related to the so-called *periodic latency problem* (Coene et al., 2011). It describes the problem during the reign of Charlemagne (768–814 AD). Counts had been appointed to govern different pieces of Charlemagne's empire, called counties. Charlemagne's challenge was to find a visiting sequence of his counts so that the time elapsed between two consecutive visits to a count would not exceed the "loyalty period" of that count. Not visiting a count for a certain period imposed a risk regarding the obedience to Charlemagne.

Figure 12.1. Network of oil pipelines near Ameland.

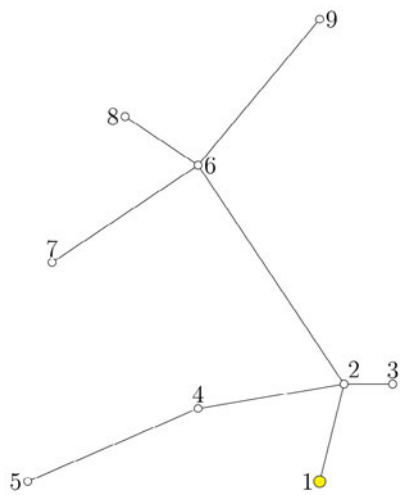
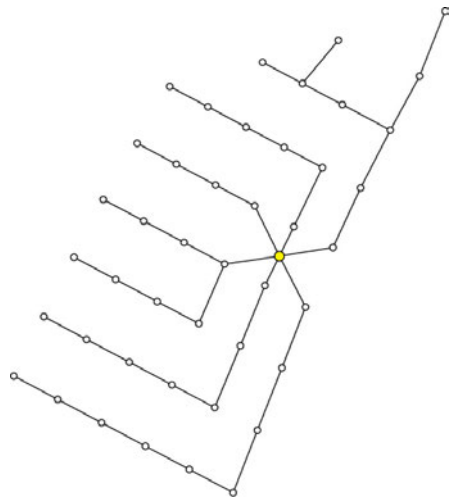


Figure 12.2. Luchterduinen wind farm.

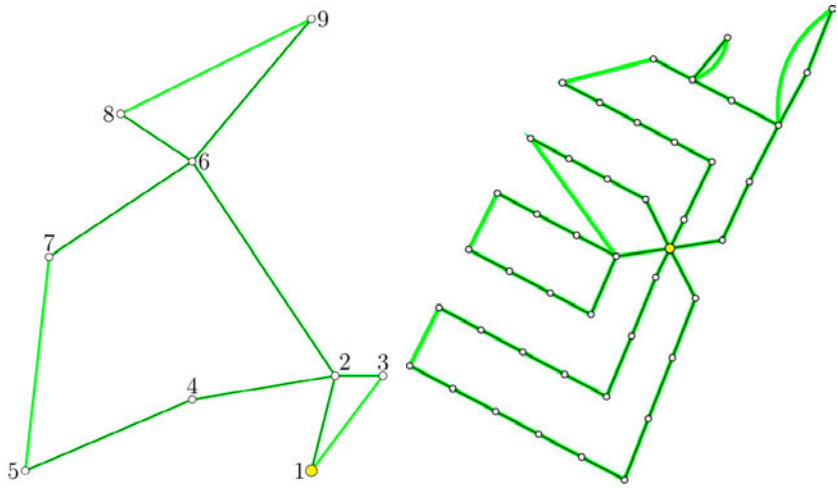


12.3.2 Modelling for risk informed decision making: output of models and discussion

Initially, we assume that we can deploy one operational UUV without range limitation that is restricted to move along the cables or pipelines. Since our networks are so-called trees, i.e., there are no cycles in the network, the optimal tours can be found by tracing the outside of the network, leading to solutions that visit each edge (pipeline or cable) in the network exactly twice, starting and ending at the yellow nodes. We note that this optimisation problem, known as the Chinese postman problem (Edmonds & Johnson, 1973), can also be efficiently solved when the network is not a tree. The total distance travelled in our first case study is 197 NM, which will take the UUV 98.5 hours. In the second case, the total distance travelled is 30 NM requiring 15 hours of surveillance time. Apart from range considerations of our UUV, the time between two visits at any position along the network is large. Therefore, we will relax the condition that the UUV can only travel along the edges of the network.

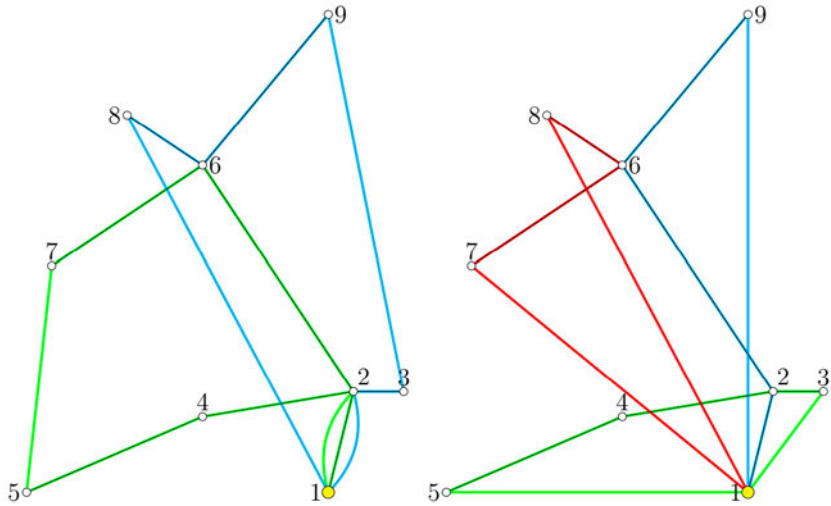
In our next problem setting, which is called the rural postman problem (Eiselt et al., 1995), we need to visit every edge at least once, where travel along non-edges is also permitted, and our goal is to find the shortest tour. In general, the rural postman problem is a computationally challenging problem, i.e., an NP-hard problem (Lenstra & Rinnooy Kan, 1976), but since our networks are connected, i.e., between any two points on the network there is a route using only cables or pipelines, the problem can be solved efficiently (Brandão & Eglese, 2008). To see this, note that the edges and non-edges used in the tour form a connected network, where the total number of edges and non-edges that are attached to any node is even. Since the edges that need to be visited already form a connected network, we only have to add non-edges in the cheapest possible way such that the nodes with an odd number of edges attached to it get a non-edge attached to it. This is done by introducing extra non-edges pairing nodes with an odd number of edges attached to it, minimising the overall length of these pairing edges. The original network, together with these pairing edges forms a minimal length tour covering the network. The resulting tours are depicted in Figure 12.3. In the first case, the total distance travelled reduces from 197 NM to 146 NM, which requires 73 operational hours. In the second case, the total distance travelled is reduced from 30 NM to 18.8 NM, which will take 9 hours and 24 minutes.

Figure 12.3. Optimal solution of the rural postman for the first case (left part), and optimal solution for the second case (right part).



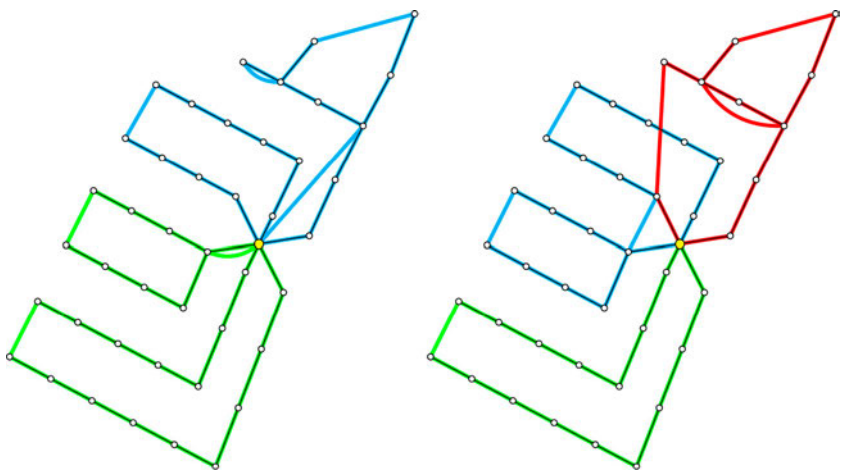
Since the inter-arrival times are equal to the total surveillance time of the tour, they are still quite large; we could deploy more UUVs to reduce the inter-arrival times. We now make a distinction between cases where the UUVs have a restricted range or an unrestricted range. If the range of the UUVs is unrestricted (or more than the length of the optimal tour for one vehicle), we can achieve an inter-arrival time which is equal to the original inter-arrival time divided by the number of UUVs. This is obtained by assigning the original tour to each UUV, where the starting locations of the UUVs are distributed uniformly along the tour. It is the best inter-arrival time obtainable given the number of UUVs. However, if the range of the UUVs is restricted, it might not be feasible that each UUV visits every edge. In that case UUVs possibly get different tours assigned, which will also result in reduced inter-arrival times. Since we aim for a low inter-arrival time at each position in the network, our objective becomes to minimise the largest tour length across all UUVs. For simplicity, we assume that each edge in the network is visited by exactly one of the UUVs. These problems can be solved using integer linear programming methods (Wolsey, 2020). The results for the first case are depicted in Figure 12.4, using two and three UUVs, respectively. It is assumed that all UUVs need to recharge at Node 1. Inter-arrival times are reduced to 49 hours and 51 minutes, and 42 hours and 2 minutes, respectively. If these inter-arrival times still exceed the range of the UUVs, more UUVs are needed for a feasible solution.

Figure 12.4: Routes for two (left part) and three (right part) UVVs for case 1.



The results for the second case are depicted in Figure 12.5. Here, the inter-arrival times reduce to 4 hours and 52 minutes, and 3 hours and 21 minutes, respectively.

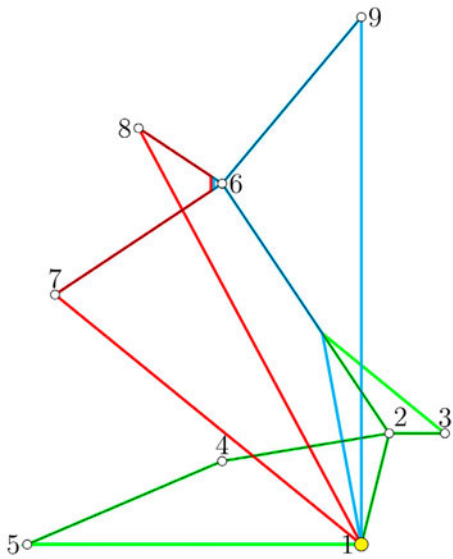
Figure 12.5. Routes for two (left part) and three (right part) UUVs for case 2.



We note that the used models are basic. However, they can easily be modified to include other real-life considerations. For example, if the endurance of the UUVs depends on the speed that is used, we could include the possibility of varying the speed along the tour and keeping track of the remaining range. Finally, we note that

the objective can be slightly improved by relaxing the requirement that each edge is visited by exactly one UUV. An illustration of this phenomenon can be found in Figure 12.6 where UUVs with slack operating time take over parts of the pipelines from the critical UUV, thus reducing the inter-arrival time slightly to 41 hours and 51 minutes. It might also be better to let certain edges be visited by multiple UUVs, like in the case with unrestricted range. Coordination between the different UUVs will be vital to employ such a strategy. Therefore, we think it is an interesting problem for further research.

Figure 12.6. Alternative solution utilising slack operating time of other UUVs.



So far, we have shown how techniques from operations research can be used to design surveillance routes that curtail the operational time of adversaries seeking to damage our networks. We will now discuss possible directions for further research.

Until now we have implicitly assumed that every cable or pipe is equally important. In reality, some parts of the network may represent a higher risk than others. Damage to cables closer to the transformation station will have a greater impact on energy production, so these cables will have to be scanned more often. Also, given the shipping routes in the North Sea and, in addition, competing interests, various risk and threat scenarios may emerge. In that case, desired inter-arrival times may differ from one location to the other. Compare Gabriel et al. (2022), who use Bayesian

Networks to assess the risk, incorporating modern data science techniques. Given the desired inter-arrival time per edge and range per UUV, the minimum number of UUVs to be deployed could be calculated. This leads to a problem related to the periodic latency problem (Coene et al., 2011, Sanchez, 2013). Other variants related to desired inter-arrival times are the window scheduling problem (Bar-Noy et al., 2012), as well as other similar problems from literature (Holte et al., 1989, Bosman et al., 2022, Gąsieniec et al., 2017, Van Ee, 2021, Evers et al., 2014).

12.3.3 Introducing uncertainty for the adversary: a game-theoretic approach

As mentioned earlier, given the desired inter-arrival time per edge, and the range per UUV, one may determine the minimum number of UUVs required. Our examples have shown that maintaining small inter-arrival times necessitates a large fleet of UUVs. However, when such a large fleet is not available, this leads to the problem of resource scarcity. Another challenge arises from intelligent adversaries who may observe the defensive surveillance pattern to estimate the inter-arrival time, allowing them to plan their attacks accordingly.

To address these issues, one possible solution is to introduce randomisation of routes or patrols in an optimal manner. This introduces uncertainty and helps counteract the problem of scarcity. One approach to introducing this uncertainty while considering adversary observation is the game-theoretic approach. Game theory has been extensively studied in the field of security games, as seen in the literature (Tambe, 2012). Defensive procedures based on these games have been implemented at locations such as LAX airport and by the US Coast Guard. By employing random patrols, these procedures maximise unpredictability for the adversary while maintaining a high probability of detecting them. For an application related to border security, involving partial information on the state of the game for both players, see Laan et al. (2019).

In this contribution, we again restrict ourselves to the network of cables. To this end, we divide the edges into smaller ones, such that traversing each edge takes one time-step. A patrol on the original network of cables then corresponds to a patrol of adjacent edges, where each edge takes one time-step. But our class of patrols is larger than before: patrols may change direction, for example halfway on an original edge. In addition, we also consider patrols that do not visit each edge, and patrols that stay at an edge for more than one time step, i.e., wait at that edge hoping to interdict the adversary.

We further assume that the adversary needs m time-steps to perform the attack on any edge: this is part of the protection time discussed in section 2.1. If it performs its attack at time t, it is present at the edge at time-steps t, t+1, ..., t+m-1. The patrol catches the intruder in the act if it visits this particular edge at some time between

t and $t+m-1$. Indeed, the game between the patrol and the adversary involves strategic choices for both players. The adversary must select which edge to attack and when to initiate the attack, while the patrol needs to determine its route and the timing of its patrol. Both players strive to optimise their strategies.

The probability of detecting the adversary is at least $1/n$, where n represents the total number of edges: the patrol can choose to stay at a uniformly randomly selected edge. To achieve stronger results, the concept of intercepting strategies can be introduced. An intercepting strategy for a given edge is a patrol that ensures the inter-arrival time for that edge is no greater than m. However, such a patrol may not visit all edges. A covering set refers to a collection of intercepting strategies where each edge is included in at least one intercepting strategy. If the number of these strategies is denoted as C, then the probability of detection is guaranteed to be at least $1/C$ by randomly selecting one of these intercepting strategies. Considering these factors, it is indeed desirable to design wind farms and the topology of their connecting cables in a way that minimises the number of required intercepting patrols (C). This contributes to the resilience of the system and strengthens its ability to withstand potential attacks.

12.4 Conclusion

In this contribution, we have presented our quantitative operational analysis approach for determining optimal surveillance patrols for seabed cables and offshore wind farms, with a specific focus on optimising protection and detection time. Our approach and the resulting insight can also be applied to the issue of how to strategically position NLCG assets at sea, enabling threat deterrence, optimal protection time, quick response time, and optimising reaction capabilities.

The theory presented here is part of the broader field of search and detection theory. Typically, the sea is divided into sectors, with each sector assigned a probability of containing the target or adversary being sought. Well-known formulas, such as the random search formula, can be utilised to calculate the probability of detection (Washburn, 2002). These formulas have been employed in various studies. This includes the optimal search for intruders in the Port of Rotterdam (Zijlstra, 2019) after initial detection of intrusion, enabling securing of evidence. Another example is the coordination of cooperative drones during area search (Zijlstra, 2022).

In this chapter, we adopted a different approach by focusing solely on patrolling the network (including hypothetical edges between nodes), as we were aware that an attacker needs to attack an edge of the network. Our objective was (1) to reduce the inter-arrival time, consequently improving the probability of detecting

an attacker, and (2) introduce randomness in the patrols in an optimal way. Our models provide insight into assumptions and give suggestions for the deployment of available resources. This hopefully supports our plea to incorporate a quantitative OA approach into the analysis of information-driven operations for maritime security. The models and the insight they provide may serve as a platform for discussions with experts in critical infrastructure security and resilience, and more specific maritime safety and security, ensuring that the maritime environment is resilient enough to facilitate the growing demand in a sustainable manner.

References

Alpern, S., Morton, A., & Papadaki, K, (2011) Patrolling games. *Operations Research*, vol. 59 (5), 1246–1257.

Babriel, A., Tecklenburg, B., & Torres, F.S. (2022) *Threat and risk scenarios for Offshore wind farms and an approach to their assessment*. Proceedings of the 19th ISCRAM conference, France, May 2022.

Bar-Noy, A., Ladner, R. E., Tamir, T., & VanDeGrift, T. (2012) Windows scheduling of arbitrary-length jobs on multiple machines. *Journal of Scheduling*, *15*, 141–155.

Bekkers, F., Teer, J., Kool, D, van Geuns, L., Bolder, P., Patrahau, I., & Sarel, M. (2021) *The High Value of The North Sea*. Report The Hague Centre for Strategic Studies.

Bosman, T., van Ee, M., Jiao, Y., Marchetti-Spaccamela, A., Ravi, R., & Stougie, L. (2022) Approximation algorithms for replenishment problems with fixed turnover times. *Algorithmica*, 84 (9), 2597–2621.

Brandão, J., & Eglese, R. (2008) A deterministic tabu search algorithm for the capacitated arc routing problem. *Computers & Operations Research*, *35*(4), 1112–1126.

Coene, S., Spieksma, F.C.R., & Woeginger, G.J. (2011) Charlemagne's challenge: The periodic latency problem. *Operations Research*, 59 (3), 674–683.

De Regt, H. (2017). *Understanding Scientific Understanding*. Oxford University Press.

Edmonds, J., & Johnson, E. L. (1973) Matching, Euler tours and the Chinese postman. *Mathematical programming*, *5*, 88–124.

van Ee, M. (2021) A 12/7-approximation algorithm for the discrete bamboo garden trimming problem. *Operations Research Letters*, 49 (5), 645–649.

Eiselt, H. A., Gendreau, M., & Laporte, G. (1995) Arc routing problems, part II: The rural postman problem. *Operations Research*, 43 (3), 399–414.

Evers L., Barros A.I., Monsuur H., & Wagelmans A. (2014) online stochastic UAV mission planning with time windows and time-sensitive targets. *European Journal of Operational Research*, 238 (1), 248-362.

European Commission (2023) Statement / 23 /1705.

Farhang, S., & Grossklags, J. (2017) When to invest in security? Empirical evidence and a game-theoretic approach for time-based security. In: *Workshop on the Economics of Information Security* (WEIS) 2017.

Gąsieniec, L., Klasing, R., Levcopoulos, C., Lingas, A., Min, J., & Radzik, T. (2017) Bamboo garden trimming problem (perpetual maintenance of machines with different attendance urgency factors). In: *SOFSEM 2017: Theory and Practice of Computer Science: 43rd International Conference on Current Trends in Theory and Practice of Computer Science, Limerick, Ireland, January 16–20, 2017, Proceedings* (pp. 229–240). Cham: Springer International Publishing.

Holte, R., Mok, A., Rosier, L., Tulchinsky, I., & Varvel, D. (1989) The pinwheel: A real-time scheduling problem. In: *Proceedings of the 22nd Hawaii International Conference of System Science* (pp. 693–702).

Houben, M.F.J. (2017) Klimaatveiligheid. *Militaire Spectator*, 186 (2), 92–93.

Jacobs, M., & Meester, R. (2023) *Van aardbeving tot zoonose. Over de inzet van modellen voor beleid*. Mazirel Pers.

Laan, C.M., Barros, A.I., Boucherie, R.J., Monsuur, H., & Timmer, J. (2019) Solving partially observable agent-intruder games with an application to border security problems. *Naval Research Logistics*, 66 (2), 174–190.

Lee, Chia-yi. (2022) Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure. *Energy Research & Social Science*, 87.

Lenstra, J. K., & Rinnooy Kan, A.H.G. (1976) On general routing problems. *Networks*, *6* (3), 273–280.

Olech, A. (2022) Terrorist threats to the energy sector in Africa and the Middle East. In: Sarah J. Lohmann, Lucas M. Cox, Denise Feldner, Trevor P. Helmy, Frank J. Kuzminski, Marcus Mohlin, Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu, Silke Ruhl, Sabrina Schulz, Máté Tóth, and Megan A. Ward, *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency* (NATO COE-DAT Handbook 2) (Carlisle, PA: US Army War College Press, 2022).

Sanchez, J. (2013) *Optimale patrouilleschema's voor het inspecteren van ankergebieden met USV's*. Bsc thesis Operational analysis, Faculty of Military Sciences, Den Helder.

Tambe, M. (2012) *Security and Game Theory. Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press.

Wolsey, L. A. (2020) *Integer Programming*. John Wiley & Sons.

Washburn, A. (2002) *Search and Detection* (4th ed). Institute for OR and MS

Zijlstra, B.E.E. (2019) *Indringer in containerterminal zoeken met een drone.* BSc-thesis MS&T. Faculty of Military Sciences, Den Helder.

Zijlstra, T. (2022) *The influence of communication protocols on the performance of a greedy search strategy for maritime S&D missions*. MSc thesis, Erasmus University, Rotterdam