Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26096-cd

A Probabilistic Model for Evaluating Critical Maritime Infrastructure Security

Lara Beßmann, Sarra Majri, Jan Stockbrügger, Frank Sill Torres

Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR), Germany.
E-mail: lara.bessmann@dlr.de, sarra.majri@dlr.de, jan.stockbruegger@dlr.de, frank.silltorres@dlr.de

Offshore infrastructures, including wind farms and subsea data and power cables, are expanding rapidly. These infrastructures face increasing threats from hybrid attacks by drones and vessels, as well as marine accidents. To support the evaluation of the vulnerability of offshore assets, we develop a model for maritime infrastructure protection analysis. The model seeks to determine the probability that a defender can intervene fast enough to prevent an attack against an offshore asset such as an infrastructure by regarding various parameters. For the computation, a Monte Carlo simulation is employed, enabling the exploration of diverse settings and conditions and producing an overall security assessment based on specific yet adjustable probability distributions to capture uncertainties that are inherent in maritime security analysis. We illustrate the model by analyzing the protection level of an offshore wind farm off the German coast, incorporating varying capability distributions for attackers and defenders. Results indicate that the model generates methodologically sound estimates of offshore protection levels and to identify and calculate factors that can enhance protection effectiveness, such as expanding the detection range, reducing reaction times, deploying faster intervention units, or stationing them closer to offshore assets. Finally, we discuss the major strengths and limitations of the model compared to other approaches and propose avenues for future research in maritime security analysis.

Keywords: Infrastructure Protection, Offshore Infrastructures, Vulnerability Assessment, Protection level, Probabilistic Model, Monte Carlo Simulation.

1. Introduction

Maritime infrastructures such as offshore wind parks and data and electricity cables are expanding rapidly and play an important role in sustaining modern societies. However, these infrastructures are also increasingly threatened by safety and security incidents with potentially disastrous consequences. These threats are amplified by geopolitical competition and growing maritime traffic near critical offshore communication and energy infrastructures. There is thus a growing need to protect maritime and offshore infrastructures.

Threats to offshore infrastructures include drones recently sighted near maritime ports and major coastal airports, sabotage of subsea infrastructures such as pipelines and cables and the growing number of vessels that deactivate their Automatic Identification System to evade sanctions and conduct espionage activities. There are also significant safety risk at sea, especially in areas with dense marine traffic (Tecklenburg et al., 2025). For example, in April 2023 the cargo vessel *PETRA L* collided with the wind park *Gode Wind 1* in the German North Sea. The vessel was sailing on autopilot kilometers off course, yet neither the wind farm operators nor traffic authorities noticed the vessel as it approached the wind farm. For the detailed survey of the incident see (Bundesstelle für Seeunfalluntersuchung, 2025).

Yet protecting maritime infrastructures against such threats is a major challenge. The vastness of the sea does not allow for complete monitoring and a permanent presence of security forces near infrastructures as indicated in (Skobiej et al., 2024). Moreover, though offshore barriers exist - such as floating barriers that prevent vessels from moving into restricted areas, see e.g. (Knysh et al., 2021) - these are rarely deployed to protect offshore infrastructures such as wind farms and converter platforms.

We develop a model for maritime infrastructure protection analysis. The model seeks to determine the probability that a defender can intervene fast enough to prevent an attack against an offshore

asset such as an infrastructure. The model helps analysts to assess the vulnerability of exposed offshore assets.

In this model we do not consider physical barriers concretely, but they are implicit included since they slow down the potential threat and thus the average velocity is just lower which is considered in the regarded scenario. This has the advantage that it is not necessary to o specify which barriers are considered or the barrier's effectiveness in preventing or delaying an attack.

In (Lichte et al., 2021) the influence of uncertainties on the vulnerability of security systems is studied. Since the impact of uncertainties is crucial, they propose a model to cope with them. Moreover, their model is feasible for terrestrial infrastructures but due to the lack of physical barriers with attached sensors, it is not directly applicable to offshore infrastructures. Nevertheless, we also include uncertainties, but we do this through multiple simulations with variance in the variables to capture as many different scenarios as possible.

This paper aims at contributing to filling a critical gap in physical security analysis. A large literature exist that develops quantitative methods to evaluate physical security and protection levels for terrestrial infrastructures such as electricity and nuclear power plants (Loveček et al., 2021; Cheikh El Wely and Chetaine, 2021). However, very few efforts have been made to develop such a model in the maritime context and to assess and quantify the security of offshore assets such as wind farms and pipelines (Niemi et al., 2025; Hara and Sagara, 2025). This research thus provides new insights into an understudied area of security research.

The paper is structured as follows. We start with the statement of our main research question and a description of our model. To underline the applicability of our model, we compute an example and present the results. The conclusion highlights the paper's main findings and includes an outlook with further research questions and extensions of our approach.

2. Evaluating Security Threats and Protection Systems

There are different approaches to evaluate security threats and protections systems that lead to results of different types.

On the one hand, the evaluation can be based on expert driven methods like Bayesian-Networks, see e.g. (Ramírez-Agudelo et al., 2021) and (Iaiani et al., 2023) or adversary sequence diagrams as used in (Iaiani et al., 2022).

On the other hand, however, security evaluation can also be made with quantitative approaches. Such methods enable us to measure and quantify protection levels or the effectiveness of a protection systems using mathematical models and simulations to produce probabilities. For example there are different approaches of risk analysis as in (Martz and Johnson, 1987) and (McGill et al., 2007).

As pointed out before, most of these approaches are used for terrestrial infrastructures. However, since there are major differences to offshore infrastructures, existing models cannot directly be used. For example, one major difference between offshore and onshore protection models is the distances involved. Distances at sea, especially for offshore wind farms or underwater cables and pipelines located far off the coast, are much larger than on land, so that security forces need more time to intervene and stop an attack. Moreover, as indicated before, barrier systems are rarely used to protect maritime infrastructures such as offshore converter platforms (Tecklenburg et al., 2025).

3. The Model

The main research question that is considered to be answered with the model is:

> What is the probability that an intervention unit reaches an offshore infrastructure earlier than a detected possible threat, depending on the distance of detection?

In this section we describe first the basic setup and then the computations that lead to the answer of this question.

3.1. *Basic Setup*

The aim is to compute the probability whether an intervention could be in time depending on the distance in which a threat vessel is detected, which can be done using any sensor technology such as radar or optical cameras, and identified as a potential threat. In the following we will call this vessel *detected threat vessel*. We do not consider how this vessel is detected and why it is classified as a potential threat. We define *being in time* as reaching the infrastructure earlier than the detected threat vessel. A scenario is *successful* if the intervention unit reaches the infrastructure in time. To include uncertainties and cover different scenarios we do a Monte Carlo simulation. More precisely, for fixed $n \in \mathbb{N}$ we do n simulations for each distance of detection and use the results to compute the probability the research question asks for.

The model describes a simplified attack scenario and does not include parameters such as specific sensors, vessel types, how a threat is identified and whether an intervention unit is capable of disrupting an attack. Instead, it focuses on key parameters in attack scenarios to determine the probability that an attack can be disrupted, thus helping to evaluate important attack vulnerabilities.

3.2. *Computations*

For the computations Python 3.10.12 and NumPy 2.2.6 are used, additionally Matplotlib 3.10 is used to plot the results and distributions.

The core parameters, which are considered to be variable, are the velocity of the detected threat vessel, the velocity of the intervention unit and the distance between the intervention unit and the threat vessel. Further, for each of these core parameters a distribution is chosen in such a way that it represents the reality best. In particular, using a distribution for each core parameter lets us consider different weather conditions that influence the velocity and uncertainties that influence the intervention distance without knowing every possible combination of parameters. For each of these core parameters n samples are picked using the functionality NumPy provides. Then we have a collection of velocities for the detected threat vessel v_V, a list of the velocities for the intervention v_I and a list of the distance of the intervention d_I. For each $i \in \{1, \dots, n\}$ a scenario is defined to consist of three numbers: (1) the velocity of the detected threat vessel $v_V[i]$, (2) the velocity of the intervention $v_I[i]$ and (3) the intervention distance $d_I[i]$.

These numbers describe the scenario and determine how it proceeds. For each $i \in \{1, \dots, n\}$ the time the intervention needs is computed by

$$t_I[i] \;=\; d_I[i]/v_I[i]. \tag{1}$$

To obtain the probability that an intervention is successful, the following computations are done for each detection distance d_{det}. For each $i \in \{1, \dots, n\}$ the time the detected threat vessel needs is computed by

$$t_V(d_{det})[i] \;=\; d_{det}/v_V[i]. \tag{2}$$

To compare the times of the intervention and the detected threat vessel the following set

$$\begin{aligned} &S(d_{det}) \\ &= \{i \in \{1, \dots, n\} \mid t_V(d_{det})[i] \;>\; t_I[i]\}\,. \end{aligned} \tag{3}$$

is considered. The cardinality $\#S(d_{det})$ is the number of samples, in which the intervention reaches the infrastructure faster than the detected threat vessel. With this number the percentage of successful scenarios is computed as

$$p(d_{det}) = \frac{\#S(d_{det})}{n}. \tag{4}$$

Hence we obtain the probability $p(d_{det})$ that the intervention reaches the infrastructure in time depending on the distance of detection d_{det}.

4. Application Of The Model

To illustrate the model, we apply it to the offshore wind park *Deutsche Bucht* in the German North Sea. We start by describing the general setting, continue with the scenario and the assumptions we make and conclude with the results we obtain.

4.1. *Setup*

The designated shipping lane and traffic separation scheme *German Bright Western Approach* is

Fig. 1. The wind park *Deutsche Bucht* is marked with the location symbol. The ports and airports are marked with the vessel and helicopter symbols, respectively. The designated shipping lane is labeled. The map is from `openseamap.org`.

roughly between 10 and 30 km away from the borders of the wind park *Deutsche Bucht*.

For the intervention, two cases are considered. In the first case, the intervention is carried out by a vessel moored in one of the ports of *Emden, Norden* and *Borkum*, which are located 145 km, 115 km and 100 km from the wind park, respectively. In the second case the intervention is done with a helicopter stationed at either of the airports of *Norden* and *Sankt Peter-Ording*, which are located at a distance of roughly 120 km and 190 km, respectively, from the wind park. For a visualization of the general setting see Fig. 1.

4.1.1. *Scenario*

Assume that a vessel that passes near the wind park on the designated shipping lane suddenly changes its course and turns towards the wind park. The question is, thus, with which probability is an intervention unit earlier at the wind park than the detected threat vessel?

4.1.2. *Assumptions*

Since the designated shipping lane is located between 10 and 30 km away from the wind park, we consider detection distances from 10 to 40 km with steps of 500 m. Because of this assumption, we capture the width of the shipping lane and a certain range nearby.

We assume the speed of the detected threat vessel to be triangularly distributed with a minimum of 10 knots, a maximum of 50 knots and a peak at 20 knots. For a million samples see Fig. 2 for the distribution of the velocity. With such a distribution we cover various different vessels, including smaller speed boats and large cargo vessels and tankers. This distribution can also capture different conditions that influence the velocity of a vessel, e.g. different weather conditions and course changes due to obstacles such as other ships that

might affect the velocity of the threat vessel.

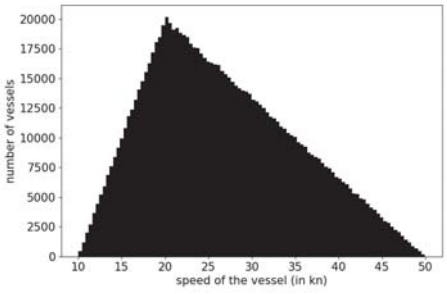

Fig. 2. Distribution of the velocity of the detected threat vessel.

For the intervention with a vessel, we assume that it is stationed at either of the ports, that means the distance of the vessel to the wind park is the distance of the port to the wind park. Moreover, we assume that in most cases the vessel departs from the nearest port. But to include cases in which the intervention vessel from a port closer to the wind farm is not available, we also regard scenarios where the vessel departs from one of the ports that are further away. Hence, the probability decreases while the distance increases. For a visualization of the distribution of a million samples for the distance of the intervention see Fig. 3. The inspiration for the velocity are the vessels

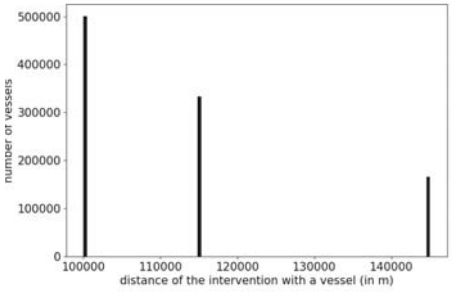

Fig. 3. Distribution of the distance of the intervention vessel.

of the federal police of Germany as described in (Bundespolizei, 2025). Hence we use a triangular distribution with minimum of 10 knots, maximum of 43 knots and the peak at 22 knots. For a visualization of the distribution of the samples for the velocity of the intervention see Fig. 4.

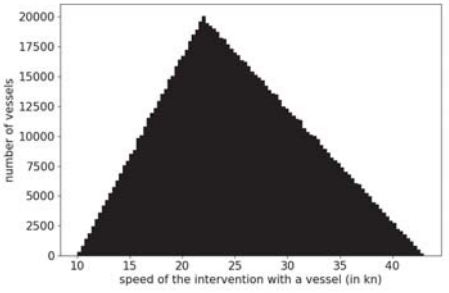

Fig. 4. Distribution of the velocity of the intervention vessel.

For the intervention with a helicopter, we assume that the helicopter is stationed at either of the airports mentioned above. We also assume, that in most cases the nearest helicopter is deployed to stop the attack. Additionally, we consider cases in which the helicopter from the airport that is farthest away is deployed. For a distribution of a million samples of the distance see Fig. 5. The

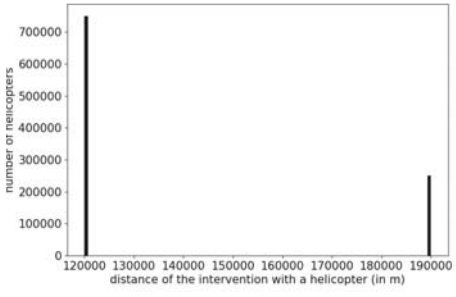

Fig. 5. Distribution of the distance of the intervention helicopter.

velocity of the helicopter is also triangularly distributed with a minimum 50 knots, a maximum of 175 knots and a peak at 130 knots. The inspiration for these numbers are the helicopters from the German navy as described at (Bundeswehr, 2025).

A visualization of the velocity is pictured in Fig. 6.

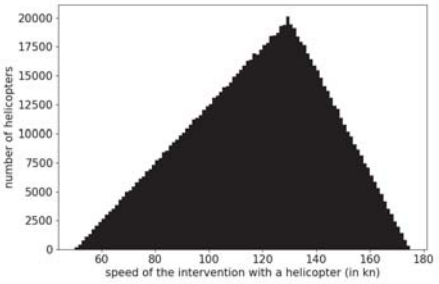

Fig. 6. Distribution of the velocity of the intervention helicopter.

For a summary of the assumptions on the velocities see Table 1.

Table 1. Summary of the velocities in the example.

	velocity (in knots)		
	min	max	peak
detected threat vessel	10	50	20
intervention vessel	10	43	22
intervention helicopter	50	175	130

4.2. *Results*

For the comparison of the probabilities whether the intervention will be in time depending on the used transportation unit see Fig. 7. The results show that only the intervention with a helicopter has a realistic chance to be in time to intercept the threat vessel.

If the vessel is detected at a distance of less or equal 25 km - which is a realistic radar detection distance - the intervention with a vessel has no chance to be in time at the wind park. Starting at a detection distance of 25.5 km, the chances start to grow slowly, but only reach a probability of 0.62% at a detection distance of 40 km.

The probability for the intervention with a helicopter has a higher chance to be successful. Even at a detection distance of only ten kilometers, the probability is not zero and at a detection distance of 17 km there is a probability of more than 10% that the intervention is in time. Moreover, at a detection distance of 29.5 km, the probability reaches more than 50% and at a detection distance of 40 km there is a probability of 75% that the intervention will be in time.

All in all, an intervention with a vessel that is stationed in a port only has a very low probability to be in time and reach the wind park before a detected threat vessel or boat. Hence, for a successful intervention either a helicopter is necessary or an intervention vessel that is very close to the wind park patrolling at a reasonable distance. Additionally, a lot of effort is needed to be able to detect a vessel and identify it as a potential threat so far away from an offshore wind park.In short, the results clearly indicate the challenges of ensuring timely intervention to intercept threats and secure offshore infrastructures. These challenges are likely to increase, as offshore wind farms located far off coastal ports are proliferating.

The results also contain key lessons for security practitioners and policymakers. They provide further evidence for the need to develop new security concepts for offshore infrastructure protection. This not only includes the need for more helicopters and aircraft, but also to use forward deployed drones and other unmanned platforms as additional intervention capabilities. Moreover, the distribution of intervention assets requires optimization to reduce intervention times and ensure intervention coverage of large maritime spaces. Additionally, further investments are required to enhance maritime surveillance capabilities around offshore infrastructures and to increase the ability of security agencies to detect potential threats before they approach a vulnerably offshore asset, thus enhancing the chances that they can intercept the threat. Finally, the paper shows that intervention capabilities need to be included in security analysis and physical protection systems for offshore infrastructures. Offshore security concepts for wind farms and other critical maritime infrastructures need to be based on integrated approaches that calculate security-levels based on detection and intervention times.

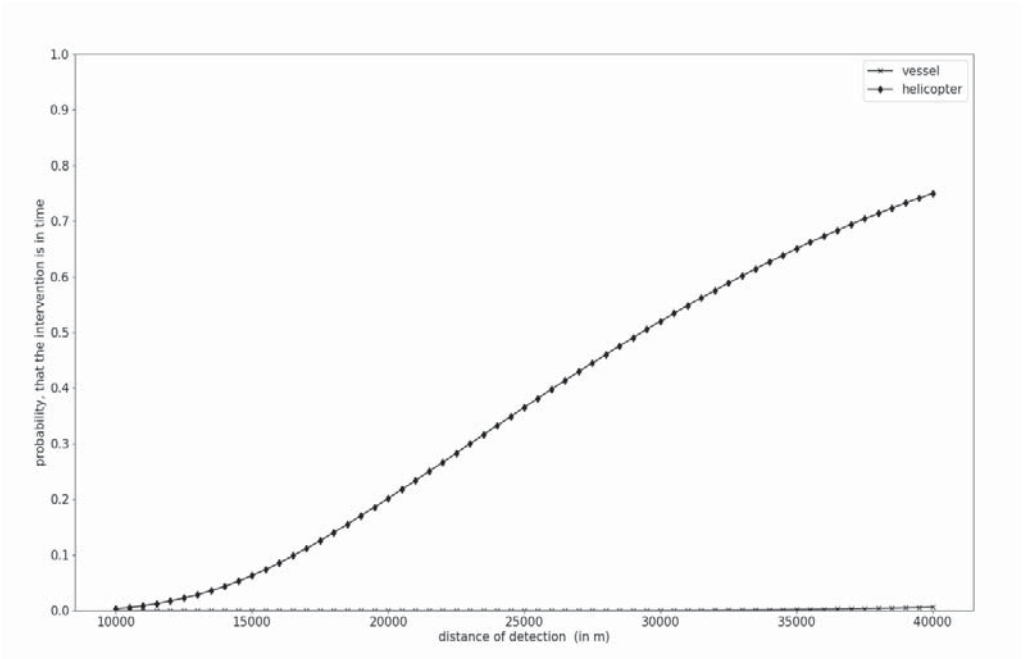

Fig. 7. The probabilities that the intervention is in time comparing the intervention with a vessel (marked with x) and a helicopter (marked with the diamond).

5. Outlook

This work provides a probabilistic model to assess and measure offshore infrastructure vulnerabilities in general and beyond specific attack scenarios. It cannot only be applied to vessels and swimming objects, but also to other obstacles like aerial vessels. The model is particularly relevant for offshore applications, since hybrid attacks involving different types of platforms become more important.

In contrast to (Zou et al., 2017) we do not evaluate a concrete security system and its effectiveness. Instead, we only consider a basic geographic setting to estimate the probability of the success of an attack. One possible extension of the model is to include the effectiveness of a protection system in our calculations so as to increase the accuracy of the derived probabilities. Including this to the model could lead to an approach for the comparison of different protection systems.

Moreover, it is possible to adapt the model to a concrete situation and additionally, to include real data for all the assumed data. This leads then to more precise probabilities for the considered scenario.

On top of that, another option is to integrate decision models, for example optimization-based approaches, to support the allocation of intervention units in offshore scenarios. In particular, this is relevant in situations with multiple intervention units and probably multiple adversaries. After the model provides an estimation of the likeliness that an intervention unit will arrive in time, the decision models can be used to optimize the decision which intervention unit should be deployed and how it should be deployed.

References

Bundespolizei (2025). Bundespolizei See - Maritime Kompetenz auf Nord- und Ostsee. URL: https://bundespolizei.de/fileadmin/user_upload/Downloads/Unsere_Aufgaben/Aufgaben_auf_See/S03_Flyer_BPOL_See_Maritime_Kompetenz_file.pdf, last checked: 15.12.2025.

Bundesstelle für Seeunfalluntersuchung (2025). Allision with an offshore wind turbine in the Gode Wind 1 wind farm by the PETRA L on 24 April 2023. URL: https://www.bsu-bund.de/SharedDocs/pdf/EN/Investigation_Report/2025/Investigation_Report_192_23.pdf?__blob=publicationFile&v=1, last checked: 14.01.2026.

Bundeswehr (2025). Hubschrauber im Bereich Marine. URL: https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr, last checked: 17.12.2025.

Cheikh El Wely, I. and A. Chetaine (2021). Analysis of physical protection system effectiveness of nuclear power plants based on performance approach. *Annals of Nuclear Energy*, 107980.

Hara, D. and H. Sagara (2025). Design of a robust physical protection system for offshore floating nuclear power plants against ship-boarding threats: (1) vital area identifications. *Journal of Nuclear Science and Technology 62*, 1–10.

Iaiani, M., A. Tugnoli, V. Cozzani, G. Reniers, and M. Yang (2023). A Bayesian-network approach for assessing the probability of success of physical security attacks to offshore Oil&Gas facilities. *Ocean Engineering 273*, 114010.

Iaiani, M., A. Tugnoli, P. Macini, E. Mesini, and V. Cozzani (2022). Assessing the Security of Offshore Oil&Gas Installations using Adversary Sequence Diagrams. *Chemical Engineering Transactions 91*, 385 – 390.

Knysh, A., J. Coyle, J. DeCew, A. Drach, M. R. Swift, and I. Tsukrov (2021). Floating protective barriers: Evaluation of seaworthiness through physical testing, numerical simulations and field deployment. *Ocean Engineering 227*, 108707.

Lichte, D., D. Witte, T. Termin, and K.-D. Wolf (2021). Representing Uncertainty in Physical Security Risk Assessment. *European Journal for Security Research 6*, 189–209.

Loveček, T., L. Straková, and K. Kampová (2021). Modeling and simulation as tools to increase the protection of critical infrastructure and the sustainability of the provision of essential needs of citizens. *Sustainability 13*, 5898.

Martz, H. F. and M. E. Johnson (1987). Risk Analysis of Terrorist Attacks. *Risk Analysis 7*(1), 35 – 47.

McGill, W. L., B. M. Ayyub, and M. Kaminskiy (2007). Risk analysis for critical asset protection. *Risk Analysis 27*(5), 1265 – 1281.

Niemi, A., N. Rosseck, N. Stockfisch, J. Stockbruegger, C. Wrede, and F. Sill Torres (2025). Evaluating european maritime infrastructure resilience through constructive simulation and infrastructure models. *Procedia Computer Science 274*, 973–982.

Ramírez-Agudelo, O. H., C. Köpke, Y. Guillouet, J. Schäfer-Frey, E. Engler, J. Mielniczek, and F. S. Torres (2021). An expert-driven probabilistic assessment of the safety and security of offshore wind farms. *Energies 14*(17).

Skobiej, B., F. Sill Torres, and F.-M. Minssen (2024). Surveillance of Offshore Installations with Patrol Routine. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 14599 LNCS*, 208 – 223.

Tecklenburg, B., J. Stockbruegger, A. Niemi, and F. Sill Torres (2025). Securing maritime infrastructures: a framework to evaluate physical protection measures for offshore wind farms. *Environmental Systems and Decisions 45*, 1–17.

Zou, B., M. Yang, J. Guo, E.-R. Benjamin, and W. Wu (2017). A heuristic approach for the evaluation of Physical Protection System effectiveness. *Annals of Nuclear Energy 105*, 302 – 310.