Understanding cyber-risks in complex next-generation maritime technologies: Autonomy and offshore wind energy operations

Kimberly Tam[1,2], Avanthika Vineetha Harish[1], Kevin Jones[1]

[1]University of Plymouth, UK

[2]The Alan Turing Institute, UK

Abstract - When developing maritime technology, each new technology is often developed and assessed separately. However, it is likely with the convergence of systems, and greater interconnectivity between systems in the sector, that new technologies will be inter-connected digitally or operationally. Understanding the cyber risks of the larger systems of systems is important. This paper looks at the potential cyber-physical risk of future autonomy and offshore renewable energy solutions co-existing together. A threat scenario is presented using real cyber-vulnerabilities in autonomy and offshore wind systems. This paper discusses potential overall vulnerabilities when combining these two emerging technologies. It concludes with suggested mitigations ranging from technical (e.g., secure communication channels) through policy (e.g., new standards for secure devices on the market) to social (e.g., cybersecurity training for remote operators). This type of multi-solution scenario can be a useful tool for analysing risks in complex circumstances and can be applied to other sectors with multiple emerging technologies.

Keywords: Maritime technology ; cyber risk ; mitigation ; autonomy ; offshore wind energy

INTRODUCTION

New technologies come with their own challenges and risks. Insights on future risks make it easier to mitigate those risks. However, with the convergence of new technologies, gleaning insight of a complex systems-of-systems, becomes harder yet more insightful.

In the maritime sector, there are currently many developments in areas like autonomy and offshore renewable energy. Studies such as [1] [2] look at these solutions in isolation, which often gains valuable insight. This can provide significant solutions and risk mitigations for these systems as they evolve. However, cybersecurity in the big picture is often about the weakest link in the chain, and only focusing on security of one entity does not mean it is unaffected by other entities. In one study [3], it was found that port operations could be vulnerable to a cyber-attack executed on an incoming ship, and efforts to secure ports cannot be limited to only port infrastructure.

In a similar holistic approach, in this paper we focus on autonomy and offshore structures like renewable energy in the maritime sector as emerging, on the horizon, technologies that are being realised now, or will be in the near future. Examples of related works and the state-of-the-art research and practices in these two areas are detailed more in the background section.

New maritime technologies will not exist in a vacuum but will, or must, co-exist in the same physical space. In this case, both autonomy and offshore structures will likely operate in similar coastal areas. Developing ways to discuss the emerging risks from the interactions of solutions may reduce them for the future. Specifically, this paper considers cybersecurity-related risks, however, this scenario can be used to discuss other risks such as safety. These scenarios can be further developed in for educational and team building as a part of mitigation, which will be discussed further in this paper.

One reason why it is useful to assess growing solutions in conjunction, instead of completely separately, is a solution for one challenge in one technology, could create a new risk in another technology. This essentially means problems moving horizontally across the sector and changing, instead of being fully removed. One potential example is maritime systems addressing the challenge of autonomy by increasing remote satellite communications. However, that increased connective increases cyber-risks by increasing the attackable surface area [4] [5].

In another example, demands for decarbonization have pushed for more digital solutions, such as digital twins and Artificial Intelligence (AI) and third-party solutions. However, many of these solutions generate carbon costs or unintentionally outsource the carbon cost to third parties [6]. Creating scenarios where complex discussions can be explored for complex challenges can help provide meaningful solutions to challenges [7].

BACKGROUND

This section covers the essentials of marine autonomous systems (MAS) and offshore wind (OW) as terms of their cyber-physical security. When considering the range of cyber-physical attacks, we define these as cyber-physical security as physical attacks that have a digital impact, but also digital cyber-attacks that have a physical impact.

A. Autonomy

In maritime, there are two main pathways to autonomy in development. First, there are traditionally crewed vessels having increased amounts of autonomy, but there is also an increase in new autonomous Uncrewed Surface Vehicle (USV) that are designed to be autonomous from design.

Typically, these USVs are smaller in physical size than traditional ships but also increasing their tiers of autonomy as defined by the IMO [8]. Because of their size, one of the growing concerns is the physical capture of USVs. Capturing a physical USV could have governance challenges (e.g., stealing another nation's USV during a conflict [9]), as well as cyber-security consequences. During penetration tests of several small autonomous USV in the Cyber-SHIP lab[1], it was found some USVs had cyber-physical security vulnerabilities in captured and readable SD cards and communication channels when physical access was possible.

In the middle tiers of autonomy (IMO 2-3) there are additional challenges of human-autonomy teaming (HAT) such as proper hand-offs for control [10]. The highest tier, which represents full autonomy, also has its unique challenges. AI is being used increasingly to solve the challenges around full autonomy and offshore resilience [11], but they also may introduce vulnerabilities if they are not designed or trained with security in mind [12].

As most autonomous vessels will stay near shore for connectivity reasons (e.g., coastal hoppers) or will need to enter/leave a port, it is highly likely that these will need to navigate around, and/or through, the growing number of wind turbines being installed offshore.

B. Offshore Wind

Renewable energy solutions have been around the 1980's, however it was not until recently when the technology became more popular due to concerns over carbon emissions. However, as land-based renewable generators become more popular, therefore public favour began to decrease due to aesthetics and the land they used [13].

To adjust to limited space and how the public viewed large windfarms, efforts have been made to move renewable energy production to oceans where there is more space, turbines are less visible, and for increased access to wind. While this solves the challenge around space on land, this has again created new challenges for offshore windfarms including, but not limited to, floating structures, fixed structures, transferring power back to land, and the complexities of monitoring and maintaining renewable energy infrastructure while it is isolated sea.

One of the power related challenges of remote wind is how to bring power from the turbines, back to shore. Doing this with crewed ships would be very costly, and so one of the proposed solutions is to use USVs to monitor, service, and ferry energy to shore. This will likely require digital communication too coordinate joint operations of USV in windfarms, and remotely.

Given how likely and closely physically, and digitally, offshore wind structures will operate with autonomous USVs and vessels in the future, the cybersecurity risks of one could possibly have a huge impact on the cybersecurity risks of the other.

[1] https://www.plymouth.ac.uk/research/cyber-ship-lab

C. *Maritime cybersecurity*

We define maritime cybersecurity as the field of understanding and mitigating cyber-physical threats (i.e., both digital and physical safety) that effect technologies related to the ocean, such as ships, ports, and offshore structures. This includes autonomous vessels, offshore wind farms, and offshore renewable energy in general.

While there are many papers on specific maritime cybersecurity vulnerabilities, this paper focuses on related state-of-the-art articles that use scenarios to outline the limits of emerging cybersecurity challenges.

In [14], a human-centered design and scenario-based training was demonstrated for maritime cyber-resilience through crews. While this was not aimed at autonomy or OW, the scenario-based training proved effective for discussion and training. Similarly, the scenario-based maritime cybersecurity training in [15] was proven effective for both novices to maritime cybersecurity, and also those with more experience, and that scenarios stimulated useful discussions about the future of autonomy and maritime cybersecurity challenges.

The strengths of the studies above are the targeted scope allowed for in-depth analysis and discussion of maritime cybersecurity challenges specific to those technologies. However, it is also clear from the context of these studies, solutions to sector challenges do not always remove the issue entirely, and many times shifts the problem to another entity or creates new issues, such as human-computer interactions and cyber-physical security.

SCENARIO

The purpose of this scenario is not to deep dive into one technology, autonomy, or offshore wind, and look at the cybersecurity of challenges of one in isolation, but instead to look at a scenario of the two technologies intertwined with each other. This is more likely to be realistic, as mentioned above, these two will likely be well connected digitally and operating in the same bodies of water.

A. *Scenario technologies*

(1) Remote control centre at port (ROC),
(2) Fleet of autonomous USVs,
(3) Windfarm that ROC and fleet of USVs oversee monitoring and servicing.

B. *Scenario vulnerabilities*

(1) The windfarm is physically vulnerable and is open enough that ocean craft can often sail through it. The windfarms themselves also obstruct monitoring of some craft sailing through [16]. This windfarm allows vessels to pass through, as it would be nearly impossible to enforce no passage, and because of the placement of the windfarm near busy ocean pathways.
(2) While AI for object recognition is being developed for situational awareness and navigation, adversarial AI can prevent the AI from correctly identifying objects [17].
(3) Hardware vulnerabilities in the USVs means physical access, if captured, can lead to data exfiltration such as swarm/ROC specific data.
(4) Network security is often weaker when considering insider attacks instead of external attackers, with examples in maritime satellite systems being true [5]. A ROC may be protected against external attacks, but if not protected internal, it may be vulnerable to internal threats.

C. *Series of events / attack chain*

This is a hypothetical series of events, a scenario, based on the three technologies and four vulnerabilities mentioned previously.

Events:

(1) An adversary can use a cyber-physical attack on USV AI to confuse a USV in a windfarm.
(2) The initial attack would lead to the physical capture a USV despite ROC control/monitoring.
(3) Physical access to the USV gives the attackers access to the wider network that USV is connected to.
(4) Using more traditional cyber-attacks, attackers can trigger a denial of service (DoS) attack across the wider network.

The potential outcome of this scenario can be multi-fold depending on the audience involved and therefore a useful tool. For example, those in the ROC may be concerned that this DoS could allow the theft of more autonomous USVs. Conversely, those in charge of the wind turbine data could be concerned about stolen information/data to connect with turbines. Those more interested in physical operations could also be concerned with physical damage, such as any connectors (e.g., cables) connecting USV to turbine or shore-based infrastructure.

DISCUSSION

From this holistic scenario, there are several discussion points and research topics that could improve the sectors' ability to analyse complex scenarios for cyber-physical risks and develop cyber defence and resilience strategies.

A. Future Work

This scenario can be used in discussion for training, as demonstrated by previous research [14] [15]. This is not only for technical training, but also for promoting more of a more positive cyber-aware culture at all levels within an organisation, such as the board. For those closer to the operations, this includes seeing cyber-security not just as a data challenge, but one that can relate to safety as well [18]. Discussions can also influence local practices, up to local/global policy as these technologies mature [16].

While previous scenario-based training have used tabletops and simulators, these are often difficult to scale due to ship simulator sizes and the need for instructors. Future research in scalable training using digital education tools like virtual reality (VR) is essential for the scalability of maritime cybersecurity education in the future, as well as improving experiences for non-experts more easily.

While scenarios are useful for initial discussion, if scenarios are not based on facts there is a concern that resulting training and policies will not be effective in real life. One of the challenges to validating scenarios, is it is dangerous to do experiments on the real equipment. While simulating and modelling threats is a useful tool, the drawback is that simulations are limited by the developers. When the environment gets more and more complex, such as cyber-physical security in a sea area with remote control over autonomous sea drones within a floating wind farm, the more challenging it becomes to simulate that with high enough fidelity for it to be useful. Alternatives to simulated systems-of-systems for testing are critical.

One way to look at complex systems is with a testbed like Cyber-SHIP [19]. As a first of its kind, both as a configurable testbed and a testbed specifically ship maritime cybersecurity (including autonomy), this testbed demonstrated the need for this level of fidelity for research. However, testbeds like this are expensive and therefore not common. Instead of building a combined autonomy and windfarm testbed for this scenario, it makes more sense to create a windfarm testbed that can connect to existing testbed and simulations for ROC and ship security.

Future work should then include building a windfarm specific cyber-physical testbed and connecting it with other facilities. This will be essential for ensuring realism within scenarios. There is a gap for understanding offshore wind, not just as a floating version of land infrastructure, but the context, other entities, and environment it will sit in, and be influenced by. To some degree, connected facilities has been done with cyber-ranges, but also cyber-ranges with physical testbeds [3]. Connecting testbeds for maritime cybersecurity research is, as far as the authors can tell, is an area of future work.

CONCLUSION

The growth rate of new technological solution for marine and maritime operations has reached new hights. While many have examined the benefits and negatives, including cyber-risks, of new technologies in isolation, once matured, these will not operate in isolation. This paper demonstrated how a scenario for multiple technologies can be created, and how it can be used to further discussions to further knowledge of maritime cyber-physical security.

ACKNOWLEDGEMENT

This project was partially funded by the Research England Cyber-SHIP project. Thanks to the research team as well.

REFERENCES

[1] T. Nimra and C.-L. Tsai, "Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives," *IEEE Access, vol. 12,* pp. pp. 17114-17136, 2024.

[2] E. Sabev, R. Trifonov, G. Pavlova and K. Rainova, "Cybersecurity Analysis of Wind Farm SCADA Systems," *Information Technologies (InfoTech),* pp. 1-5, 2021.

[3] K. Tam, R. Hopcraft, K. Moara-Nkwe, J. P. Misas, W. Andrews, A. V. Harish, P. Gimenez, T. Crichton and K. Jones, "Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety," *Journal of Transportation Technologies,* 2022.

[4] J. Pavur, D. Moser, M. Strohmeier, V. Lenders and I. Martinovic, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *Security and Privacy*, 2020.

[5] J. Gurren, A. V. Harish, K. Tam and K. Jones, "Security implications of a satellite communication device on wireless networks using pentesting," in *nternational Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2023.

[6] C.-J. Wu, R. Raghavendra, U. Gupta, B. Acun, N. Ardalani, K. Maeng, G. Chang, F. Aga, J. Huang, C. Bai, M. Gschwind, A. Gupta, M. Ott, A. Melnikov, S. Candido, D. Brooks and Ch, "Sustainable AI: Environmental Implications, Challenges and Opportunities," in *Machine Learning and Systems* , 2022.

[7] C. Sellberg, "From briefing, through scenario, to debriefing: the maritime instructor's work during simulator-based training," *Cognition, Technology and Word*, vol. 20, pp. 49-62, 2018.

[8] IMO, "International maritime organization MSC100/20 add.1," in *report of the maritime safety committee on its 100th session.*, 2018.

[9] D. Murray, "US Navy thwarts Iran's attempt to steal one of their sea drones," Independent, 14 September 2022. [Online]. Available: https://www.independent.co.uk/news/world/americas/us-navy-iran-drone-b2156611.html. [Accessed 15 06 2024].

[10] T. Ellwart and N. Schauffel, "Human-Autonomy Teaming in Ship Inspection: Psychological Perspectives on the Collaboration Between Humans and Self-Governing Systems," *Smart Ports and Robotic Systems,* pp. 343-362, 2023.

[11] A. Knack, Y. K. H. Syn and K. Tam, "Enhancing the Cyber Resilience of Offshore Wind," CETaS Research Reports, June 2024.

[12] M. J. Walter, A. Barrett, D. J. Walker and K. Tam, "Adversarial AI testcases for maritime autonomous systems," *AI, Computer Science and Robotics Technology,* 2023.

[13] M. Karydis, "Public attitudes and environmental impacts of wind farms: a review," in *Global NEST* , 2013.

[14] E. Erstad, R. Hopcraft, A. V. Harish and K. Tam, "A human-centred design approach for the development and conducting of maritime cyber resilience training," *WMU Maritime Affairs,* vol. 22, pp. 241-266, 2023.

[15] J. D. P. Misas, R. Hopcraft, K. Tam and K. Jones, "Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness," *Journal of Marine Engineering & Technology,* 2024.

[16] MOD, "Policy paper Mitigating the adverse effects of offshore wind farms on air defence radar: concept demonstrations," 24 May 2022. [Online]. Available: https://www.gov.uk/government/publications/mitigating-the-adverse-effects-of-offshore-wind-farms-on-air-defence-radar-concept-demonstrations/mitigating-the-adverse-effects-of-offshore-wind-farms-on-air-defence-radar-concept-demonstrations. [Accessed 15 June 2024].

[17] M. J. Walter, A. Barrett and K. Tam, "A Red Teaming Framework for Securing AI in Maritime Autonomous Systems," *arXiv,* 2023.

[18] R. Hopcraft, K. Tam, J. D. P. Misas, K. Moara-Nkwe and K. Jones, "Developing a maritime cyber safety culture: Improving safety of operations," *Faculty of International Maritime Studies,* 2023.

[19] K. Tam, K. Forshaw and K. Jones, "Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities," in *nternational Conference on Marine Engineering and Technology*, Oman, 2019.