Understanding Cybersecurity Risks in Offshore Wind Farms

Mary Ann Hoppa
Department of Computer Science
Norfolk State University
Norfolk, Virginia USA
mahoppa@nsu.edu

ABSTRACT

Like many other nations, the United States is pursuing renewable energy, with plans to build enough offshore wind turbines to power over 10 million American homes by 2030. This paper documents findings from a recent short-burst project in which a team of student research assistants explored whether offshore wind farms create significant cybersecurity risks for critical infrastructure such as the power grid and maritime operations. Despite limited published literature on U.S. offshore wind farms, documented incidents from onshore and international offshore wind farms were used to understand their typical operational characteristics and cybersecurity vulnerabilities. Feasible cyber attacks were proposed and considered, along with the extent to which U.S. offshore wind farms may be susceptible to them, and potential impacts of successful attacks. This investigation concluded that the risk of cyber attacks, while presently low, is likely to grow as this nation becomes more dependent on offshore wind energy. Furthermore, the likelihood of successful attacks will remain high until offshore wind farm cybersecurity receives elevated attention. Additional directions for future work are proposed to build upon these findings.

CCS CONCEPTS

• Cybersecurity •

KEYWORDS

Offshore wind farm, cybersecurity, risk assessment, critical infrastructure

ACM Reference format:

Mary Ann Hoppa, 2023. Understanding Cybersecurity Risks in Offshore Wind Farms. In *Proceedings of Association of Computer Science Departments at Minority Institutions Conference (ADMI'23). ACM, Virginia Beach, VA, USA, 5 pages.* https://doi.org/10.1145/1234567890

1 Introduction

This project aimed to increase awareness and understanding of offshore wind farms (OWFs), potential cybersecurity threats they may be subject to, and potential risks they may create for critical infrastructure including the power grid and maritime operations. This is an important problem since the United States (U.S.), like many other nations, is vigorously pursuing renewable energy such as wind power. Plan are underway to build thousands of offshore wind turbines along the East Coast by 2030, enough to power over 10 million American homes [1]. Utility companies are slated to integrate OWFs into the so-called smart grid which represents an enhancement of traditional power infrastructure.

This massive network-of-networks – composed of millions of heterogeneous, interconnected intermediary and endpoint devices, applications and systems – comprises a huge cyber attack surface including highly vulnerable legacy industrial control systems (ICS) [2]. And such a future vision evokes worrisome cybersecurity risks for critical U.S. infrastructure including power and the maritime domain.

Wind farm analysis to date has largely focused on efficiency, capacity, health concerns, environmental impacts, and economic considerations. While admittedly these are important concerns, by contrast the physical and technical differences among onshore, offshore and distributed (small wind) farms, along with potential cybersecurity issues and unclear areas of responsibility, have been treated in an uneven, scattered fashion. In other words, an astute observer is likely to conclude that cybersecurity has been set aside as something to worry about later on. In addition, since OWFs in the U.S. are less mature than European markets, there is little published open-source literature to assist academics who wish to learn and conduct relevant research.

Understanding cybersecurity vulnerabilities and risks in OWFs, along with what should be occurring now to mitigate them before a serious cybersecurity incident, was the tremendously important and challenging charge for a Summer 2021 research team whose findings are summarized here. The remainder of this paper is organized as follows. Section 2 presents background information, and Section 3 presents related work, both of which motivated the project. Section 4 explains methodologies used for the investigation. Section 5 discusses findings. Section 6 gives a summary recap and suggests ways to build upon this work.

2 Background

2.1 Cybersecurity

Cybersecurity generally refers to the measures undertaken to protect electronic assets from criminal or unauthorized access or corruption. *Cyber attacks* refer to specific exploitations attempted against systems, software, and technologies with the goal to

breach them. *Direct attacks* – in which an attacker is physically present to initiate the exploit at a vulnerable node – remain a viable traditional tactic. However, modern architectures and wireless communication pathways also enable *indirect attacks*. Unlike direct or kinetic attacks, attackers from anywhere at any time potentially can remotely access vulnerable nodes in the target environment, compromise them, then virtually migrate within the network-of-networks to desired target systems and/or endpoints.

2.2 Offshore Wind Farms

An OWF can be informally described as a power plant that contains all the capabilities needed to capture wind power, transform it into electricity, then supply it to the main electricity network. For economic reasons (e.g., consolidated planning, construction, maintenance), many wind turbines are installed at the same time in one location resulting in the "farm" moniker. At a high level, an OWF is comprised of wind turbines, cables, and substations. Turbines are basically generators on high poles (a.k.a. "masts") that convert wind power into electric power. The electric power produced by a farm's turbines is transferred via cables to an offshore substation. There it is stabilized, maximized, transferred via cables to an onshore substation, and consequently added to an electricity grid. A simplified diagram of a typical OWF is shown in Figure 1.

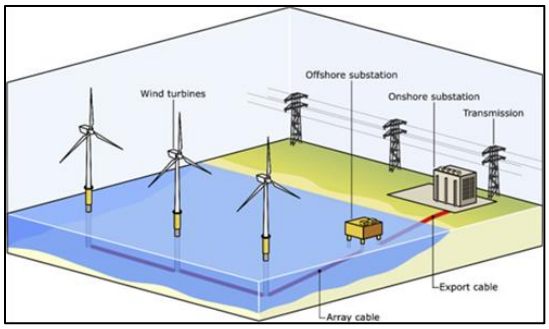

Figure 1: A notional offshore wind farm [3]

3 Related Work

When embarking upon this project, the proprietary nature of wind farm technology and suspected security restrictions on cybersecurity details created significant information discovery barriers. There are few authoritative public sources for technical specifics on U.S. OWFs. Since renewable energy options have only recently garnered intense interest in the U.S., only a few studies and roadmaps relevant to OWF cybersecurity assessment have been published in the open literature recently [4, 5, 6].

Researchers successfully demonstrated wind farm hacks as long ago as 2015 [7], with real-world breaches occurring as recently as March 2022 [8] and attributed to hackers sympathetic to Russia regarding the war in Ukraine. However there is little evidence shared about penetration testing U.S. windfarms to show they have been hardened to resist known cybersecurity attacks, although obviously some thought is being invested in how to do this now [9, 10, 11]. Currently, it is unknown how many U.S. wind farms have conducted or regularly conduct cybersecurity assessments of their assets, what assessment strategies if any are used, nor what the findings may be [5].

4 Methodology

This project ultimately aimed to explore cybersecurity exploits – both known and conjectured – that might threaten or involve OWFs. In addition, it sought to examine the extent to which OWFs may create genuine cybersecurity risks for critical U.S. infrastructure including the power grid and maritime operations. A final goal was to bring together many fragmentary details of various aspects of the cyber-physical ecosystem in which OWF operate to support analysis from a more integrated and holistic perspective.

A number of constraints had to be accounted for in the overall methodology to accomplish the work. The level-of-effort and timeline for accomplishing all planned activities was limited to 1800 staff hours over a ten-week period. The student research assistants supporting the project had little to no background preparation in cybersecurity, wind farms or critical infrastructure. Thus the effort was front loaded with start-up learning activities, including studying a seminal textbook [12] and additional directed readings/viewings of related literature. Additional tasks included collecting and documenting known cybersecurity incidents and proposing new ones that might be directed toward OWFs.

This short-burst project involved a team of four research assistants from two institutions working under a faculty advisor, supplemented with additional guidance from relevant subject-matter experts (SMEs). The timeline drove the methodology as follows:

- Weeks 1&2: orientation; project start up; baseline cybersecurity and maritime systems learning
- Weeks 3&4: "deeper dive" learning in four areas: cybersecurity; maritime systems; critical infrastructure; historical ICS/maritime cybersecurity attacks
- Weeks 5&6: SME interviews; OWF attack scenario formulation and validation; web development learning
- Week 7&8: leave-behind website construction and report authoring
- Weeks 9&10: final briefings and next-steps planning

As mentioned earlier, limited technical and cybersecurity specifics regarding U.S. OWF could be found in the open literature. Consequently reasonable assumptions and extrapolations were made based on known details about onshore wind farms, European OWFs, and by engaging in non-attributional discussions with OWF SMEs. Investigations were conducted "on paper" versus via direct penetration experimentation on wind farms, subsurface/surface/aerial/space vehicles, or land-based equipment and systems.

5 Findings and Discussion

The research assistants involved in this project began with little baseline cybersecurity knowledge. After surprisingly little start-up training they were able to conjecture reasonable viable attack scenarios involving OWFs from a pessimistic, worst-case viewpoint. That is, without evidence that a given step of a proposed attack vector is effectually impossible, the team assumed it was a credible step. This is a reasonable assumption since there is virtually no zero risk cyber environment today. In addition, none of the team's assumptions and deductions was refuted when presented to national cybersecurity experts working in this field.

5.1 Offshore Wind Farm Ecosystem

Presently many wind farms are "one-off" in nature, often consisting of a heterogeneous mix of equipment makes, models and configurations, including aftermarket upgrades; consequently, there is no authoritative reference architecture or standard blueprint for U.S. OWFs. This project used the graphic of a typical generic OWF shown in Fig. 2 as a thinking tool for exploring potential cyber vulnerabilities and malware injection points in the overall ecosystem.

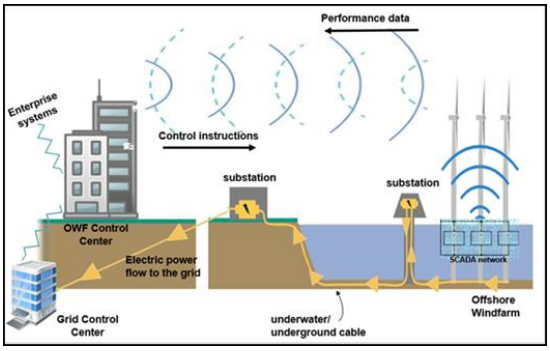

Figure 2: Simplified depiction of typical OWF environment

5.2 Threat Actors

The following categories of adversaries were considered viable to be involved in exploits that may try to take advantage of physical or electronic vulnerabilities in OWFs:

1. **Criminals**: Hackers seeking financial gain; for example, exfiltration/resale of proprietary intellectual information or holding electronic content or operations for ransom.
2. **Nation-state actors**: Hackers working on behalf of hostile foreign entities – including government and military – whose goals may include tactical or political advantage, crippling critical infrastructure such as the power grid, etc.
3. **Insiders**: Former or current employees who use physical or electronic access to pursue retaliation or financial gain. Such individuals may knowingly initiate cyber criminal activities; or they may be coerced into doing so; or they may unwittingly create compromises as a result of social engineering tactics undertaken by attackers or outright mistakes.
4. **Terrorists**: Individuals or groups who sabotage or destroy physical assets or capabilities for political or ideological reasons.
5. **Activists/Hacktivists**: Individuals or groups who believe their acts of sabotage/destruction serve a positive purpose, such as raising social awareness.

5.3 Potential Vulnerabilities

Due to the relatively small footprint of the niche U.S. wind farm marketplace at this time, and in the absence of any evidence to the contrary, it was deemed reasonable to assume that OWFs are using information and operational technology (IT/OT) systems similar to their onshore counterparts. Thus OWF IT/OT can be expected to exhibit similar vulnerabilities and to be at risk to similar attacks as those that have plagued legacy ICS. Some general known soft spots in ICS include: legacy components of insecure design; previously stove-piped systems and commercial products combined with inadequate integration testing; wireless-enabled remote access; foreign access to domestic infrastructure networks through outsourcing arrangements; and lack of appropriate security/safety education for personnel.

Known vulnerabilities specific to wind farms include: turbines with direct connections to/from the public internet, and controllers using legacy software like Windows 2000. These weaknesses put wind farms at risk to attacks such as directory traversal, cross-site scripting, information disclosure, malware injection and denial of service [13]. Vendors with remote virtual private network access to the farm's control networks (for purposes like monitoring, software upgrades, maintenance, research and development) offer attack opportunities via vectors including phishing, malicious insiders or physical breaches whereby instructions could be intercepted, then manipulated or even fabricated to shut down the farm or cause it to operate erratically. Wireless communications between land and farm or among the on-site ICS make farms vulnerable to common attacks including sniffing, spoofing, man-in-the-middle, denial-of-service and jamming.

OWF by their nature are remote and unattended, making them susceptible to various forms of physical and electronic sabotage. At least five viable attack points include: physical access at wind turbine(s); physical access at substations; cyber access via vendor networks; cyber access via technician equipment; and cyber access via compromised supply chains [14]. Even if mechanisms are in place to detect intrusions, the farms' remote locations mean it could take considerable time for security responders to arrive on the site of a breach, so that exploits have a greater window of opportunity to be successful.

5.4 Attack Scenarios Summary

Figure 3 compactly summarizes in a pick-list format some likely attack scenarios involving OWFs as proposed by the team. Purely cyber, cyber-physical, and purely physical (kinetic) attacks all were considered and deemed viable vectors. Based on successful

historical exploits, it was clear that many proposed attacks on OWFs would be undertakings that require significant, long-term planning and technical expertise, thereby earmarking nation-state actors and well-provisioned hacktivists as the most likely attackers. Other exploits, like malware injections via insiders and direct physical attacks such as ramming a boat into a mast base or implanting improvised explosive devices, can be more low-tech and opportunistic, yet equally effective depending on the desired impact.

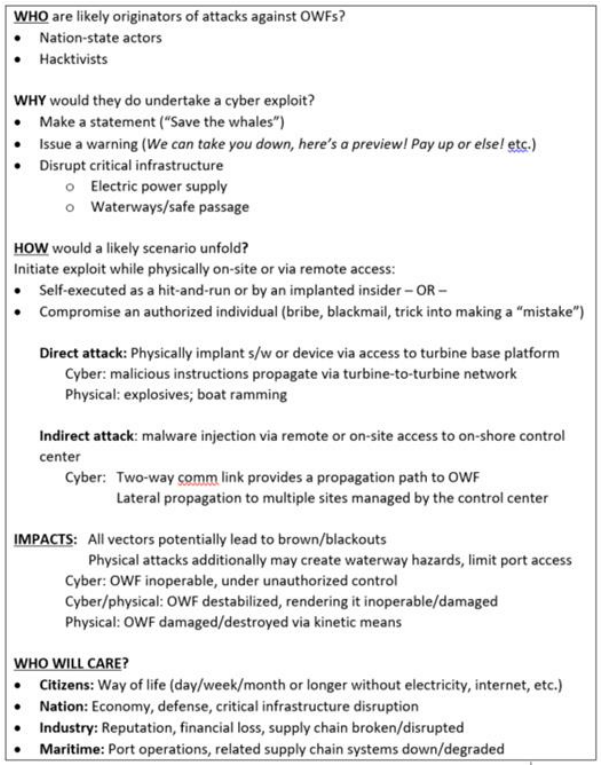

Figure 3: Rollup of likely OWF cyber attack characteristics

5.5 Qualitative Risk Analysis

Although limited in scope and facing information discovery hurdles, the team's efforts concluded that OWFs are at risk for being targeted by cyber attacks as well as serving as stepping stones in cyber exploits aimed at taking down larger critical infrastructures in which they play a role. Because of the technical expertise and extensive planning required for many such exploits, the most likely attackers would be well-organized, well-resourced nation-state actors or hacktivists; however low-tech direct physical attacks must be considered worrisome possibilities too.

The IT/OT used in OWFs can be assumed to be readily hackable due to: a plethora of known vulnerabilities validated in the onshore wind farm segment; an increasing use of wireless communication pathways in OWF architectures for remote and centralized control and monitoring; the potential for lateral attacks when OWF clusters are managed by common control centers; and the huge overall attack surface created when OWFs are integrated with the smart grid and Internet of Things devices.

The specter of successful cybersecurity attacks involving OWFs – potentially resulting in electric power blackouts, physical damage/destruction to the wind farms themselves, or debris obstructions in shipping lanes – are relevant and potentially impactful to homeland security. Blackouts can disable port operations and essential civilian and military systems. In addition to inconveniencing and endangering everyday citizens, the propagation of malwares injected to/from OWFs and critical infrastructure has potential impacts on the overall defense posture of the U.S.

Based on the small footprint of OWFs in the U.S. right now, the likelihood of an OWF cyber attack at this time is low, but the likelihood can be expected to grow steadily as the U.S. becomes more dependent on offshore wind as a significant electric energy source. This is because dependency means the consequences of successful OWF take-downs will be more disastrous and impactful – thereby making them more worthwhile targets in the eyes of potential attackers.

6 Summary and Future Directions

6.1 Summary

From a cybersecurity perspective there is no such thing as an unhackable system; the only question is whether the likelihood of cyber attacks occurring and/or succeeding is low, medium or high, along with what mitigations should be undertaken. This observation is as true for OWFs as it is for any other cyber-physical system. Due to the immaturity of OWFs in the U.S., much about their specific cybersecurity vulnerabilities – and potential side effects should breaches succeed – remains unexplored. However, this quick study – conducted by inexperienced students – revealed there is enough information online to devise plausible scenarios in which OWFs could play a role in cybersecurity threats to critical infrastructure including maritime operations.

A recent effort saw over 150 United Nations members commit to an international agreement advocating peace and security in cyberspace; however, since the agreement is non-binding there should be no expectation it will result in fewer offensive cyber attacks in any segment [15] There also should be no doubt that bad actors will take advantage of any latency or inaction in defensive OWF cybersecurity to lay the groundwork now for future cyber attacks (that is, advanced persistent threats). Therefore the likelihood of successful cyber attacks on OWFs is high whether attempted now or in the future, unless intervening focused efforts to harden OWFs against them are undertaken quickly.

The extent of cybersecurity risk created by OWFs must be explored further and characterized in greater detail, both for focusing defensive measures and future research on these plants,

and to assure the public about their overall cybersecurity posture. With OWFs continuing to be built around the word, it is essential that cybersecurity be retro-fitted into legacy architectures and baked into new designs. The findings of this intensive, short-burst examination of OWFs through a cybersecurity lens substantiate the need for creating broader understanding of these serious concerns and stimulating a sense of urgency that OWF cybersecurity efforts need elevated prioritization.

The National Renewable Energy Laboratory (NREL) and six leading industry organizations recently joined forces to develop a national Wind Cybersecurity Consortium to collaborate on analysis, development and information sharing. This marks an important step forward to strengthen cybersecurity preparedness for OWFs and the overall energy sector [16].

6.2 Future Directions

An enduring challenge is how to communicate about cybersecurity matters in ways meaningful with others who are not familiar with cybersecurity the many complex technologies (e.g., ICS) involved in OWFs – whether that audience is business or government decision-makers, out-of-discipline students, practitioners and researchers, or the general public. A leave-behind website (owflearning.cyberwaze.org) was created by student research assistants to document key learnings from the research experience, including more details about potential cybersecurity attack scenarios involving OWFs. The product can benefit stakeholders who need to rapidly get up to speed on OWF basics and cybersecurity concerns, as well as serving as a jumping-off point for future research teams to improve and expand.

OWFs are embedded in a large, complex ecosystem. Diversity in the physical construction of wind farms and their systems adds to the analytic complexity. Functional and information flow models are needed to make the identification and assessment of possible cybersecurity risks more methodical. Many vulnerabilities might be mitigated by relatively simple measures such as: disabling unnecessary remote interfaces; changing default IT/OT configurations and passwords; eliminating unused features and functionalities; and stronger encryption and authentication practices. Establishing "no-sail" zones around OWFs may help deter physical attacks and accidental collisions with sea-going vessels that can damage or destroy farm assets.

One planned way-ahead direction to build upon this work is to develop a semi-automated approach to creating OWF system architectures based upon a reference architecture. Implementing such a capability as a low-to-no-cost tool will invite broader participation and understanding, particularly by under-resourced academics and organizations who wish to contribute to the field. An additional benefit will be positioning cybersecurity researchers and analysts to render comparable and integratable OWF models for teaching, learning and conducting experiments and assessments in controlled laboratory settings.

ACKNOWLEDGMENTS

This research was performed in part under an appointment to the Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs SRT Program for Minority Serving Institutions, administered by Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by Oak Ridge Associated Universities (ORAU) under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of NSU, DHS, DOE, ORAU/ORISE or other research partners.

REFERENCES

[1] Madeleine Stone, "Offshore wind is poised to take off in the U.S.," 2021, https://www.nationalgeographic.com/environment/article/offshore-wind-is-poised-to-take-off-in-the-us-but-it-wont-be-easy/.

[2] U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, "Common Cybersecurity Vulnerabilities in Industrial Control Systems," 2011, https://us-cert.cisa.gov/sites/default/files/ recommended_ practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

[3] Trevor M. Letcher, Ed. Future Energy Improved, Sustainable and Clean Options for our Planet, New York: Elsevier, 2020, https://doi.org/10.1016/B978-0-08-099424-6.00032-6/.

[4] U.S. Department of Homeland Security, "Cybersecurity & Infrastructure Security Agency, "Security Industrial Control Systems: A Unified Initiative," 2020, https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_ Control_Systems_S508C.pdf.

[5] Department of Energy, Office of Energy Efficiency & Renewable Energy, "Roadmap for Wind Cybersecurity,", 2020, DOE/GO 102020 8441. Washington, DC.https://www.energy.gov/eere/wind/downloads/roadmap-wind-cybersecurity/

[6] Iosif Progoulakis, Nikitas Nikitakos, Paul Rohmeyer, et al., Perspectives on Cyber Security for Offshore Oil and Gas Assets. Journal of Marine Science and Engineering, 9(2), 112, 2021. https://doi.org/10.3390/jmse9020112

[7] Andy Greenberg, "Researchers Found They Could Hack Entire Wind Farms," 2017, https://www.wired.com/story/wind-turbine-hack/.

[8] Marian Willuhn, "Satellite cyber attack paralyzes 11GW of German wind turbines," 2022, https://www.pv-magazine.com/2022/03/01/satellite-cyber-attack-paralyzes-11gw-of-german-wind-turbines/

[9] U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy, "Labs Coordinate To Protect Wind Power from Cyberattacks," R&D Newsletter, Spring 2020, https://www.energy.gov/eere/wind/articles/spring-2020-wind-rd-newsletter/

[10] Sarah Freeman, Jake Gentle, Tim Conway. Cyber Resiliency Within Offshore Wind Applications. Marine Technology Society Journal, 54(6), pp. 108-113, 2020.

[11] Jake Gentle and Jay Johnson,"Cybersecurity for Wind Energy," presented at Best Practices in Utility Cybersecurity Conference, 27 January 2020, San Antonio, Texas, https://protectourpower.org/bestpracticesconference-2020/#presentations/

[12] Gary C. Kessler and Steven D. Shepard, Maritime Cybersecurity: A Guide for Leaders and Managers. Columbia, SC, Independently Published, 2020.

[13] Harm van den Brink, "Hacking wind turbines – Explained," 2022, https://harmvandenbrink.medium.com/hacking-wind-turbines-explained-230997db62f6/.

[14] Jason Stags, David Ferlemann, Sugeet Shenoi, "Wind farm security: Attack surface, targets, scenarios and mitigation," International Journal of Critical Infrastructure Protection, March 2017, https://www.sciencedirect.com/science/ article/abs/pii/S1874548217300434?via%3Dihub/

[15] Clark, Laurie, "UN countries agreed to a more peaceful cyberspace," TechMonitor April 2021, https://techmonitor.ai/policy/geopolitics/un-countries-cybersecurity-deal-state-sponsored-attacks

[16] National Renewable Energy Laboratory, "NREL Joins Industry in Leading Cybersecurity Threat Evaluation for the U.S. Wind Fleet," 2021, https://www.nrel.gov/news/program/2021/nrel-joins-industry-in-leading-cybersecurity-threat-evaluation-for-us-wind-fleet.html/