12-2022

A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience

Megan Egan
Boise State University

A RETROSPECTIVE ON 2022 CYBER INCIDENTS IN THE WIND ENERGY SECTOR AND BUILDING FUTURE CYBER RESILIENCE

by

Megan Egan

A project completed in fulfillment

of the CORe 591 requirements for the degree of

Master of Science in Cyber Operations and Resilience

Boise State University

December 2022

A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience

Megan Egan
meg.egan11@gmail.com
Cyber Operations and Resilience Program, Boise State University, 1910 W University Dr, Boise, ID, United States of America

Highlights:

- Wind energy sector facing increase in cyber-attacks
- Redundant communications systems critical for cyber resilience
- Cyber-attacks at scale are possible and most impactful

Abstract: Between February and June 2022, multiple wind energy sector companies were hit by cyber-attacks impacting their ability to monitor and control wind turbines. With projected growth in the United States of 110.66 GW from 2020 to 2030, wind energy will increasingly be a critical source of electricity for the United States and an increasingly valuable target for cyber-attacks. This paper shows the importance of redundant remote communications, secure third-party providers, and improving response and recovery processes that would ensure this growth period fulfills its potential as a unique opportunity to build in cyber resilience from the outset of new installations as threats and risks to the sector increase.

Keywords:

- Cyber-attacks, wind energy, renewable energy, cybersecurity, industrial control systems, resilience engineering

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

Prior to November 2021, a Google search of “wind energy cyberattack” brought up mostly research, opinion articles, or guidance on the threats but only one real example – a limited denial of service attack on a Utah-based renewable energy company from October 2019. Now, the search brings up the several incidents that have occurred within the past year impacting large wind energy companies like ENERCON, Nordex, and Vestas. This paper presents three case studies of four of these incidents to describe where the wind energy sector is falling short on implementing cyber resilient systems and practices. Overarching lessons learned from these cyber-attacks include the need for redundant remote communications pathways for monitoring and control, the prevalence of third-party company access to wind farm control systems and the resulting increased attack surface, and the risk of a cyberattack on the wind energy sector at scale, which would significantly complicate response and recovery.

Wind turbines operate mostly autonomously within internal controls and monitoring to maximize efficiency and safety, but also convey a significant amount of data to their owners, operators, builders, grid managers, and other external companies. This vast network of connections and systems introduces cyber risk not generally found in other electricity generation assets.

Resilience in a system can be assessed through four attributes: robustness, redundancy, resourcefulness, and rapidity. These attributes were established by Kathleen Tierney and Michel Bruneau in their 2007 article “Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction”. [1] Wind turbines and farms have generally been built according to these principles with regards to resilience from natural threats including the winterization of turbines in colder climates, internal brakes preventing turbine blades from being damaged in high winds, and remote monitoring to address maintenance concerns predictively and proactively. Unfortunately, the same cannot be said for the inclusion of cyber resilient designs with many turbines and their surrounding infrastructure having only limited protections against cyber-attacks. As the sector continues to grow and moves to more remote and distributed locations, including offshore, it is important for these resilience principles to be applied to cyber risks as well as natural risks.

This paper will start with a review of two foundational documents on cybersecurity for wind energy. Following this section, prior to presenting these case studies, this paper provides an overview of the types and generalized configurations found within wind turbines, within wind farms, and external to wind farms. Three case studies are then presented: the cyberattack on satellite communications impacting ENERCON, ransomware attacks at Nordex and Deutsche WindTechnik, and an espionage campaign against wind energy sector companies operating in the South China Sea. Each of these case studies includes an overview of the event, background and context, an overview of the impact to wind energy, and lessons learned. Finally, the discussion and conclusion sections will look at the case studies collectively to draw out the commonalities in improving the cyber resilience of wind energy and some recommendations on policies to do so.

2. Related Work

Other publications provide a great introduction to cyber resilience concerns within the wind energy sector including work done by researchers at the University of Tulsa and officials at the U.S. Department of Energy (DOE). These works were published prior to 2022 and therefore this paper will take established concerns from these publications and apply them to the cyber incidents occurring in 2022 to assess where improvements are still needed.

The primary published work looking at the feasibility of cyber-attacks on wind turbines is the 2017 paper by Jason Staggs, David Ferlemann and Sujeet Shenoi from the University of Tulsa, "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigations". This paper provides an overview of wind farm communications and control infrastructure, the attack surface of wind turbines and farms from both a physical and cyber security standpoint, attack targets within a wind farm, and major attack scenarios and mitigations. [2]

DOE's "Roadmap for Wind Energy Cybersecurity" is a robust entry-level product for explaining the context and basics of wind energy cybersecurity while also laying out challenges, strategies, and near-, mid- and long-term milestones and goals for improving the state of cybersecurity within the wind power industry. Importantly, the report presents key findings including the need to shift the cybersecurity paradigm within the industry from the design phase, the existing cyber threats to wind energy technology, the need for additional research in the sector, and the requirements for further development of wind energy-specific standards. [3]

DOE's Roadmap lays out only a few vague examples of cyber threats to wind energy systems, but in Staggs et al.'s section on major attack scenarios, the authors provide four concrete examples of how an attacker could impact wind turbine control, wind turbine damage, wind farm disruption and damage, and substation disruption and damage. One scenario discusses how attackers could gain access of a wind turbine using a custom tool developed by the authors which would be installed on a rogue device within the operations control system. From that device, the tool transmits OPC-XML-DA write request messages to change the turbine's operating state which could including starting or stopping the turbine and changing the direction of the blades or turbine. They also discuss opportunities to propagate these attacks through an entire wind farm using a wormmable program. The wind turbine damage example is similar and would use this tool to operate the turbine in a way that accelerates mechanical wear of critical turbine components. [2]

Staggs et al. identify six primary attack targets for a cyber threat actor seeking to disrupt wind farm operations or damage equipment: control networks, network devices, programmable logic/automation controllers, operation stations, engineering workstations, and data historians. These elements of wind farm control systems will be laid out in the next section of this paper based in large part on the details and graphics from DOE's report. Staggs et al.'s discussion of each primary attack target focuses on its role on the local network of a wind farm but lacks information on attack targets related to centralized remote control centers and operations. Opportunities for remote (i.e. outside of physical proximity to the wind farm) are highlighted briefly in the paper's section on cyber access using a wind farm vendor network where the authors state, "During a security assessment of a wind farm conducted by the authors of this paper, a vendor was observed to have remote access (from abroad) to the wind farm operations network." [2] This topic is not discussed in depth but is what happened with

several cyber incidents impacting wind farms in 2022, primarily with wind turbine vendors and maintenance companies that experienced ransomware attacks on corporate networks. [4]

Many of the mitigations presented by Staggs et al. remain effective for improving cyber resilience of wind turbines and farms, however, they are somewhat vague and may not prevent an advanced cyber threat actor seeking to attack at scale. The paper first presents the need to ensure physical security, describing physical access as "the most significant threat to wind farms". Although this may be true in select cases, none of the attacks seen in 2022 required physical access to turbines and physical access is less likely to provide the scale of a cyber-attack needed to substantially impact U.S. electricity generation from wind energy. The authors' recommendations for system hardening, system assurance, and policies and procedures are key to creating a cyber resilient wind energy sector but require substantially more detail than is provided in this paper. [2]

DOE's roadmap provides significantly more detail than Staggs et al. about future actions that can be taken to improve resilience across the sector. Mapped to the NIST Cyber Security Framework, there are 21 cybersecurity research and development topics described alongside a categorization of the responsible party: internet service providers, wind plant owners/operators, wind turbine original equipment manufacturers, and components supplies. Explanations of many of these topics also include how DOE has programs that can improve resilience, such as the Cyber Testing for Resilience of Industrial Control Systems (CyTRICS) program and the Electricity Information Sharing and Analysis Center's (E-ISAC) Cybersecurity Risk Information Sharing Program. There is also a robust section on the industry stakeholders the U.S. Government needs to engage in order to make these improvements including specific equipment manufacturers, owners/operators, and utility companies. [3]

DOE's report also provides eight conclusions for a path forward in the development of effective cybersecurity for wind turbines. Their conclusions are: Research and develop better technologies, methods, and tools for wind energy cybersecurity; Conduct routine cyber assessments; Participate in cyber-emergency response and other cyber preparedness exercises; Define cybersecurity roles and responsibilities within wind entities, and throughout industry; Develop robust, consistent cybersecurity programs at wind facilities; Further develop cybersecurity standards for wind energy technologies; Define and implement basic cyber hygiene; and finally, Develop and encourage participation in wind-specific cybersecurity information-sharing mechanisms. [3] This paper is an example of one of the roadmap's goals at work: to regularly document lessons learned from cyber incidents and make them available to the wind energy community and the energy sector.

3. Overview of Wind Energy Control Environments

3.1 Control Systems Within a Turbine

Wind turbines run mostly autonomously during routine operations, allowing them to maximize their generation and efficiency. In order to enable this autonomy, there is a local control system in each turbine with a Programmable Logic Controller (PLC) and communications to various other components. Figure 1 shows an illustration of wind turbine's internal

components and control system. The turbines each have their own sensors for wind speed and direction and this information is fed into the PLC for analysis. Using this data, the PLC can direct the turbine to change its yaw (the direction the turbine is facing) and its pitch (the angle of the blades). Adjusting one or both parameters maximizes electricity generation. [5]

The PLC can also communicate to the turbine's internal braking system which is used when the turbine is shut off at low or high windspeeds outside of the safe and effective operating parameters. This is particularly critical when high windspeeds could damage turbine components and the brake ensures the turbine does not rotate in in these conditions.

The PLC serves as a hub for communications external to the turbine through its connection to the wind farm's Supervisory Control and Data Acquisition (SCADA) system. The PLC and the turbine may also be accessible through a wireless communications device, including satellite communications modems or wireless access points. These devices are used for access by local maintenance workers who can stay on the ground near the turbine and still perform requisite maintenance or for remote monitoring and operation by distant control centers for owners and operators.

Communications within and external to the turbine vary based on the turbine vendor, other original equipment manufacturers (OEMs), wind farm owner specifications, or other factors. Communication protocols that may be found within a turbine include Controller Area Network bus (CANbus), Ethernet for Control Automation Technology (EtherCAT), MODBUS, and PROFINET. [3]

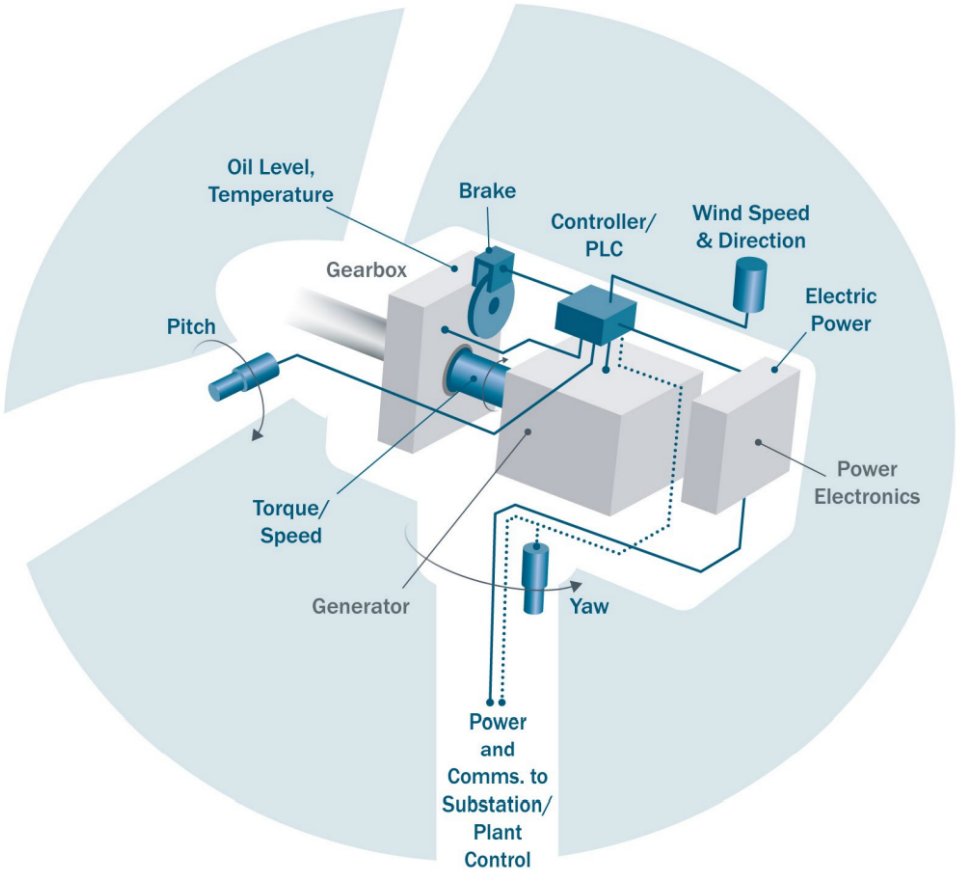

Figure 1: Components and controls inside a wind turbine [6]
Source: U.S. Department of Energy

3.2 Control Systems Within a Wind Farm

As with the turbine, the network within a wind farm will vary by installation but some generalizations can be made to frame discussions of resilience. Each turbine will typically be connected through a switch as the base of the tower to an Ethernet-based SCADA network. The specific technology and protocols used in this SCADA network will depend on the vendors and integrators chosen by the wind farm builder. For example, as seen in Figure 2, a wind farm utilizing Siemens equipment will primarily rely on the PROFINET protocol running over the Ethernet because it's Siemens preferred industrial communications protocol. [6] A GE wind farm control system is more likely to use ModBus or OPC protocols, according to company documents. [7] The wind farm SCADA network will also incorporate control infrastructure through servers and historians. In instances where a wind farm has a local control center, this SCADA network will typically be housed in and monitored by this control center through engineering workstations and human-machine interfaces (HMIs), however, not all wind farms have onsite control centers. [3] They are typically reserved for very large installations.

Ideally, the wind farm network will also include security protections by integrating firewalls or demilitarized zones (DMZs). These protections are not generally applied between the SCADA and the turbine but may be found in between the turbines and the control system within the SCADA and are far more likely to be found in between a local SCADA and remote control centers with VPN tunnel internet connections to the SCADA. [3]

Wind farm network communications are standardized by IEC 61400-25. This standard is used to ensure consistent internal exchanges of information and remote control across various vendors and integrators. [8] The standard addresses range of proprietary communication systems, variety of protocols, labels, and terminology to make communications vendor-agnostic with approximately 2670 total tags used for wind turbine monitoring. [9] Notably, IEC 61400-25 only applies at the wind farm control level and does not apply to communications within the turbine. [9]

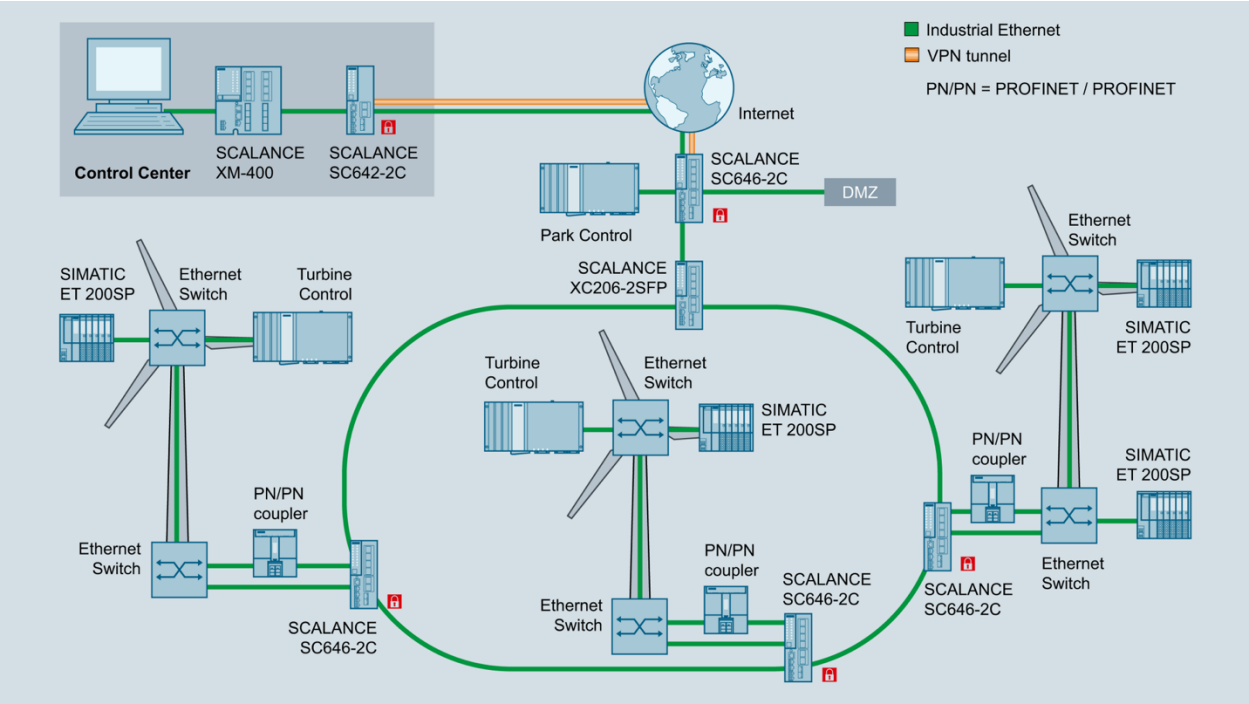

Figure 2: Generalized wind farm communications infrastructure using Siemens equipment
Source: Siemens

3.3 Control Systems Outside a Wind Farm

With a significant number of wind farms being designed and installed in the last ten years, digitization and remote access for these assets has become increasingly important as owners and operators consolidate operations from far away locations. For example, as of 2016 energy giant BP owned 16 wind farms in nine U.S. states. These wind farms were operated during daytime hours by field teams but were constantly monitored by a remote operations center, who also operated the farms outside of regular business hours. [10] Turbines

communicate an immense amount of data to these centralized control centers, as many as 1000 data points per turbine and another 1000 per onsite substation. Control centers need to receive data from and talk to the turbines to operate and troubleshoot them. [11] Beyond wind farm operation control centers, turbine data is either directly or indirectly monitored by many other third parties including turbine manufacturers, third-party maintenance companies, and transmission operators. This can result in as many as six to ten different companies having access to the data from a wind farm. [11]

4. Case Study: Russian Attack on Satellite Communications Impacting ENERCON Wind Turbines

4.1 Case Study Overview

On February 24, 2022, around 30,000 satellite communication (SATCOM) terminals were hit by a cyber-attack, causing them to stop working. This included SATCOM modems in 5800 wind turbines across 1217 wind farms operated by ENERCON, a Germany-based wind energy company. The impacted turbines, which generate over 10 gigawatts of electricity combined, continued to operate but could no longer be monitored using their SCADA system. [12] The cyber-attack was ultimately attributed to Russian state-sponsored cyber actors who targeted a European subsidiary of U.S. SATCOM company Viasat in an attempt to impact Ukrainian military command and control communications during the Russian invasion the same day; the wind turbine communications were simply collateral damage. [13]

4.2 Attribution and Context

Three months after the attack on SATCOM terminals across Europe but particularly in Ukraine, the U.S government formally attributed the cyber-attack to Russian state-sponsored actors with the motivation “to disrupt Ukrainian command and control during the invasion” but also noting “those actions had spillover impacts into other European countries. [13] Similar to many other cyber-attacks Russia launched against Ukraine before and during the invasion, the cyber actors used a wiper malware. Prior to formal attribution, cybersecurity research company Sentinel Labs did an in-depth investigation on the incident, discovering the wiper and naming it ‘AcidRain’. [14] In their release on the incident, Viasat stated the attackers were able to exploit a misconfigured VPN appliance in order to gain a trusted level of access to the management tools for the KA-SAT SATCOM network. From there, they used their access to execute the malware against all the modems simultaneously, overwriting key data in the flash memory of the devices and disconnecting them from the network. [15]

4.3 Impact on Wind Farm Operations

The loss of SATCOM modems inside the turbines meant the turbines could no longer communicate with ENERCON's SCADA system and server. As shown in Figure 2, this means both ENERCON's service centers and customer operations centers likely lost the ability to communicate with, monitor, and control the impacted turbines. In their press release, ENERCON stated that "grid operators continue to have unrestricted access to the wind energy converters to control their behaviour in the power grid – for example to restrict the feed-in power if necessary for grid stability." It's not clear exactly how the grid operators communicate with the wind farms, whether they only had access to the onsite substations and could control turbine interactions with the power grid that way or if the grid operators could still communicate directly with the turbines through a different communications path.

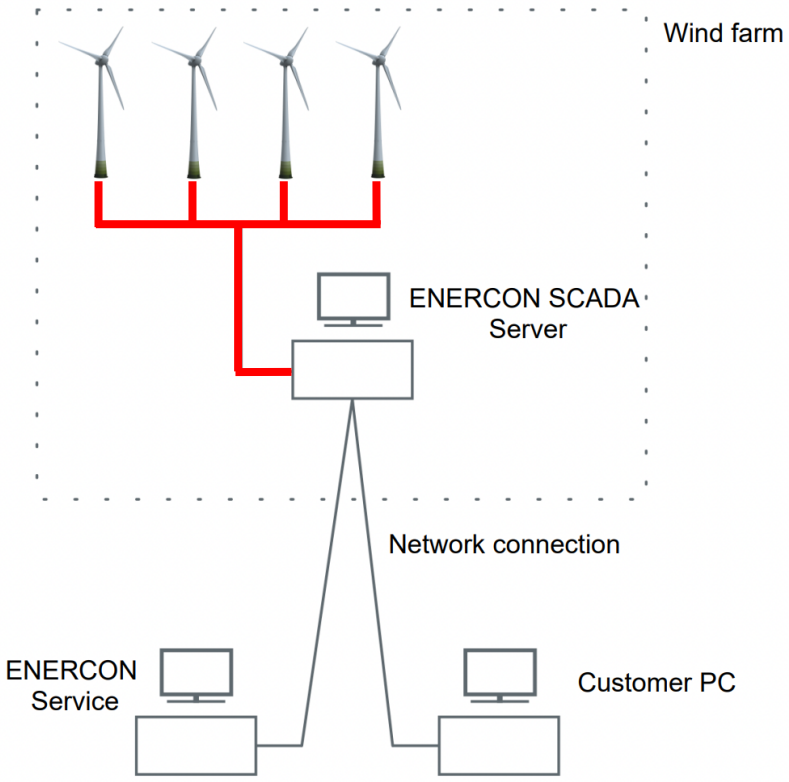

Figure 3: Schematics of ENERCON SCADA system with the communications segment likely impacted by the cyber-attack highlighted in red
Source: ENERCON

4.4 Lessons Learned

One reason the attack on SATCOM impacting ENERCON terminals is remarkable is the recovery time, which exemplifies how long an attack on wind turbines at scale can take to remediate. In this case, ENERCON service teams had to travel to impacted turbines to replace the SATCOM modem. After almost two months, ENERCON reported over 95 percent of the impacted turbines were back online either through replacement of the SATCOM modem or by

switching to LTE or other mobile communications. [12] ENERCON lacks the resilience attribute of rapidity in this case because they were not able to restore functionality in a timely manner. The company was able to compensate for some of their lack of rapidity through their resourcefulness, which allowed them to use alternative methods like LTE and meant that they had enough spare SATCOM modems to use where necessary. The recovery process is long for distributed land-based turbines but would be significantly exacerbated if a cyber-attack impacted offshore turbines – the next major area of growth for wind energy.

Similar to the other case studies to be presented, this attack brings to light how critical redundant communication paths are for distributed assets like wind farms. ENERCON noted the lack of backup communication links to replace the original connection in case of fault or failure was a key challenge for them and their turbine owners and operators. After the attack, the company began offering LTE-based retrofit packages, but installation of this backup communications mechanism would be optional and extra cost for ENERCON's customers. [12] Because this redundant communication is optional, ENERCON is less likely to improve the overall resilience of its customer's wind energy systems.

Finally, and perhaps most importantly, the cyber-attack impacting ENERCON's turbines demonstrated how wind energy can be attacked at scale. ENERCON's SCADA is a critical component for operation of 5800 turbines across 1217 wind farms amounting to 10GW of electricity, which means impacting this software, its servers, or its communications can have a broad impact across thousands of turbines. In examining the wind energy business, it's clear there are many of these critical nodes whether they are software programs, operations centers, vendors, owners, or operators. A cyber actor seeking to make a demonstrable impact on U.S. electricity generation might only need to target a handful of these nodes.

5. Case Study: Ransomware Attacks on Nordex Group SE and Deutsche Windtechnik

5.1 Case Study Overview

On March 31, 2022, Nordex Group SE, a major wind turbine manufacturer, was impacted by a ransomware attack. According to the company's press release on the incident "The intrusion was noted in an early stage and response measures initiated immediately in line with crisis management protocols. As a precautionary measure, the company decided to shut down IT systems across multiple locations and business units." This response procedure included shutting off Nordex's remote communications to managed wind turbines. [16]

Two weeks later, on April 11, 2022 the German wind turbine maintenance company Deutsche Windtechnik faced a similar situation – the company's IT systems were hit by a cyber-attack resulting in them disabling remote connectivity and control to 2,000 wind turbines across Germany. The company's press release said the incident was a "targeted professional cyber-attack", but Matthias Brandt, director of Deutsche Windtechnik, later said "Cyber security experts working with Deutsche Windtechnik are investigating whether the ransomware attack used Conti malware". [17] [18]

5.2 Ransomware and Attribution of Attacks

The attacks on both Nordex and Deutsche Windtechnik have been unofficially attributed to the Conti ransomware group. A source for the technology news website Bleeping Computer told the outlet the Nordex was impacted by a Conti ransomware attack shortly after it occurred, and Conti claimed responsibility for the Nordex attack a few days later. [16] Nordex has not attributed the attack in any of their official press releases. Similarly, Deutsche Windtechnik originally claimed the attack they suffered was a "sophisticated cyberattack" but a company executive later said they were investigating whether or not it was an attack by Conti. [18] The ransomware element has been confirmed in other news sources, but suspected attribution to Conti was not confirmed by any other sources. [19]

When a company is hit by a ransomware attack, the malware will encrypt everything on the network it can, rendering it unavailable, and post a ransom note on the device screens. The company can either pay a ransom, at which point the group responsible will unencrypt the files and the network will be usable again, or the company can choose to attempt to recover the network on their own or with the help of a cyber incident response company. [20]

Conti was a prolific ransomware group prior to shutting down operations in June 2022. They were responsible for some of the most disruptive and harmful ransomware attacks in the books, including shutting down the IT systems of Ireland's Health Service Executive and Department of Health for multiple weeks and leaking over 650GB of data allegedly taken from the Costa Rican government after they refused to pay an extortion fee of $10 million. According to the U.S. Government in February 2022, "Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000." [21] Although in this case study the focus is the group's attacks on wind energy companies, Conti targets relatively indiscriminately and has a much larger target list than just energy sector companies.

5.3 Impact on Wind Farm Operations

Like the attack on SATCOM impacting ENERCON turbines, the ransomware attacks on Nordex and Deutsche Windtechnik resulted in the loss of communications between the wind turbines and remote monitoring/operations centers. Both companies stated their wind turbines continued to operate and generate power, with Nordex adding "wind farm communication with grid operators and energy traders was and remains unaffected". [17] [22] Fortunately for these companies and the wind farm owners, the remote access paths were turned off as precautionary measures only and not because they were directly impacted by the ransomware attacks. This meant recovery times were measured in days and not weeks or months as seen with ENERCON. Although the impact to the wind turbines, farms, and electricity generation was limited, these attacks demonstrate the lack of resilience these companies and operations have in the face of cyber-attacks.

5.4 Lessons Learned

Two of the lessons learned from the attack on ENERCON's SATCOM systems previously discussed also apply to the cyber-attacks on Nordex and Deutsche Windtechnik – the lack of redundancy for remote communications and the centralization of monitoring and operations enabling cyber-attacks on wind energy assets at scale. Neither of the companies impacted by a

ransomware attack felt confident their wind turbine and other farm assets were segmented enough from their IT networks to prevent the spread of ransomware and felt the need to preventatively disable their remote access. The attacks exposed the lack of resiliency in these networks because the companies didn't have redundant remote communications,

The scale of these attacks is also notable – although Deutsche Windtechnik is reported to control over 7500 turbines, the ransomware attack caused them to sever remote access to only 2000. [19] [18] It's not clear how many turbines were impacted when Nordex opted to cut off their remote communications after the ransomware attack. Despite the variability in evidence for understanding the full scale of these attacks, it's clear both targets could provide more deliberate cyber actors with the ability to target thousands of turbines at the same time or at least in one campaign. As seen with ENERCON, attacks at scale require companies to have far more resiliency in the form of resourcefulness and rapidity. These attributes were not put to the test for Nordex and Deutsche Windtechnik to the extent they were at ENERCON but given their need to disable their single remote communications mechanism during these attacks, it appears unlikely they would have the necessary resourcefulness and rapidity either. As a turbine vendor – Nordex – and a turbine maintenance company – Deutsche Windtechnik – these attacks also show the variety of companies with remote access to turbines, reinforcing the risk presented by increasing the number of potential access vectors for cyber actors seeking to target specific wind energy assets or the sector and its electricity generation more broadly.

6. Case Study: Chinese Malware Campaign Targeting South China Sea Wind Turbines

6.1 Case Study Overview

In August 2022, cybersecurity research company Proofpoint and consulting firm PwC's joint threat intelligence teams released a report detailing a cyber espionage campaign which, among other victims, primarily targeted companies involved with wind turbines in the South China Sea. This campaign ran from at least April to June 2022 and used ScanBox malware. The threat actors used phishing e-mails often posing as a fictional media company, the "Australian Morning News", and would send a URL to a malicious domain that delivered the ScanBox malware framework. Proofpoint and PwC reported targets fell mostly into three groups: Australian government or private entities, Malaysian energy and financial companies, or global companies related to the supply chain of offshore energy projects in the South China Sea. They specifically stated targets included "heavy industry and manufacturers responsible for the maintenance of offshore wind farms [and] manufacturers of installation components used in offshore wind farms". [23] This campaign was attributed to a threat group called Red Ladon, a "China-based, espionage-motivated threat actor" which overlaps with APT40, according to the report. [23]

6.2 Background and Context

This campaign is not Chinese cyber actor's first foray into targeting renewable energy companies. Eight years ago, in 2014, the U.S. Department of Justice (DoJ) charged five hackers associated with the Chinese People's Liberation Army on thirty-one counts for computer

hacking and economic espionage impacting six American companies. One of those companies was the U.S. subsidiary of a German solar panel manufacturing company, SolarWorld. The DoJ stated the information stolen from SolarWorld by the cyber actors "would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles." [24] Chinese cyber actors have routinely been accused of or confirmed to be targeting internationally strategically important sectors to further China's own national-level economic or strategic policies.

Although it's been several years since the SolarWorld AG campaign, more recent activity is also worth highlighting for context. Before April - June campaign, in late March 2022, Proofpoint observed the same group conducting phishing activity against a European equipment manufacturer whose components were utilized in the installation of an offshore wind farm in the Strait of Taiwan. According to the report, "Specifically, the manufacturer targeted was a key supplier of equipment for entities involved in the construction of the Yunlin Offshore Windfarm… The project began to encounter construction delays which resulted in several major contractors terminating contracts and leaving the project unfinished between November 2021 and February 2022." The researchers concluded, "The targeting of supply chain entities by TA423 during this period of project uncertainty is notable, since the group has previously targeted projects in the South China Sea during key moments in their development timeline." [23]

APT40, which overlaps with the group Red Ladon Proofpoint and PwC attribute this activity to, has been indicted by the U.S. DoJ for illicit computer network exploitation. The U.S. Government has stated APT40 cyber actors work for a front company, Hainan Xiandun Technology Development Company, under orders from the Chinese Ministry of State Security's (MSS) Hainan State Security Department. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), "These MSS-affiliated actors targeted victims in the following industries: academia, aerospace/aviation, biomedical, defense industrial base, education, government, healthcare, manufacturing, maritime, research institutes, and transportation". [25] Cybersecurity research company Mandiant describes APT40 as "a cyber espionage operation targeting crucial technologies and traditional intelligence targets" as well as highlighting activity from the group targeting strategically important countries to Chinese growth and outreach initiatives including China's Belt and Road Initiative. [26] This profile aligns with the idea that Chinese actors would be targeting wind energy projects in the strategically important South China Sea for espionage purposes.

6.3 Impact to Wind Energy Sector and Lessons Learned

With this campaign focused purely on espionage, according to the report, there was no demonstrable, direct impact to wind turbine or electricity generation operations which makes it more difficult to assess the performance of resiliency attributes in this incident. However, this activity brings to light some future concerns for the global wind energy sector and represents a valuable case study for the United States in particular.

First, the victimology of this campaign demonstrates an understanding by cyber threat actors of how many entities are involved in wind energy generation, as well as the capability to and value in targeting a broad swath of them. In this instance, the activity targeted multiple

companies involved in the maintenance and multiple companies involved in installation components of the offshore wind farms. We have no evidence to suggest additional types of companies involved in the offshore wind farms were also targeted, but cyber threat actors could add several types of companies to this list for an even broader picture including turbine vendors, wind farm owners, wind farm integration companies, SCADA or other software providers, and grid operators or energy market firms that receive generation and/or data from the farms. Having higher numbers of companies involved in each wind installation means each of them need to be independently robust in the face of cyber-attacks so an attack on one cannot materially impact the others and the critical function of electricity generation.

Second, the Chinese threat actor recognition of the strategic importance of wind energy generation in the South China Sea and what they were able to learn about its build specifications and operational details may transfer to U.S. wind energy sector entities in the future. As wind energy becomes a larger portion of the U.S. electricity generation mix, particularly with major growth in offshore farms anticipated in the next 5-10 years, the Chinese likely understand the value in being able to hold those assets at risk. Although there may be more political reasons the farms in the South China Sea were targeted due to the history and political controversy of the region, this espionage activity may be a signal for what to expect on the U.S. side as well.

7. Exploratory High-Impact, Low-Probability Analysis: Manipulation of Wind Farm Efficiency Resulting in Foreign Control

7.1 Defining High-Impact, Low-Probability Analysis

One of the many structured analytic techniques promoted for intelligence analysts by the U.S. Government is high-impact, low-probability analysis. This technique "highlights a seemingly unlikely event that would have major policy consequences if it happened." [27] It is used for events that, although unlikely to occur, have not been given much consideration and possible consequences are not well understood. As the U.S. Government's Tradecraft Primer notes, "the fall of the Shah, the collapse of the Soviet Union, and the reunification of Germany were all considered low probability events at one time; however, analysts might have benefited from considering the consequences of such events and how they might plausibly have come about." [27]

7.2 Analysis: Manipulation of Wind Farm Efficiency Resulting in Foreign Control

Like other electricity generation industries, the wind energy sector is first and foremost a business with the primary goal of turning a profit. With significant investment required upfront to build a wind farm, running efficiently and reducing maintenance and downtime are key goals for wind farm owners and operators who need to recoup their initial investment costs. For example, the Boswell Springs Wind Project in Wyoming, slated to begin operation in 2024 and run for 30 years, will have 97 wind turbines with a capacity of 331 megawatts and is projected to cost $528 million. [28]

Because of the need to maximize electricity production from these wind farms, the efficiency of the wind turbines is monitored constantly, however, it's also vulnerable to disruption from a stealthy cyber-attack. A nation state cyber actor with intimate knowledge of wind farm control systems, wind turbine operations, and the IEC 61400-25 standard that standardizes wind farm communications could devise an attack that changes set points for turbine pitch and yaw across an entire wind farm and potentially multiple farms operated out of the same remote control center. The cyber actor would also need to mask their activity to remote and local monitoring so the efficiency reductions would not be detected, but with access to the farm's SCADA system, this is practical and spoofing a reporting message a well-known tactic for stealthy cyber-attacks on control systems.

Over time, this reduction in efficiency would reduce the profitability of the wind farms and could lead the owner to believe their investment will not pay off in their expected timeline. Facing this prospect, it's very possible the owner would seek to sell the wind farms, which would open up an opportunity for the nation state that conducted the cyber-attack to have a state-backed company (or a U.S. subsidiary of the company) purchase the wind energy assets. Ultimately, and if done at scale, this could result in foreign control over an increasingly important source of U.S. electricity generation and allow them to hold this generation at risk or potentially disconnect it in times of increased tension or outright conflict.

8. Discussion

The three case studies presented in this paper have provided several lessons learned for improving cyber resilience of the wind energy sector. Systemic issues prevalent throughout wind energy sector companies include the criticality of remote communications without built-in resiliency and a complex and vast network of companies in the supply chain and operating environment increasing the attack surface. Furthermore, processes, time and investment required for response and recovery will only increase as the sector grows and offshore and distributed resources become more prevalent. Lastly, as the cyber-attack impacting ENERCON's turbines demonstrated, cyber-attacks against wind energy at scale are possible, leaving these assets vulnerable to a disruption that could have a tangible impact on the U.S. grid moving forward or an even bigger impact on the power supply for countries more reliant on wind energy. All of these considerations paired with the likelihood wind energy will be targeted more by cyber actors as a strategic source of electricity generation equates to a sector with a significant need for improvement in cyber resilience.

From the case studies, it's clear remote communications play a key role in the operation of wind farms but are vulnerable to disruption from even low-sophistication cyber-attacks conducted without the intent to impact control systems. As ENERCON stated in their press release on recovery from the attack on their SATCOM systems, there are redundant communication methods available including mobile/LTE, but these are often optional and provided only at additional cost to the wind farm builder. [12] Resiliency for wind farm communications would improve with regulations for redundant communication systems, both for remote and local operations, or a choice by turbine vendors to include these systems by default and increase their costs accordingly. Additionally, segmentation of communications over different pathways to operators, vendors, electric grid entities, and other companies

receiving datapoints from the turbines would allow continued remote monitoring and control even if one entity's communications are impacted by a cyber-attack. Both options increase the redundancy built into a wind farm, thereby increasing its resilience in line with the R4 framework presented in the introduction. This redundancy may also benefit the overall system resilience by improving resourcefulness and rapidity because, in the event all the redundant communication paths fail, various technologies and organizations could be used to decrease recovery time.

Being able to impact many turbines at once by targeting wind energy sector centers of gravity such as large operations, maintenance, and vendor companies is appealing for cyber actors and the sector provides a wealth of options. Turbine vendors in particular are concentrated to just a handful of key companies worldwide. As seen with Nordex, Deutsche Windtechnik, and ENERCON, a single attack can impact thousands of turbines at once. The Chinese cyber espionage campaign on companies involved in South China Sea wind farms also demonstrated these U.S. adversaries already understand the breadth of the attack surface. Mitigating this aspect of wind energy generation is complicated and will take a whole-of-sector effort.

First, limiting the number of companies with the ability to access wind farm SCADA constantly and directly can cut down on potential access vectors for a cyber actor. Centralizing control at one company and allowing only them to grant temporary and limited access to other companies for maintenance or other activities heightens the cybersecurity requirements for that central company but reduces the overall attack surface. Using technology like data diodes can allow other companies to view the datapoints they need from turbines without the risk of cyber actors being able to exploit this connection. As previously mentioned, redundant data streams would also complicate a cyber actor's ability to spoof reporting messages and could allow for earlier detection of manipulation of turbine operations.

Finally, improving capacity for response and recovery of wind farm operations in the wake of a cyber-attack will also be important for ensuring cyber resiliency in the sector in the future. Additional resourcefulness and rapidity are critical for wind energy companies to improve resilience. As seen with the ENERCON attack, it took nearly two months to recovery normal operations for 5800 turbines by replacing SATCOM modems or restoring communications via LTE/mobile. Fortunately, ENERCON was able to secure requisite SATCOM modems in a time of worldwide supply chain constrictions that could have extended recovery time far longer – the mark of a resourceful strategy for recovery. Still, this recovery time is unsustainable when paired with the potential for future cyber-attacks at a scale of the attack on ENERCON or even larger. They are especially unsustainable with the future growth in offshore wind farms where mechanisms for a rapid recovery drop precipitously with the complications and time associated with accessing these assets. There is a clear need for better guidance on recommended cyber-attack response and recovery operations for the wind energy sector. More robust and redundant remote communication pathways can also support this by allowing turbine components to be restarted, re-flashed, or otherwise updated remotely, but these more resilient communications are not currently implemented across the sector. Tabletop exercises and other planning and practice activities could also help improve both resourcefulness and rapidity because of the experience gained during exercises and the ability to adapt based on lessons learned.

9. Conclusion

The wind energy sector has been focused on growth and increasing capacity but has deprioritized key aspects of cyber resilience in the process. The case studies presented in this paper – a Russian cyber-attack on ENERCON wind turbine SATCOM systems, ransomware attacks on Nordex and Deutsche Windtechnik, and a Chinese cyber espionage campaign targeting wind farm companies in the South China Sea – provide opportunities for the wind energy sector to learn from its current lack of cyber resilient technologies and operating procedures. Including redundant remote and local communications by default, reducing the cyber-attack surface introduced by third-party companies, and improving resourcefulness and rapidity through improved recovery procedures for cyber-attacks at scale will all result in a more resilient wind energy sector. Building this resilience has requirements for governments, owners, operators, and vendors, but it will be necessary to meet the U.S. goal of having wind energy produce 20 percent of electricity across the country by 2030 in a secure and sustainable way.

References

[1] K. Tierney and M. Bruneau, "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction," *TR News,* no. 250, pp. 14-18, May-June 2007.

[2] J. Staggs, D. Ferlemann and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection,* vol. 17, pp. 3-14, June 2017.

[3] U.S. Department of Energy, "Roadmap for Wind Cybersecurity," 1 July 2020. [Online]. Available: https://www.energy.gov/sites/prod/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf. [Accessed November 2022].

[4] J. Greig, "German wind farm operator confirms cybersecurity incident," Recorded Future, 29 April 2022. [Online]. Available: https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/. [Accessed November 2022].

[5] M. Froese, "Improving wind-turbine performance with PLCs," WTWH Media LLC, 5 May 2016. [Online]. Available: https://www.windpowerengineering.com/improving-wind-turbine-performance-plcs/. [Accessed Nov 2022].

[6] "Wind power needs communication," Siemens, [Online]. Available: https://new.siemens.com/global/en/markets/wind/equipment/industrial-communication.html. [Accessed 26 November 2022].

[7] GE, "Digital Wind Cyber Security from GE Renewable Energy," GE, January 2017. [Online]. Available: https://www.ge.com/digital/sites/default/files/download_assets/GE-Digital-Wind-Cyber-Security-Brochure.pdf. [Accessed 12 December 2022].

[8] E. Telmo, I. Canales, J. Villate, E. Robles and S. Apinaniz, "The Use of IEC 64100-25 to Integrate Wind Power Plants into the Control of Power System Stability," in *European Wind Energy Conference & Exhibition*, Milan, 2007.

[9] International Electrotechnical Commission (IEC), "IEC 61400-25 Wind energy generation systems: Communications for monitoring and control of wind power plants," International Electrotechnical Commission (IEC), Geneva, 2017.

[10] "Taking remote control: a day in the life of US wind operations," 16 May 2016. [Online]. Available: https://www.bp.com/en/global/corporate/news-and-insights/reimagining-energy/houstons-wind-remote-operations-centre.html. [Accessed November 2022].

[11] D. Unger, "Behind the scenes: Inside a renewable energy control center in downtown Chicago," 23 June 2017. [Online]. Available: https://energynews.us/2017/06/23/behind-the-scenes-inside-a-renewable-energy-control-center-in-downtown-chicago/. [Accessed November 2022].

[12] Enercon, "Over 95 per cent of WECs back online following disruption to satellite communication," Enercon, 19 April 2022. [Online]. Available: https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/. [Accessed 25 November 2022].

[13] A. J. Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," U.S. Department of State, 10 May 2022. [Online]. Available: https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/. [Accessed 25 November 2022].

[14] J. A. Guerrero-Saade, "AcidRain | A Modem Wiper Rains Down on Europe," Sentinel Labs, 31 March 2022. [Online]. Available: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. [Accessed 25 November 2022].

[15] Viasat, Inc., "KA-SAT Network cyber attack overview," Viasat, 30 March 2022. [Online]. Available: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. [Accessed 25 November 2022].

[16] L. Abrams, "Wind turbine firm Nordex hit by Conti ransomware attack," 14 April 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/. [Accessed November 2022].

[17] Deutsche Windtechnik , "Cyber attack on Deutsche Windtechnik," 22 April 2022. [Online]. Available: https://www.deutsche-windtechnik.com/us/news/news/detail/cyber-attack-on-deutsche-windtechnik/. [Accessed 24 November 2022].

[18] "European Wind-Energy Sector Hacking Linked to Conti Ransomware Group," CyberSecurity Connect, 27 April 2022. [Online]. Available: https://www.cybersecurityconnect.com.au/critical-infrastructure/7772-european-wind-energy-sector-hit-in-wave-of-hacks. [Accessed 25 November 2022].

[19] V. Petkauskas , "Deutsche Windtechnik hit with a cyberattack, a third on Germany's wind energy sector," Cybernews, 27 April 2022. [Online]. Available: https://cybernews.com/news/deutsche-windtechnik-hit-with-a-cyberattack-a-third-on-germanys-wind-energy-sector/. [Accessed 20 November 2022].

[20] A. Gillis and B. Lutkevich, "Ransomware," TechTarget, December 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/ransomware. [Accessed 29 November 2022].

[21] "Alert (AA21-265A) Conti Ransomware," U.S. Cybersecurity and Infrastructure Security Agency, 9 March 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-265a. [Accessed 29 November 2022].

[22] Nordex, "Update on cyber security incident," Nordex Group, 12 April 2022. [Online]. Available: https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/. [Accessed 20 November 2022].

[23] M. Raggi and S. Scenarelli, "Rising Tide: Chasing the Currents of Espionage in the South China Sea," Proofpoint and PWC, 30 August 2022. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea. [Accessed November 2022].

[24] Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, 19 May 2014. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. [Accessed 29 November 2022].

[25] "Alert (AA21-200A) Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department," U.S. Cybersecurity and Infrastructure Security Agency, 20 July 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-200a. [Accessed November 2022].

[26] F. Plan, N. Fraser, J. O'Leary, V. Cannon and B. Read, "APT40: Examining a China-Nexus Espionage Actor," Mandiant, 4 March 2019. [Online]. Available: https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor. [Accessed 29 November 2022].

[27] U.S. Government, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009. [Online]. Available: https://www.stat.berkeley.edu/~aldous/157/Papers/Tradecraft%20Primer-apr09.pdf. [Accessed November 2022].

[28] Power Intelligence Center, "Boswell Springs Project, US," Verdict Media, 7 December 2021. [Online]. Available: https://www.power-technology.com/marketdata/boswell-springs-project-us/. [Accessed December 2022].

[29] A. Greenberg, "Researchers Found They Could Hack Entire Wind Farms," 28 June 2017. [Online]. Available: https://www.wired.com/story/wind-turbine-hack/. [Accessed November 2022].