INL/JOU-21-63192-Revision-0

CYBERSECURITY CONCERNS FOR THE ENERGY SECTOR IN THE MARITIME DOMAIN

December 2021

Dr. Ian Ralby, Andy Bochman

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/JOU-21-63192-Revision-0

CYBERSECURITY CONCERNS FOR THE ENERGY SECTOR IN THE MARITIME DOMAIN

Dr. Ian Ralby, Andy Bochman

December 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

CYBERSECURITY CONCERNS FOR THE ENERGY SECTOR IN THE MARITIME DOMAIN

Dr. Ian Ralby and Andy Bochman

Executive Summary

The world has seen a number of high-profile maritime disasters in recent months and years, and has felt the impact of them. At the same time, the world has also seen a number of high-profile cyberattacks. It has felt their impact, as well. And, likely no sector has been more affected by the maritime and cyber incidents than the energy sector, as fuel prices often spike or trough, and access to energy resources can become an instant source of concern, tension, or even conflict. As energy sectors—in all their forms—continue to rely on the maritime domain or even increase that reliance, they must be mindful that traditional maritime threats—like piracy, theft, and weather events—are not the only threats they face today. Maritime cybersecurity concerns are among the most potentially disruptive to energy-sector interests and, yet, are among the least understood and least addressed. This paper identifies nine areas in which the energy sector faces harmful cyber vulnerabilities in the maritime domain, to provide enough insight and examples to allow for action to be taken to reduce the risk of harm from these different vulnerabilities. The paper develops the example of offshore wind energy to model how to assess cyber considerations more fully. Ultimately, it concludes with a series of recommendations that offer policymakers, energy-sector actors, and security and law-enforcement professionals steps to minimize the exposure of the maritime energy sector to harmful cyberattacks.

Introduction

Two months before a cyberattack shut down the Colonial Pipeline, creating fuel shortages and spiking fuel prices in the eastern United States, the world watched the drama of the *Ever Given*, stuck blocking the Suez Canal for more than six days in March 2021.[1] That seemingly short disruption of maritime commerce caused by a single vessel was enough to have tangible impact on energy supplies in different places around the world.[2] More than 90 percent of world trade happens by sea, and more than 30 percent of the maritime industry is operating in support of the energy sector at any given time.[3] The nexus

[1] Max Rust and Roque Ruiz, "Why the Colonial Pipeline Shutdown Is Causing Gasoline Shortages," *Wall Street Journal*, May 13, 2021, https://www.wsj.com/articles/why-the-colonial-pipeline-shutdown-is-causing-gasoline-shortages-11620898203; "Oil Prices Rebound on Fears Suez Canal Blockage May Last Weeks," *ET Energy World*, March 26, 2021, https://energy.economictimes.indiatimes.com/news/oil-and-gas/oil-prices-rebound-on-fears-suez-canal-blockage-may-last-weeks/81698811.

[2] "War-Torn Syria Rations Fuel Amid Ongoing Closure of Suez Canal," Al Jazeera, March 28, 2021, https://www.aljazeera.com/news/2021/3/28/war-torn-syria-rations-fuel-amid-ongoing-closure-of-suez-canal.

[3] Sam Meredith, "A Global Shipping Revolution Is Weeks Away—Here are the likely winners and losers," CNBC, October 30, 2019, https://www.cnbc.com/2019/10/30/imo-2020-the-winners-and-losers-of-a-global-shipping-revolution.html; Ian Ralby and David Soud, *Oil on the Water: Illicit Hydrocarbons*

between the energy sector and the maritime domain is only poised to grow as offshore oil and gas production continues, offshore wind expands dramatically, and both wave capture and floating solar plants become viable realities—not to mention the ongoing shipment of energy products and the raw materials and minerals that support the energy system.[4] The *Ever Given* may have been an accident, but it provides a stark reminder of how vulnerable the maritime domain is to disruption. That, in turn, is a vulnerability of critical concern for the energy sector. After millennia of engineering, seamanship, and experience, these two interconnected industries—maritime and energy—are perhaps most vulnerable to harm thanks to a relatively new concern: cybersecurity. Saturating the discussion of maritime transport and energy systems with fear, uncertainty, and doubt as to what a cyberattack is, or is not, however, only serves to confuse. With increasing technological advancement and dependence on both ships and maritime infrastructure, the maritime and energy sectors must be proactive in identifying and addressing cybersecurity concerns. This report seeks to provide a baseline for that process with regard to the energy sector's equities in the maritime space.

A Context of Confusion

The maritime world is esoteric; it has different laws, different terminology, and different priorities. Unfortunately, however, this means that the world's population tends to be profoundly "sea blind," as maritime matters are generally out of sight and out of mind for many people.[5] Furthermore, it is not easy to quickly understand the interests and equities that drive decision-making in the maritime domain without a significant degree of immersion.

For many, the cyber world is equally esoteric, considered the purview of mysterious hackers with skills that allow them to do seemingly impossible things. Despite a constant stream of news stories about oddly named cyberattacks and concerns about both hacking and cybersecurity, even experts in other areas of security often profess as much "cyber ignorance" as the general public has "sea blindness."[6] Further complicating matters, the difference between information technology (IT) and operational technology (OT) is lost on many who are not at least minimally familiar with cyber matters. In broad terms, IT refers to both the hardware and software of computer technology, whereas OT refers to

---

Activity in the Maritime Domain, *Atlantic Council*, April 10, 2018, https://www.atlanticcouncil.org/wp-content/uploads/2018/04/Oil_on_Water_WEB.pdf.

[4] "Offshore Wind Energy Will Surge to over 234 GW by 2030, Led by Asia-Pacific," *Wind Energy and Electric Vehicle Magazine*, August 5, 2020, https://www.evwind.es/2020/08/05/offshore-wind-energy-will-surge-to-over-234-gw-by-2030-led-by-asia-pacific/76266; "Outlook on the Worldwide Wave Energy Industry to 2026—Opportunity Analysis for New Entrants," GlobeNewswire, May 18, 2020, https://www.globenewswire.com/news-release/2020/05/18/2034865/0/en/Outlook-on-the-Worldwide-Wave-Energy-Industry-to-2026-Opportunity-Analysis-for-New-Entrants.html#; "World's Biggest Floating Solar Farms," *Power Technology*, last updated February 23, 2021, https://www.power-technology.com/features/worlds-biggest-floating-solar-farms/.

[5] Butch Bracknell and James Kraska, *Ending America's "Sea Blindness," Atlantic Council*, December 6, 2010, https://www.atlanticcouncil.org/blogs/new-atlanticist/ending-americas-sea-blindness/.

[6] Tarah Wheeler, "Cybersecurity Ignorance is Dangerous," *Foreign Policy*, May 3, 2021, https://foreignpolicy.com/2021/05/03/cybersecurity-ignorance-is-dangerous/.

the devices that control the physical world. Yet, both are grouped together as cyber concerns and often seen as a subset of something else—either engineering or security.

One of the problems is that the intersection of maritime matters and cybersecurity concerns leaves most feeling out of their depth. The maritime world feels alienated by the cyber world, and the cyber world struggles to understand the legal and practical oddities of the maritime world. While naturally a fair number of experts from both camps have made the jump across that divide, the majority are either: at the technical and tactical level; within a company whose cybersecurity knowledge and practices are considered trade secrets; or within a government that classifies all of its work in this space. Consequently, it is extremely difficult to have an informed discussion about maritime cybersecurity in an unclassified environment, particularly at the strategic level. In other words, there is a dearth of literature and insight that is simultaneously accurate and insightful, while not being so technical on either the maritime or cyber fronts as to lose the meaning altogether. This void makes it difficult for leaders who lack expertise in the maritime cyber domain to make sound assessments of their needs and, thus, to make sound decisions about how to protect their interests.

Within that context of confusion, the further specialized set of interests and issues relating to the energy sector only adds another layer of complexity. Nearly a third of global maritime commerce is focused on moving or supporting the energy sector, and the majority of offshore infrastructure at this point is focused on extraction of oil or production of energy. With new policies and strategies around the world centering on offshore energy—including a rapidly growing offshore wind market that is projected to have a 23.4-percent increase in production between 2020 and 2027—this sector is poised to grow considerably in the next few years.[7] Grounded understanding of the myriad challenges related to cybersecurity for the energy sector in the maritime domain is therefore critical for navigating the course ahead. This analysis, therefore, seeks to bridge the divides between these fields by offering a practical, and not overly technical, review of some of the leading cybersecurity concerns for the energy sector in the maritime domain. This is not a catalogue of all maritime cyber vulnerabilities but, rather, a survey of those vulnerabilities whose exploitation could truly harm the energy sector, followed by an example of a deeper dive into one area of emergent concern—the cybersecurity considerations for offshore wind-energy production—to demonstrate the extent of the work that still needs to be done to generate greater understanding of this space.

A Survey of Harmful Vulnerabilities

Given the expanse of maritime activities relevant to the energy sector, the sets of cybersecurity concerns could be grouped in many different ways. To make the most sense

[7] Carolyn Amon and Marlene Motyka, "US Offshore Wind Market Could See Rapid Growth," *Offshore*, February 1, 2021, https://www.offshore-mag.com/renewable-energy/article/14190124/deloitte-us-offshore-wind-market-could-see-rapid-growth; "Global Offshore Wind Energy Market Is Estimated to Account for 188.35 GW by the End of 2027, Says Coherent Market Insights (CMI)," GlobeNewswire, March 12, 2021, https://www.globenewswire.com/news-release/2021/03/12/2192163/0/en/Global-Offshore-Wind-Energy-Market-is-estimated-to-account-for-188-35-GW-by-end-of-2027-Says-Coherent-Market-Insights-CMI.html.

of the key considerations, however, this analysis will examine nine areas, providing examples of each, including

1. human error or human ignorance;
2. fraud;
3. attacks to facilitate crime;
4. navigational attacks;
5. operational attacks;
6. indiscriminate attacks;
7. compound attacks;
8. infrastructure attacks; and
9. future concerns.

While these nine considerations are applicable in other fields as well, their specific relevance to the energy sector—broadly defined to include the full spectrum of energy companies, but focused on those with direct maritime interests—is highlighted in each instance.

1. Human Error or Human Ignorance

While it may seem paradoxical, the biggest cyber vulnerability is almost always human beings. Either from error or from ignorance, humans are able to create more harm than most hackers could ever imagine. While it may be possible for a highly skilled hacker to access sensitive or important data stored on a laptop, it is much easier to access that data directly on that laptop if it is left at a bar and ends up in the wrong hands. In the maritime space, the scope for human error is huge, even before mentioning the cyber aspects. Cybersecurity training—even basic training on the "cyber hygiene" good practices that limit some of these human-generated vulnerabilities—is not commonly incorporated into the training for seafarers. The international mandated Standards of Training, Certification, and Watchkeeping (STCW), developed in 1978 and most prominently updated in 1995 and 2010, address a range of security and safety concerns on ships; cyber considerations are not included. Furthermore, outsourcing to contractors brings a range of actors—from engineers to longshoreman to stevedores to security guards—into direct contact with ships, maritime infrastructure, and maritime technology. So, from crew members sharing operational information on social media to offshore platform workers taking technology home with them, the range of cyber-related harm from basic human error or ignorance can be huge.

Energy-Sector So What

The energy sector moves a tremendous amount of hydrocarbons by sea and produces a substantial amount of energy offshore. While all of that may be within energy companies' contractual control, it is not always within their direct control. So, the sector must be proactive in ensuring adequate cyber training throughout the supply chain to minimize the odds of human error or ignorance opening the door to cyber-related harm. Even seemingly low-level contractors like harbor pilots, bunkering operators, or supply vessels could create significant cyber complications through human error or ignorance.

2. Fraud

While fraud is usually an attempt to induce human error on someone else's part, it is a distinct category of concern. Cyber fraud is one of the most famous forms of scamming in recent years, as a range of tactics have cost individuals and companies huge amounts of money. While most maritime and energy companies are unlikely to fall for the "Nigerian Prince" email scams, they are very susceptible to other forms of cyber fraud. Of course, any employee at any company could fall victim to link manipulation or some other inducement that leads to "malware" infecting the company's network. But, in the maritime space, there are more maritime-specific concerns. Take, for example the common practice of "spear phishing." Phishing is using emails to convince the recipients to go to a site or do something that will cause them harm in some way, but spear phishing is a targeted version of this activity. So, rather than a generic email, it is specific, calculated, and often directed to the specific recipient.

For example, a company security officer (CSO) at a shipping line might receive an email just before the close of business on a Friday that purports to be from a canal authority. Seemingly official and legitimate, the email includes a lot of accurate details about that company's vessel, which is due to transit the canal over the weekend. It indicates, however, that someone has neglected to pay the required $100,000 bond for transit, and that the vessel will not be allowed to proceed without doing so. Not wanting to be fired for delaying the vessel unnecessarily, the CSO scrambles to authorize payment of the bond, even though it would not normally be her responsibility. After a weekend of feeling satisfied that she helped sort out her company in a pinch, she comes in to discover that the $100,000 is gone and that the email had an underscore in the address that does not appear in the actual canal authority's emails. While this example is financially focused, cyber fraud can create any number of harmful circumstances, even venturing into blackmail and extortion.

Energy-Sector So What

Seen by many criminals as both "deep pockets" and the source of various forms of injustice, the energy sector is a target for criminals who may take interest either in creating harm or in obtaining an illicit windfall. The esoteric nature of the maritime space combined with general sea blindness—wherein the maritime space is woefully undervalued and largely ignored—makes it a prime venue for targeting the energy sector. The risk of getting caught in the maritime domain is far lower than on land, given the lack of monitoring and absence of rapid response. Rather than physically pirating a vessel and stealing the oil cargo, therefore, cyber criminals may use fraud as way of producing a similar result.

3. Attacks to Facilitate Crime

Beyond fraud, there are other cyber means to either perpetrate harm or obtain an illicit windfall. Cyberattacks—including hacking into databases, records, or logistics systems—

can help facilitate a wide array of other crime. In the Port of Antwerp, for example, hackers facilitated a massive drug-trafficking operation for years by modifying the records of certain containers, allowing for goods to move through the port undetected.[8] Cyber activities can create confusion and blind spots that criminals then leverage to their advantage. If a ship's crew, for example, is involved in a smuggling or trafficking operation, it may even tamper with its own ship's automatic identification system (AIS)—the internationally required means of monitoring the movement of vessels—to indicate a fake route. The data would then suggest that the ship moved in a certain way, whereas, in reality, it was somewhere else. This could then obscure activity such as a meeting with another vessel to transfer the smuggled or trafficked goods, or even to offload part of an oil cargo via a ship-to-ship transfer.

Perhaps the main form of attack for facilitating crime is the deployment of "ransomware." In such attacks, the cyber interference is used to demand a ransom. One of the most visible ransomware attacks was the 2021 Colonial Pipeline incident. While the attackers actually apologized for the harm they created, noting that they were just trying to make money and had not anticipated such acute damage, they were using a cyberattack to extort funds.[9] Incidentally, that matter had maritime implications as well: in addition to the well-publicized fallout on land, including fuel shortages and panic purchasing of fuel in large quantities, the Jones Act—the US cabotage law—had to be suspended to facilitate rapid tanker deliveries of fuel along the coast.[10]

Energy-Sector So What

There have been incidents in which terminal records have been amended to obscure entire tankerloads of oil. In other words, ships can call at a port, load up a full cargo, and leave without any record of such an "off the books" transaction occurring.[11] Given the spectrum of crime—particularly theft—that could occur within the maritime space, the energy sector needs to be proactive in identifying methods to limit the opportunities for cyber activity to facilitate crime.

4. Navigational Attacks

Maritime navigation has been a distinct skillset for thousands of years. Over the last several decades, however, the stars and sextants have been replaced by technology, including the Global Positioning System (GPS) and the Global Navigational Satellite System (GNSS). Some maritime academies have greatly reduced, or even eliminated, traditional navigational training in favor of relying on GPS and GNSS, which have become vital technologies for maritime commerce. For about $300, however, a criminal can

[8] Tom Bateman, "Police Warning after Drug Traffickers' Cyber-Attack," BBC News, October 16, 2013, https://www.bbc.com/news/world-europe-24539417.
[9] Samantha Lock, "Colonial Pipeline Hackers, DarkSide, Apologize, Say Goal 'Is to Make Money,'" *Newsweek*, May 11, 2021, https://www.newsweek.com/colonial-pipeline-hackers-darkside-apologize-say-goal-make-money-1590327.
[10] "Biden Approves Second Jones Act Waiver to Address Fuel Shortage," *Maritime Executive*, May 14, 2021, https://www.maritime-executive.com/article/biden-approves-second-jones-act-waiver-to-address-fuel-shortage.
[11] Ralby and Soud, *Oil on the Water*.

procure the technology needed to make all the vessels at sea in a particular area believe they are actually on land. In the Black Sea, such spoofing of the GNSS has occurred. In 2017, roughly twenty ships at sea reported that their navigational equipment placed them on land at an airport.[12] Some have even questioned whether such attacks on a less dramatic scale have contributed to recent ship collisions and other marine casualties.[13] In that respect, it is far less dangerous if the navigational systems are obviously wrong—indicating that the ship is on land—then if it seems that they may be right (showing that the ship is in the water), but are providing inaccurate positioning. The 2019 spoofing of the navigational systems of the *Stena Impero*, for example, led to it being unintentionally in Iranian waters, resulting in its arrest by Iranian authorities.[14] It was detained in Iran for more than two months before ultimately being released.[15] Evidence suggests the *Stena Impero* is by no means the only vessel that has experienced such spoofing.[16]

Energy-Sector So What

If one of the ships in the Black Sea was not prepared for manual navigation, the spoofed GNSS could have led to a collision or allision that, in turn, could have created environmental harm, a hazard to navigation, or even loss of human life. Given the potential implications of a disoriented vessel carrying more than a million barrels of oil, or filled with highly flammable gas, the energy sector must establish protocols to rapidly identify such spoofing and ensure adequate navigational training to switch from the newer technologies to analogue or traditional techniques. Furthermore, given the harm that could come from a disoriented vessel in close proximity to offshore or submarine infrastructure—for example, dropping and dragging anchor to stop the ship pending reorientation or crashing into a windfarm—there need to be predetermined mechanisms for alerting mariners and averting disaster.

5. Operational Attacks

As noted, there is often a failure to distinguish between IT and OT. While various IT attacks could have operational impact, the cyber vulnerability of OT is generally underappreciated in the maritime domain. While some consider IT the purview of cybersecurity and OT the purview of cyber safety, both have huge safety and security implications in the maritime space.[17] Industrial Control Systems (ICS)—devices that help

[12] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" *Maritime Executive*, July 11, 2017, https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.
[13] Elias Groll, "U.S. Navy Investigating if Destroyer Crash Was Caused by Cyberattack," *Foreign Policy*, September 14, 2017, https://foreignpolicy.com/2017/09/14/u-s-navy-investigating-if-destroyer-crash-was-caused-by-cyberattack/.
[14] Michelle W. Bockmann, "Seized UK Tanker Likely 'Spoofed' by Iran," Lloyd's List, August 16, 2019, https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran.
[15] "Stena Impero: Seized British tanker leaves Iran's waters," BBC News, September 27, 2019, https://www.bbc.com/news/world-middle-east-49849718.
[16] "Why Vessels Passing Near Iran May Have Trouble Staying on Course," *Economist*, May 22, 2021, https://www.economist.com/middle-east-and-africa/2021/05/22/why-vessels-passing-near-iran-may-have-trouble-staying-on-course.
[17] Andrej Androjna, et al., "Assessing Cyber Challenges of Maritime Navigation," *Journal of Marine Science and Engineering* 8, 2020, https://doi.org/10.3390/jmse8100776.

operate or automate industrial processes—have changed how ships function. Newer ships may be larger than ever, but the technology onboard has actually reduced the number of crew needed to operate them. This technology, however, comes with vulnerability, because even without an IT-based cyberattack, a nefarious actor could remotely interfere with the OT to produce dramatic effect. For example, when the *Ever Given* became wedged into Suez Canal, creating global economic shockwaves, cyber experts began to speculate as to whether it was the victim of a cyberattack.[18] Specifically, there remain concerns about whether the erratic propulsion of the ship may have been due to intentional interference with the ICS. An effective attack in this space will usually appear to be an accident, and given that any number of reasons could account for the erratic propulsion, including a change in responsiveness to the new low-sulphur fuel required under the "IMO 2020" marine fuel regulations, it may never be possible to determine exactly what happened. Operational attacks, however, are likely to increase in parallel with the reliance of ships on technology. And, just as IT back doors have been created through attacks like Solar Winds, back doors built into OT on ships could create any number of operational challenges.

In addition to propulsion, any number of functionalities on a vessel could fall victim to an operational attack. Ballasting controls, rudder movements, and fuel metering are some of the more obvious areas where harm can occur. And, on most ships, there is no noticeable difference and no means of checking whether a command to do something (e.g., release ballast, or change direction) comes from the bridge of the ship, the headquarters of a company, or a nefarious actor. "Air gaps"—or not connecting technology to a network—are often mentioned as a "solution." As a practical matter, however, this is unrealistic and should not be entertained, as most OT can be networked, even unintentionally.

Energy-Sector So What

A cyberattack on OT within the ICS on a ship in service of the energy sector, or on the operation of an offshore installation, could create immense issues. Everything from causing a ship to burn extra fuel to shutting down the power on a vessel or rig to pressurizing a pipeline to the point of rupture is all within the realm of possibility for an operational attack. Ports have also become a major area of concern. While many of the systems at a port may be susceptible to IT attacks—and there are plenty of examples of both ransomware and malware incidents—the OT at ports is also increasingly the target of hackers. For example, the OT systems of Shahid Rajee Port in Iran were attacked in June 2020, resulting in shipping chaos and a cessation of tanker traffic.[19] A separate study by Lloyds of London indicated that insurance companies would not be able to cover the

[18] Joe Weiss, "Was the Ever Given hacked in the Suez Canal?" *Control Global* (blog), April 13, 2021, https://www.controlglobal.com/blogs/unfettered/was-the-ever-given-hacked-in-the-suez-canal/.
[19] Jasmina Ovcina, "Ports Increasingly Targeted by Cyberattacks as Maritime Incidents Surge," *Offshore Energy*, July 20, 2020, https://www.offshore-energy.biz/ports-increasingly-targeted-by-cyberattacks-as-maritime-incidents-surge/.

costs associated with a compromise of OT systems in fifteen ports in Asia, the damage of which could be upward of $110 billion.[20]

6. Indiscriminate Attacks

While many forms of cyberattack and cyber-related harm are intentional, and even targeted, the maritime space can be the victim of cyberattacks "by accident." Given the networked nature of global business and international commerce, an attack on one place, entity, or server can have an impact and cause harm on the maritime domain. On June 27, 2017, the Notpetya attack on a server in Ukraine led to $300 million of harm to Maersk Line, the world's largest shipping line. Simultaneously, all the computer screens across the company's 547 offices went blank and a message demanded payment in cryptocurrency to regain access to the computers.[21] Maersk was not the target, but global maritime commerce felt the impact. Or, as Andy Greenberg, technology journalist for *Wired*, famously said: "The weapon's target was Ukraine. But its blast radius was the entire world."[22]

Energy-Sector So What

The energy sector needs to be conscious that such indiscriminate cyberattacks may impact its maritime interests at any time. A ransomware or malware attack, for example, could shut down an offshore rig or an entire offshore wind farm. Protocols and response mechanisms are needed to mitigate and respond to attacks. Lessons should be learned from the companies that have experienced such situations. While both the energy and maritime sectors are notoriously competitive, security is not an area of competition that benefits any legitimate actor.

7. Infrastructure Attacks

Various forms of maritime infrastructure, from ports to offshore installations to submarine pipelines, could be the subject of a cyberattack, and they need to be protected in a variety of ways. The Colonial Pipeline attack should draw corollary concerns for subsea pipelines, but equal uncertainty around whether a 2008 explosion in the Baku-Tbilisi-Ceyhan pipeline points to worrying possibilities for subsea infrastructure.[23] While that incident was ultimately determined to be a physical rather than a cyberattack, the

[20] Simon Jessop, "Cyber Attack on Asia Ports Could Cost $110 Billion: Lloyd's," Reuters, October 29, 2019, https://www.reuters.com/article/us-lloyds-of-london-cyber-ports/cyber-attack-on-asia-ports-could-cost-110-billion-lloyds-idUSKBN1X900G.
[21] Adam Bannister, "When the Screens Went Black: How NotPetya Taught Maersk to Rely on Resilience—Not Luck—to Mitigate Future Cyber-Attacks," *PortSwigger*, May 18, 2021, https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks.
[22] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[23] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," Bloomberg, December 10, 2014, https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

possibility exists to remotely pressurize a subsea pipeline to the point of explosion.[24] While most attacks are likely to be less spectacular, interfering with infrastructure can cause harm to both global supply chains and the global economy if the attacks are sufficiently disruptive.

One form of maritime infrastructure, however, is uniquely critical to cyber matters. A network of roughly 420 privately owned submarine cables, no wider than a garden hose, lying on the ocean floor, is the physical backbone of the Internet. Between 97 and 99 percent of all telephonic and Internet data move through submarine cables. Roughly $10 trillion in transactions traverse that submarine network each day. While other forms of maritime infrastructure may be subject to cyberattacks, submarine cables are a component of maritime infrastructure that, if attacked, can actually stop all cyber activity and cause immense harm from the absence of it. In January 2019, for example, the island nation of Tonga experienced a total phone and Internet blackout because a submarine cable was cut.[25] While damage to submarine cables is not quite the same as a cyberattack, it is effectively a physical attack on a cyber system.

Energy-Sector So What

Given how many submarine cables have been cut by ships' anchors, this is an area about which any maritime operator needs to be aware, given the impact it can have on life on land and the global economy. Also, as offshore installations turn to submarine cables for connectivity, the concerns of an accidental or intentional attack mean that the energy sector needs to plan for resilience in the case of a cable fault.

8. Compound Attacks

Most forms of maritime cyberattacks are focused on the ship or infrastructure of interest. But, with the growing presence of technology in the maritime domain, there are new matters about which the energy sector should be both aware and concerned. Remotely operated unmanned aerial vehicles and underwater vessels open the door to cyber interference that could create significant physical harm. In other words, a cyberattack on one bit of technology could then be used to perpetrate a secondary, or compound, attack on something else. Take, for example, the increase in long-range payload carrying supply drones that are capable of moving goods several miles from ship to shore or shore to ship. If hacked and remotely controlled by a nefarious actor, they could be used to cause harm to a ship. In Singapore, for example, the port has recently started piloting the use of autonomous drones for delivering parcels from shore to ships.[26] Just as the *USS Cole* was attacked in 2001 when terrorists committed suicide by ramming a small boat into the hull

[24] Robert M. Lee, "Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline," SANS blog, June 15, 2015, https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/.
[25] Daniel Victor, "Could You Last 11 Days Without the Internet? Tonga Finds Out the Hard Way," *New York Times*, January 31, 2019, https://www.nytimes.com/2019/01/31/world/asia/tonga-internet-blackout.html.
[26] "Pilot Launch in Singapore: Autonomous Drone Delivery of Parcels from Shore to Ship," Wilhelmsen, https://www.wilhelmsen.com/ships-agency/maritime-drone-delivery/.

of the US warship, an unmanned system could be commandeered through a cyberattack to perpetrate similar harm.

Energy-Sector So What

Since 2019 in the Middle East alone, there have been numerous incidents in which different actors have used marine mines to attack tankers at sea, and drones to attack oil infrastructure. Compound attacks involving a cyberattack to perpetrate a physical attack are eminently foreseeable. The consequences for the energy sector could be catastrophic, depending on the target and the extent of damage produced.

9. Future Concerns

The movement toward autonomous shipping—no longer a theoretical possibility, but now an exigent reality currently being introduced in a number of contexts, tested in others, and projected to be worth $165 billion by 2030—and increased technology in the maritime domain creates a world of new opportunities for cyber attackers and a world of new challenges for those who operate legally in the maritime domain. Autonomous vessels—when controlled or overridden either through IT or, perhaps more likely, through OT interference—could become weapons.[27] Given the increase in maritime attacks in recent years, such an eventuality is not farfetched. The imaginary realms of literary fiction, like that of Peter Singer and August Cole's "Ghost Fleet," are rapidly entering the realm of genuine possibility. However, in security it is often a mistake to equate the most spectacular with the most significant. Something as simple as a backdoor in an OT device that allows a saboteur to remotely create frequent but "explainable" maintenance needs may be an effective way to bleed a competitor. And, as watchkeeping and navigation skills erode amid the reliance on technology, minor incidents caused by cyberattacks may become, by design, even harder to detect. Blanketing the maritime space in uncertainty and doubt about what is or is not a cyberattack will only complicate matters further.

Energy-Sector So What

The energy sector is a major player in the maritime domain, and can drive trends and innovation. As its leaders push for greater technological capacity and capability, they must also be mindful of greater vulnerability. "Red teaming," or playing devil's advocate with new ideas, as well as with minor variations in the range of known issues, is a wise approach to recognizing how nefarious actors might view a new development. For example, working out how hackers might manipulate the controls on a submarine pipeline to obscure the fact that they were tapping it to steal the oil, or thinking through how an autonomous vessel could be taken over and used to disrupt offshore drilling, or how a hacked supply drone could damage an offshore wind turbine, can all help spark new thinking about how to foreclose criminal opportunities. This is particularly important with new installations, new technologies, and new personnel. Thinking like a criminal

[27] "IMO Explores Issues for Regulation of Autonomous Shipping," *Maritime Executive*, May 25, 2021, https://www.maritime-executive.com/article/imo-explores-issues-for-regulation-of-autonomous-shipping.

organization—a skillful, well-resourced one—will help identify areas that need greater defenses and more extensive resiliency planning. The energy sector's interest in technology is often to increase efficiency and reduce cost. But, with the pervading problem of sea blindness and the general lack of understanding of potential harm emanating from cyber activity, maritime cybersecurity could become the energy sector's Achilles heel.

A Deeper Dive: Cyber Risks to Offshore Wind-Energy Systems

This section drills down on the cyber challenges facing one of the many types of maritime transportation system (MTS) energy assets: offshore wind-energy systems. Other than micro reactors and thermal storage under consideration for shipping, offshore wind-turbine farms, and particularly floating offshore wind turbines (FOWTs), which—sited farther from the coast to capture more consistently high-speed winds—represent the latest field of maritime power production.[28] As such, they take advantage of the latest digital processing and communications technologies, and, in fact, could not exist without them.[29]

Some of its content and suggestions are specific to offshore wind; however, the majority of issues described in this section are common to every manner of modernized and modernizing MTS energy system. At the highest level, the issue is the presence of—and near-total dependency on—software, supply chains, and communications. Software, most often an amalgamation of code from multiple sources with unknown provenance, including open source, is nearly guaranteed to have exploitable vulnerabilities present by accident, or inserted intentionally by adversaries. Supply-chain security is now top of mind in Washington, DC, as a spate of recent executive orders have made clear.[30] And, communications technologies are what make monitoring and control at a distance possible, which means determined adversaries, upon achieving access, may misuse these capabilities for purposes not intended by designers, owners, or operators. As every MTS energy system now in the field depends on constant or intermittent access to computer networks reached by a variety of communications technologies and protocols, and ranging from long globe-encircling satellite communications, to industrial control system (ICS)-specific ones (e.g., Modbus, DNP3), to the hyper local (e.g., Bluetooth, Zigbee, Wi-Fi) placed under the heading of the Internet of Things (IoT), to the grandaddy of them all, the bane of all cybersecurity practitioners, the Internet itself.

Markets largely determine the composition of future electricity-generation portfolios, and physics bounds what can and cannot become an affordable, reliable energy source. In

---

[28] Harry Valentine, "Small-Scale Nuclear Power for Commercial Ship Propulsion," *Maritime Executive*, August 30, 2020, https://www.maritime-executive.com/editorials/small-scale-nuclear-power-for-commercial-ship-propulsion.

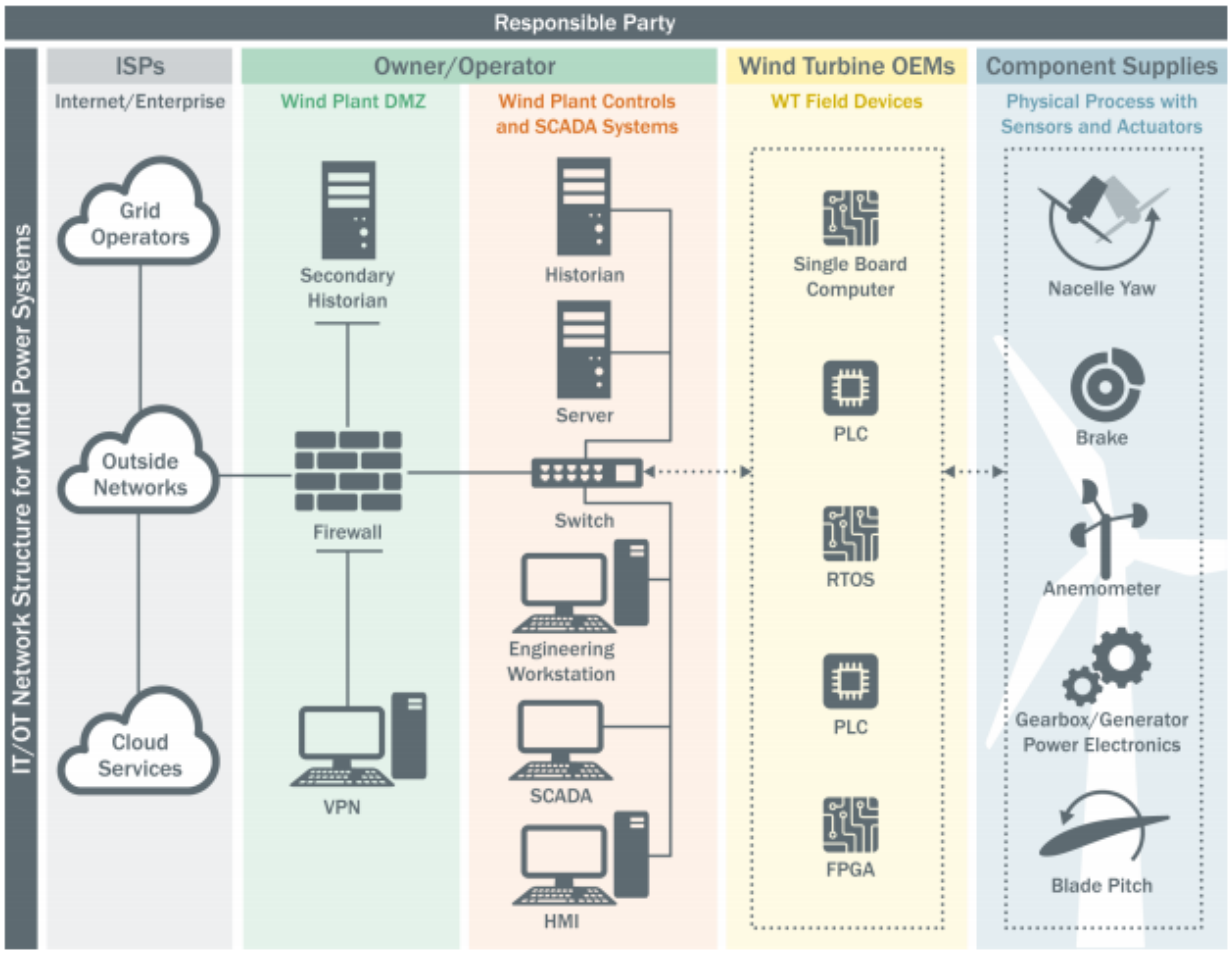
[29] V. Leble and G.N. Barakos, "A Coupled Floating Offshore Wind Turbine Analysis with High-Fidelity Methods," *Energy Procedia* 94, 2016, 523–530, https://doi.org/10.1016/j.egypro.2016.09.229.

[30] Beau Woods and Andy Bochman, *Supply Chain in the Software Era*, *Atlantic Council*, May 30, 2018, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/;
Robert Chesney and Trey Herr, "Everything You Need to Know About the New Executive Order on Cybersecurity", May 13th, 2021, https://www.lawfareblog.com/everything-you-need-know-about-new-executive-order-cybersecurity

2021, while liquid fuels look likely to continue their domination of marine surface and air transport, all signs point to a continuing decline in the role of fossil fuels in global electricity production.

While on-land wind and solar generation, increasingly backed by energy storage, continue their ascent, percentage-wise, offshore wind—soon to include a large number of floating turbines capable of operating in deeper water—may be the category most likely to really take off.

Wind-Turbine Generation 101



US Department of Energy's schematic representation of digital wind-plant infrastructure.[31]

[31] "Roadmap for Wind Cybersecurity," US Department of Energy, July 2020, https://www.energy.gov/sites/default/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf.

While modern turbines on land or at sea appear sleek and simple at first glance, under their smooth exteriors they are completely dependent on local and remote sensors, software, and communications to operate safely and efficiently. As the figure above shows from left to right, owner/operators interact with these assets from afar, passing through security protections like firewalls, to reach OT systems that monitor, log, and give instructions to local digital devices like programmable logic controllers (PLCs) that send precise control signals to effect physical/mechanical changes.

When this gear is working properly and under the control of its intended operators, it is a modern marvel of sophisticated engineering. However, this paper is concerned with other-than-optimal circumstances. The pathways for bad actors to access systems and potentially disrupt operations are many, and most stem from the critical role communications technologies play in this domain. A few representative examples include

- for the asset owner to monitor, operate, and control assets;
- to ensure connectivity to the regional transmission operator (RTO) to ensure safe transfer of offshore power to the land-based grid; and
- to enable direct communication connections to the turbine manufacturer for remote diagnostics.[32]

Designers and integrators of these complex systems of systems must do so with the adversary in mind. Long past are the days when it could be assumed that the only people with access to controls would be fully vetted, trusted, and trained individuals. Today, design, development, and construction must adhere to "secure by design" or "cyber-informed engineering" principles, which begin with the premise that bad actors will seek to gain access by a variety of means, and then use that access to mis-operate the equipment in ways that were never intended.[33]

All Eyes on the Supply Chain

Offshore wind helps illustrate these core security concerns and need for improved risk management by maritime energy sectors developed throughout this paper and in further detail in *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*.[34] Importance noted by a security analyst is one thing. Strategic risk realized and acted upon by business executives in the companies that own and operate these assets, in the credit-rating firms that determine the interest rates they'll pay, and by the insurance companies that determine premiums based on their appraisal of risk, is quite another. With cyber

[32] S. Freeman et al. "Cyber Resiliency Within Offshore Wind Applications," *Marine Technology Society Journal,* 54, 6, 59.
[33] Robert Anderson, et al., "Cyber-Informed Engineering," Idaho National Laboratory, March 2017, https://inldigitallibrary.inl.gov/sites/sti/sti/7323660.pdf.
[34] Will Loomis, et al., *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*, *Atlantic Council*, June 30, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity/.

risk, there's always been a significant lag between what experts are calling out and what decision-makers are doing, and that includes government oversight bodies.

Every communications pathway presents an opportunity for access by cyber attackers. Ideally, best practices call for properly configured and fully patched firewalls to allow only authorized traffic and block all others—and virtual private networks (VPNs), which also require patching, to encrypt both inbound and outbound network traffic. Both of these types of cybersecurity tools are made from software, and have been found to contain about as many exploitable vulnerabilities as other categories of enterprise software. So, the product bought and deployed for protection can itself become the pathway for attackers.

Consider the Solar Winds episode, a clear-cut case of nation-state on nation-state cyber espionage. This demonstrably useful network-management and security-tool suite was recently in use at hundreds of thousands of clients, including the vast majority of Fortune 500 companies and many US government agencies, including the Department of Energy and its national labs. Like almost all other products, it contained security flaws that provided skilled cyber attackers the means of entry, as well as lateral movement within their targets, facilitating the vacuuming up of vast amounts of sensitive information and collection of access-control credentials that may be employed in later attempts at disruptive or destructive cyber-enabled sabotage.

When a software or software-enabled product is as popular as Solar Winds (and many are), it is called horizontal cyber risk. Though not quite this simple, essentially, would-be adversaries need to study just one product in depth to acquire knowledge enabling them to breach many target organizations. It is then, by virtue of these products' success in the marketplace and widespread use, that they represent inordinately attractive targets to attackers who can "learn once and use many times" their knowledge of potential weaknesses in these products. In the MTS there are many such things, often segmented by function. Here are a few examples: port operations systems such as highly automated cranes; propulsion and navigation systems for commercial transport, tugs, and military ships; power generation for offshore wind turbines; and dynamic positioning and blowout-prevention systems for deep-water drilling rigs. This is in no way shape or form an exhaustive list, but is intended to demonstrate the potential for horizontal risk within the MTS.

Conclusion

The intersection of cybersecurity and the energy sector in the maritime domain provides one of the most fertile areas for criminal attack or nefarious state action. The general sea blindness and lack of attention to maritime matters have opened the door to an increase in criminality at sea in recent years.[35] With the energy sector relying heavily and increasingly on both maritime transport and maritime infrastructure, it remains one of the most critical targets for illicit activity in the maritime domain. While security professionals and law-enforcement officials are perpetually working to improve the

[35] Ian Ralby, "Navigating Maritime Governance Challenges and the Future of the Global Economy," *Diplomatic Courier*, September 5, 2020, https://www.diplomaticourier.com/posts/navigating-maritime-governance-challenges-and-the-future-of-the-global-economy.

physical security of energy-sector interests at sea, there remains a great degree of cyber ignorance that is being exploited in a variety of ways with equally varied impact. This analysis has shed light on nine key areas of concern, raising issues and examples along the way. The deeper dive into offshore wind considerations helps demonstrate some of the analysis that is needed to really understand both the cyber vulnerabilities of the energy sector in the maritime domain and what their implications might be. Resolving them, however, requires a variety of approaches.

Based on this analysis, the following are some key recommendations that the spectrum of actors concerned with maritime cybersecurity for the energy sector should consider.

- **Get comfortable with the maritime domain.** With a range of oddities that make it a world unto its own, the maritime domain is often a source of confusion. The law functions and applies differently at sea, and the location and type of either a vessel or offshore infrastructure can determine the extent to which law-enforcement officials can do anything to protect it. So, at least a basic sensitization to the law of the sea and to general maritime dynamics is important for understanding what needs to be protected and why.

- **Get comfortable with the cyber domain.** A confusing mystery to many, cybersecurity comes with terminology even more esoteric than that of the maritime world, and an operating space that is invisible to most. Knowing even basic cyber principles—including cyber hygiene—can help engender sufficient comfort to at least tackle some of the critical areas where cyber concerns arise.

- **Take stock of technology in use.** To know what they must protect, defenders need to know what systems they manage and how they are interconnected. This seems a simple recommendation, but a rigorous accounting of all the technology—both IT and OT—across maritime infrastructure and transportation system is a difficult task. That said, it is a crucial step for defenders to identify those vulnerabilities that could have the most serious impact.

- **Think like the adversary.** Defenders thinking like a criminal or state actor is important for discerning their own weaknesses and more effective means to address them.

- **Prioritize defenses according to impact.** Vulnerabilities will always exist. The question is: how much can they affect owners and operators? Discerning potential impact allows for prioritization according to what is most detrimental.

- **Invest in meaningful cyber defenses.** The impact of cyberattacks are increasingly obvious. While the complexity and diversity of the maritime domain complicates matters, the Federal Energy Regulatory Commission's Notice of Public Record on "Incentives for Cybersecurity Investments" provides a useful guide to

help policymakers do everything in their power to incentivize investments in defensive cyber tools and services whenever and wherever possible.[36]

- **Build resiliency through analog redundancy.** While there are always going to be sophisticated cyber defenses to sophisticated cyberattacks, true resiliency may require shifting the mode of operation to an analog alternative. As the heart of the Securing Energy Infrastructure Act (SEIA), putting trusted humans back in the decision loop, and the selective reintroduction of analog systems, stopgaps, and failsafes, ready for when control and/or trust is lost in cyber-enabled systems, should be examined for the highest consequence functions, missions, and systems.[37]

- **Establish response protocols.** Rapidly identifying a potential cyber incident is critical, but so is ensuring that information gets to key decision-makers in a timely fashion. There need to be protocols for detecting incidents and standard operating procedures for how information gets shared, initial investigations are conducted, and response mechanisms are activated.

- **Prepare for the worst.** The best way to be effective and efficient in responding to a cyberattack is to practice. Scenario-based tabletop exercises can simultaneously make all actors more comfortable and confident in abiding by response protocols, and more sensitized to potential cybersecurity concerns. This latter aspect may be critical to ensuring that a cyber incident is noticed and addressed in a timely manner.

- **Be vigilant.** The maritime domain is constantly changing with new challenges, new regulations, and new threats. The cyber world is exceedingly dynamic, with new developments and new dangers almost daily. And, the energy sector is equally undergoing perpetual change. There is no place, therefore, for either arrogance or complacency when it comes to cybersecurity in the maritime domain for the energy sector. Vigilance and agility are key to even maintaining a level of consistency, much less achieving the objective of continual improvement in the face of multivariable threats.

---

[36] "FERC Proposes Incentives for Cybersecurity Investments by Public Utilities," Federal Energy Regulatory Commission, December 17, 2020, https://www.ferc.gov/news-events/news/ferc-proposes-incentives-cybersecurity-investments-public-utilities.

[37] Dave Kovaleski, "Sens. King, Risch Applaud Passage of Securing Energy Infrastructure Act," *Homeland Preparedness News,* December 31, 2019, https://homelandprepnews.com/stories/41889-sens-king-risch-applaud-passage-of-securing-energy-infrastructure-act/. Recall the reintroduction of sextant training for midshipmen at the United States Naval Academy in 2016 after a ten-year hiatus. And, remember the one thing that can be trusted, when confidence in automated digital-systems waivers, is first-principles engineering based on the laws of physics. Those principles, in the hands of seasoned engineers and operators, served human beings well until the dawn of the computer age, and continue to serve well for certain things. But, with every passing year, people put more trust in automation and remove human expertise and judgement from functions and processes. The seasoned man in the loop has been removed in the name of cost savings and efficiency. He or she can be invited back.

Perhaps a little fiction might prove instructive, to illuminate how reintroducing some of the past into the present might help us proceed more securely, more confidently into the future.

> In the late 1970s TV show *Battlestar Galactica*, humans, having migrated to outer space, find their ships devastated by a hostile series of cyber attacks, with only one spaceship surviving. The outdated destroyer, *Battlestar Galactica*, last in line for the fleet-wide upgrade to digital controls, proves to be immune to cyber attacks and lives to fight another day. Like the famed *Battlestar*, industrial control systems were entirely analog in their original incarnations. In most U.S. nuclear power plants today, analog safety systems are still the norm. However, a seemingly inexorable fleet-wide digital upgrade is underway, and despite knowing in our bones that we're adding complexity, uncertainty, and cyber risk to our nuclear plants, absent a better way of thinking, most seem resigned to this fate. When considering the risks and rewards of going fully digital in the most critical of critical infrastructure systems, the optimal solution will often be a hybrid architecture where the benefits of digital are realized while the determinism of analog is drawn upon as an impermeable bulwark of cyber defense.[38]

It's a cliché now, but hope can no longer have a place in policy or practice in either of the ways it has, until now, confounded better judgement: hope that individual organizations will not catch the attention of cyber targeters; and/or hope that if they do become targets, that cyber defenses will be up to the challenge. Because the consequences of disruption are so high in the maritime domain, ports, ships, and offshore rigs *are* targets. And, as ever, accumulating and accelerating accounts of successful cyberattacks mount, it is clear that current approaches to cyber governance and hygiene in this and related domains are inadequate. To the greatest extent possible, it is time to return to first-principles thinking in this world. As former Department of Homeland Security Cybersecurity Director Marty Edwards has implored critical infrastructure owners, operators, and defenders on many occasions, think like the adversary; but act like an engineer.[39] Or, in other words, a prioritized and more proactive approach to cybersecurity is desperately needed for MTS energy systems and there couldn't be a better time than right now, in the wake of the many high-visibility cyber incidents of 2020 and 2021.

[38] Michael Assante, Tim Roxey, and Andy Bochman, "The Case for Simplicity in Energy Infrastructure," Center for Strategic and International Studies, October 2015, 6–7, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf.
[39] "'Think Like Hackers, Act Like Engineers' Says Leading Cyber Expert Ahead of Major Industry Conference," EINPresswire, June 11, 2018, https://www.einnews.com/pr_news/451038234/think-like-hackers-act-like-engineers-says-leading-cyber-expert-ahead-of-major-industry-conference.