Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure

Virginia A. Greiman
Boston University, MA, USA

ggreiman@bu.edu

Abstract: As of 2021, the World Nuclear Association reports 440 Nuclear reactors are in operation worldwide in 30 countries generating capacity of 390 (GW) which is equivalent to about 10% of the world's electricity. After Hydroelectric power, nuclear is the world's second largest source of low-carbon power. Important new nuclear technologies including the Small Modular Reactors (SMRs) are being developed globally creating more efficient and safer reactors that can be reproduced off site. While governments redoubled their commitments to reducing greenhouse gas emissions at the UN Climate Change Conference (COP26) in Glasgow, the recovery of economies following the harsh impacts of COVID-19 led to a surge in energy demand that surpassed the growth in production from clean sources including nuclear. The safety and security of nuclear power has received renewed attention since the Russian invasion of Ukraine presenting growing concern about the potential threat of increased malevolent cyber activity against Ukraine's critical infrastructure. Moreover, there have been more than 20 known cyber incidents worldwide at nuclear facilities since 1990. To address these concerns this paper focuses on the progress of cyber security and cyber resilience in the nuclear industry globally. The 2015 cyber-attack on the Ukrainian Kyivoblenergo, a regional electricity distribution company was analyzed by multiple sources including private companies, investigators in Ukraine, and the U.S. government. The analysis revealed many opportunities to stop or prevent this attack, however, the nuclear industry continues to face serious challenges in protecting against cyber threats. This research will investigate through a comparative analysis the recent government regulations, rules and standards, for nuclear cyber security safety in the United States and internationally to determine whether these laws adequately protect energy infrastructure from cyberattacks and hold responsible parties accountable. Recent initiatives by government and the private sector to enhance the opportunities for improving cyber security in the nuclear sector will be reviewed to determine best practices for improving nuclear safety and cyber resilience.

Keywords: Nuclear Cyber Security, Cyber Resilience, Nuclear Regulation, Nuclear Power Plant Cyberattacks

1. Introduction

The recent cyber-attacks on a nuclear facility in the United States and Saudi Arabia, highlights the vulnerabilities of nuclear facilities. On March 24, 2022, the Department of Justice released sealed indictments against four Russian officials who hacked into the Wolf Creek operating system, Kansas' first nuclear power generating station and compromised a petrochemical facility in Saudi Arabia. According to the Indictment, the group used their hacking skills in two separate conspiracies which targeted the global energy sector between 2012 and 2018 (DOJ 2022). "Russian state-sponsored hackers pose a serious and persistent threat to critical infrastructure both in the United States and around the world," said Deputy Attorney General Lisa O. Monaco. "Although the criminal charges reflect past activity, they make crystal clear the urgent ongoing need for American businesses to harden their defenses and remain vigilant" (DOJ 2022).

According to the indictments, the four officials, including three members of Russia's domestic intelligence agency, the Federal Security Service, or F.S.B., are accused of breaching hundreds of energy companies around the world, showing the "dark art of the possible," a Justice Department official said at a briefing with reporters. Investigators believed at the time that the intrusion was meant to trigger an explosion, but said that a mistake in the code prevented one (DOJ 2022). Undeterred, the next year the hackers researched refineries in the United States and tried to breach the computers of an American company that managed similar critical infrastructure facilities in the United States, according to court filings. They used several tactics to gain access to computer networks, including spear phishing attacks that targeted more than 3,300 users at more than 500 American and international companies (DOJ 2022). They targeted government agencies such as the Nuclear Regulatory Commission, and in some cases they were successful.

The cyber-attack in India's largest civil nuclear facility – the Kudankulam Nuclear Power Plant (KNPP) in Tamil Nadu in September 2019 highlights the seriousness of cyber-attacks, and raises new concerns about the vulnerability of nuclear plants to serious destruction and potential loss of life (Chaudhury, 2019). Malware was discovered in systems used to manage administrative activities at the Kudankulam nuclear power plant and the attack was linked by the Nuclear Power Corporation of India to the Lazarus Group, operating from North Korea (Campbell and Singh 2019). Though the KNPP attack was not intended to cause destruction but to extort the confidential data and reconnaissance, future attacks may have more serious consequences.

Cyber-attacks provide a new opportunity for hostile powers to cause mayhem at nuclear facilities without ever having to have direct access to the facility. The compromise of networks in nuclear facilities can be used to facilitate sabotage, malicious acts involving nuclear material, compromise sensitive data, and create a reactor catastrophe. This is of grave concern in densely populated countries like India, as any radiation release from a nuclear facility would cause tremendous damage and loss.

The contributions of this paper are two-fold. First, this research discusses the increasing risk that nuclear plants face and the urgent need for a focus on stronger oversight of the nuclear industry that places responsibility on the parties best positioned to control the risk of a cyber-attack. Second, to review the cyber security regulatory environment specific to the nuclear industry followed by a discussion and recommendations on the initiatives that governments and the private sector – can and should take - in reducing the likelihood and impact of cyber-attacks on nuclear facilities.

2. Cyber security risk and nuclear power

The recent cyber-attacks in the nuclear industry reflect a growing threat to nuclear facilities globally. According to the U.S. Department of Energy, the past 20 years have seen the threat from malicious cyber attackers increase substantially, powered by new incentives for conducting attacks, such as drawing a ransom payment (DOE 2022). Cyber-attacks could be associated with business espionage, technology theft, a disgruntled employee, a recreational hacker, a cyber activist, organized crime, a nation state, or a terrorist organization (Arinze, et al. 2020). The overall expansion of the cybersecurity threat is a rising tide for all sectors; however, it is especially important to the energy sector (ODNI 2021). Lloyd's City Risk Index 2015-2025 reports due to an increasingly interconnected and technologically dependent world, that nearly half of the total GDP at risk is linked to manmade threats, including market crash, human pandemic, cyber-attack, power outage and nuclear accident (Lloyd's 2015).

The United States (U.S.), Russia, United Kingdom (UK), South Korea, and China have raised concerns about securing their facilities from catastrophic incidents. The Chernobyl incident of 1986 (WNA 2022a) and the Fukushima Daiichi nuclear disaster of 2011 (WNA 2022b) have also shown that disastrous consequences that can occur when the proper safety and security protocols are not followed (Kobayashi 2019). These events are indications of weak security and safety controls, resulting in reputation damage, loss of trust, reduction in shareholder value, financial fallout, and loss of human lives.

The most important security responses must be national and unilateral, focused on hygiene, redundancy, and resilience (Nye 2023). It is likely, however, that major governments will gradually discover that cooperation against the insecurity created by nonstate actors will require greater priority and attention. The world is a long distance from such a response at this stage in the development of cyber technology (Nye 2011).

3. Global sources of nuclear power

After Hydroelectric power, nuclear is the world's second largest source of low-carbon power. According to the World Nuclear Association (2023a) 13 countries in 2020 produced at least one-quarter of their electricity from nuclear. France gets around 70.6% of its electricity from nuclear energy, Slovakia and Ukraine get more than half from nuclear, while Hungary, Belgium, Slovenia, Bulgaria, Finland, and Czech Republic get one-third or more (WNA 2023a). South Korea normally gets more than 30% of its electricity from nuclear, while in the US, UK, Spain, Romania, and Russia about one-fifth or 20% of electricity is from nuclear.

Beyond power generation, nuclear technologies have medical applications that will help combat serious viruses like COVID 19. The International Atomic Energy Agency (IAEA) is providing diagnostic kits, equipment, and training in nuclear-derived detection techniques to countries asking for assistance in tackling the worldwide spread of the novel coronavirus causing Covid-19.

The International Thermonuclear Experimental Reactor (ITER) is presently building the world's largest and most advanced experimental tokamak nuclear fusion reactor in Provence, southern France (ITER 2022). ITER is an international nuclear fusion research and engineering megaproject. This is a true international endeavor run by seven member entities: the European Union, China, India, Japan, Russia, South Korea, and the United States. Overall, 35 countries are participating in the project directly or indirectly. The project was initiated in 1988 and is expected to start full deuterium-tritium fusion experiments in 2035.

Recently, as an alternative to large reactors, the U.S., the U.K. and Canada, three major nuclear markets, have all signaled growing support for the small modular reactors (SMRs) currently in development. Canada, for example, launched a 27-point SMR national action plan to demo and deploy the technology, update regulations and create employment. The global market for SMRs is expected to be worth up to $300 billion a year by 2040 (WEF 2021).

4. Nuclear cyber security regulations

Even though there has been some progress in developing enhanced cybersecurity measures across the nuclear industry, the research highlights the fragmentary and inconsistent response to cyberthreats at nuclear facilities by national governments and private-industry (Brunt and Unal 2019).

The 2020 Nuclear Security Index, published by the Nuclear Threat Initiative (NTI), shows progress on global nuclear security has slowed significantly over the past two years, despite sizeable gaps that continue to leave nuclear materials and facilities vulnerable to theft and acts of sabotage (NTI 2020).

According to the Index, regulatory requirements for nuclear security are not comprehensive, with significant weaknesses in important areas such as insider threat prevention, security culture, and cybersecurity, leaving dangerous gaps and vulnerabilities around the world. The Nuclear Security Index (NTI) found that 25% of countries with nuclear reactors don't have basic cybersecurity measures in place demonstrating an inconsistent global approach to cybersecurity programs at nuclear facilities (NTI 2020). Based on a country by country assessment NTI strongly recommended that significant steps be taken to improve cyber security at nuclear facilities thus reducing the potential for serious nuclear catastrophic events (NTI 2020). These include putting in place regulatory structures to implement national security, increasing global participation by strengthening global security, sharing information, and developing adequate regulatory and human resources to manage client countries' nuclear security responsibilities (NTI 2020).

4.1 United States nuclear security requirements

A year after the 9/11 attacks, the Nuclear Regulatory Commission (NRC) issued an order that included cyberattacks among the threats that nuclear plants would be required to defend against. Additional guidance for dealing with cyber threats was released during the next several years, and NRC issued formal cybersecurity regulations in March 2009 ("Protection of Digital Computer and Communications Systems and Networks," 10 CFR 73.54). NRC published a regulatory guide for the program in January 2010 (NRC 2010) (and in 2022 a proposed revision has been noticed) (NRC, 2022). Later that year, the Nuclear Energy Institute (NEI) also published implementing guidance in NEI 08-09, "Cyber Security Plan for Nuclear Power Plants" (and in 2018, an addendum). These documents provide information to aid licensees in developing cybersecurity plans. NRC's cybersecurity regulations require each nuclear power plant to submit a cybersecurity plan and implementation schedule. The plan must provide "high assurance" that digital computer and communications systems perform certain safety and security functions to provide adequate protection against design basis attacks.

NRC began inspecting the implementation of nuclear plant cybersecurity plans in January 2013. The inspections are part of NRC's Cyber Security Oversight Program, which is being incorporated into the existing Reactor Oversight Program (NRC 2020).

The Energy Policy Act of 2005 as amended (EPACT05, P.L. 109-58) imposed specific criteria for the NRC to consider in revising the "Design Basis Threat" (DBT), which specifies the maximum severity of potential attacks that a nuclear plant's security force must be capable of repelling. Among other changes, the revisions expanded the assumed capabilities of adversaries to operate as one or more teams and attack from multiple entry points (Holt and Andrews 2014)

Nuclear power plants are protected from cyberattacks by layers of safety precautions, with the first line of defense being isolation (NEI 2016). This means they have no direct access to web, nor do they have indirect access because they are not connected to the plants' internal networks" (NEI 2016). Some steps nuclear power plants have taken to protect against cyber threats include: "[i]solat[ing] key control systems;" "[e]nhanc[ing] and implement[ing] strict controls over the use of portable media and equipment;" and "[p]erform[ing] detailed cyber security assessments." (NEI 2016). Despite all of the layers of protection in the nuclear industry, it is still vulnerable to cyberattacks.

Notably, existing U.S. nuclear power reactors, designed in the 1960s and '70s, are controlled primarily by analog systems that are resistant to cyberattack. However, new reactors are being designed with digital controls, and

existing analog plants increasingly rely on digital computers to run auxiliary and monitoring systems. This increasing use of digital systems in nuclear power plants, along with post 9/11 security concerns and at least one "worm" infection at a U.S. reactor, (Kesler 2001) have prompted increased NRC attention to cybersecurity.

4.2 Global cyber regulation of nuclear power

Beyond the United States, the topic of cybersecurity in nuclear programs has been examined at the international scale as well (Pickering and Davies 2021). The Nuclear Threat Initiative (NTI) "cyber score index" illustrates the wide range of how seriously cyber threats are being addressed, from countries with well-developed nuclear power capabilities, such as the United States, Canada, France, Switzerland, and Russia, to countries with nuclear reactors and much more limited oversight, such as Mexico, Brazil, Italy, Kazakhstan, and China (NTI 2020). The NTI identified four overarching priorities they believe would substantially reduce the risk of damaging cyber-attacks on nuclear facilities. The priorities include institutionalizing cyber security, mounting an active defense, reducing complexity, and pursuing transformation. These recommendations are ambitious and not easily achieved, but if implemented, they would dramatically reduce the probability of a successful cyber-attack (NTI 2020).

One of the common threads among countries with limited nuclear capabilities according to NTI's 2020 Cyber Score Index is the lack of an institutional body or organizational structure focused on cyber security threats in the nuclear industry. For example, Ankara, Turkey is still trying to prepare necessary regulations and legislations to be ready for a proper establishment of the nuclear facility's infrastructure (NTI 2020). All ministries and public offices are approaching the problem from a micro perspective and are regulating their areas of interests. However, there is no coordinating authority to concentrate these micro perspectives into a macro one (NTI, 2020). Secondly, Turkey has no Industrial Control System (ICS)-specific cyber security organization, which could coordinate the private and state stakeholders in the sector (NTI 2020). By considering the recent political developments in Turkey and the ambiguity of international law on cyber-attacks, Turkey has to develop its own defensive and offensive cyber security capacity. Ankara has to persistently focus on coordination and strategic communication among necessary parties (NTI 2020).

To address the problem faced by Turkey and other countries with limited capacity to manage large nuclear facilities, the International Atomic Energy Agency (IAEA) and other international organizations are actively working to provide guidance and recommendations for cyber protection of nuclear facilities (IAEA 2021). Nuclear security is the responsibility of each individual country, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes.

The position of the International Atomic Energy Agency (IAEA) is that security is a national responsibility (IAEA, 2021). For the civil nuclear sector, the IAEA publishes nuclear security recommendations that reflect internationally accepted best practice, but there are no recognized international regulations as such. Other non-governmental organizations and lobbying groups, such as the World Institute for Nuclear Security (WINS, 2014), have issued high-level guidance documents on how national infrastructure for cybersecurity might be prepared, while instruction from organizations that set industry guidance such as the Nuclear Energy Institute (NEI) have also provided useful technical advice. Most recently, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has released numerous Alerts and Malware Analysis Reports regarding Russia's malign cyber activities, including the activities discussed in the indictments (CISA 2022). The National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce, has developed guidance specifically to assist nuclear facilities in complying with multi-faceted regulations to verify that the computers, digital communications and systems in CNI are protected from cyberattacks (NIST 2018).

5. Recommended initiatives

An analysis of the laws, regulations and standards governing nuclear cyber security and safety reveals that better organizational structures and frameworks are needed to adequately protect energy infrastructure from cyberattacks. The failure of accountability for cyber-attacks is a gap that must be remedied through proactive and coordinated efforts between governments and the private sector that support more rigid standards, tighter security control systems, a national cyber oversight authority, and development and enforcement of cyber security policies and regulations.

Through this research recent initiatives and lessons learned by governments and the private sector to enhance the opportunities in the nuclear sector have been explored and various approaches considered. Based on this analysis, the following four initiatives are recommended for improving nuclear facilities cyber security strategy:

(1) A cyber resilient approach to recovery, (2) preparation for cyber-attacks through more engaged public private partnerships, (3) early detection through mindful organizing, and (4) understanding where security has failed and improving the security of nuclear cyber security systems.

5.1 Cyber resilience as a solution to recovery from nuclear cyber attacks

The looming threat of a cyber-attack on the nuclear industry that will cause serious harm is real and possibly imminent. A key concept that supports the survivability of a cyber-attack is resilience. Though often connected with cyber security, cyber resilience has a distinct and significant purpose. For too long, the focus of response to cyber-attacks across industries has been cyber security. This paper recommends that complementary to cyber security, cyber resilience be adopted as a critical approach to resolving cyber-attacks in the nuclear industry (Greiman and Bernardin 2021). Today's world complexity leads researchers and practitioners to focus on the ability of the organizations to recover from setbacks, adapt well to change, and keep going in the face of adversity. "It is not just the physical structure which must withstand a blow and come back, we need resilient staff, resilient management, resilient plans, and planning" (Manto and Lockmer 2015, p. 199).

The National Institute of Standards and Technology (NIST) defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." The resilience of nuclear energy is the result of the combination of high levels of safety, operational flexibility and continuous learning from previous events. As recommended, by the Cyber Security and Infrastructure Security Agency (CISA), the organization's resilience to a destructive cyber incident must be maximized by test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by a destructive cyberattack (CISA, 2022).

As reflected in the OECD's Nuclear Energy Agency Policy (NEA, 2020) nuclear energy provides resilience on four main levels: (1) The first level is security by design. Design and beyond design nuclear power plants are conceived following the principles of defense-in-depth: prevention, protection and mitigation. This results in the implementation of redundant, independent and diversified safeguards designed to withstand external hazards. (2) The second level is the organizational level where resilience includes emergency preparedness, safety culture, continuous learning and international cooperation (Nucnet 2020). (3) The third level is the system level which has the following features: dispatchable and flexible; grid stability (inertia, reactive capacity, frequency control); on-site strategic fuel stockpiles; and simplicity of centralised systems. (4) The fourth Level is socio-economic, whereby there are competitive electricity prices; stable long-term investment; local high-paying jobs; and economic spill-over.

Resilience is a long-term endeavor that necessitates technology neutral policy actions beyond well-designed stimulus packages to properly guide investment decisions over time and correct potential market flaws (NEA 2020).

5.2 Preparation for cyber-attacks: Public private partnerships

In addition to resilient approaches to respond to cyber- attacks, a second important recommendation is to assess preparation for cyber-attacks at the national level, particularly through strong military offense and defense capabilities. According to the Defense Science Board (DSB 2017) as offensive cyber capabilities continue to grow, and are likely to outpace cyber defense, there are likely to be growing risks of misperception that could lead to rapid cyber escalation – and the potential for rapid escalation to armed conflict. In the United States, "[t]he U.S. Government must work with the private sector to intensify efforts to defend and boost the cyber resilience of U.S. critical infrastructure in order to avoid allowing extensive vulnerability to these nations.

The nuclear industry must also share information with other sectors. Without an ability to collaborate the nuclear industry cannot identify the attack patterns discovered by other sectors nor can it apply fool-proof security controls. It is no more palatable to allow the United States to be held hostage to catastrophic attack via cyber weapons by such actors than via nuclear weapons" (DSB 2017). Secondly, public-private partnerships for large-scale infrastructure projects have proven to be a formidable tool to reignite the economy and achieve social cohesion during previous crises (OECD 2019).

Early detection through mindful organizing

The wisdom of learning from failure is incontrovertible. Yet organizations that do it well are extraordinarily rare. High-reliability-organizations (HROs) are an example of organizations that have developed practices to help prevent catastrophic failures in complex systems like nuclear power plants through early detection. According to Weick & Sutcliffe, (2015) so-called high-reliability organizations (HROs) demonstrate particular characteristics in the way they operate: anticipating problems (being aware of what is happening in the work system; being alert to ways in which an incident could occur; looking beyond simplistic explanations for incidents); and containing problems (being prepared to deal with contingencies; using relevant expertise regardless of where it is situated within the organizational hierarchy). In their research on "high reliability organizations" they analyzed how highly regulated and standardized organizations such as nuclear plants, aircraft carriers and firefighting units achieve resilience in a complex environment. They found that technical checklists were not the key to success but instead a list of cultural features they define as "mindful organizing." They identified five principles that include preoccupation with failure, a reluctance to simplify, a sensitivity to operations, a commitment to resilience and a deference to expertise as a shared set of values that foster resilience through constant communication and recalibration in the face of unknowable risks (Weick & Sutcliffe 2015). High reliability theory should be explored in the cyber field because of the high potential for catastrophic outcomes from a cyber incidence. For instance, a cyber-attack on a nuclear plant could have long lasting and deadly consequences.

5.3 Improving the security of nuclear cyber security systems

Much has been written in the literature about nuclear security and safety in terms of nuclear reactors, waste disposal, site protection and security by design. However, little attention has been paid to the security of the cyber security system itself and the potential for catastrophic loss as magnified in the 2020 Solar Winds case in the United States where the country's largest multinationals and the U.S. government were caught off guard by an attack on their cyber security vendor (Constantin 2020). The Solar Winds cyber-attack illustrates the necessity of having a link between the supply chain and the organizations they support (Greiman and Bernardin 2021). Just as frightening as the scope of the attack is how smoothly the attack circumvented government and private-sector cyber defenses (Morris and Hackett 2021).

The application of 'security by design' in nuclear new builds will improve the protection of the plant and reduce the need for costly security improvements during its operating life. Security by design cannot fully protect a nuclear power plant from rapidly evolving cyberattacks, however, careful design of security systems and architecture can achieve levels of protection that exceed current norms and expectations (Brunt and Unal 2019). Security by design may well include a requirement for a technical support organization to conduct quality assurance of cyber defenses and practices, and this regime should be endorsed by a facility's executive board and continued at regular intervals after the new build facility has been commissioned. "Security by design cannot be a panacea, but it is an important factor in the establishment of a robust nuclear security – and cybersecurity – culture" (Brunt and Unal 2019).

6. Conclusion

Cyber security risk in nuclear power plants in the U.S. and around the world is a major national security threat impacting all nations. In light of the growing need for cleaner, low carbon technologies nuclear energy continues to evolve through the development of small modular reactors and newer fusion technologies. Countries seeking to develop nuclear energy capabilities should put in place the regulatory structures required to implement nuclear security, such as an independent regulatory body and a comprehensive set of regulations. Regulations should address the vital areas of insider threat prevention, cybersecurity, cyber resilience and a security culture, as well as traditional areas such as physical protection, control and accountability, and response capabilities. Moreover, national governments should take an active role in overseeing and centralizing at an institutional level the risks from cyber-attacks on nuclear facilities and the opportunities to mitigate these risks through more resilient structures. It is imperative that policy makers and private industry work together in partnership to develop more resilient security at the design, operational, systems and socio economic levels.

Acknowledgements

I would like to thank Renee Macasaet, my graduate research assistant for the collection and organization of extensive amounts of research for this paper.

References

Arinze, U.C., Longe, O.B., and Eneh, A. H.(2020) "Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues," International Journal of Nuclear Security Vol 6, No. 1, Article 3. https://doi.org/10.7290/ijns060103 Available at: https://trace.tennessee.edu/ijns/vol6/iss1/3

Atomic Energy Act of 1954, as Amended in NUREG-0980. Atomic Energy Act of 1954 (P.L. 83–703). https://www.nrc.gov/docs/ML1536/ML15364A497.pdf#page=23.

Brunt, R. and Unal, B. (2019) Briefing: Cybersecurity by Design in Civil Nuclear Power Plants. Chatham House, Royal Institute of International Affairs, International Security Department. London, UK.

Campbell, A. and Singh, V. (2019) "Lessons from the cyberattack on India's largest nuclear power plant" November 14, Bulletin of the Atomic Scientists.

Chaudhury, D.R. (2019, Aug 19) Kudankulam power plant 3rd unit moves towards operationalization ahead of PM's Russia trip. The Economic Times, Noida, Uttar Pradesh, India https://economictimes.indiatimes.com/industry/energy/power/govt-may-fund-unrealised-input-cost-of-gas-based-central-power-psus/articleshow/96892616.cms.

Constantin, L. (2020, December 15) SolarWinds attack explained: And why it was so hard to detect, IDG Communications. https://www.solar winds attack.

Cyber Security and Infrastructure Security Agency (2022) Shields-Up. CISA, Washington, D.C. https://www.cisa.gov/shields-up.

Department of Defense Science Board (DSB, 2017) Final Report of the Task Force on Cyber Deterrence, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C., February.

Greiman, V. A. and Bernardin, E. (2021) Cyber Resilience: A Global Challenge. Academic Conferences and Publishing Ltd. (ACPIL), Reading, UK.

Holt, M. and Andrews, A. (2014) Nuclear Power Plant Security and Vulnerabilities. Congressional Research Service, Washington, D.C.

International Atomic Energy Agency (2021) IAEA Nuclear Security Series No. 42-G Implementation Guide: Computer Security for Nuclear Security, IAEA, Vienna Austria.

ITER Organization. (2022) What is Iter? https://www.iter.org/proj/inafewlines.

Kesler, B. (2001) "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights,* spring 2001, p. 15. http://www.nps.edu/Academics/Centers/CCC/Research-Publications/StrategicInsights/2011/Apr/SI-v10-i1_Kesler.pdf.

Kobayashi, T., Suzuki, T., and Iwata, K. (2019) Accident Cleanup Costs Rising to 35-80 Trillion Yen in 40 Years. Follow up Report of Public Financial Burden of the Fukushima Nuclear Accident. Japan Center for Economic Research (JCER).

Lloyd's. (2015) Lloyd's City Risk Index 2015-2025. Lloyd's, London, England.

Manto, C.L. and Lokmer, S. (eds.) (2015) Planning Resilience for High-Impact Threats to Critical Infrastructure, p. 199, Infraguard, Westphalia, Press.

Morris, B.Z. and Hackett, R. (2021, Jan 29) After SolarWinds: Untangling America's cybersecurity mess. Fortune, New York, NY.

National Energy Agency (NEA) (2020, June) Building low-carbon resilient electricity infrastructures with nuclear energy in the post-COVID-19 era. NEA Policy Brief, NEA, Organization for Economic Cooperation and Development (OECD), Paris, France.

National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, U.S. Department of Commerce, Washington, D.C. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Nucnet (2020) Coronavirus: EDF implements Emergency Plan for French Nuclear Fleet, www.nucnet.org/news/edf-implements-emergencyplan-for-french-nuclear-fleet-3-5-2020.

Nuclear Energy Institute (2016) Cybersecurity for Nuclear Power Plants. NEI, Washington, D.C. Nuclear Energy Institute. (2016) NEI 08-09 Cyber Security Plan for Nuclear Power Reactors, Rev. 6. NEI, Washington, D.C.

Nuclear Threat Initiative (NTI) (2020) NTI Nuclear Security Index. NTI, Washington, D.C.

Nye, J.S. (2023, Jan 14) The Mouse Click that Roared. The Korea Times. https://www.koreatimes.co.kr/www/opinion/2022/02/197_142756.html

Nye, Jr., Joseph S. 2011. "Nuclear Lessons for Cyber Security" Strategic Studies Quarterly Vol 5, No. 4, pp. 18-38.

Office of the Director of National Intelligence (ODNI) (2021) Annual Threat Assessment of the U.S. Intelligence Community. U.S. Director of National Intelligence, 9 Apr. 20. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

Organization for Economic Cooperation and Development (OECD) (2019) Resilience strategies and approaches to contain systemic threats, OECD Publishing, Paris.

Pickering, S. Y. and Davies, P. B. (2021) "Cyber Security of Nuclear Power Plants- US and Global Perspectives" Georgetown Journal of International Affairs*, online:* https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/.

U.S. Department of Energy (2022) Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid. USDOE, Washington, D.C.

U.S. Department of Justice (2022, Mar 24) Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide. DOJ, Office of Public Affairs. https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

U.S. Nuclear Regulatory Commission (NRC) (2010) Cyber Security Programs for Nuclear Facilities Regulatory Guide 5.71, January. http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

U.S. Nuclear Regulatory Commission (NRC) (2020) Report to Congress on the Security Inspection Program for Operating Commercial Power Reactors and Category I Fuel Cycle Facilities: Results and Status Update - Annual Report for Calendar Year 2020 (NUREG-1885, Revision 14). NRC, Washington, D.C.

U.S. Nuclear Regulatory Commission (NRC) (2022) Draft Regulatory Guide DG-5061, Rev. 1 Proposed Revision 1 to Regulatory Guide 5.71. NRC, Washington, D.C.

Weick KE, Sutcliffe KM. (2015) Managing the Unexpected: Sustained Performance in a Complex World. (3rd ed.) John Wiley & Sons, Hoboken, NJ.

World Economic Forum (2021, Jan. 13) Nuclear: These countries are investing in small modular reactors. https://www.weforum.org/agenda/2021/01/buoyant-global-outlook-for-small-modular-reactors-2021.

World Institute for Nuclear Security (WINS) (2014) 4.3 Security of IT and IC systems at Nuclear Facilities, WINS International Best Practice Guide, https://wins.org/document/4-3-security-of-it-and-ic-systems-at-nuclear-facilities.

World Nuclear Association (WNA) (2023a) Nuclear Power in the world today. WNA, London, England. https://world-nuclear.org/information-library/current-and-future-generation/nuclear-power-in-the-world-today.aspx.

World Nuclear Association (2023b) Ukraine: Russia-Ukraine War and Nuclear Energy. WNA, London England.

World Nuclear Association (2022a) Chernobyl Accident 1986. WNA, London, England.

World Nuclear Association (WNA) (2022b) Fukushima Daiichi Accident (Updated May 2022) WNA, London, England.