Committee: Disarmament and International Security Committee (GA1)

Topic: Addressing the threat of cyber attacks on nuclear facilities

Student Officer: Grace Konidari

Position: Co-Chair

Personal Introduction

Dear delegates,

I am beyond honoured to welcome you to the Disarmament and International Security Committee (GA1) of the 13th CSMUN conference in 2025. My name is Grace Konidari, and I am an IB1 student attending Pierce - The American College of Greece. It is of great honour to serve as a co-chair of GA1.

I would like to congratulate you all on your participation as delegates in Model United Nations. MUN is a great way of expanding your knowledge on global diplomacy and current affairs, as well as enhancing your skills in public speaking and independent research, all while meeting new people.

The purpose of this study guide is to provide information about the threat of cyber attacks on nuclear facilities, an issue which poses great danger to humanity. While this study guide is essential for your holistic understanding of the issue, you are highly encouraged to do further research on your own in order for you to gain a view of the member state's policy and the stance you are representing. Having been a delegate myself, I know a conference can seem intimidating. Being an advanced committee, GA1 topics can be difficult to understand at first. Therefore, should you have any questions or need any kind of clarification, please do not hesitate to contact me via the email below.

I look forward to meeting you all!

Best regards,
Grace Konidari
g.konidari@acg.edu

Topic Introduction

A cyberattack refers to accessing unauthorised data with the intention to steal, alter or use it. In the digital age, cyberattacks have become a rapidly growing threat to global security. One of the most critical targets of these attacks is nuclear facilities, which refer to power stations, research reactors or even nuclear weapon infrastructures. Specifically, cyber threats to nuclear materials, nuclear facilities and nuclear command, control and communications are becoming more sophisticated every day, yet the global technical capacity to address the threat is limited.[1]

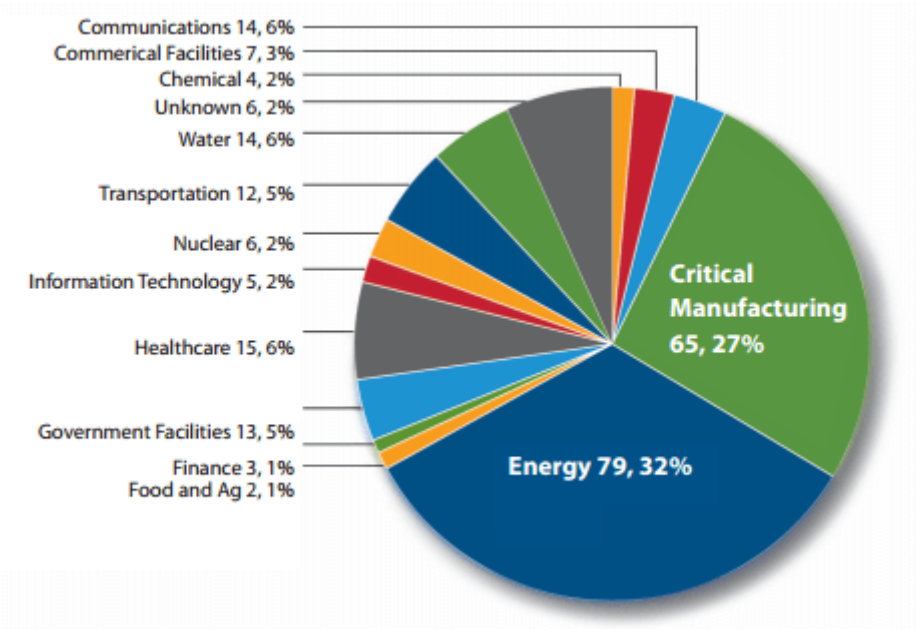

Figure 1: Chart demonstrating cyberattacks in different industries in 2014 [2]

Undeniably, cyberattacks on nuclear facilities are particularly hazardous, as not only could they result in nuclear accidents, but also in the acquisition of dangerous materials by terrorist groups and organisations, potentially causing millions of casualties. Cyber-attacks are additionally seen as an opportunity by hostile powers to create widespread instability at nuclear facilities, undermining the

[1] Stoutland, Page. "Addressing Cyber-Nuclear Security Threats." *The Nuclear Threat Initiative*,www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.
[2] OPSWAT. "How the Energy Industry Can Survive Targeted Attacks - OPSWAT." OPSWAT, 31 Mar. 2015, www.opswat.com/blog/how-energy-industry-can-survive-targeted-attacks.

security of nuclear materials and facility operations.[3] The compromise of networks in nuclear facilities can facilitate sabotage, threaten sensitive data, and even create a reactor catastrophe.[4]

Nuclear security efforts have traditionally focused on averting physical threats like using weapons and guards to prevent unauthorised access to nuclear command, control, and communication systems. Important progress has been made in this "traditional" nuclear security field, but not with cyberattacks, making countries with nuclear sites very vulnerable. As of now, the technical ability to address the cyber threat is extremely limited, even in More Economically Developed Countries (MEDCs). There exist almost no measures to prevent the incidence of nuclear cyber attacks.

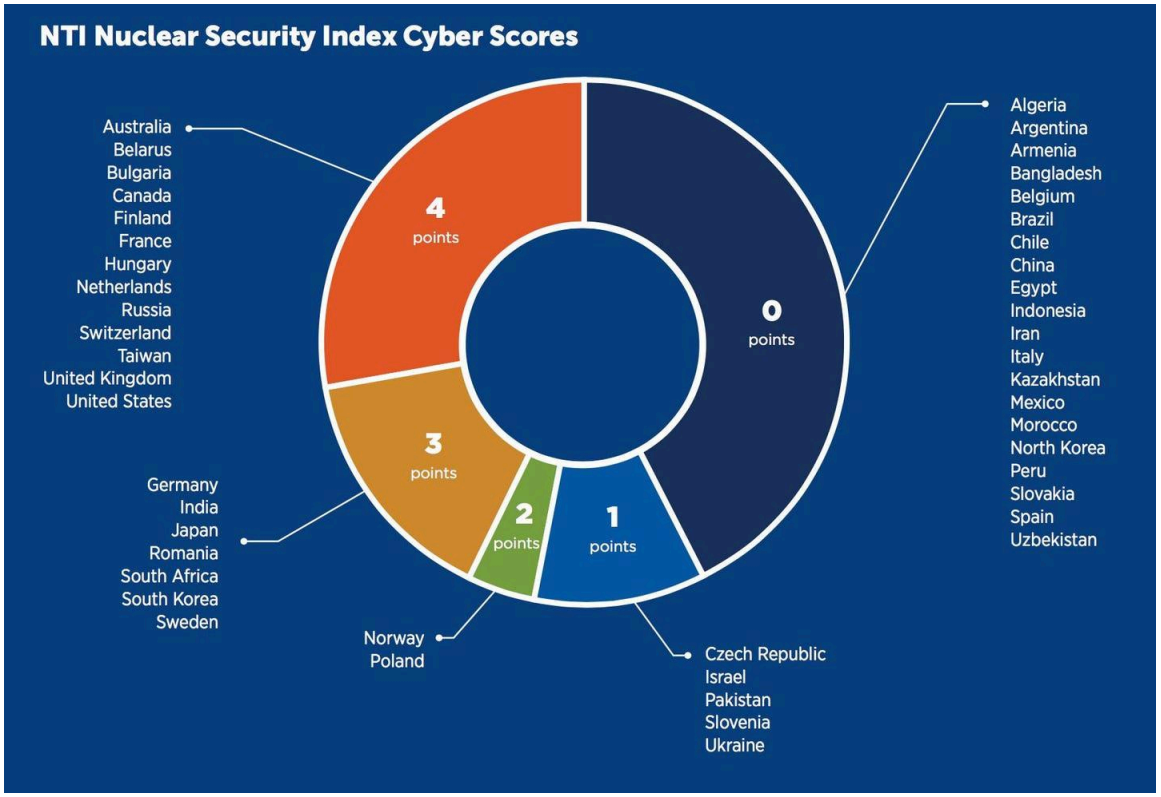

Figure 2: Chart indicating how well the nuclear industry of different countries is protected from cyber threats[5]

[3] Stoutland, Page. "Addressing Cyber-Nuclear Security Threats." *The Nuclear Threat Initiative*,www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/.
[4] https://papers.academic-conferences.org/index.php/iccws/article/download/1042/932/3388
[5] Conca, James. "How Well Is the Nuclear Industry Protected from Cyber Threats?" *Forbes*, 8 Nov. 2019, www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats/.

Addressing this threat is vital, because the consequences of a successful cyber attack on a nuclear facility could be catastrophic. Countries must strive to enhance collective security and ensure global stability. Therefore, preventing cyberattacks in nuclear facilities is not just a technological issue but is also a challenge to global security that demands action at both national and international levels.

Definition of key concepts

Cyberattack

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorised access to a network, computer system or digital device.[6] In the digital era, cyber attacks are becoming increasingly dangerous in the context of nuclear facilities, threatening not only the economy and the environment but humanity as a whole.

Nuclear Reactor

Nuclear reactors are devices that can initiate and control a self-sustaining series of nuclear fissions, which are central physical processes in nuclear power generation. They are used as research tools and, more importantly, as the source of energy generation for nuclear power plants.[7]

Terrorism

Terrorism can be characterised as violent criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organisations or nations.[8] In the case of cyberattacks, cyber terrorism is increasing, where such organisations attempt to gain control of key nuclear infrastructure and manipulate vital data.

Nuclear Facilities

Nuclear facility means a reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of the Department of Energy (DOE) and includes any related area, structure, facility, or

[6] IBM. "Cyberattack." *Ibm.com*, 15 Aug. 2021, www.ibm.com/think/topics/cyber-attack.
[7] Spinrad, Bernard I, and Wade Marcum. "Nuclear Reactor | Definition, History, & Components." *Encyclopædia Britannica*, 7 Feb. 2018, www.britannica.com/technology/nuclear-reactor.
[8] FBI. "Terrorism." *Federal Bureau of Investigation*, 2024, www.fbi.gov/investigate/terrorism.

activity to the extent necessary to ensure proper implementation of the requirements established by this Part.[9]

Command, Control and Communications (C3)

Command, Control and Communications of nuclear weapons (C3) are critical to the safe transportation operations of these weapons. C3 includes the ability and critical information necessary to plan, coordinate, communicate, and control operations.[10] An attack on a nuclear facility undermines its C3 system, thus putting a country in immediate danger, as it entails sensitive data on the facility's operations.

Nuclear material

Nuclear materials are substances that contain fissile isotopes and can sustain a nuclear chain reaction. These materials are americium-241, americium-243, californium, curium, deuterium, enriched lithium, neptunium-237, plutonium-238, plutonium-239-241, plutonium-242, thorium, tritium, depleted uranium, normal uranium, enriched uranium, and uranium-233.[11] An attack on a nuclear facility containing nuclear materials could trigger a nuclear chain reaction, which could have catastrophic consequences.

Research Reactor

Research reactors are nuclear reactors used for research, development, education and training. They produce neutrons for use in industry, medicine, agriculture and forensics, among others.[12]

Threat Receptors

Threat receptors are a type of protective measure implemented by the International Atomic Energy Agency (IAEA). They refer to several technical controls, such as radiation detection portals,

---

[9] Department of Energy. "Nuclear Facility." Doe.gov, 2023, www.directives.doe.gov/terms_definitions/nuclear-facility.

[10] "Command, Control, and Communications (C3) - Assure." *Assure*, 2 Aug. 2024, assureuas.org/capability/command-control-and-communications-c3/.

[11] "Nuclear Material(S)." *Doe.gov*, 2023, www.directives.doe.gov/terms_definitions/nuclear-materials.

[12] International Atomic Energy Energy. "Research Reactors." *Www.iaea.org*, 13 Apr. 2016, www.iaea.org/topics/research-reactors .

surveillance cameras, X-ray scanners for detecting hidden weapons or explosives, and interior and exterior intrusion detection sensors.[13]

Hacking

The activity of getting into someone else's computer system without permission in order to find out information or carry out illegal activities.[14] Hacking a nuclear base system could pose a significant threat to humanity as it would grant permission to confidential data.

Failsafe Review

A failsafe review or penetration testing is an assessment of a system to identify potential failure points and ensure that, in the event of a failure, the system will either automatically revert to a safe state or minimise harm to people or equipment.[15] It is essential that this method is adopted in all nuclear infrastructures in order to prevent cyberattacks and strengthen cybersecurity.

Red Teaming

Red teaming is a process for testing cybersecurity effectiveness where ethical hackers conduct a simulated and nondestructive cyberattack. The simulated attack helps an organisation identify vulnerabilities in its system and make targeted improvements to security operations.[16]

Background Information

Function and Methods of Cyberattacks

Most cyberattacks occur due to a vulnerability being exploited. It is estimated that 99.9% of cyberattacks happen because of poor cyber hygiene or a lack of security awareness.[17] Hence,

---

[13] International Atomic Energy Agency. "Security Aspects of Nuclear Facilities | IAEA." Iaea.org, 9 Dec. 2016, www.iaea.org/topics/security-aspects.

[14] "HACKING | Meaning in the Cambridge English Dictionary." *Dictionary.cambridge.org*, dictionary.cambridge.org/dictionary/english/hacking.

[15] The Nuclear Threat Initiative . 27 Oct. 2022, www.nti.org/wp-content/uploads/2022/10/Failsafe-Factsheet.pdf.

[16] Anderson, Evan. "What Is Red Teaming? | IBM." *Www.ibm.com*, 13 May 2024, www.ibm.com/think/topics/red-teaming.

[17] NI Cyber Security Centre. "How Cyber Attacks Happen." *NI Cyber Security Centre*, 4 Feb. 2020, www.nicybersecuritycentre.gov.uk/how-cyber-attacks-happen.

mundane mistakes like a user choosing an easy-to-guess password can much more likely prompt cyberattacks.

Cyberattacks can occur due to exposure of identity and login credentials, such as usernames and passwords.[18] Nuclear facilities' databases heavily depend on passwords and identification systems, which could be hacked and exploited by cyberattackers. Weak passwords and a lack of password protection allow passwords to be guessed and compromised electronically. What is more, cyber threats exploit security vulnerabilities exposed due to software and systems not being patched. In order to avoid this issue, any security updates should be installed immediately upon release. Furthermore, a lack of anti-malware software and services installed on devices can also make cyberattacks occurrence more likely. This is exacerbated by the fact that cyberattacks can take advantage of the information posted on social media. For example, hackers could use details from employees' social media posts, such as workplace photos showing security badges or control room layouts, to plan a targeted cyberattack on a nuclear facility.

Moreover, 'Phishing' is a common way to gain access to a system, which involves extracting personal information under false pretences.[19] Phishing refers to deceptive emails or messages that appear to come from trusted sources, tricking individuals into revealing login credentials or clicking on malicious links. Once access is gained, attackers can attack secure systems and steal sensitive data. This has even happened to a top official in the Democratic Party in the run-up to the 2016 US election, leading to the release of 60,000 private emails.[20] Another method of cyberattacks is the Denial-of-Service system, and specifically the Distributed Denial of Service (DDoS), where vast amounts of traffic are sent to a system in order to crash it, as a system can only handle so many requests at one time. Once this happens, legitimate users can no longer access the service, meaning lost revenue for the organisation and potentially more serious repercussions if the service was essential, like a nuclear facility. A DDoS on a nuclear facility would more likely target supporting IT

[18] NI Cyber Security Centre. "How Cyber Attacks Happen." NI Cyber Security Centre, 4 Feb. 2020, www.nicybersecuritycentre.gov.uk/how-cyber-attacks-happen.

[19] EQUIFAX. "How Cyber Attacks Happen | Equifax UK." *Www.equifax.co.uk*, www.equifax.co.uk/resources/identity-protection/how-cyber-attacks-happen.html.

[20] Harding, Luke. "Top Democrat's Emails Hacked by Russia after Aide Made Typo, Investigation Finds." *The Guardian*, The Guardian, 14 Dec. 2016, www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds.

systems and not directly reactor controls. While unlikely to cause a meltdown, such an attack could disrupt operations, delay response times, or overall create a broader cyber threat.

Notable Attacks

As political instability is rising, computer security has intensified in the last decade, while clear and recurring proof of the vulnerabilities of computer systems has come to light[21].

2003 - "Slammer" worm

The "Slammer" worm, also known as the Sapphire Worm, was the fastest computer worm in history. As it spread throughout the Internet, it doubled in size, notably every 8.5 seconds. Within 10 minutes, it infected more than 90% of vulnerable hosts[22], including a US nuclear power plant, demonstrating the vulnerability of safety monitoring systems. This occurred because administrators had failed to install a critical security patch that Microsoft had released six months earlier,[23] leaving the system exposed to exploitation. As a result, plant operators were temporarily unable to monitor reactor conditions in real time, creating a serious safety risk even though the core itself was not directly compromised. Slammer reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities, including water treatment plants and gas lines.

The Stuxnet worm

The Stuxnet worm, discovered in June 2010, was a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant[24]. A worm infects a computer network and spreads on its own. A virus, on the other hand, is installed by a victim. The Stuxnet was believed to be a joint US-Israeli operation in 2010 formed to cause damage to Iranian nuclear centrifuges, indicating a significant threat to nuclear security[25]. The worm's complexity and resources required for its development led many cybersecurity experts to believe it was the result of

[21] *Computer Security at Nuclear Facilities*. www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.
[22] "The Spread of the Sapphire/Slammer Worm." *CAIDA*, www.caida.org/catalog/papers/2003_sapphire/.
[23] "The Spread of the Sapphire/Slammer Worm." *CAIDA*, www.caida.org/catalog/papers/2003_sapphire/.
[24] Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 24 May 2024, spectrum.ieee.org/the-real-story-of-stuxnet.
[25] Trellix. "What Is Stuxnet? | Trellix." Www.trellix.com, 2024, www.trellix.com/security-awareness/ransomware/what-is-stuxnet/.

a state-sponsored operation.[26] Leaked reports and later journalistic investigations pointed toward a joint U.S.-Israeli operation, with the United States' National Security Agency (NSA) and Israel's Unit 8200 (the Israeli military's cyber-intelligence division) identified as key players. Experts call Stuxnet an incredibly complex piece of code and the world's first cyberweapon. It may have physically degraded nearly 1000 Iranian centrifuges. The worm manipulated the centrifuges' operating speed, creating enough stress to damage them. Stuxnet took its time, waiting weeks to slow down the centrifuges after accelerating them temporarily, making its activities hard to detect.[27]

Korea Hydro and Nuclear Power (KHNP) in 2014

In 2014, South Korea's nuclear plant operator said its computer systems had been breached,[28] raising fears that hackers, including those with possible links to North Korea, could affect key infrastructure. This raised serious concerns about national security, especially with suspicions of North Korea aiming to destabilise critical infrastructure and peace.

More about the attack:
https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack

Dangers

Nuclear facilities have numerous functions. They are vital for energy production, scientific research, and national defence. However, with the evolution of technology, they now heavily rely on digital systems and automation which makes them prone to cyberattacks. Hence, hackers could sometimes easily steal sensitive data or sabotage systems, particularly systems which control alarms and threat receptors. Such breaches threaten public safety and national security.

Radioactive releases

[26] The Guardian . "Stuxnet Worm Heralds New Era of Global Cyberwar." *The Guardian*, 30 Sept. 2010, www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar.
[27] "What Is Stuxnet?" *Malwarebytes*, 2023, www.malwarebytes.com/stuxnet.
[28] McCurry, Justin. "South Korean Nuclear Operator Hacked amid Cyber-Attack Fears." *The Guardian*, 23 Dec. 2014, www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack.

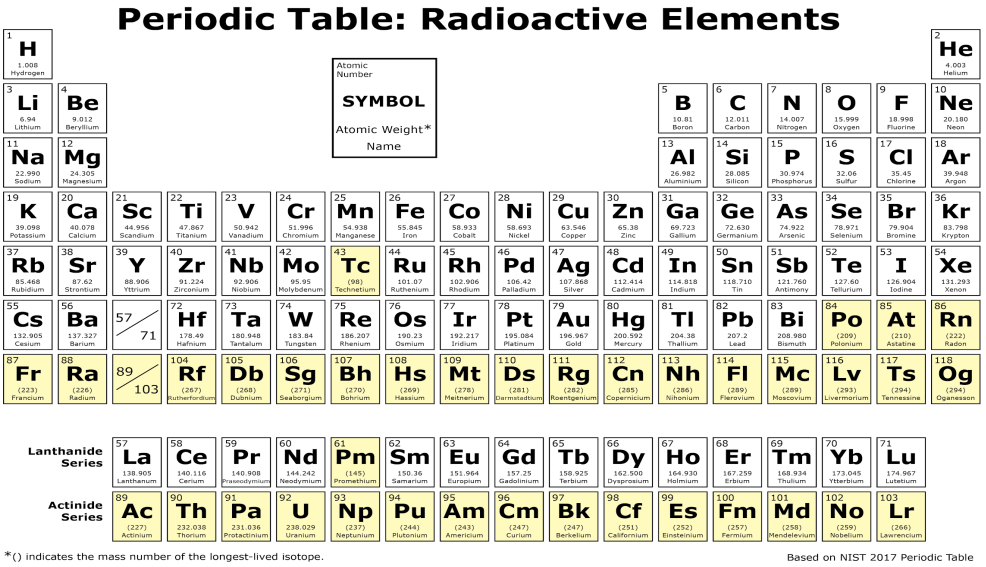

Figure 3: Periodic Table with Radioactive Elements highlighted[29]

A cyberattack could disable safety systems, which could have detrimental consequences. For instance, it could cause a release of radioactive material, prompting negative long-term health effects or even mass evacuations. A crisis like this necessitates emergency measures such as immediate evacuations from cities near nuclear infrastructure, as well as long-term solutions such as tax raises to improve national defence, and even subsidies to technology firms to help prevent future cyberattacks. All these measures can strain the economy and result in deep financial crises.

Physical damage

Cyberattacks can also take advantage of and attack the Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems, aiming to cause physical harm to nuclear infrastructure. For example, the Stuxnet worm damaged Iran's uranium enrichment centrifuges.

Theft of sensitive information

Cyberattacks can lead to the unauthorised access of classified data and information, which adversaries or terrorists can take advantage of. Internal vulnerabilities of a country could be released

[29] US EPA,OAR. "Radioactive Decay | US EPA." *US EPA*, 22 May 2015, 19january2021snapshot.epa.gov/radiation/radioactive-decay_.html.

by terrorist organisations if they access classified government or military data. This can be used to execute targeted attacks with greater impact, challenging the concept of collective security and endangering civilian lives. Because of the rapid advancement of technology and, thus, the improvement of cyber capabilities, the risk of cyber terrorism intensifies. This underlines that cybersecurity measures should become a vital component of counterterrorism strategies.

Case Study: The Stuxnet Worm

The Stuxnet worm, discovered in June 2010, is widely regarded as the world's first cyber weapon designed to cause physical destruction. It targeted Iran's nuclear enrichment program, specifically at the Natanz facility. Stuxnet was a 500-kilobyte worm that exploited multiple vulnerabilities in Microsoft Windows software. The worm is believed to have destroyed approximately 1,000 centrifuges, significantly disrupting Iran's uranium-enrichment efforts.[30] The attack delayed Iran's nuclear program by several years without requiring traditional military intervention. Importantly, Stuxnet demonstrated that cyberattacks could move beyond data theft or disruption and cause real-world, physical damage to critical infrastructure.

Although no government has officially claimed responsibility, multiple intelligence leaks and expert analyses attribute the operation codenamed "Operation Olympic Games" to a joint effort by the United States' National Security Agency (NSA) and Israel's Unit 8200. The complexity and resources required for Stuxnet far exceeded the capabilities of independent hackers, suggesting state sponsorship.

Stuxnet highlighted that nuclear facilities are not immune to cyberattacks. It showed how cyber operations can be used as strategic alternatives to kinetic warfare. Stuxnet proved that malware could be weaponised to achieve strategic objectives, setting a precedent for future cyber conflicts. Today, it serves as a critical case study in understanding the intersection of cybersecurity and modern warfare.

[30] "What Is Stuxnet?" *Malwarebytes*, 2023, www.malwarebytes.com/stuxnet.

Date	Description of the event
January 2003	The "Slammer" Worm spread across the internet, demonstrating the vulnerability of certain nuclear safety systems.
1 July 2004	The Budapest Convention came into force on July 1st 2004, becoming the first international treaty aimed at combating cybercrime by improving international cooperation
2006	The Nuclear Security Series (NSS) was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States.
17 June 2010	The Stuxnet Worm was a cyber weapon discovered that targeted Iran's nuclear facilities, causing great damage.
December 2014	Korea Hydro and Nuclear Power (KHNP) is South Korea's largest nuclear power operator and was targeted in a cyberattack, exposing sensitive reactor data.
December 2016	The Cloud Hopper Campaign was publicly exposed in 2016–2017, when cybersecurity firms and Western governments released reports attributing the attacks to APT10.

Major countries, organisations and alliances

United States of America

After a suspected joint operation by the U.S. National Security Agency (NSA) and Israel, targeting Iran's uranium enrichment facility, the USA has adopted a range of policies to prevent cyberattacks on its own nuclear facilities. The country is working on ensuring that its failsafe reviews are credible and involve top experts from within and outside of the government to improve national

cybersecurity.[31] In addition, the Cybersecurity and Infrastructure Security Agency (CISA) is being deployed to improve the security of important infrastructure by conducting risk assessments and building resilient programs. The Department of Energy (DOE) has also implemented specialised programs like the Office of Cybersecurity to protect nuclear energy facilities. Additionally, the US is strengthening their cybersecurity by constantly monitoring its network, performing penetration testing and even AI-based threat detection.

Iran

Iran is believed to have strengthened its cyber capabilities in response to Stuxnet. Iranian cyber units, particularly operations linked to the Islamic Revolutionary Guard Corps (IRGC), have developed tools for cyber espionage and sabotage.[32] These capabilities include the manipulation of foreign networks which target important infrastructure of rival states, like the United States and Israel. Additionally, Iran is investing in training cyber personnel and focusing on building new hacking tools as well as using hacker groups to deny access to their domestic nuclear systems.

China

There are accusations that China is using cyber tools to gather intelligence on nuclear technologies. It targets state-linked research and nuclear institutions in various countries through hacking groups, such as Advanced Persistent Threat (APT40 and APT10). One example is the Cloud Hopper Campaign (2016–2018), when the APT10 attempted to gain access to sensitive intellectual and customer data, among them were organisations with sensitive information related to nuclear energy.[33] These groups transform and exploit proof-of-concept(s) (POCs) of new vulnerabilities and immediately use them against target networks.[34] China's aim for military modernisation and enhancement of nuclear capabilities is a valid motive for cyber espionage efforts.

---

[31] NTI. "The Cyber-Nuclear Threat: Explained." *The Nuclear Threat Initiative*, 31 Oct. 2022, www.nti.org/analysis/articles/cyber/.

[32] CARNEGIE MIDDLE EAST CENTER. "Iran's Cyber Threat: Espionage, Sabotage, and Revenge." *Carnegie Endowment for International Peace*, 2018, carnegieendowment.org/research/2018/01/irans-cyber-threat-espionage-sabotage-and-revenge?lang=en¢er=middle-east.

[33] Richmond, Nathaniel . "Operation Cloud Hopper Case Study." *SEI Blog*, 4 Mar. 2019, www.sei.cmu.edu/blog/operation-cloud-hopper-case-study/.

[34] Cybersecurity Infrastructure Security Agency . "People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 8 July 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a.

National Security Agency (NSA)

The National Security Agency (NSA) of the United States is a body operating for the protection of national infrastructure, particularly nuclear facilities, from cyber threats. The Tailored Access Operations (TAO) division was built by the NSA not only to conduct cyberattacks like Stuxnet, but also to develop cybersecurity policies to safeguard national systems. These policies mainly focus on enhancing the function of threat receptors, hence facilitating the detection of intrusions in collaboration with the Department of Energy and the Department of Homeland Security.[35] Such policies also pertain to strengthening encryption standards for domestic nuclear systems. The NSA aims to build a resilient "armour" against cyberattacks and ensure the integrity of the nation's nuclear infrastructure.

Previous attempts to solve the issue

Commercial U.S. nuclear generator using Waterfall Unidirectional Gateways

Air gapping is the physical isolation of computer systems or networks so they can't physically connect to other computer systems or networks.[36] Air gaps were implemented to protect digital assets from potential damage caused by hackers, viruses or natural disasters. Systems that control vital infrastructure, like nuclear power, are protected by multiple air gaps as they entail highly classified information. A commercial nuclear power producer in the USA requested to monitor nuclear control and safety networks. The Waterfall's Unidirectional Solution was to secure the nuclear control system network perimeter from external threats with Unidirectional Security Gateways.[37] The goal was real-time enterprise visibility while eliminating remote attack paths into safety and control systems, providing an "air-gapped" barrier for inbound connectivity. However, it is not foolproof, as insider threats or external infected devices like USB drives can still undermine air-gapping systems, as shown by the Stuxnet attack.

The Nuclear Security Series (NSS) (2006)

[35] U.S. Department of Homeland Security . "DHS and DOE National Laboratories | Homeland Security." *Www.dhs.gov*, www.dhs.gov/science-and-technology/dhs-and-doe-national-laboratories.
[36] IBM. "Air Gap." *Ibm.com*, 10 Oct. 2024, www.ibm.com/think/topics/air-gap.
[37] Waterfall Security Solutions . *Securing the Digital Nuclear Generation Perimeter* . waterfall-security.com/wp-content/uploads/Waterfall-Nuclear-Use-Case.pdf.

The International Atomic Energy Agency (IAEA) provides guidance and assistance to facilitate the development of information security activities in the United States.[38] It aims to enhance or implement new digital security frameworks for nuclear power plants and has, hence, worked with agencies such as the Nuclear Regulatory Commission (NRC) to achieve this. It entails documents like the Nuclear Security Series (NSS), including NSS No. 17, which contains details on computer security at nuclear facilities. The IAEA's Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security.[39] It was created to bring world leaders together to strengthen global nuclear security and prevent nuclear terrorism.

Scorpion Labs Red Teaming and Penetration Testing

Scorpion Labs is K logix's (a people-first cybersecurity company with practice areas in cyber risk consulting, security testing services, cyber research, and technology resale[40]) offensive security team, consisting of security researchers and penetration testers, trying to identify high-impact vulnerabilities in networks.[41] Penetration testing and red team assessments have become the main way of testing the technical infrastructure and security resilience of an organisation.[42] States are constantly hiring ethical hackers to simulate attacks on nuclear facilities to uncover vulnerabilities. It is important for countries to be aware of unknown flaws before real attackers do. Scorpion Labs invests in reconnaissance and enumeration, tailoring every test around the specific applications and embedded systems of the client, rather than applying a one-size-fits-all approach.[43] This focus enables them to identify subtle attack surfaces that are often overlooked. Once vulnerabilities are identified, the team doesn't just list them; instead, they craft tailored exploitation paths to

[38] International Atomic Energy Agency . "Computer and Information Security." *Www.iaea.org*, 8 June 2016, www.iaea.org/topics/computer-and-information-security.
[39] International Atomic Energy Agency. "Nuclear Security Series | IAEA." *Iaea.org*, 7 July 2017, www.iaea.org/resources/nuclear-security-series.
[40] KLogix. "Home." *Klogixsecurity.com*, 2024, www.klogixsecurity.com/.
[41] Klogix. "Penetration Testing." *Klogixsecurity.com*, 2024, www.klogixsecurity.com/scorpion-labs?gad_source=1&gad_campaignid=22375835204&gbraid=0AAAAArA4S-sH7D9kWMa8YZMb0u9TdmFcZ&gclid=CjwKCAjwy7HEBhBJEiwA5hQNojZVO2DJakgNd9gU7HzxcbuFrCMeWFsSw3nvO1mIUVLAeeatIufX4xoCnYQQAvD_BwE.
[42] PricewaterhouseCoopers. "Red Teaming and Penetration Testing - What's the Difference?" *PwC*, www.pwc.com/mt/en/publications/technology/red-teaming-and-penetration-testing.html.
[43] Klogix. "Penetration Testing." *Klogixsecurity.com*, 2024, www.klogixsecurity.com/scorpion-labs?gad_source=1&gad_campaignid=22375835204&gbraid=0AAAAArA4S-sH7D9kWMa8YZMb0u9TdmFcZ&gc

demonstrate the real-world impact. This approach evidences a commitment to showing exactly how an attacker could exploit weaknesses to access or disrupt nuclear systems.

Possible solutions

Cyber Readiness Audits

A key proposal is to incorporate cyber readiness audits into the IAEA's Integrated Regulatory Review Services (IRRS) and allow for evaluations of nuclear facilities' cyber defences. Facilities would be required to conduct regular self-assessments, using standardised checklists aligned with IAEA cybersecurity guidance. This would ensure continuous monitoring of vulnerabilities, staff training and threat response preparedness. To provide objectivity and credibility, nuclear facilities could also be evaluated by independent cybersecurity experts or third-party auditing firms accredited by the IAEA. These external reviewers would conduct penetration testing and red-team simulations to identify weaknesses that might be overlooked internally.

UN-led Cybersecurity Training Programs

A UN-led cybersecurity training program for nuclear facility operators would provide the human resources with the skills to detect, respond and prevent cyber threats. This would minimise the possibility of human error as such initiatives strengthen the human aspect of cyber defence. Such training could include hands-on simulations on how to identify suspicious activity in IT systems and technical skill-building like using live simulation exercises to test response to real-world threat scenarios.

AI Detection Systems

AI could be used to prevent cyberattacks as it detects anomalies in system behaviour and recognises cyber threats from early stages. Artificial Intelligence could swiftly prevent threats like intrusion or sabotage on the grounds that it has the ability to process huge amounts of data in a really short time and immediately recognise patterns that may pose a threat. This data might include traffic logs, authentication records, control system telemetry, and access control logs from employees entering secure zones. AI systems can detect anomalous patterns, for example, unusual login activity that might indicate a cyber intrusion or sabotage attempt. If the AI system does detect such anomalies, it could automatically trigger a rapid response. Hence, such an approach significantly improves

response time. However, reliance on AI introduces new risks that are particularly concerning in the context of nuclear security. For instance, sensitive data fed into AI systems could be exposed or misused if not properly safeguarded and faulty algorithms could lead the system to overreact or underreact.

Information sharing and early warning systems

The International Nuclear and Radiological Event Scale (INES) is a tool used by Member States to rate and communicate events that occur within their territory.[44] It could be proposed to create a secure international platform for real-time sharing of threats in nuclear facilities. Specifically, it would be an early warning mechanism for cyber incidents threatening nuclear infrastructure. Such a mechanism would act as a cyber alarm system, preventing small breaches from escalating into full-scale attacks. With the proper international cooperation, member states can rapidly share information on the threat or attack imposed on their nuclear facility and request assistance.

Bibliography

Anderson, Evan. "What Is Red Teaming?" *IBM*, 13 May 2024, www.ibm.com/thought-leadership/red-teaming.

CAIDA. "The Spread of the Sapphire/Slammer Worm." *CAIDA*, www.caida.org/catalog/papers/2003_sapphire/.

Carnegie Middle East Center. "Iran's Cyber Threat: Espionage, Sabotage, and Revenge." *Carnegie Endowment for International Peace*, 2018, carnegieendowment.org/research/2018/01/irans-cyber-threat-espionage-sabotage-and-revenge?lang=en&region=middle-east.

Conca, James. "How Well Is the Nuclear Industry Protected from Cyber Threats?" *Forbes*, 8 Nov. 2019, www.forbes.com/sites/jamesconca/2019/11/08/how-well-is-the-nuclear-industry-protected-from-cyber-threats.

[44] International Atomic Energy Agency. "International Nuclear and Radiological Event Scale (INES) | IAEA." *Iaea.org*, IAEA, 31 May 2019, www.iaea.org/resources/databases/international-nuclear-and-radiological-event-scale.

Cybersecurity and Infrastructure Security Agency. “People’s Republic of China: Ministry of State Security APT40 Tradecraft in Action.” *CISA*, 8 July 2024, www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a.

Dafny, Nachum. “Pain Principles (Section 2, Chapter 6) Neuroscience Online: An Electronic Textbook for the Neurosciences | Department of Neurobiology and Anatomy - the University of Texas Medical School at Houston.” Tmc.edu, 2019, nba.uth.tmc.edu/neuroscience/m/s2/chapter06.html.

Department of Homeland Security. “DHS and DOE National Laboratories.” *U.S. Department of Homeland Security*, www.dhs.gov/science-and-technology/dhs-and-doe-national-laboratories.

EPA. “Radioactive Decay | US EPA.” *U.S. EPA*, 22 May 2015, www3.epa.gov/radtown/radioactive-decay.html.

EQUIFAX. “How Cyber Attacks Happen | Equifax UK.” *Equifax.co.uk*, www.equifax.co.uk/resources/identity-protection/how-cyber-attacks-happen.html.

FBI. “Terrorism.” *Federal Bureau of Investigation*, 2024, www.fbi.gov/investigate/terrorism.

Federal Bureau of Investigation. “Terrorism.” *FBI*, 2024, www.fbi.gov/investigate/terrorism.

Fortinet. “What Is SCADA and SCADA System?” Fortinet, www.fortinet.com/resources/cyberglossary/scada-and-scada-systems.

IBM. “Cyberattack.” *IBM.com*, 15 Aug. 2021, www.ibm.com/think/topics/cyber-attack.

International Atomic Energy Agency. “Nuclear Security Series | IAEA.” *Iaea.org*, 7 July 2017, www.iaea.org/resources/nuclear-security-series.

International Atomic Energy Agency. “Research Reactors.” *Www.iaea.org*, 13 Apr. 2016, www.iaea.org/topics/research-reactors.

International Atomic Energy Agency. “Security Aspects of Nuclear Facilities | IAEA.” *Iaea.org*, 9 Dec. 2016, www.iaea.org/topics/security-aspects.

Klogix. “Home.” *Klogixsecurity.com*, 2024, www.klogixsecurity.com/.

Klogix. "Penetration Testing." *Klogixsecurity.com*, 2024, www.klogixsecurity.com/scorpion-labs?gad_source=1&gad_campaignid=22375835204&gbraid=0AAAArA4S-sH7D9kWMa8YZMb0u9TdmFcZ&gc.

Knapp, Eric E. *About Industrial Networks*. 1 Jan. 2015, pp. 9–40, doi.org/10.1016/B978-0-12-420114-9.00002-2.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 24 May 2024, spectrum.ieee.org/the-real-story-of-stuxnet.

McCurry, Justin. "South Korean Nuclear Operator Hacked amid Cyber-Attack Fears." *The Guardian*, 23 Dec. 2014, www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack.

National Nuclear Security Administration. "Computer Security of Nuclear Facilities." *U.S. Department of Energy*, www.puba.jaea.go.jp/MTC/MTCD/publications/PDF/Pub1527_web.pdf.

NCC Group. "The Lazarus Group: North Korean Source for Cyber Operations." *NCC Group*, 30 June 2022, www.nccgroup.com/us/the-lazarus-group-north-korean-source-for-cyber-ops-for-10-years.

NI Cyber Security Centre. "How Cyber Attacks Happen." NI Cyber Security Centre, 4 Feb. 2020, www.nicybersecuritycentre.gov.uk/how-cyber-attacks-happen.

NTI. "The Cyber-Nuclear Threat: Explained." *The Nuclear Threat Initiative*, 31 Oct. 2022, www.nti.org/analysis/articles/cyber.

NTI. "Nuclear Materials." *Doe.gov*, 2023, www.directives.doe.gov/terms_definitions/nuclear-materials.

The Nuclear Threat Initiative. "The Nuclear Threat Initiative." *NTI*, 27 Oct. 2022, www.nti.org/wp-content/uploads/2022/10/Failsafe-Factsheet.pdf.

"Threat of the Sapphire/Slammer Worm?" *CAIDA*, www.caida.org/papers/2003_casaphire.

The Guardian. "Stuxnet Worm Heralds New Era of Global Cyberwar." *The Guardian*, 30 Sept. 2010, www.theguardian.com/technology/2010/sep/30/stuxnet-new-era-global-cyberwar.

Treilix. “What Is Stuxnet? | Trellix.” *Www.trellix.com*, 2024, www.trellix.com/security-awareness/ransomware/what-is-stuxnet/.

Trend Micro. “Industrial Control System - Definition - Trend Micro USA.” Trendmicro.com, 2019, www.trendmicro.com/vinfo/us/security/definition/industrial-control-system.

OPSWAT. “How the Energy Industry Can Survive Targeted Attacks.” *OPSWAT Blog*, 31 Mar. 2015, www.opswat.com/blog/how-energy-industry-can-survive-targeted-attacks.

PwC. “Red Teaming and Penetration Testing: What’s the Difference?” *PwC*, www.pwc.com/mt/en/publications/technology/red-teaming.html.

Spindel, Bernard I., and Wade Marcum. “Nuclear Reactor | Definition, History, & Components.” *Encyclopædia Britannica*, 7 Feb. 2018, www.britannica.com/technology/nuclear-reactor.

Stoutland, Page. “Addressing Cyber-Nuclear Security Threats.” *The Nuclear Threat Initiative*, www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats.

U.S. Air Force. “Air & Bomb.” *IBM.com*, 10 Oct. 2022, www.ibm.com/thought-leadership/topics/air-bomb.

Waterfall Security Solutions. *Securing the Digital Nuclear Generation Perimeter*. waterfall-security.com/wp-content/uploads/Waterfall-Nuclear-Use-Case.pdf.