Research Paper

International Law Programme

International Security Programme

July 2024

Cybersecurity of the civil nuclear sector

Threat landscape and international legal protections in peacetime and conflict

Talita Dias, Joyce Hakmeh and Marion Messmer

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Summary

— The expansion in the use of nuclear energy worldwide highlights the need for robust cybersecurity measures to protect civil nuclear infrastructure from cyberthreats. This paper explores the evolving cybersecurity risks that the civil nuclear sector faces both in peacetime and during conflict, and examines which protections international law offers. It also proposes steps – drawing on international law specifically, or involving global and regional cooperation as well as national structures and best practices more generally – for improving the cybersecurity of civil nuclear infrastructure.

— Key cybersecurity vulnerabilities in the civil nuclear sector stem from a range of technical and non-technical factors, including the use of older software, the targeting of personnel by threat actors, and the lack of sufficient sector-wide awareness of – and collaboration on – cybersecurity.

— Existing international law already offers robust safeguards against cyberthreats to civil nuclear infrastructure, though no single legal regime specifically addresses such risks. Whether through general rules or specific legal regimes, international law requires states to refrain from conducting, or to prevent, cyber operations targeting civil nuclear facilities. In addition, it requires states to redress the effects of such incidents when they occur.

— General rules applicable to cyber-nuclear risks and harms include sovereignty, non-intervention, the prohibition on the use of force, and due diligence obligations. International human rights law and international humanitarian law (IHL), along with nuclear-specific treaties, are among the specific legal regimes that protect civil nuclear infrastructure from malicious cyber operations.

— States should consider offering specific interpretations of those rules and regimes for the cyber-nuclear context, as well as adopting additional non-binding norms or standards to complement them. States should also develop strategies to enhance the enforcement of international law in cyberspace, and to ensure accountability for unlawful cyber operations targeting civil nuclear facilities in particular.

— Effective mitigation of cyberthreats to civil nuclear infrastructure, and to critical infrastructure more generally, requires a multi-tiered approach: enhancing international and regional cooperation, refining national cybersecurity frameworks and fostering public–private partnerships. Implementing these strategies will help ensure the safe and secure development of the civil nuclear sector, thereby better supporting nuclear energy's potential to provide societal and environmental gains.

1. Introduction

Many states are becoming more interested in nuclear energy as a means to help achieve environmental goals, economic development and energy security. A declaration by 25 countries – including the US, the UK and Canada – during the COP28 UN Climate Change Conference in December 2023 exemplified this trend, announcing an ambition to triple nuclear energy capacity by 2050 as part of efforts to achieve net zero greenhouse gas emissions and limit global warming.[1]

The commitment emphasized not only the potential role of nuclear energy in supporting sustainable development but also the consequent importance of maintaining safety, sustainability, security and non-proliferation standards in the civil nuclear industry. As growth in the use of nuclear energy would imply that more nuclear power plants will come into operation, considerations of safety and security in the civil nuclear industry – including around cybersecurity, the specific subject of this paper – are likely to become more critical than ever.

Since Russia's full-scale invasion of Ukraine in February 2022, there has been a notable shift in many Western countries' energy security strategies. Global interest in nuclear energy has been reawakened, driven by a desire to reduce dependencies on external suppliers and bolster domestic energy security.[2] Even before the full-scale invasion of Ukraine, expansion of nuclear energy was on the agenda of many developing countries. As of 2021, 28 countries without existing nuclear power plants were actively pursuing plans to incorporate nuclear energy into their energy portfolios.[3] This surge in interest can be attributed in part to nuclear energy's reliability, resilience and low carbon footprint. Nuclear energy's compatibility with renewable energy sources, complementing the role of renewables in reducing carbon emissions, further increases its potential appeal for countries aiming to minimize their carbon footprint and achieve decarbonization goals across various sectors.

However, any expansion of nuclear capabilities also brings new challenges, particularly in cybersecurity. Cyber operations targeting civil nuclear systems have been reported worldwide.[4] Such operations pose significant risks, with potential harms including information theft, equipment malfunction, disruption of energy supplies, environmental damage and health impacts. The risks are prevalent both in peacetime and during conflicts. Of increasing concern is the vulnerability to cyberattacks, as well as physical attacks, of nuclear power plants located in conflict zones. The damage to Ukraine's nuclear infrastructure since 2022

---

1 U.S. Department of Energy (2023), 'At COP28, Countries Launch Declaration to Triple Nuclear Energy Capacity by 2050, Recognizing the Key Role of Nuclear Energy in Reaching Net Zero', 1 December 2023, https://www.energy.gov/articles/cop28-countries-launch-declaration-triple-nuclear-energy-capacity-2050-recognizing-key.
2 See, for example, Department for Energy Security & Net Zero (2024), 'Civil nuclear: roadmap to 2050 (accessible webpage)', policy paper, updated 26 January 2024, https://www.gov.uk/government/publications/civil-nuclear-roadmap-to-2050/civil-nuclear-roadmap-to-2050-accessible-webpage.
3 International Atomic Energy Agency (IAEA) (2021), *International Status and Prospects for Nuclear Power 2021*, Board of Governors General Conference, 16 July 2021, https://www.iaea.org/sites/default/files/gc/gc65-inf6.pdf.
4 See, for example, Trend Micro (2016), 'Malware Discovered in German Nuclear Power Plant', 27 April 2016, https://www.trendmicro.com/vinfo/gb/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant; and Das, D. (2019), 'An Indian nuclear power plant suffered a cyberattack. Here's what you need to know.', *Washington Post*, 4 November 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know.

exemplifies this type of risk.[5] Moreover, as small modular reactors (SMRs) become more widespread in civil nuclear infrastructure, the likelihood of nuclear facilities becoming targets in conflict situations will rise.

Despite these risks, the nuclear sector lacks a comprehensive understanding of the threat landscape around cybersecurity. The sector also lacks effective resilience strategies. While existing international law and norms outline states' obligations and responsibilities in cyberspace, how these obligations and responsibilities apply to civil nuclear infrastructure remains underexplored. Addressing this gap will be crucial to protecting nuclear power plants from cyberthreats, especially as the transition from fossil fuels will potentially result in such plants increasing in both importance and number.

This research paper seeks to contribute to the debate so that robust policies can be developed in this area. Section 2 discusses the threats and risks to civil nuclear infrastructure, particularly from a cybersecurity perspective. Section 3 details the applicable international legal framework that can help protect against them. Section 4 recommends policies and best practice for governments and other relevant stakeholders, with a focus on the role of existing commitments and institutional channels in preventing malicious cyber operations against civil nuclear systems, and in holding to account those responsible for such operations or the threat thereof.

2. Threats and risks to civil nuclear infrastructure

a. General threats and risks

i. Existing cyber vulnerabilities in the civil nuclear sector

This paper builds on previous Chatham House research into the cybersecurity of civil nuclear facilities. The paper draws on an extensive review of existing work in the field, as well as on interviews with a wide range of relevant stakeholders in the cybersecurity and nuclear industries.[6] Three themes emerged from our latest work in this area.

Firstly, it is clear that the nuclear industry was a comparatively late starter in considering cybersecurity, at least relative to other industries associated with critical national infrastructure (CNI) or to commercial sectors such as finance. The nuclear industry's strong pre-existing physical security, and its use of bespoke or uncommon industrial control software, meant that there was a sense within the sector that all aspects of security were sufficiently covered. However, in recent years, as ever more systems in nuclear power plants have acquired digital elements, including commercial off-the-shelf software solutions, more cyber vulnerabilities have been introduced. This has increasingly left systems and facilities open to a potential attack vector that has been insufficiently addressed. In some respects, the civil nuclear industry is thus still playing catch-up. The UK's 2022

5 Hibbs, M. (2022), *Civil Nuclear Energy Risks from Russia's Invasion of Ukraine,* Carnegie Endowment, https://carnegieendowment.org/posts/2022/04/civil-nuclear-energy-risks-from-russias-invasion-of-ukraine?lang=en.
6 Baylon, C. with Brunt, R. and Livingstone, D. (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Report, London: Royal Institute of International Affairs, https://www.chathamhouse.org/archive/cyber-security-civil-nuclear-facilities-understanding-risks.

Civil Nuclear Cyber Security Strategy[7] exemplifies the problem by setting goals that, while sensible, should ideally have been reached several years earlier. Similar shortcomings in national cybersecurity frameworks have been pointed out repeatedly since the mid-2010s by a variety of actors, including the International Atomic Energy Agency (IAEA).

Secondly, due to the specific regulatory environment involved, the nuclear industry is isolated from other industries when it comes to exchange of best practice. This makes learning from best practice on cybersecurity difficult, as pathways to knowledge exchange are ad hoc, often informal, and largely based on the personal drive and networks of individuals in cybersecurity roles. There is also a lack of transparency about cybersecurity incidents, due to concerns both about acknowledging and advertising vulnerabilities, and about how vulnerabilities might be perceived by the public. The nuclear industry's preoccupation with perceptions can get in the way of transparency, even though stronger disclosures would help to bolster confidence in the safety of working practices.

The nuclear industry's preoccupation with perceptions can get in the way of transparency, even though stronger disclosures would help to bolster confidence in the safety of working practices.

Thirdly, governments often have limited ability to enforce cybersecurity standards. In part, this reflects the fact that nuclear energy installations are privately operated in many countries. Efforts to ensure private operators meet cybersecurity standards are often ineffective or inefficient, resulting in delays, slow progress and inconsistencies between operators. While government regulators, such as the Office for Nuclear Regulation (ONR) in the UK, typically conduct regular inspections and can recommend and mandate requirements, the nature of licensing systems for nuclear operators means that long periods of risky working practices are often tolerated, and that government often has limited power to intervene. Even where civil nuclear infrastructure is state-owned, moreover, facilities may operate at arm's length from government.

Some of the challenges in this area were highlighted by the investigation into cybersecurity at the Sellafield nuclear waste site in the UK. Sellafield was repeatedly flagged in ONR inspections for 'enhanced regulatory attention' on cybersecurity practices.[8] ONR then brought criminal charges against the operator Sellafield Limited for having gaps in its cybersecurity from 2019 to 2023, charges to which Sellafield Limited pleaded guilty in June 2024.[9] Concerns about regulators' ability to influence the cybersecurity practices of operators, and about the accessibility

7 Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy (2022), 'Civil nuclear cyber security strategy 2022', policy paper, 13 May 2022, https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022.
8 Office for Nuclear Regulation (ONR) (2023), *Chief Nuclear Inspector's annual report on Great Britain's nuclear industry*, September 2023, p. 17, https://www.onr.org.uk/media/omfesnqv/cni-annual-report-2023.pdf.
9 ONR (2024), 'Sellafield Ltd pleads guilty to cyber security offences', 20 June 2024, https://onr.org.uk/news/all-news/2024/06/sellafield-ltd-pleads-guilty-to-cyber-security-offences.

of best-practice recommendations, are not exclusive to the UK. A review by the George Washington University of cybersecurity practices across a range of nuclear operators in different countries found that 'none of the proposed guidelines have holistically provided detailed security procedures specific to the architecture and working of [nuclear power plants]'.[10] France's nuclear regulator, the Autorité de sûreté nucléaire (ASN), highlighted concerns about EDF's supply-chain management, especially for SMR projects, in a January 2024 press update.[11]

To address some of the challenges outlined above, the IAEA has done important work to standardize and improve cybersecurity guidance across the civil nuclear industry globally.[12] This can help address the fact that some national regulators provide only general cybersecurity guidance that fails to take into account challenges specific to the civil nuclear industry. Cybersecurity challenges require a higher level of attention across all levels of the industry, to ensure gaps in risk mitigation can be closed swiftly. Some of the barriers to achieving this exist globally. They include: 1) a lack of transparency across the industry, with regulators often discussing cybersecurity gaps only with specific operators rather than sharing concerns more widely, and operators reluctant to disclose their own cybersecurity gaps for fear of the impact on trust in their services; 2) the gap between guidance and implementation; 3) differing levels of capacity and investment in cybersecurity from one country to another.[13]

ii. Risks of cybersecurity incidents occurring in civil nuclear infrastructure

Civil nuclear infrastructure is vulnerable to cyber operations due to its high value as a target, and due to features inherent in the information technology required to run and operate facilities.[14] The nuclear sector's designation as critical national infrastructure (CNI) in many countries could encourage cyber operations originating from a range of actors – including both states and non-state groups – and for a range of motives. Such actors could, for instance, include: anti-nuclear-energy hacktivists; cybercriminals looking to blackmail facilities, operators or governments, seeking ransom, or intending to steal confidential information; state actors wanting to target another state's CNI to jeopardize that state's energy security or gain military advantage; or terrorists looking to advance their own agenda.[15]

---

10 Masood, R. (2016), *Assessment of Cyber Security Challenges in Nuclear Power Plants: Security Incidents, Threats, and Initiatives*, Cyber Security and Privacy Research Institute, the George Washington University, 15 August 2016, https://scholar.google.com.au/citations?view_op=view_citation&hl=en&user=4E0WoloAAAAJ&citation_for_view=4E0WoloAAAAJ:UeHWp8X0CEIC.
11 Autorité de sûreté nucléaire (2024), 'ASN's New Year's greetings to the press for 2024: at a time of transition for the fleet of nuclear facilities and nuclear activities, ASN underlines the points requiring particular attention with regard to nuclear safety and radiation protection', press release, 19 February 2024, https://www.french-nuclear-safety.fr/asn-informs/news-releases/asn-s-new-year-s-greetings-to-the-press-for-2024.
12 IAEA (undated), 'Computer and information security', https://www.iaea.org/topics/computer-and-information-security; and IAEA (2023), 'International Conference on Computer Security in the Nuclear World: Security for Safety', 19–23 June 2023, https://www.iaea.org/events/cybercon23.
13 Collett, R. (2021), 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', *Journal of Cyber Policy* 6, No. 3, 2 September 2021, p. 299, doi:10.1080/23738871.2021.1948582.
14 Kulugh, V. E., Mbanaso, U. M. and Chukwudebe, G. (2022), 'Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure', *SN Computer Science* 3, 217, 10 April 2022, https://doi.org/10.1007/s42979-022-01108-x.
15 Brewster, B., Kemp, B., Galehbakhtiari, S. and Akhgar, B. (2015), 'Cybercrime: Attack Motivations and Implications for Big Data and National Security', in Akhgar, B. et al. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies*, Elsevier, pp. 108–27, doi:10.1016/B978-0-12-801967-2.00008-2.

Cyber incidents can also occur accidentally as a result of existing vulnerabilities in commercial software. These vulnerabilities include: entry points such as inadequate IT infrastructure maintenance; missing patches and updates; and unsafe working practices such as connection to unprotected networks, the use of portable storage devices, the use of legacy systems, and inadequate data protection. Crucially, these vulnerabilities can also open a backdoor for targeted cyber operations, providing an attack vector for hostile actors. This range of potential threats makes it doubly essential to ensure *fundamentally* secure working practices, as it is very difficult to identify and protect against every individual vulnerability.[16]

The cyber vulnerabilities of civil nuclear facilities are summarized in Table 1:[17]

Table 1. Key cybersecurity vulnerabilities of civil nuclear facilities

Technical vulnerabilities	• Relying on 'security by obscurity'. This involves assuming that an information and communication technology (ICT) system is distributed at too small a scale to have well-known vulnerabilities that can be exploited. This approach is particularly common in older nuclear power plants with bespoke or rare industrial control systems. • Using software built on insecure foundations and requiring frequent patches or updates. • Relying on software that has reached the end of its supported lifespan and can no longer be updated. • Being insufficiently aware of the risks of data breaches in general management software such as human resources systems; such breaches can expose sensitive data on personnel.
Personnel-related and physical vulnerabilities	• Insider threats, e.g. personnel stealing or leaking information for financial gain or retribution. • Adversaries or criminals targeting power plant personnel either as infiltration vectors or as victims. • Disruption or interception of communications between nuclear power plants, operators and regulators, potentially disrupting the reliability of the energy grid. • Interference (by a cyber operation) with a nuclear power plant's controls, potentially causing physical damage or – in an extreme case – leading to radiation release.
Sector-wide and cultural vulnerabilities	• Insufficient awareness of cybersecurity. • Insufficient numbers of qualified cybersecurity personnel in the nuclear industry. • A general assumption that the nuclear industry 'takes security seriously' and therefore is already covering all bases when it comes to cybersecurity.

A significant limiting factor when assessing past cases of cyber operations targeting nuclear power plants is the lack of publicly available information on such incidents. This can reflect concerns on the part of operators, regulators and governments about the release of sensitive data, and about the potential for revelations of cybersecurity failures to reduce public trust in nuclear energy. However, publicly known past

16 IAEA (2021), *Computer Security Techniques for Nuclear Facilities: Technical Guidance*, IAEA Nuclear Security Series, No. 17-T (Rev. 1), https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities.
17 Baylon with Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities*.

examples of cyber operations against civil nuclear infrastructure cover a range of scenarios. One of the earliest-known incidents was in 2003, when the Slammer worm infiltrated the management and operational information and communication technology (ICT) systems of the Davis-Besse nuclear power plant in the US.[18] Slammer was able to access the power plant's system through an IT consultant's infected device. While this was an accident, it exemplifies how malicious actors could go about engineering an attack.

Two other well-researched examples are the 2010 Stuxnet worm attack in Iran, and the 2014 hack of a South Korean nuclear power operator, Korea Hydro and Nuclear Power Co., Ltd (KHNP). These two examples show the range of harms that cyber operations can cause, from the theft of sensitive data to physical damage. The Stuxnet example was extraordinary in the extent of the damage it caused, whereas the KHNP example is more typical of other cyber operations against nuclear power plants. What both have in common is that the attackers were alleged to be states: Israel and the US in the case of the Stuxnet attack on Iran's nuclear facilities; and North Korea in the case of KHNP.

Stuxnet remains one of the most famous intentional cyber operations targeting nuclear infrastructure. The operation sought to disrupt operations at Iran's Natanz nuclear enrichment facility. Stuxnet was a computer worm targeting supervisory control and data acquisition (SCADA) systems. Once inside the industrial control system, the worm caused the control software to accelerate rotation of the centrifuges to the point of physical damage.[19] This makes it one of the only examples of a cyber operation having caused physical damage.

KHNP, South Korea's state-run nuclear power operator, was targeted in December 2014. In this cyber operation, sensitive information was stolen, including blueprints for reactors, electrical flow charts and personal details of employees. One of the hackers' goals was to undermine public trust in the safety of the nuclear power plant.[20] But the South Korean government said that the hackers had not managed to access any control systems.[21]

iii. Impact of cyber operations

As the Stuxnet episode shows, cyber operations have the potential to cause tangible damage to physical assets.[22] The impact of a cyber operation targeting civil nuclear infrastructure can be as wide-ranging as the theft of sensitive information, the loss of access to or control over monitoring and control software, operating difficulties, or – in the worst-case scenarios – reactor shutdown or difficulties controlling nuclear storage, for example through loss of access to external power sources for cooling.[23]

---

18 Kesler, B. (2011), 'The Vulnerability of Nuclear Facilities to Cyber Attack', *Strategic Insights*, Volume 10, Issue 1, Spring 2011, Center on Contemporary Conflict, Department of National Security Affairs, Naval Postgraduate School in Monterey, California, https://apps.dtic.mil/sti/tr/pdf/ADA541955.pdf.
19 Denning, D. E. (2012), 'Stuxnet: What Has Changed?', *Future Internet* 4, No. 3, 16 July 2012, p. 673, doi:10.3390/fi4030672.
20 Lee, S. (Helen) (2024), 'Revisiting the 2014 Korea Hydro and Nuclear Power Hack: Lessons Learned for South Korean Cybersecurity, *38 North*, Stimson Center, 22 March 2024, https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity.
21 Cho, H. S. and Woo, T. H. (2017), 'Cyber Security in Nuclear Industry – Analytic Study from the Terror Incident in Nuclear Power Plants (NPPs)', *Annals of Nuclear Energy* 99, p. 862, doi:10.1016/j.anucene.2016.09.024.
22 Denning (2012), 'Stuxnet: What Has Changed?'.
23 Cho and Tae (2017), 'Cyber Security in Nuclear Industry – Analytic Study from the Terror Incident in Nuclear Power Plants (NPPs)', pp. 863–68.

There is only a small possibility that a cyber operation would cause loss of control over a nuclear reactor to the point of meltdown or a significant release of radiation. This is because nuclear power plants have other redundant safety features such as back-ups for cooling.[24] However, the potential impacts if a meltdown or major radiation release did occur could be very significant, including deaths or long-term health problems among nuclear power plant workers or members of the public exposed to radiation, as well as long-term environmental damage and contamination.

A cyber operation targeting a nuclear facility also has the potential to disrupt the electric grid. States that have nuclear power plants often rely on nuclear power to provide a reliable baseload of energy to their electric grid. This dependency is increasing as countries transition away from fossil fuels. A stable baseload is required for a steady availability of energy throughout the day. However, not all types of energy generation offer a uniform power supply over the course of a day. Solar and wind power rely on certain environmental conditions for optimal performance. On a rainy or windless day, for example, other forms of energy generation must make up for the lack of solar- or wind-generated power. Nuclear energy, in contrast, can always generate power. If an electric grid became unreliable because nuclear power was unable for some reason to provide a reliable baseload – for example, as a result of a cyber operation – this could disrupt many aspects of daily life. Affected areas could include economic activity, the functioning of government, transport links, healthcare facilities and other critical public services. This in turn could cause elevated levels of distress in the population, and even excess deaths if healthcare functions were compromised.[25] Given that many countries are considering nuclear energy due to increasing energy demand and a desire to transition away from fossil fuels, it is now all the more critical to ensure that new nuclear power plants and new reactor types are designed with cybersecurity in mind.

iv. Changing risks through changes in technology

The following section explores two emerging technological developments and their impacts on the risk landscape for civil nuclear infrastructure. The first is the evolution of nuclear reactor technologies themselves, as well as their increased distribution through the advent of small modular reactors (SMRs) and microreactors. The second is the rise of artificial intelligence (AI), in terms of both its increasing capabilities and widening usage. AI could lower the barrier to malicious cyber operations by making tools for cyber intrusions more accessible and affordable for a wider range of actors, including potential hackers or cybercriminals.[26]

The development of SMRs and microreactors provides an opportunity to increase energy security in areas where a traditional, larger nuclear power plant might be too difficult or expensive to build. In comparison to traditional nuclear infrastructure, which tends to take decades to plan and build, SMRs or microreactors could be deployed more quickly in areas where there is a significant energy

24 World Nuclear Association (2022), 'Safety of Nuclear Power Reactors', updated 2 March 2022, https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.
25 Agrafiotis, I. et al. (2018), 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* 4, No. 1, 1 January 2018, doi:10.1093/cybsec/tyy006.
26 National Cyber Security Centre (2024), 'The near-term impact of AI on the cyber threat', 24 January 2024, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

need. Some SMRs are designed to be transported or deployed offshore, making them potentially more versatile than traditional nuclear power plants. The IAEA is aware of over 80 different SMR designs and concepts that are at different stages of development and implementation. As of early 2024, five SMR designs were under construction or operating.[27]

The operating and monitoring software used in SMRs and microreactors will be less bespoke than in some older models of nuclear power plant. Indeed, one of the selling points of the newer designs is that SMRs and microreactors are easier to run, given that staff are more likely to be familiar with the operating software. Likewise, one of the purported advantages of SMRs and microreactors is that it is possible to control several reactors remotely at the same time. In some cases, SMRs and microreactors are intended to be operated fully remotely, without any staff on site. This increases the requirements for software solutions that are cloud-based or connected to the internet.

Cybersecurity is typically a consideration in the design of newer reactors in a way that has not been the case with traditional nuclear power plants, as older plants were developed at a time when cybersecurity standards did not yet exist or were just emerging.

The risk landscape around such designs is mixed. On the one hand, newer reactors are designed to be fundamentally safer and more secure from a cybersecurity point of view. Cybersecurity is typically a consideration in their design in a way that has not been the case with traditional nuclear power plants, as older plants were developed at a time when cybersecurity standards did not yet exist or were just emerging. In this way, some vulnerabilities might be removed at the design stage by drawing on cybersecurity best practice.

On the other hand, the fact that SMRs are less bespoke than many more traditional reactor designs, and in many cases are connected to the internet, makes them more likely to have cyber vulnerabilities. In turn, this makes newer reactors more of a target for opportunistic cybercriminals. Security solutions such as 'air gapping' (which means not connecting critical parts of the control system to the internet) are often not possible in such cases due to the requirement for remote access.

In addition, increased deployment of SMRs and microreactors could create novel risks. First, if there are more reactors overall, the risk of any one reactor falling victim to a cyber operation increases. Another risk stems from the construction supply chain. Many companies are likely to be involved in the production of parts for these reactors. It is unclear whether such parts will consistently be designed

27 OECD Nuclear Energy Agency (2024), *The NEA Small Modular Reactor Dashboard: Second Edition*, p. 13, March 2024, https://www.oecd-nea.org/jcms/pl_90816/the-nea-small-modular-reactor-dashboard-second-edition; IAEA (undated), 'Small modular reactors', https://www.iaea.org/topics/small-modular-reactors.

with cybersecurity principles in mind. Therefore, the security of the supply chain could become very difficult to guarantee in its entirety.[28] The IAEA is working with SMR designers to ensure that all new designs meet stringent safety standards for reactor and fissile-material safety. But ensuring the cybersecurity of the supply chain for SMRs and microreactors could present additional challenges, because a wide range of hardware manufacturers and software developers might all be suppliers for the same SMR or microreactor project. This highlights how important – and difficult – it will be for manufacturers to audit and monitor their supply chains for cybersecurity.

In addition to these inherent risks, it is envisaged that many SMRs and microreactors will be deployed in countries that may have lower cybersecurity capacity to begin with.[29] Such countries might struggle to ensure the additional cybersecurity requirements of nuclear reactors. The IAEA provides guidance on how to ensure a high standard of cybersecurity for nuclear reactors. However, as implementation is down to national governments, standards can vary according to the awareness and capacity of each government or operator.

As mentioned, adding to the civil nuclear industry's risk of exposure to malicious cyber operations is the fact that hacking is arguably getting easier. Hacking tools are more widely available, and the emergence of AI-assisted programming tools may lower the barrier to entry for cybercriminals. Vulnerable sectors such as CNI could thus be targeted by a wider range of criminals who previously may not have been able to use cyber tools.[30]

b. Specific threats and risks in conflict

Russia's seizure of the Zaporizhzhia nuclear power plant in Ukraine, combined with the fighting that has gone on around the plant, has increased international awareness of the security risks that can arise when civil nuclear infrastructure is caught up in conflict. While nuclear power plants and other civil nuclear facilities are not specifically designed to operate in war zones, such facilities have several layers of physical safety built in to protect reactors and hazardous materials from kinetic threats.[31] However, the combination of physical and cyber operations increasingly seen in modern warfare creates a new type of threat – one potentially able to overwhelm a limited operating staff, or to create a diversion enabling unauthorized access to nuclear materials.

This vulnerability could be exploited by combatants, or by a non-combatant criminal group that might be interested, for example, in stealing fissile materials or sensitive information about a nuclear facility. The IAEA has identified 'insider threats' as one particular vector through which cyber operations against nuclear

28 IAEA (2022), *Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain*, https://www.iaea.org/publications/15259/computer-security-approaches-to-reduce-cyber-risks-in-the-nuclear-supply-chain.
29 Collett (2021), 'Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures', pp. 303–05.
30 National Cyber Security Centre (2024), 'The near-term impact of AI on the cyber threat'.
31 Dolzikova, D. (2023), 'Degradation Everywhere: The Long-Term Risks at Ukraine's Zaporizhzhia Plant', Royal United Services Institute for Defence and Security Studies, 18 September 2023, https://www.rusi.org/explore-our-research/publications/commentary/degradation-everywhere-long-term-risks-ukraines-zaporizhzhia-plant.

power plants could be facilitated.[32] The reduction in staff numbers at Zaporizhzhia, combined with the chaos of the Russian occupation, could increase the likelihood of unauthorized actors gaining access to the site. Among other things, it is difficult for a smaller staff to keep track of the comings and goings of visitors to a nuclear facility.

While the situation at the Zaporizhzhia plant is unusual, this is not the first time that a nuclear reactor has been caught up in the middle of a war. The Vinca research reactor in Serbia was a source of much concern during the Yugoslav Wars (1991–2001). Research staff at the Vinca Institute for Nuclear Science requested IAEA support in 1995, as they feared that highly enriched uranium fuel at the facility could be stolen amid high levels of political unrest in the country. The IAEA carried out several inspections between 1995 and 1999 to ensure the safety of the facility and assist staff.[33] If nuclear reactors become more widespread in the future, for example due to the use of SMRs and microreactors, the risk of reactors being caught up in conflict will increase.[34]

3. Legal protections for civil nuclear infrastructure

The IAEA and other stakeholders, such as the Nuclear Threat Initiative (NTI) and Chatham House, have issued comprehensive guidance on how to enhance the cybersecurity of nuclear facilities at the national and international levels.[35] Some states have also enacted domestic regulations to address cyber-nuclear risks in line with this guidance.[36] Yet little work has been done to assess the rules of international law that apply to the protection of civil nuclear infrastructure from malicious cyber operations.

States have agreed that international law continues to apply in cyberspace, just as it applies to other technologies.[37] This means that international law also applies to the cybersecurity of the civil nuclear sector and other critical infrastructure, including healthcare facilities, public transport, financial networks, and water

---

32 IAEA (2021), *Computer Security Techniques for Nuclear Facilities: Technical Guidance*, IAEA Nuclear Security Series, No. 17-T (Rev. 1).
33 World Nuclear Association (2022), 'Security of Nuclear Facilities and Material', 12 March 2022, https://world-nuclear.org/information-library/safety-and-security/security/security-of-nuclear-facilities-and-material.aspx.
34 Chatham House (2023), 'Ten conflicts to watch in 2023', 11 January 2023, https://www.chathamhouse.org/events/all/members-event/ten-conflicts-watch-2023.
35 See IAEA (undated), 'Computer and information security', https://www.iaea.org/topics/computer-and-information-security; Van Dine, A., Assante, M. and Stoutland, P. (2016), *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities,* NTI, 7 December 2016, https://www.nti.org/analysis/articles/outpacing-cyber-threats-priorities-cybersecurity-nuclear-facilities; Baylon with Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities*.
36 IAEA (2011), *Computer Security at Nuclear Facilities: Technical Guidance Reference Manual*, IAEA Nuclear Security Series No. 17, pp. 1, 9, https://www-pub.iaea.org/mtcd/publications/pdf/pub1527_web.pdf.
37 OEWG Open-ended Working Group on security of and in the use of information and communications technologies (2021), *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Annex I, Final Substantive Report*, UNGA Resolution 75/816 (18 March 2021), para 7; UNGA Resolution 266 (2 January 2019), preambular para 12; UNGA Resolution 70/237 (30 December 2015), para 1. See also Akande, D., Coco, A. and de Souza Dias, T. (2022), 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies', 99 *International Law Studies* 4.

and sanitation systems.[38] The rules of international law are also mirrored in several norms of responsible state behaviour in the use of ICTs. These norms were developed by the UN Group of Governmental Experts (GGE) in 2015, and reaffirmed by all UN member states in 2021.[39] Although the norms are not legally binding, they reflect 'the expectations and standards of the international community regarding the behaviour of States in their use of ICTs'.[40] International law, on the other hand, is binding on states through various sources, including treaties (i.e., agreements concluded between states governed by international law) or customary international law (i.e., unwritten rules that are formed through general state practice accepted as law).[41]

No specific international legal regime protects the civil nuclear sector from cyber operations or other cybersecurity risks. Nonetheless, several rules of international law – whether general or specific in nature – apply to the issue, both in peacetime and during armed conflict.

No specific international legal regime protects the civil nuclear sector from cyber operations or other cybersecurity risks. Nonetheless, several rules of international law – whether general or specific in nature – apply to the issue, both in peacetime and during armed conflict. The purpose of this section is to lay out some of those rules, outlining the nature and level of protection they afford to civil nuclear infrastructure against the different cyberthreats discussed in the previous section. This section focuses on general rules of international law, such as sovereignty and non-intervention, as well as on some specific legal regimes, such as international human rights law and international humanitarian law (IHL). However, other rules and regimes not dealt with here for reasons of space might also apply to different aspects of the protection of civil nuclear infrastructure from cyber operations. Examples include international criminal law and disaster relief laws.

It is also important to note that most rules of international law, including some of those discussed here, are primarily binding on *states*. Therefore, any violation of such rules depends on the relevant conduct – an act or omission – being attributable to a state.[42] Acts of private entities, however, are fairly common in the cyber context. Such acts may be attributed to a state insofar as the private entity concerned is, for example, under the complete dependence, direction or effective control of the state in question.[43]

---

38 OEWG (2012), *Final Substantive Report*, paras 19, 31.
39 GGE (2015), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, para 13; OEWG (2021), *Final Substantive Report*, para 24.
40 OEWG (2021), *Final Substantive Report*, para 24.
41 Article 38(1)(a)-(b), Statute of the International Court of Justice, 18 April 1946.
42 International Law Commission (ILC), Articles on State Responsibility, UNGA Res 56/83 (2001), Articles 5–11.
43 Ibid., Articles 5 and 8 and *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua/United States of America)*, Merits, Judgment, ICJ Rep 1986, p. 14 ('*Nicaragua*'), paras 110 and 115.

a. General protections under international law

i. Sovereignty

There is some controversy over whether sovereignty is just a guiding principle or a binding rule of customary international law.[44] However, the latter view is more widely accepted.[45] Assuming that sovereignty is indeed a binding rule, it stipulates that states have sovereign rights over their territories, property and population, as well as an obligation not to interfere in the sovereign prerogatives of other states.[46] This rule might be breached by physical incursions into another state's territory, and arguably by remote activity that interferes with or usurps another state's inherently governmental functions.[47] This means that when a state carries out a cyber operation that causes physical harm – or, in some instances, loss of functionality of ICT equipment or infrastructure – in another state's territory, such action could amount to a violation of sovereignty.[48] This notably includes instances where a cyber operation results in the need to repair or replace physical components of the targeted infrastructure.[49] For example, a cyber operation that permanently or temporarily disables nuclear centrifuges or temperature sensors used for cooling nuclear reactors would likely violate the affected state's sovereignty.

There are different views on whether cyber espionage *per se* is lawful under international law.[50] But there is some agreement that, depending on the methods used, an intelligence operation could amount to a violation of a state's sovereignty or other rules of international law.[51] This means that the mere fact that an operation had a surveillance purpose would not preclude it from being internationally wrongful.

---

44 Cyber Law Toolkit (undated), 'Sovereignty,' https://cyberlaw.ccdcoe.org/wiki/Sovereignty; Moynihan, H. (2019), *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Research Paper, London: Royal Institute of International Affairs, paras 20–21, 46–54, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.
45 See, for example, Schmitt, M. N. (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, Rule 4; and African Union (2024), 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace', PSC/PR/COMM.1196, paras 12–19. For a contrary view, see Braverman, S. (2022), 'International Law in Future Frontiers', speech at Chatham House, 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers; Ney, P. C. (2020), 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference', U.S. Department of Defense, 2 March 2020, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.
46 *Island of Palmas Case (or Miangas), United States v Netherlands*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), 839; *S.S. 'Lotus', France v Turkey*, Judgment, Judgment No 9, PCIJ Series A No 10 (1927), 18–19; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 2.
47 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 4, paras 6, 10.
48 Ibid., Rule 4, paras 11–13.
49 Ibid., Rule 4, para 13. See, for example, Republic of Costa Rica, Ministerio de Relaciones Exteriores y Culto (2023), 'Costa Rica's Position on the Application of International Law in Cyberspace', para 20, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.
50 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 4, paras 7–9; Cyber Law Toolkit (undated), 'Peacetime cyber espionage', https://cyberlaw.ccdcoe.org/wiki/Peacetime_cyber_espionage.
51 Oxford Institute for Ethics, Law and Armed Conflict (2022), 'Virtual Workshop: The Protection of IT Supply Chains under International Law, Executive Summary & Key Takeaways', in *The Oxford Process on International Law Protections in Cyberspace: A Compendium*, p. 280, para 2, https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf; Coco, A., Dias, T. and van Benthem, T. (2022), 'Illegal: The SolarWinds Hack under International Law', 33 *European Journal of International Law* 1275, p. 1278; Republic of Costa Rica (2023), pp. 6–7; Austria (2024), 'Position Paper of the Republic of Austria: Cyber Activities and International Law', pp. 4–5, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf.

In the civil nuclear sector, cyber operations affecting the confidentiality, integrity or availability of data can seriously disrupt critical services, including the provision of energy and medical treatments using radiological materials. Such operations could, therefore, violate the sovereignty of targeted states.[52]

ii. Non-intervention

A corollary of state sovereignty is the prohibition of intervention: states must not interfere in the internal or external affairs of other states by coercive means. A state's internal or external affairs include the choice of its political, economic, social and cultural systems, its foreign policy, and other matters on which it can freely decide.[53] The principle of non-intervention is well grounded in customary international law and applies in the cyber context.[54]

There is no question that choices relating to nuclear or energy policy are a state prerogative and, as such, part of a state's internal or external affairs. Accordingly, a cyber operation such as a distributed-denial-of-service attack or a ransomware attack directly damaging or disrupting a civil nuclear facility could easily be construed as coercive even if the targeted facility were operated by a private company. This would be the case, for example, if such an operation sought to curtail – or in effect curtailed – the targeted state's ability to determine how best to use its nuclear resources.[55] Certain information operations affecting the civil nuclear sector may also be coercive; these may include threats to attack civil nuclear facilities, and disinformation about radiation levels or the safety of nuclear energy more generally.

iii. Non-use of force

Under Article 2(4) of the UN Charter[56] and customary international law, states must refrain from the threat or use of force against the territorial integrity or political independence of any state.[57] Uses of force that rise to the level of an armed attack trigger the right to individual and collective self-defence, as recognized in Article 51 of the UN Charter and customary international law.[58] Both the prohibition on the use of force and the right to self-defence apply in cyberspace.[59] This means that cyber operations that, by their scale and effects, are akin to a kinetic use of force or that amount to a threat to use force would violate the prohibition.[60] Examples include cyber operations causing or expected to cause death, injury or physical damage in the territory of another state, as was arguably the case

---

52 IAEA (2011), *Computer Security at Nuclear Facilities*, pp. 42–45.
53 *Nicaragua* (1986), para 205. See also *Case Concerning Armed Activities in the Territory of the Congo* (*Democratic Republic of Congo v Uganda*) Judgment, ICJ Rep 2005, p. 168, paras 162–64; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 66, paras 6–8.
54 Cyber Law Toolkit (undated), 'Prohibition of intervention', https://cyberlaw.ccdcoe.org/wiki/Prohibition_of_intervention; Moynihan (2019), *The Application of International Law to State Cyberattacks*, paras 77–113.
55 On the question of whether coercion must actually occur or may be simply attempted, see Hollis, D. B. (2022), 'From Corollaries to Contents? Elaborating the Principle of Non-Intervention in Cyberspace', in Delarue, F. and Gery, A. (eds), *International Law and Cybersecurity Governance*, EU Cyber Direct, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/fQBr45KY/international-law-and-cybersecurity-governance.pdf.
56 Charter of the United Nations (1945), 1 UNTS XVI.
57 Dörr, O. (2019), 'Use of Force, Prohibition of', *Max Planck Encyclopedia of Public International Law*, para 1, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e427.
58 Ibid., para 40. For a contrary view, arguing that any use of force triggers the right to self-defence, see, for example, Koh, H. (2012), 'International Law in Cyberspace', 54 *Harvard International Law Journal* 1, 7.
59 OEWG (2023), *Draft Annual Progress Report*, A/AC.292/2023/CRP.1, para 30(c).
60 Roscini, M. (2014), *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, pp. 46–47; Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 69.

with the Stuxnet worm in 2010.[61] In the same vein, cyber operations of a higher intensity that are comparable to a conventional armed attack would trigger the right to individual and collective self-defence.[62] Cyber operations causing *significant* loss of life or damage to or destruction of property could qualify as armed attacks.[63]

Some states have specifically indicated in their national positions on international law in cyberspace that cyber operations targeting civil nuclear infrastructure, especially nuclear plants or reactors, could amount to a prohibited use of force or an armed attack.[64] They have pointed to a nuclear plant meltdown, disruption to a nuclear reactor's cooling process, and the ensuing widespread loss of life or damage as potential consequences of such cyber operations.

iv. Due diligence obligations

Another important corollary of state sovereignty is the obligation, incumbent on each and every state, 'not to allow knowingly its territory to be used for acts contrary to the rights of other States' – this is known as the Corfu Channel principle.[65] A related obligation is the no-harm principle, which requires states to 'take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof'.[66] Both are so-called 'obligations of due diligence', grounded in customary international law. They require states to behave responsibly with a view to preventing, stopping or redressing certain harms, irrespective of who or what is the source of harm – whether a state, a non-state actor or an accident.[67] The higher the degree of harm or risk of harm, the greater the degree of care required from states.[68] Where there is a risk of serious or irreversible environmental damage – as with the release of radiation – the precautionary principle comes into play, encouraging states to take preventive measures even in the face of scientific uncertainty.[69]

There has been some debate as to whether these due diligence obligations apply in cyberspace. Part of the controversy comes from the fact that the GGE has recognized that states 'should not knowingly allow their territory to be used for internationally wrongful acts using ICTs' as a non-binding norm of responsible state behaviour in cyberspace.[70] That said, the GGE also made clear in its report that 'norms do not seek to limit or prohibit action that is otherwise consistent

---

61 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 71, para 10.
62 Ibid., Rule 71.
63 Ibid., Rule 71, para 8.
64 Koh, H. H. (2012), 'International Law in Cyberspace', U.S. Department of State, 18 September 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm; Wright, J. (2018), 'Cyber and International Law in the 21st Century', speech, Attorney General's Office and The Rt Hon Sir Jeremy Wright KC MP, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Federal Department of Foreign Affairs (2021), 'Switzerland's position paper on the application of international law in cyberspace', p. 4, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf; Department of the Prime Minister and Cabinet, New Zealand (2020), 'The Application of International Law to State Activity in Cyberspace', para 8, https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.
65 *Corfu Channel Case (United Kingdom v Albania)*, Merits, Judgment, ICJ Rep 1949, p. 4 at 22.
66 ILC (2001), 'Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries', A/56/10, Article 3.
67 Coco, A. and de Souza Dias, T. (2021), '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', 32 *European Journal of International Law*, pp. 771, 775, 783–94.
68 ILC (2001), 'Draft articles on Prevention', Article 3, para 18.
69 Ibid., Article 5, paras 5–7; Rio Declaration on Environment and Development, 31 ILM 874 (1992), Principle 15.
70 GGE (2015), *Report*, para 13(c).

with international law'.[71] This suggests that the non-binding 'norm' framing cannot deprive a certain rule of its pre-existing international legal status.[72] Thus, due diligence obligations arguably apply in the cyber context, given their wide scope and general applicability across all areas of state activity.[73]

In cyberspace, compliance with those obligations means that states must do what they can to prevent, stop or redress known or foreseeable cyber operations that could contravene the rights of another state or cause significant harm in another state. There is little doubt that such harm includes *physical* damage such as loss of life, injury, or damage to property or the environment.[74] These are all possible consequences of cyber operations targeting a civil nuclear facility's industrial control systems.

Several measures could fulfil due diligence obligations in the civil nuclear sector. Of particular importance are the computer security measures recommended by the IAEA, which include: nuclear and computer security laws, regulations and policies; risk assessment and management; incident detection and response; control of access to nuclear facilities and their systems; network security; patch management; encryption; security audits and assessment; information sharing; incident response and reporting; training and awareness; capacity-building; and international cooperation.[75]

b. Specific legal regimes

i. International human rights law

International human rights law is made up of human rights treaties as well as customary international law. These give rise to obligations a) to respect or refrain from interfering with human rights, b) to protect those rights, i.e. to take positive steps to prevent or redress human rights violations, and c) to ensure the full and progressive realization of those rights.[76] There is no question that human rights apply online as they do offline,[77] subject to jurisdictional requirements.[78] Several human rights are implicated by cyber-nuclear risks, but the most prominent are the rights to life, health and privacy, and the freedoms of information and expression.

---

71 Ibid., para 10.
72 Cyber Law Toolkit (undated), 'Due diligence', https://cyberlaw.ccdcoe.org/wiki/Due_diligence; *Tallinn Manual* (2017), Rule 6, para 3.
73 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 6, para 4; Coco and de Souza Dias (2021), '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', pp. 778–83.
74 Coco and de Souza Dias (2021), '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', pp. 785, 791–92.
75 IAEA (2021), *Computer Security for Nuclear Security: Implementing Guide*, IAEA Nuclear Security Series No. 42-G, https://www-pub.iaea.org/MTCD/publications/PDF/PUB1918_web.pdf.
76 Human Rights Committee (2004), *General Comment No. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, paras 6–8.
77 UN General Assembly (2013), *Resolution adopted by the General Assembly on 18 December 2013, The right to privacy in the digital age*, A/68/167, para 3; GGE (2015), *Report*, para 28(b).
78 An example of a jurisdictional clause is Article 2(1), International Covenant on Civil and Political Rights (1966) 999 UNTS 171 (ICCPR). Different views exist on the meaning of human rights jurisdiction. See, for example, UN Human Rights Committee (2005), *Consideration of Reports Submitted by State Parties Under Article 40 of the Covenant, Third Periodic Reports of States Parties Due in 2003: United States of America*, Annex I, UN Doc CCPR/C/USA/3, pp. 109–10; European Court of Human Rights (1995), *Loizidou v. Turkey*, App. no. 15318/89, paras 59–64; UN Human Rights Committee (2019), *General comment No. 36 – Article 6: right to life*, CCPR/C/GC/36, para 63.

As noted earlier, cyber operations targeting industrial control systems at civil nuclear facilities can lead to equipment malfunction and the release of ionizing radiation. Radiological release, even if unlikely, can cause death or serious illness in human beings and damage to the environment, which are harms that might breach the rights to life and health.[79] The same conclusion applies to cyber operations that manipulate, corrupt or block the transmission of data from sensors in nuclear equipment, where correct measurements are essential to the equipment's proper functioning.[80] Cyber operations can also disrupt energy supply, in turn affecting the health and well-being of an entire population.[81] Moreover, cyber operations targeting health facilities where radioactive materials are used, such as in X-ray machines and radiotherapy centres, can directly interfere with the delivery of essential medical treatment.

Cyber operations targeting civil nuclear infrastructure can also affect the privacy of individuals, particularly the staff of nuclear facilities.[82] This is especially the case with electronic surveillance operations targeting personal data held by civil nuclear facilities. Another example would be spear-phishing campaigns targeting staff to gain access to those facilities.[83] Cyber operations against the civil nuclear sector can also have a psychological impact. Concerns such as the reasonable fear of radiation release may affect the mental well-being of individuals, thus breaching the rights to health and privacy.

Information operations involving the civil nuclear sector can also interfere with the right to freedom of expression and information – the right of individuals to freely seek, receive and impart information and ideas of all kinds, regardless of frontiers.[84] In particular, this right requires states to refrain from disseminating false or misleading information, and to promote the dissemination of truthful information, online and offline.[85]

ii. International humanitarian law

International humanitarian law (IHL) is grounded in treaties and customary international law. It applies during international or non-international armed conflict to govern the deployment of all kinds of weapons and military operations, which would logically include any involving ICTs.[86] IHL prohibits attacks against civilian objects, including civil nuclear facilities and arguably civilian data stored therein.[87] Cyber operations 'reasonably expected to cause injury or death to persons

---

79 UN Human Rights Committee (2019), *General Comment 36*, para 27; Article 12(1), International Covenant on Economic, Social and Cultural Rights (1976) 993 UNTS 3 (ICESCR); Committee on Economic, Social and Cultural Rights (CECSR) (2000), *General Comment No. 14: The right to the highest attainable standard of health*, E/C.12/2000/4, paras 1, 4, 15, 17.
80 IAEA (2011), *Computer Security at Nuclear Facilities*, pp. 44 and 55.
81 Article 12(1)(b), ICESCR; CECSR (2000), General Comment 14, paras 4, 11 and 15.
82 Article 17, ICCPR.
83 See IAEA (2011), *Computer Security at Nuclear Facilities*, pp. 56–57; Van Dine, Assante and Stoutland (2016), *Outpacing Cyber Threats*, pp. 10, 23, 25, 27, 31–32; Pearson, J. and Bing, C. (2023), 'Exclusive: Russian hackers targeted U.S. nuclear scientists', Reuters, 6 January 2023, https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06.
84 Article 19(2), ICCPR.
85 UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information (2017), 'Joint Declaration on Freedom of Expression And "Fake News", Disinformation and Propaganda', 3 March 2017, para 2(c)-(d), https://www.osce.org/files/f/documents/6/8/302796.pdf.
86 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] ICJ Rep 226, para 226.
87 Rule 1, ICRC Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule1.

or physical damage or destruction to objects by means or effects' constitute an attack for the purposes of IHL.[88] As noted earlier, this is arguably the case with cyber operations targeting industrial control systems at civil nuclear facilities. In the view of the International Committee of the Red Cross (ICRC), cyber operations designed to disable or render dysfunctional a computer or a computer network and that significantly disrupt essential services may also constitute an attack under IHL, even if no physical damage ensues.[89] This could include cyber operations against a variety of systems used by nuclear power plants – including those other than industrial control systems, such as databases and commercial networks – where such operations significantly disrupt the provision of nuclear energy.

Under Additional Protocol I to the Geneva Conventions, and arguably under customary international law as well, particular care must be taken in the case of installations containing dangerous forces, including nuclear electrical generating stations, to prevent such forces from being released and severe losses from occurring among the civilian population.

The principle of precaution requires parties to an armed conflict to take constant care to spare civilians and civilian objects during any military operation.[90] Under Additional Protocol I to the Geneva Conventions, and arguably under customary international law as well, particular care must be taken in the case of installations containing dangerous forces, including nuclear electrical generating stations, to prevent such forces from being released and severe losses from occurring among the civilian population.[91] The principle of proportionality also stipulates that the expected incidental harm against civilians and civilian objects must not be greater than the concrete military advantage anticipated from an attack.[92] Given the potentially catastrophic effects of cyber operations against civil nuclear infrastructure, it is hard to see how the incidental harms could be proportionate in such cases.[93]

---

88 Schmitt (ed.) (2017), *Tallinn Manual 2.0*, Rule 92, para 2.
89 ICRC (2020), 'ICRC Position Paper: International humanitarian law and cyber operations during armed conflicts', March 2020, https://international-review.icrc.org/articles/ihl-and-cyber-operations-during-armed-conflicts-913.
90 Rule 15, ICRC Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule15.
91 Article 56, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 UNTS 3, 8 June 1977. See also Rule 42, ICRC Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule42.
92 Rule 14, ICRC Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14.
93 Similarly, Aikman, I. (2024), 'Ukraine war: UN body urges restraint after Zaporizhzhia nuclear plant hit', BBC News, 8 April 2024, citing IAEA head Rafael Grossi, https://www.bbc.co.uk/news/world-europe-68757082.

For example, in 2017, during the armed conflict in eastern Ukraine, a cyber operation hit the Chernobyl power plant, crippling its radiation-monitoring system.[94] This system is vital to maintaining the safety of civilians on the site and in areas around it. Thus, the cyber operation likely amounted to an armed attack under IHL, and its risks likely outweighed any military advantage sought. Similarly, as discussed earlier, the effects of a cyber or hybrid attack against the Zaporizhzhia nuclear power plant could include not only the disruption of power supply to civilians in Ukraine but also the release of radiation. Therefore, such an attack would likely be disproportionate.

To bolster the implementation of IHL at the national level, states should consider including specific sections on how IHL applies to cyber operations against civil nuclear infrastructure in their national defence and cybersecurity strategies, as well as in their military manuals and rules of engagement.

iii. Nuclear-specific treaties

Several treaties deal with different aspects of nuclear safety and security.[95] These do not have specific provisions for cyber-nuclear threats. However, their scope is sufficiently wide to cover different types of intentional or accidental cyber incidents affecting civil nuclear facilities.

The most relevant of these treaties is the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment.[96] As noted by the IAEA, 'computer security is a cross-cutting discipline that has interactions with all other areas of security in a nuclear facility'.[97] Accordingly, 'electronic compromise can lead to degradation or loss of certain physical protection functions'.[98] On this basis, intentional cyber operations targeting civil nuclear facilities could amount to the crime of nuclear sabotage. Under Article 7 CPPNM, nuclear sabotage includes any 'act directed against a nuclear facility, or an act interfering with the operation of a nuclear facility, where the offender intentionally causes, or where he knows that the act is likely to cause, death or serious injury to any person or substantial damage to property or the environment by exposure to radiation or release of radioactive substances'. Furthermore, under Article 2A CPPNM, states must establish, implement and maintain an appropriate physical protection regime applicable to nuclear material and nuclear facilities under their jurisdiction. The aim is to protect nuclear material and nuclear facilities against sabotage, and to mitigate or minimize the radiological consequences thereof. Further, where there is a credible threat of sabotage of nuclear material, states must cooperate, including by sharing relevant information with other states and the IAEA, in line with Article 5 CPPNM.

The International Convention for the Suppression of Acts of Nuclear Terrorism criminalizes as 'nuclear terrorism' serious forms of nuclear sabotage, including any unlawful and intentional use of or damage to a nuclear facility in a manner that releases or risks the release of radioactive material – whether by physical

---

94 Ilyushina, M. and Levenson, E. (2017), 'Chernobyl monitoring system hit by global cyber attack', CNN, 27 June 2017, https://edition.cnn.com/2017/06/27/europe/chernobyl-cyber-attack/index.html.
95 IAEA (undated), 'Nuclear security conventions', https://www.iaea.org/topics/nuclear-safety-conventions.
96 UN General Assembly, *Convention on the Physical Protection of Nuclear Material*, No. 24631, 26 October 1979, 1456 UNTS 246; IAEA, *Amendment to the Convention on the Physical Protection of Nuclear Material*, IAEA International Law Series No. 2, IAEA, Vienna (2006).
97 IAEA (2011), *Computer Security at Nuclear Facilities*, pp. 11–12.
98 Ibid., p. 25.

or digital means.[99] This convention also requires states to cooperate with a view to preventing and countering acts of nuclear terrorism in their territory, including when such acts are carried out or facilitated by cyber operations.[100] States parties must also 'make every effort to adopt appropriate measures to ensure the protection of radioactive material, taking into account relevant recommendations and functions of the [IAEA]'.[101]

4. Conclusion and recommendations

The increasing complexity and scale of cyber risks against civil nuclear infrastructure are closely tied to advancements in technology, which in turn have helped expand access to nuclear energy to a broader range of countries. Understanding and addressing these risks is essential for the safe and secure development and expansion of nuclear energy, which can offer significant social, economic and environmental benefits.

From a legal perspective, although no single legal regime specifically addresses cyberthreats to civil nuclear infrastructure, existing international law already offers robust safeguards – if not in practice, at least in principle. These safeguards encompass both general rules and specific regimes, and require states to refrain from conducting cyber operations targeting civil nuclear facilities, and to redress the effects of such incidents when they occur.

In the long term, states should develop strategies to both enhance the enforcement of international law in cyberspace and ensure accountability for unlawful cyber operations, including those targeting civil nuclear facilities. States may also need to evaluate the necessity of developing new treaties or adapting existing rules of customary international law to address cyber-nuclear threats comprehensively. In the short term, states should consider providing specific interpretations of existing rules and adopting additional non-binding norms or standards to complement them.

Previous Chatham House research proposed various measures to protect against cyber incidents targeting civil nuclear facilities. These recommendations included: the establishment of an international cybersecurity management strategy; coordinated plans of action to address technical shortfalls; initiatives to foster a culture of cybersecurity among the nuclear community; robust dialogue between nuclear engineers and contractors to raise awareness of cybersecurity risks; promotion of cyber insurance; network monitoring; promotion of vulnerability disclosure; establishment of national computer emergency response teams (CERTs) specialized in industrial control systems; promotion of the concept of 'security by design'; steps to ensure sufficient redundancy in digital systems; and measures to protect the integrity of digital supply chains.[102]

---

99 Article 2(1)(b), UN General Assembly, International Convention for the Suppression of Acts of Nuclear Terrorism, A/59/766, 13 April 2005 (ICSANT).
100 Article 5, ICSANT.
101 Article 7, ICSANT.
102 Baylon with Brunt and Livingstone (2015), *Cyber Security at Civil Nuclear Facilities*, pp. ix–x; Brunt, R. and Unal, B. (2019), *Cybersecurity by Design in Civil Nuclear Power Plants,* Chatham House Briefing Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/2019/07/cybersecurity-design-civil-nuclear-power-plants.

Expanding on this research, and building on the analysis above, this paper offers recommendations structured across three levels:

International

— **Initiate capacity-building initiatives** to raise awareness of current cyber risks against civil nuclear infrastructure. Amplify existing guidance on how to protect against such risks, and develop new guidance to address gaps, where needed, to ensure the safety and security of both existing and future nuclear energy endeavours. This should be done by states as well as by non-state actors, including the private sector, academia, international organizations and civil society.

— **Use existing multi-stakeholder platforms and initiatives to conduct focused discussions.** The IAEA has produced numerous guidelines on how to protect civil nuclear infrastructure from cyberthreats. These guidelines can serve as building blocks for future discussions on the matter. Platforms like the Global Forum on Cyber Expertise, the Paris Call on Trust and Security in Cyberspace, the Cybersecurity Tech Accord and others can use this guidance to start dedicated discussions on the cybersecurity of civil nuclear infrastructure that bring together the international cyber capacity-building community and the nuclear community. These forums could also serve as useful spaces for discussion to ensure that SMRs and microreactors are designed with the right cybersecurity considerations from the start.

— **Initiate dedicated discussions at UN level.** The UN Open-Ended Working Group (OEWG) on ICTs could hold dedicated discussions on addressing cybersecurity risks in the civil nuclear sector as part of a larger and more detailed discussion around the protection of critical infrastructure. These discussions, which could be championed by UN member states and non-government stakeholders alike, should seek to raise awareness of existing risks, explore the application of current rules and norms to this sector, and brainstorm additional protection strategies. Moreover, as the discussions progress, it will be crucial to consider how they can be integrated into a dedicated mechanism for regular institutional dialogue on ICT threats in the future. This future mechanism, whether in the form of a Programme of Action or otherwise, should be designed to ensure sustained engagement and progress on addressing cybersecurity threats to critical infrastructure, including in the civil nuclear sector.

Regional

— **Build capacity through regional organizations.** Regional organizations should play an active role in helping to enhance the capacity of their member states to safeguard civil nuclear facilities and bolster critical infrastructure. This can be achieved through organized discussions at a regional level, which can facilitate the sharing of best practice and lessons learned.

— **Develop context-specific cybersecurity frameworks.** Regional efforts can focus on developing cybersecurity frameworks for the protection of critical infrastructure, including in the civil nuclear sector. These should be tailored to the unique needs of member states, with targeted actions designed

to enhance the cybersecurity of civil nuclear infrastructure. Regional discussions can sometimes achieve substantial consensus on these matters among neighbouring nations, or among states sharing similar perspectives or contexts. Subsequently, such regional or multilateral agreements can serve as viable models for testing and potentially expanding developments more widely in the international arena. These discussions can also be organized between like-minded states or within a different grouping. They can foster cooperation and alignment in addressing cybersecurity challenges on a broader scale, and can ensure the protection of vital assets.

National

- **Continue to invest in cybersecurity preparedness.** States should continue to develop their cybersecurity preparedness through their CERTs and computer security incident response teams (CSIRTs), and should deepen their understanding of all cyberthreat vectors against critical infrastructure, including against the civil nuclear sector.
- **Conduct incident-response planning.** States should incorporate cybersecurity of civil nuclear infrastructure in their domestic civil contingency and resilience plans, including by designing and carrying out tests and simulation exercises specific to cyber-nuclear risks and involving all relevant stakeholders.
- **Interpret international rules and guidance within a national context.** States and other stakeholders should initiate efforts aimed at interpreting and applying international rules, norms and guidance, such as the IAEA guidance, in their national contexts.
- **Facilitate public–private partnerships (PPPs).** States should facilitate PPPs to protect the civil nuclear industry by promoting information exchange and collaboration between government and industry stakeholders.
- **Engage in collaborative awareness-raising efforts.** States should actively engage with relevant stakeholders, including regulatory bodies, industry associations, academia and civil society, to collectively raise awareness on best practices aimed at strengthening cybersecurity measures and resilience within the civil nuclear sector.

By implementing these recommendations at all levels, states and other key stakeholders can collaborate to mitigate cybersecurity risks and ensure the safe and secure development and growth of the civil nuclear sector. This can help maximize the benefits of this sector for societies, economies and the environment.

About the authors

Dr Talita Dias is the senior research fellow in the International Law Programme at Chatham House. Her current research focuses on the application of international law to new technologies, including ICTs, AI and online platforms. Previously, she was the Shaw Foundation Junior Research Fellow in Law at Jesus College, University of Oxford, and a research fellow with the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government, University of Oxford.

She is a founding member of the Oxford Process on International Law Protections in Cyberspace, a research project looking to clarify the extent to which international law applies to ICTs.

Talita is an international lawyer with over 10 years of combined academic, policy and practical experience. Her work has been published in leading international law journals and cited by different states and international institutions, such as the International Criminal Court.

Joyce Hakmeh is the deputy director of the International Security Programme at Chatham House and the co-editor of the *Journal of Cyber Policy*. She leads the institute's work on cyber policy, and provides regular analysis on issues that sit at the nexus between technology and geopolitics. She also oversees the research agenda of the International Security Programme and supervises its researchers.

Her recent research has focused on the geopolitics of cyberspace, international cyber capacity-building, gender-transformative approaches in cyber policy, the role of China in cyberspace, and the impact of emerging technologies on international security.

Joyce chaired the Global Forum on Cyber Expertise working group on cybercrime in 2018–22, and is a frequent panellist and chair at conferences at national and global events. She currently sits on the advisory boards of the Global Cyber Alliance and the DNS Research Federation. Previously, Joyce worked for the UN, the International Federation of Red Cross and Red Crescent Societies, and various non-profit organizations. She received her master's degree in international law from SOAS, University of London.

Dr Marion Messmer is a senior research fellow in the International Security Programme at Chatham House. She has expertise in arms control, nuclear weapons policy and Russia–NATO relations.

Before joining Chatham House, Marion was the co-director of BASIC, where she led on the organization's nuclear risk reduction and disarmament work.

Marion is an N2 Innovation Fellow (2020–21) and an ACONA Fellow (2021–22), and holds a PhD in security studies from King's College London.

Acknowledgments

We are grateful to Microsoft and, in particular, Michael Karimian for their support for this project. We would also like to thank the anonymous reviewers for their invaluable comments and feedback on this paper. Special thanks also go to our colleagues in the International Law Programme and International Security Programme at Chatham House, particularly Rowan Wilkinson. Thanks also to Alex Vines at Chatham House for his advice. Finally, the authors would like to thank Jake Statham, managing editor of the Publications team at Chatham House, for his editorial guidance and support.

Cover image: The Pivdennoukrainsk nuclear power plant in Ukraine, September 2022.

ISBN 978 1 78413 616 1
DOI 10.55317/9781784136161

Cite this paper: Dias, T., Hakmeh, J. and Messmer, M. (2024), *Cybersecurity of the civil nuclear sector: Threat landscape and international legal protections in peacetime and conflict*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136161.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223