(Vol 2, Issue 1, 2025) pp 25-35
Pak. J. Integ. Soc. Sci

ISSN (Online): 3104-3771 ; **ISSN (Print):** 3104-3763
DOI: https://doi.org/10.51846/pjiss.v2i1.4680

Pakistan's Civil Nuclear Security Architecture and The Paradigm of Emerging Technologies

Maheera Munir[1]*, Nidaa Shahid[2]

[1]Maheera Munir is a Research Assistant at the Centre for Aerospace and Security Studies (CASS) Lahore.
[2]Nidaa Shahid is an Associate Director at the Centre for Aerospace and Security Studies (CASS) Lahore.

Cite this article:
Munir, M., & Shahid, N. (2025). Pakistan's Civil Nuclear Security Architecture and The. *Pakistan Journal of Integrated Social Sciences* , 2(1), 25-35.

Received: Jan 30, 2025; **Revised:** March 25, 2025; **Accepted:** May 09, 2025 **Published:** June 25, 2025

Abstract

Nuclear energy stands as a pivotal solution to the burgeoning global energy demand, yet its dual nature as a potent energy source and a potential security threat necessitates rigorous attention to nuclear security measures. Globally, nuclear security faces two persistent threats, including terrorist threats from non-state actors and increasing cyber intrusions, posing risks of contamination, radioactive emissions, and challenges to national security and sovereignty. To effectively counter these threats, Pakistan has a state-of-the-art civilian nuclear security regime constituting legislative and regulatory frameworks, institutions and organizations, and other systematic measures. It also complies with the global nuclear security architecture. However, emerging technologies, such as Artificial Intelligence, Unmanned Aerial Systems, and 3D Printing, etc., given their dual-use nature, are a rapidly evolving threat which all countries with civilian nuclear programs, including Pakistan, will have to contend with. This article argues that while Pakistan has been internationally recognized as a responsible nuclear state with an impeccable nuclear security regime, the complex landscape of emerging technologies poses formidable challenges. To secure the country's civilian nuclear architecture against these evolving threats, Pakistan needs to further fortify its civilian nuclear security regime, thereby mitigating risks and safeguarding against any potential vulnerabilities in the future.

Keywords: Nuclear security, civilian nuclear regime, pakistan, cybersecurity, emerging technologies

Introduction

Nuclear energy is one of the greatest scientific inventions to fulfil the growing demands of the global population by improving the energy mix of developing and developed nations. At the same time, its potential to cause massive devastation and stir a global crisis poses a considerable threat to human and international security. Nuclear security is, thus, a matter of great concern for nation-states due to risks of contamination, terrorist attack or sabotage, threats to environment and ecology, health hazards, human displacement, threats of proliferation, and now the increasing challenges of emerging technologies.

The concern multiplies for developing countries who face considerable challenges in ensuring the safety and security of their nuclear installations, including nuclear power plants and other civilian nuclear infrastructure. Here, it is imperative to distinguish between nuclear security and safety. While nuclear safety refers to protection of people from assets, nuclear security pertains to protection of assets from people through effective prevention of, and timely response to, incidents like theft, sabotage, unauthorized access, radioactive emissions, etc. (IAEA, 2022). The scope of this article is limited to nuclear security in civilian domain since

***Correspondence:** Maheera Munir (maheeramunir8@gmail.com)

the security of the military nuclear program is highly sensitive and secretive. No state in the world has disclosed the measures it takes to safeguard its military nuclear program, hence the lack of available data.

When it comes to Pakistan's civil nuclear infrastructure, Pakistan is the first Muslim country to build and generate energy from nuclear power plants. It has 6 fully-functional nuclear power plants, generating total energy of 3,530 megawatts (MW). By 2030, Pakistan plans to install more nuclear power plants to increase the nuclear energy generation to 8,800 MW (PAEC, n.d.-b.) The use of nuclear energy and technology extends to civilian applications in agriculture, biotechnology, engineering, and medical industry. For instance, the Pakistan Atomic Energy Commission (PAEC) operates 19 Cancer Hospitals across the country with high-end application of nuclear technology for medical purposes (PAEC, n.d.-a.).

Pakistan considers nuclear security a national responsibility and has an efficient security regime in place. The country is also compliant with global nuclear security architecture and has been regarded as a responsible state. According to the most recent Nuclear Threat Initiative's Nuclear Security Index report 2023, Pakistan ranked three points higher than its 2020 score, gaining an overall score of 49/100, ranking above India, Iran and North Korea (Nuclear Threat Initiative, 2023).This article argues that Pakistan's successful and responsible measures for nuclear security are commendable however, a myriad of new threats have now come to the forefront due to a wide range of dual-use, emerging technologies such as AI, Machine Learning, Unmanned Aerial System (UAS), 3D Printing, etc., which offer opportunities to enhance nuclear security but have also introduced new vulnerabilities.

To article briefly provides a global threat assessment with respect to nuclear security followed by an overview of Pakistan's civil nuclear regime and steps Pakistan has taken to secure its civil nuclear infrastructure. It further looks into the evolving domain of emerging technologies to analyze new challenges and opportunities for nuclear security. It then provides response options for Pakistan to further enhance its civil nuclear security architecture for protection against the prevalent threats as well as the threats surfacing from emerging technologies.

Threats to Nuclear Security

There are certain looming threats that continue to raise questions and concerns in the academic, media, and political circles about nuclear security at global and national levels. Existing literature highlights that nuclear security, all across the world, is subjected to two major threats: non-state actors and cyber threats.

Threat from Non-State Actors

Since 9/11, the security threat from terrorist groups has continued to evolve. The increased interest of non-state actors in acquiring nuclear resources and materials emphasizes the need to put adequate measures in place to prevent such illicit acquisition. Ali (2007) argues that while the degree of security at nuclear facilities like power plants is quite high, the major challenge remains the security of industrial, medical, agricultural and engineering facilities using nuclear material, which are potential sources of commercial radioactivity It is pertinent to note here that although the nuclear material used commercially only includes low-enriched uranium, which cannot be processed into nuclear weapons, it can be used to make dirty bombs (Ali, 2007).

Ali and Sadiq (2023) highlight another potential scenario of nuclear terrorism, one involving attack or sabotage on a nuclear facility, leading to high radioactive emissions. The execution of this kind of attack requires complete physical and operational knowledge of the facility such as security measures and the loopholes to bypass those measures. It also requires highly sophisticated technical tools and weapons to cause a significant radioactive release (Ali & Sadiq, 2023). These factors highlight the degree of improbability and lower chances of success in case terrorists attack the facilities.Another potential concern is non-state actors gaining access to personnel working at a nuclear power plant or any civil nuclear facility and manipulating them to use their authorised access to cause damage to the organization through terrorism, espionage, information disclosure to malicious actors, sabotage, etc. (Bunn, 2017). For instance, in August 2014, an insider sabotaged a Doel-4 nuclear power station in Belgium,

resulting in the destruction of a reactor turbine, causing a heavy damage of $200 million. This insider was a contractor, Ilyass Boughdalab, who passed his security clearance in 2009 but in 2012, joined a terrorist group in Syria (Bunn, 2017). Thus, personnel reliability remains a major concern.

Cyber Threats

In the wake of technological advancements and growing cyber threats, the traditional focus on physical protection has now expanded to include cyber security of nuclear facilities. Cyber threats constitute threats to computer networks, even the air gapped ones. Khan (2021) argues that usually, the primary objective of an adversary is to identify and exploit vulnerabilities within computer networks in order to gain control, execute false commands, and maintain a persistent presence. Cyberattacks may cause serious damages such as theft of sensitive information, theft of radioactive materials, radiation emission, and impairing operability of the facility (Khan, 2021).

Civil nuclear security faces two major threats in the cyber domain. Firstly, as nuclear facilities are connected through computer systems, they are prone to cyberattacks through malware (Naseer et al., 2020). A malware implanted in the system can infiltrate into a nuclear facility, manipulate data, steal files, or sabotage the plant. In 1979, the American Air/Aerospace Defence Command suffered a nuclear cyberattack which triggered a false declaration of a state-level nuclear war (Naseer et al., 2020). Timely handling of the false alarm prevented what might have been a nuclear exchange between the U.S.and USSR.

A game-changing incident in the domain of cyber warfare was the 2010 Stuxnet virus implemented into Iran's Natanz enrichment facility which sabotaged the enrichment process, damaging up to 1,000 centrifuges (Naseer et al., 2020). Moreover, in 2016, a computer virus known as W32.Ramnit infiltrated the Gundremmingen nuclear power plant in Germany, which can potentially steal sensitive data, disable software security, and create a backdoor for external access to the system (Steitz & Auchard, 2016). In 2022, the U.S. also accused Russia of conducting cyberattacks against its Kansas nuclear power plant (Benner & Conger, 2022). Recently, Russia's cyber warfare in the Russia-Ukraine war to attack Ukraine's nuclear power plants, target critical infrastructure, and disrupt power supply has further highlighted the degree of threats posed by this emerging technology (Willet, 2022).

Secondly, cyber espionage has appeared as another grave threat. Most commonly, states are involved in conducting cyber nuclear espionage which largely violates the principle of state sovereignty. For example, Israel conducted a state-sponsored cyber espionage against Syria in 2007 under Operation Orchard, which allowed Israel to install a Trojan in government institutions in order to collect data about Syria's nuclear ambitions. Overall, cyber warfare has become more sophisticated and the technical capacity to undermine consequent nuclear security risks is still quite limited, even in countries with highly-advanced technology and research programs.While the existing literature points out major threats to civilian nuclear security, there is a limited discussion around how emerging technologies, given their dual-use nature, also pose serious threats that need immediate attention, a gap that this article aims to cover.

Pakistan's Civil Nuclear Security Regime

According to the International Atomic Energy Agency (IAEA), a nuclear security regime is a "physical protection regime" based on a set of legislative, regulatory and administrative measures put in place by institutions and organizations within a state (IAEA, 2013b). Its purpose is to maximize security against unauthorized access or removal of nuclear material, prevent theft and sabotage, and to minimize the impacts of sabotage (IAEA, 2011).

Domestic Level

Pakistan's civil nuclear infrastructure falls under the purview of the PAEC and the Pakistan Nuclear Regulatory Authority (PNRA), and is further supported by an integrated intelligence system, a strong regulatory framework, a systematic export control regime, and rigorous international cooperation. Such a comprehensive civil nuclear security regime ensures physical protection whilst dealing with material control and radioactive waste management,

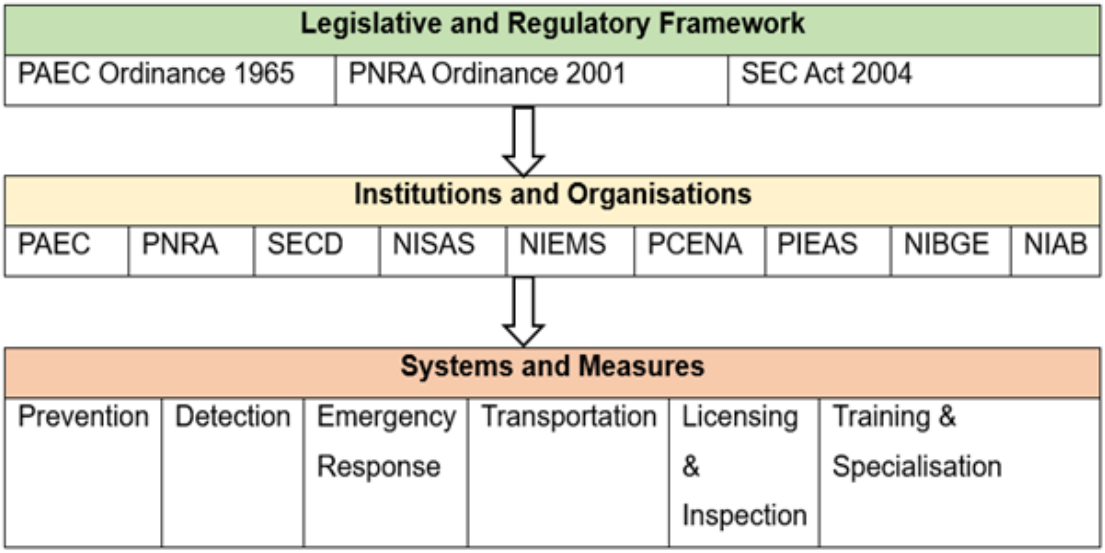
border controls, and radiological emergencies. Moreover, all six of the country's nuclear power plants function under the IAEA safeguards. The regime comprises (i) legal and regulatory framework, (ii) institutions and organizations, and (iii) preventive mechanisms.

The legislative and regulatory framework includes national policies and laws responsible for the security of nuclear material and infrastructure. Under the Pakistan Atomic Energy Commission Ordinance 1965, PAEC owns and operates all nuclear installations under the federal government (Noor, 2023). Under the PNRA Ordinance 2001, PNRA regulates the authorization, licensing, inspection, and enforcement of nuclear energy and technology at all nuclear facilities, be it power plants, hospitals, industries or agricultural sector to ensure proper compliance and risk aversion. The Strategic Export Control Act 2004 underlines regulations for control over export and transportation of nuclear materials and technologies, and resulted in establishment of the Strategic Export Control Division (Noor, 2023).

The legislative framework is further strengthened by multiple institutions and organizations. PNRA has established the National Institute of Safety and Security (NISAS) and the Nuclear Emergency Management System (NEMS) to oversee and prevent nuclear or radiological crises (Jalil, 2023). Furthermore, Pakistan has also established the Centre of Excellence for Nuclear Security (PCENS) and the Pakistan Institute of Engineering and Applied Sciences (PIEAS) to offer training, specialization, and post-graduate studies, respectively. In the agricultural domain, the Nuclear Institute for Agriculture and Biology (NIAB) and the National Institute for Biotechnology and Genetic Engineering (NIBGE) oversee and promote the use of nuclear energy in agricultural production to enhance crop resistance against pests and climate change (Jalil, 2023).

Global Level

Figure 1.
Pakistan's Civil Nuclear Security Regime



Pakistan is also compliant with the global nuclear security architecture established by the IAEA under various instruments. Pakistan is party to the Convention on the Physical Protection of Nuclear Materials (CPPNM) and its 2005 amendment, adheres to the IAEA Code of Conduct on the Safety and Security of Radioactive Sources, and is party to the Global Initiative to Combat Nuclear Terrorism (GICNT) (Noor, 2023). Pakistan's civil nuclear security regime and adherence to international instruments and protocols reflect its obligation and capability to ensure nuclear security and be a responsible nuclear actor at the international level.

Steps Taken to Secure Civil Nuclear Infrastructure

On practical grounds, there has been no incident of nuclear terrorism in Pakistan. To protect against loss, theft, and unauthorized access to radioactive materials, PNRA has formulated rules, regulations and laws for nuclear security and radiation protection at all

commercial facilities. Through periodic inspections, PNRA ensures the security of radioactive material under its Nuclear Security Action Plan (NSAP) as well as the Nuclear Security Cooperation Programme (NSCP) signed in collaboration with the IAEA since 2005. Both the NSAP and NSCP focus on physical protection of materials and facilities through capacity building and establishment of adequate infrastructure (PNRA, 2020).

However, there can be an attack from adversarial states such as India and Israel. Reports of Israel's plan to attack the Kahuta nuclear research laboratory during the 1980s and 1990s make it important to contend with the possibility of such malicious intent by adversaries. To counter threats from external actors, especially hostile neighbour like India, Pakistan has a number of confidence-building measures in place. For instance, in 1988, Pakistan and India bilaterally formalised the Agreement on the Prohibition of Attack Against Nuclear Installations and Facilities, which ensures that in peace or war, Pakistan and India will neither attack each other's nuclear facilities nor assist any foreign powers in doing so (Ministry of Foreign Affairs, 2020). Under this agreement, both countries have been exchanging lists of their nuclear facilities since 1992 on 1st January every year to prevent any intended or accidental targeting (Yamin, 2008).

Next, to eliminate any potential insider risks, Pakistan implements a long series of vetting procedures. The military personnel working at nuclear facilities undergo a rigorous screening process, known as the Personnel Reliability Program (PRP), and the civilian personnel are required to go through the Human Reliability Programme (HRP). The screening does not only occur at the beginning of induction but is conducted every two years by Pakistan's intelligence agencies (Azad & Dewey, 2023).

With regard to cyber threats, Pakistan, being a nuclear power, is highly prone to cyber-attacks with nuclear installations, communication networks, government departments, and other critical infrastructure being the main targets. Although Pakistan has not yet experienced any incident of a cyber-attack on any nuclear facilities, the evolving nature of these threats require that effective and efficient countermeasures be put in place, especially given India's growing cyber security cooperation with Israel (Farooq & Ali, 2022). To effectively counter cyber threats, Pakistan has an integrated capacity building infrastructure in place including NISAS, PCENS and PIEAS to enhance skills and specialization in areas of physical security, intelligence, and radioactive control (Ahmad & Ahmad, 2020). The IAEA has highly commended these efforts, underscoring Pakistan's exceptional capabilities in safeguarding against a wide threat spectrum.

Emerging Technologies: The Evolving Threat Domain

Emerging technologies can be understood as technological innovations which might impact nuclear security operations as they evolve and proliferate. However, their implications are yet uncertain (Rotolo et al., 2015). Emerging technologies come with a wide range of threats and opportunities for nuclear and radiological security. As these technologies evolve and become accessible to adversaries, be it hostile states or aggressive non-state actors, the capability gap decreases, resulting in difficulty to prevent theft or sabotage. One of the most immediate risks of emerging technologies is technological surprise. Operators might fail to anticipate and counter the threat, leaving nuclear and radiological material vulnerable to attack, theft or sabotage (Roth et al., 2021).

Moreover, the integration of emerging technologies into nuclear facilities and infrastructure for production, storage, and safety presents a range of new vulnerabilities (Roth et al., 2021). While emerging technologies can play an advanced role in digitalization, automation, and functioning of nuclear power plants, they can also disrupt the operations and compromise security. Some of the most prominent emerging technologies include AI, Machine Learning, UAS, and 3D Printing. Given their dual-use nature (offensive/defensive), these technologies have enormous benefits for nuclear security but also present significant threats.

AI and Machine Learning

AI refers to new technologies that are capable of mimicking human intelligence to solve complex problems in no time (Pluff & Nair, 2023). Machine learning can be understood as the ability of computers to learn patterns and programs without extensive back-end programming (Schwartz et al., 2022). This way, AI and machine learning technologies come with adaptive

learning capabilities and algorithms, allowing quicker access to information and computer security through swift identification of threats such as unauthorized access, cyberattack, or anomalous data. With reduced human interference, AI and machine learning automate network monitoring and security, leaving nuclear security personnel to more strategic tasks.

The early warning systems, equipped with AI, allow defense planners to detect and observe threats quicker, and with greater accuracy than traditional methods. Nevertheless, the absence of human judgment and oversight, combined with the opaque nature of AI and machine learning algorithms, may result in increased risks of destabilizing accidents and false alarms (Johnson, 2023). Moreover, it is pertinent to note here that no technology is immune to failure. Thus, any failure or malfunction in the AI system can undermine security and add to nuclear vulnerability. Similarly, AI and machine learning technologies are capable of both reducing and increasing susceptibility to cyberattacks. On the one hand, AI cyber-defense tools can automatically identify vulnerabilities in software code, potentially creating a secure layer of defense against cyber intrusions. On the other hand, AI systems are highly vulnerable to malware which can let the adversary take control or manipulate the pattern recognition systems or exploit information in these autonomous systems (Johnson, 2020).

The disruptive nature of AI and machine learning has created a dual-use security dilemma, which creates ambiguity regarding whether these technologies would be used for peaceful, civil purposes or destructive, military objectives (Lupovici, 2021). Such ambiguities add to the risk of misperception and miscalculation, resulting in disruptions in the computer networks. Addressing these ambiguities and ensuring responsible use of these technologies in nuclear security frameworks is essential to mitigating risks and maintaining stability in the nuclear landscape. While Pakistan has not yet integrated AI into its civil nuclear infrastructure, it is important to bear these challenges in mind before taking a step toward AI and machine learning adoption, for the threats these technologies pose may override the benefits.

Unmanned Aerial Systems (UAS)

Another emerging technology which has now become a potential threat to nuclear security is the UAS, also referred to as drones. UAS now operates as a billion-dollar industry and are widely available. UAS can be used both as a tool and a threat. It comes with an extensive list of applications, including mobile shipment, monitoring, communication, enhanced visibility, inspection and detection, and emergency response (Aaron, 2018). On the contrary, UAS pose several threats such as surveillance of a nuclear/radioactive material in transport, collision, and improvised explosive device. If an adversary obtains nuclear material, the UAS can be used as a radiation dispersing device (Aaron, 2018). Frequency jamming is another malicious use of the UAS (Mohsan et al., 2022). The UAS can also be used for active surveillance of a nuclear facility to obtain information such as camera locations, guard movements, and other sensitive areas. Gathering this information provides malicious actors an opportunity to plan a coordinated attack at a nuclear site to obtain nuclear/radioactive materials or disrupt the operations. Due to these potential threats the UAS poses, they are categorized as disruptive innovation (Martin et al., 2017).

A developing UAS threat which can threaten the security of nuclear infrastructure is drone swarms i.e., deploying hundreds of drones, equipped with autonomous information sharing and decisionmaking, in a coordinated attack to achieve specific objectives. UAS swarms pose significant security concerns in four payload categories: chemical, biological, radiological, and nuclear (Kallenborn & Bleek, 2018). In either of these categories, a coordinated attack by a swarm of drones can have severe consequences. Moreover, it is crucial to note that not every UAS within a swarm needs to be engaged in the attack. Drones in a swarm may have various roles, including attack, sensor, communication, or decoy functions (Kallenborn & Bleek, 2018).

Over the past decade, the number of attacks on critical infrastructure using UAS technology has greatly increased. In 2019, the Houthis conducted a drone attack against Saudi Arabia's Aramco oil refinery, resulting in the loss of 6 million barrels of oil in a day (Krane, 2020), highlighting the vulnerability of such a well-secured infrastructure against this emerging technology. In another incident back in 2012, Israel claimed that a Hezbollah UAS was shot down taking photographs of its Dimona nuclear research centre (Hoenig, 2014). Moreover, there have been several drone sightings over French nuclear power plants in recent years. In 2018, a

UAS flew into one of France's nuclear power plant and slammed into the wall (Gliadkovskaya, 2018). In April 2024, a drone hit Russia-controlled Zaporizhzhia nuclear power plant in Ukraine (Alberti et al., 2024), demonstrating the susceptibility of such critical facilities against UAS attacks and the need to strengthen airspace protection around such infrastructure.

3D Printing

3D printing, or additive manufacturing, is the production of intricate shapes and designs through digital drawings using laser beams, guided by a computer system. This technology ensures lesser waste, reduced human error, low weight, and economized manufacturing (Ashton, 2023). 3D printing represents significant strides in automation and supply chain optimization. The nuclear industry is shifting toward 3D printing after its extensive success in automotive and aeronautical industries. In 2017, Slovenia employed 3D printing to manufacture pump impeller for a nuclear reactor (Volpe, 2019). Similarly, the U.S.-based Oak Ridge National Laboratory has used 3D printing to create channel fasteners for nuclear reactors. In 2022, Sweden manufactured stainless steel fuel component for its nuclear power plant. Moreover, Russia and South Korea are also widely adopting 3D printing in nuclear industry (Ashton, 2023). These first-use cases of 3D printing across the globe highlight the potential benefits this emerging technology has brought.

However, like other emerging technologies, this dual-use technology has become a tool for malicious actors to carry out destructive agendas. In 2019, a terrorist attack in Germany involved a partially 3D printed firearm, and the cases of terrorist use of 3D printing to produce firearms have grown ever since (Koehler, 2019). Similarly, the threat extends to nuclear security as 3D printing, now widely accessible, can provide access to designs and blueprints through a technique known as generative design (Daase et al., 2019). As 3D printing rules out the need for technical proficiency, it becomes potentially dangerous for nuclear security and can increase clandestine proliferation.

Moreover, currently there is no international export controls surrounding the use of additive manufacturing for nuclear value chain purposes. It paves way for an open proliferation pathway for state and non-state actors alike, and is a huge concern for nuclear states. Thus, 3D printing is another evolving threat that Pakistan needs to consider.

Other Potentially Emerging Technologies

There are several other potentially emerging technologies which can pose grave challenges to nuclear security. Most significantly, satellite and remote- sensing technologies could be targeted for disruption or jamming, undermining space-based surveillance of nuclear facilities, and hindering detection of potential security breaches or illicit nuclear activities, resulting in reduced situational awareness overall (Lawrence, 2019).Similarly, robotics and automation systems can also pose a threat to nuclear security as they are vulnerable to malware or cyberattacks, compromising their functionality and leading to any nuclear accidents or providing unauthorized access to sensitive areas (Shubayr, 2024). Therefore, while automation systems ease down the production and operational aspects, they can also result in the disruption of these very aspects.Moreover, advanced sensors are now being embedded for an added layer of security, but they can be susceptible to spoofing or tampering. Malicious actors could also use countermeasures to prevent detection by these sensors, potentially enabling them to transport nuclear material or sabotage critical infrastructure without triggering alarms (IAEA, 2013a).

Pakistan's Response Options

Pakistan needs to ensure that it incorporates the threats from the aforementioned emerging technologies into its nuclear security culture and work toward devising effective countermeasures. For that, following are some immediate response options:

Formulate a Cybersecurity Task Force

Pakistan could further enhance the overall security of its civil nuclear infrastructure by formulating a cybersecurity task force responsible for monitoring and defending against cyber threats to nuclear facilities. Some significant cybersecurity measures that can be adopted include encryption, regular security audits, biometric access controls, and blockchain technology.

Strengthen Inter-Institutional Intelligence Sharing

Pakistan should establish a joint task force to strengthen inter-institutional intelligence sharing and cooperation, comprising intelligence agencies, law enforcement, and military personnel. This would allow facilitation in real-time information sharing and efficient coordination in identifying and neutralizing any emerging threats.

Ratify the International Conventions and Protocols Aimed at Countering Nuclear Terrorism

While Pakistan has already ratified the CPPNM and actively participates in the GICNT, it should look for further ways to enhance international cooperation. In September 2023, Pakistan signed the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) but has not yet ratified it. This ICSANT entails criminalization of nuclear terrorism and calls for cooperation between law enforcement agencies and judiciary for prevention, investigation, and punishment of such acts. Pakistan should promptly ratify the convention and other such protocols which aim at enhancing transnational cooperation in mitigating the nuclear threats arising from terrorist outfits.

Capacity Building and Regulatory Framework

Apropos of emerging technologies, Pakistan has nascent technical skills and expertise. Although the PCENS in Chakri near Rawalpindi is actively working towards capacity building and training programs to build the technical expertise of personnel tasked with nuclear security, this should be followed by developing a regulatory framework to govern the implementation and use of emerging technologies. The framework must constitute guidelines for adoption of emerging technologies, conduction of risk assessment procedures before and during implementation, and enforcing compliance with established security and quality standards. Only then, emerging technologies can be actively used for defensive purposes.

Ensure Human-Machine Synchronisation in the Implementation of Emerging Technologies

Another important aspect in the deployment of emerging technologies such as AI, drones, remote-sensing, biometric controls, and blockchain, etc. is the human-machine synchronization. Adoption of emerging technologies must not eliminate human oversight from the nuclear security equation. It is crucial to maintain a balance so that human oversight can eliminate machine faults while technologies undermine human error.

Conclusion

For countries like Pakistan, which are working toward the integration of nuclear energy into their development matrix, safeguarding nuclear installations is of paramount importance. Unfortunately, despite stringent measures to cater to present and evolving threats, Pakistan's turbulent history of terrorism and extremism continues to influence perspectives over its nuclear security regime. However, Pakistan rising above India in the NTI's Nuclear Security Index Report 2023 speaks of its impeccable nuclear security architecture. Pakistan's nuclear security regime, comprising of regulations, institutions, and crucial measures ensures compliance with the global security standards, enhances situational awareness, and improves the country's overall nuclear security landscape. While traditional threats from malicious actors and turn-cloaks remain constant areas of concern, periodic inspections, threat assessments, and rigorous screening act as effective countermeasures. Nevertheless, as the nuclear threat matrix continues to evolve, it is important to ensure that Pakistan's nuclear security mechanism is not static and evolves in tandem with threats.

As discussed in the article, one of such evolving threats is from the rapid advancements in cyber domain and proliferation of emerging technologies. Like any other nuclear state, Pakistan remains vulnerable to cyberattacks from non-state actors as well as adversarial states. Similarly, while technologies like AI, Machine Learning, UAS, and 3D Printing, etc. offer significant benefits, their dual-use nature also introduces new vulnerabilities and risks. Although Pakistan has not witnessed any offensive attack from these dual-use emerging technologies yet, the threat lingers and should not be ruled out. For that, Pakistan must adopt beneficial emerging technologies for enhanced surveillance and threat detection as well as put effective cybersecurity measures in place to ensure the protection of its civil nuclear infrastructure. This

way, nuclear energy will continue to assist in meeting Pakistan's growing energy needs and offer benefits in areas like medical, engineering, and agriculture, overall contributing to the country's national growth and development.

Conflict of Interest

The authors declare that there are no financial or non-financial conflicts of interest related to the subject matter discussed in this manuscript.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon request.

Funding Statement

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

References

Aaron, A. (2018). *Unmanned Aerial Systems as an Enhancement and Threat to Material Transport and Physical Security.* International Atomic Energy Agency. https://conferences.iaea.org/event/129/contributions/3956/attachments/2514/2951/IAEA-CN-254-163.pdf

Ahmad, I., & Ahmad, A. (2020). *Capacity building in nuclear security education and job specific trainings in Pakistan. In IAEA Nuclear Security Conference 2020* (Vienna, Austria). International Atomic Energy Agency (IAEA). https://conferences.iaea.org/event/181/contributions/15305/attachments/8448/11192/IAEA-CN-278-42.pdf

Alberti, M., Pennington, J., & Edwards, C. (2024, April 7). Russian-controlled Zaporizhzhia nuclear reactor damaged following drone attack. CNN. https://www.cnn.com/2024/04/07/europe/russian-controlled-zaporizhzhia-nuclear-reactor-damaged-following-drone-attack/index.html

Ali, I., & Sadiq, M. (2023). The Perils of Non-State Actors in Pakistan: Assessing the Risks of Nuclear Safety and Security. *International Journal of Nuclear Security, 8*(1), Art. 5. https://doi.org/10.7290/ijns082376

Ali, Z. (2007). *Pakistan's Nuclear Assets and Threats of Terrorism: How Grave is the Danger?* (pp. 1–19). The Henry L. Stimson Center . https://www.stimson.org/wp-content/files/file-attachments/Pakistan's%20Nuclear%20Assets%207.6.07%20Zafar%20Ali%20FINAL%20PDF.pdf

Ashton, L. (2023). Embracing the Promise of Additive Manufacturing for Advanced Nuclear Reactors. *IAEA Bulletin, 64*(3). https://www.iaea.org/bulletin/embracing-the-promise-of-additive-manufacturing-for-advanced-nuclear-reactors

Azad, T., & Dewey, K. (2023). Understanding Pakistan's Nuclear Security Regime . *Journal of Strategic Security, 16*(4), 180–202. https://doi.org/10.5038/1944-0472.16.4.2121

Benner, K., & Conger, K. (2022, March 24). U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant. *The New York Times.* https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html

Bunn, M. (2017). *Scenarios of insider nuclear threats – and steps to strengthen protection. In Nautilus Institute Workshop on Reducing the Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia.* Belfer Center for Science and International Affairs, Harvard Kennedy School. https://scholar.harvard.edu/files/matthew_bunn/files/japan-insider-scenarios_2017.pdf

Chavez, K., & Swed, O. (2020). Off the Shelf: The Violent Nonstate Actor Drone Threat. *Air & Space Power Journal, 34*(3), 29–43. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf

Daase, C., Christopher, G., Dalnoki-Veress, F., Pomper, M., & Shaw, R. (2019). *WMD Capabilities Enabled by Additive Manufacturing.* The Middlebury Institute of International Studies at Monterey. https://nonproliferation.org/wp-content/uploads/2019/09/NDS_Report_1908_WMD_AM_2019.pdf

Farooq, A., & Ali, A. (2022). India's Growing Cyber Partnerships and Challenges for Pakistan. *Margalla Papers, 26*(2), 49–61. https://doi.org/10.54690/margallapapers.26.2.121

Gliadkovskaya, A. (2018, July 3). Greenpeace pilots and crashes drone into nuclear plant's no-fly zone. *Euro News.* https://www.euronews.com/2018/07/03/greenpeace-activists-pilot-and-crash-drone-into-french-nuclear-plant-s-no-fly-zone

Hoenig, M. (2014). Hezbollah and the Use of Drones as a Weapon of Terrorism. *Public Interest Report, 67*(2), 1–5. https://uploads.fas.org/2014/06/Hezbollah-Drones-Spring-2014.pdf

International Atomic Energy Agency. (2011). *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (pp. 1–100). IAEA. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

International Atomic Energy Agency. (2013a). *Nuclear and Other Radioactive Material out of Regulatory Control - IAEA Nuclear Security Series No. 21*. IAEA.

International Atomic Energy Agency. (2013b). *Objective and Essential Elements of a State's Nuclear Security Regime.* IAEA. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1590_web.pdf

International Atomic Energy Agency. (2022). *IAEA Nuclear Safety and Security Glossary*. IAEA.

Jalil, G. Y. (2023). Pakistan's Nuclear Security: *A Journey of Excellence (M. Q. Mustafa, Ed.). Institute of Strategic Studies*. https://issi.org.pk/wp-content/uploads/2023/08/IB_Ghazala_Aug_30_2023.pdf

Johnson, J. (2020). Artificial Intelligence in Nuclear Warfare: A Perfect Storm of Instability? *The Washington Quarterly, 43*(2), 197–211. https://doi.org/10.1080/01636600x.2020.1770968

Johnson, J. (2023). *AI and the Bomb: Nuclear Strategy and Risk in the Digital Age.* Oxford University Press.

Kallenborn, Z., & Bleek, P. C. (2018). Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons. *The Nonproliferation Review, 25*(5-6), 523–543. https://doi.org/10.1080/10736700.2018.1546902

Khan, P. (2021). Building a Bilateral Framework for Cybersecurity in South Asia. *In Nuclear Security in South Asia: Regional Views on Prospects and Priorities* (pp. 27–33). Stimson Centre.

Koehler, D. (2019). The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. *CTC Sentinel, 12*(11), 14–20. https://ctc.westpoint.edu/halle-germany-synagogue-attack-evolution-far-right-terror-threat/

Krane, J. (2020). Security amid Instability: Oil Markets and Attacks in the Persian Gulf. *Georgetown Journal of International Affairs, 21*(1), 120–128. https://doi.org/10.1353/gia.2020.0010

Lawrence, C. (2019). Heralds of global transparency: Remote sensing, nuclear fuel-cycle facilities, and the modularity of imagination. *Social Studies of Science, 50*(4), 508–541. https://doi.org/10.1177/0306312719879769

Lupovici, A. (2021). The dual-use security dilemma and the social construction of insecurity. *Contemporary Security Policy, 42*(3), 1–29. https://doi.org/10.1080/13523260.2020.1866845

Martin, P. G., Tomkinson, N. G., & Scott, T. B. (2017). The future of nuclear security: Commitments and actions – Power generation and stewardship in the 21st century. E*nergy Policy, 110,* 325–330. https://doi.org/10.1016/j.enpol.2017.08.038

Ministry of Foreign Affairs. (2016). *Pakistan's National Statement: Nuclear Security Summit Washington.* https://mofa.gov.pk/pakistans-national-statement-nuclear-security-summit-washington-31-march-1-april-2016

Ministry of Foreign Affairs Government of Pakistan. (2023, January 1). *Annual Exchange of Lists of Nuclear Installations and Facilities between Pakistan and India.* https://mofa.gov.pk/annual-exchange-of-lists-of-nuclear-installations-and-facilities-between-pakistan-and-india

Mohsan, S. A. H., Khan, M. A., Noor, F., Ullah, I., & Alsharif, M. H. (2022). Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review. *Drones, 6*(6), 147. https://doi.org/10.3390/drones6060147

Naseer, R., Amin, M., & Shaheen, K. (2020). Cyber Security Challenges in South Asia and Room for Cyber Diplomacy. *NDU Journal, 34,* 97–114.

Noor, S. (2023). Assessing Nuclear Security Risks in Pakistan. *International Journal of Nuclear Security, 8*(1). https://doi.org/10.7290//ijns088924

Nuclear Threat Initiative. (2023). *The 2023 NTI Nuclear Security Index: Falling Short in a Dangerous World.* NTI. https://www.ntiindex.org/wp-content/uploads/2023/07/2023_NTI-Index_Report.pdf

Onderco, M., & Zutt, M. (2021). Emerging technology and nuclear security: What does the wisdom of the crowd tell us? *Contemporary Security Policy, 42*(3), 286–311. https://doi.org/10.1080/13523260.2021.1928963

Pakistan Atomic Energy Commission. (n.d.-a). *Cancer Hospitals.* https://paec.gov.pk/Medical/

Pakistan Atomic Energy Commission. (n.d.-b). *Nuclear Power: A Viable Option for Electricity Generation*. https://paec.gov.pk/NuclearPower/

Pluff, A., & Nair, S. (2023). "*Don't Blame the Robots" – Artificial Intelligence Bias & Implications for Nuclear Security.* Stimson Centre. https://www.jstor.org/stable/resrep51827

PNRA. (2020). *20 Years of PNRA, 2001-2020.* https://www.pnra.org/upload/pnrarpt/PNRA%20Report%202020.pdf

Roth, N., Earnhardt, R., & Andrews, I. (2021). *A Multilevel Approach to Addressing Emerging Technologies in Nuclear Security.* Stimson Centre. https://www.stimson.org/wp-content/uploads/2021/10/a430.pdf

Rotolo, D., Hicks, D., & Martin, B. (2015). What is an Emerging Technology? *Research Policy, 44*(10), 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Saman, C. (2022). Pakistan's Nuclear Security Regime: Potential Threats, Risk Assessment and Risk Management for Safe Future. *NDU Journal, 34*, 115–130. https://ndujournal.ndu.edu.pk/site/article/view/65/50

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf

Shubayr, N. (2024). Nuclear security measures: A review of selected emerging technologies and strategies. *Journal of Radiation Research and Applied Sciences, 17*(1), 100814. https://doi.org/10.1016/j.jrras.2023.100814

Siddiqui, Z. H., & Qureshi, I. H. (2005). Nuclear Power in Pakistan. *The Nucleus, 42*(1-2), 63–66. http://thenucleuspak.org.pk/index.php/Nucleus/article/view/1056/709

Steitz, C., & Auchard, E. (2016, April 27). German nuclear plant infected with computer viruses, operator says. *Reuters.* https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS/

Volpe, T. A. (2019). Dual-use distinguishability: How 3D-printing shapes the security dilemma for nuclear programs. *Journal of Strategic Studies, 42*(6), 814–840. https://doi.org/10.1080/01402390.2019.1627210

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival, 64*(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193

Yamin, B. T. (2008). Pakistan's Nuclear Policy & Doctrine Ten Years Hence – Where do we Go from Here? *Margalla Papers, 12*(2), 13–42.

Yemen's Houthis claim drone attack on refinery in Saudi capital. (2022, March 11). *Middle East Monitor.* https://www.middleeastmonitor.com/20220311-yemens-houthis-claim-drone-attack-on-refinery-in-saudi-capital/