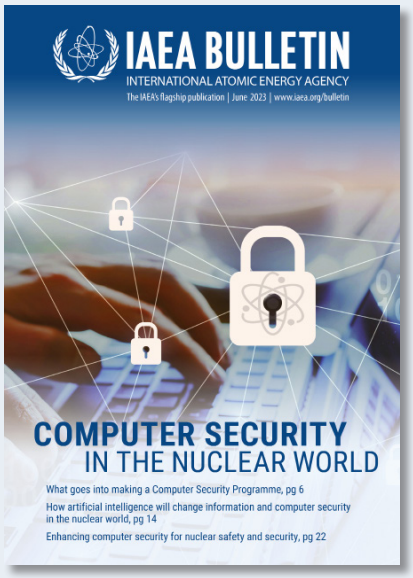
IAEA BULLETIN

INTERNATIONAL ATOMIC ENERGY AGENCY

The IAEA's flagship publication | June 2023 | www.iaea.org/bulletin

COMPUTER SECURITY IN THE NUCLEAR WORLD



IAEA BULLETIN
is produced by the
Office of Public Information
and Communication (OPIC)
International Atomic Energy Agency
Vienna International Centre
PO Box 100, 1400 Vienna, Austria
Phone: (43-1) 2600-0
iaeabulletin@iaea.org

Managing Editor: Emma Midgley
Design & Production: Ritu Kenn

IAEA BULLETIN is available online at
www.iaea.org/**bulletin**

Extracts from the IAEA material contained in the IAEA Bulletin may be freely used elsewhere provided acknowledgement of their source is made. If the attribution indicates that the author is not an IAEA staff member, permission to republish other than for the use of review must be sought from the author or originating organization.

Views expressed in any signed article appearing in the IAEA Bulletin do not necessarily represent those of the International Atomic Energy Agency and the IAEA accepts no responsibility for them.

Cover:
(Adobestock.com)

Follow us on

IAEA

The International Atomic Energy Agency's mission is to help prevent the spread of nuclear weapons and to help all countries — especially in the developing world — benefit from the peaceful, safe and secure use of nuclear science and technology.

Established as an autonomous organization under the United Nations in 1957, the IAEA is the only organization within the UN system with expertise in nuclear technologies. The IAEA's unique specialist laboratories help transfer knowledge and expertise to IAEA Member States in areas such as human health, food, water, industry and the environment.

The IAEA also serves as the global platform for strengthening nuclear security. The IAEA has established the Nuclear Security Series of international consensus guidance publications on nuclear security. The IAEA's work also focuses on helping to minimize the risk of nuclear and other radioactive material falling into the hands of terrorists and criminals, or of nuclear facilities being subjected to malicious acts.

The IAEA safety standards provide the fundamental principles, requirements and recommendations to ensure nuclear safety and reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from the harmful effects of ionizing radiation. The IAEA safety standards have been developed for all types of nuclear facilities and activities that serve peaceful purposes, as well as for protective actions to reduce existing radiation risks.

The IAEA also verifies through its inspection system that Member States comply with their commitments under the Nuclear Non-Proliferation Treaty and other non-proliferation agreements to use nuclear material and facilities only for peaceful purposes.

The IAEA's work is multi-faceted and engages a wide variety of partners at the national, regional and international levels. IAEA programmes and budgets are set through decisions of its policymaking bodies — the 35-member Board of Governors and the General Conference of all Member States.

The IAEA is headquartered at the Vienna International Centre. Field and liaison offices are located in Geneva, New York, Tokyo and Toronto. The IAEA operates scientific laboratories in Monaco, Seibersdorf and Vienna. In addition, the IAEA supports and provides funding to the Abdus Salam International Centre for Theoretical Physics, in Trieste, Italy.

The essential role of computer security in nuclear security and safety

By Rafael Mariano Grossi, Director General, IAEA

The pace of digital innovation is astonishing, with technologies such as artificial intelligence (AI) making game-changing strides even in the past few months. These advances will help us to improve digitally controlled operations and automation technologies at nuclear facilities, with the potential benefits of improved operational efficiency, reduced labour costs and better safety and security.

Advanced nuclear reactor designs, such as small modular reactors (SMRs) and microreactors, already include plans to use AI and machine learning (ML) to enable innovative features such as automation, remote supervisory control and maintenance, and shared control rooms. But digital innovations, such as AI and ML, also pose a threat. They require constant vigilance to ensure the integrity of sensitive assets and to protect information at nuclear and radiological facilities.

While gates and guards have always been used to ensure nuclear facilities are protected from sabotage or malicious actors, today we are becoming increasingly dependent on digital systems. Instrumentation and control systems at nuclear facilities are used for key safety and security applications. This improves efficiency but means we have to be especially vigilant in protecting these computer systems. Countries around the world are recognizing this as a priority.

The IAEA plays a unique role in fostering cooperation between countries and enabling the sharing of technological know-how and best practice in the adoption of rapidly developing technologies. At the same time, we advise countries on how to minimize and mitigate the accompanying potential vulnerabilities affecting computer security. In just the past two years, our global computer security assistance activities have increased by more than a quarter, with a particular focus on national-level support for computer security regulations/inspections and computer security exercises.

The IAEA has been responding to the nuclear security challenges of its Member States with a host of activities, including through the provision of guidance documents and training that enable them to put in place robust national information and computer security programmes. This guidance is also used as a benchmark for the assessment of a country's information and computer security programme during an International Physical Protection Advisory Service, known as IPPAS.

In addition, we are launching a school to train experts in drafting computer security regulations. Soon, many more countries will be able to access IAEA computer security training courses with the launch of an online virtual learning platform.

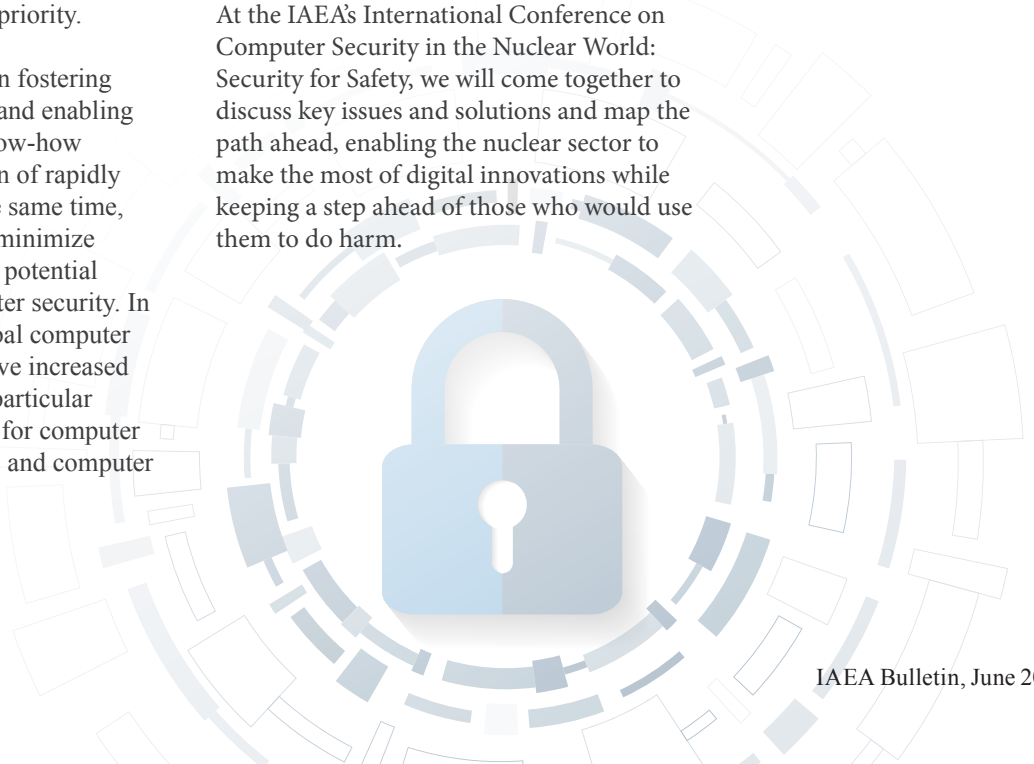
In parallel, the IAEA supports national and regional computer security exercises that raise awareness of the threat of cyberattacks and their potential impact on nuclear security. We foster cooperation between international experts and policymakers and enable accompanying research.

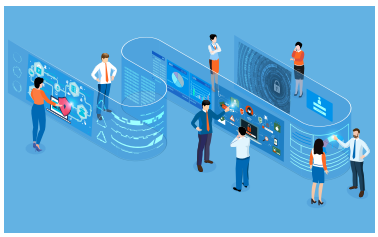
The IAEA's computer security activities are set to grow, as countries, including low and middle income countries, increasingly turn to nuclear technology to meet their priorities, including in clean energy, cancer care, nutrition and research.

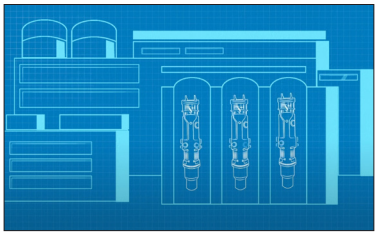
At the IAEA's International Conference on Computer Security in the Nuclear World: Security for Safety, we will come together to discuss key issues and solutions and map the path ahead, enabling the nuclear sector to make the most of digital innovations while keeping a step ahead of those who would use them to do harm.

"The IAEA's computer security activities are set to grow, as countries, including low and middle income countries, increasingly turn to nuclear technology to meet their priorities, including in clean energy, cancer care, nutrition and research."

— Rafael Mariano Grossi, Director General, IAEA







Q&A

WORLD VIEW

IAEA UPDATES

Addressing computer security threats

The evolution of the IAEA's assistance programme

By Vasiliki Tafili

The shift to digitally networked societies, where daily activities are interlinked with the help of computer-based systems, artificial intelligence (AI) and digital technologies, is having a huge impact on nuclear safety and security. The essential role of digital technologies in maintaining safety and security functions at facilities handling nuclear material or other radioactive material cannot be overstated.

"The anticipated significant growth in the use of peaceful nuclear applications, specifically nuclear power programmes, makes it imperative to consider information and computer security as an integral part of nuclear security."

— Elena Buglova, Director, Division of Nuclear Security, IAEA

"Computer-based systems and digital technologies are vital for facilities and associated activities where nuclear and other radioactive material is used," said Elena Buglova, Director of the IAEA's Division of Nuclear Security, emphasizing the need for all countries to implement computer security programmes and improve nuclear security defence in depth. "As technology advances, protecting the confidentiality, integrity and availability of sensitive information and assets requires continuous vigilance to prevent and mitigate risks, and a robust information and computer security programme."

The need for addressing computer security threats, malicious cyberattacks and any potential vulnerabilities that digital technologies may introduce, as well as the importance of computer security for nuclear security, was first identified in a nuclear security resolution adopted by the IAEA's General Conference at its 55th regular session in 2011. It noted the IAEA's efforts "to raise awareness of the growing threat of cyber attacks and their potential impact on nuclear security". This resolution also encouraged the IAEA to develop appropriate guidance documents, provide training courses, and host further expert meetings specific to cyber security at nuclear facilities to assist countries in protecting themselves against cyberattacks.

"Following up on the 2011 General Conference resolution, IAEA activities focused on improving computer security capabilities at the State and facility levels," said Buglova, adding that these activities were then included in the IAEA's subsequent Nuclear Security Plans, including the details for the current implementation of the IAEA computer security activities which are outlined in the Nuclear Security Plan 2022–2025.

How does the IAEA help countries to develop or improve their computer security?

The establishment of a robust and up-to-date computer security programme is a key element to guard countries against cyberattacks in all types of critical infrastructure. The IAEA has been agile in providing assistance to countries at all stages of developing national information and computer security programmes, including the provision of guidance documents and training.

Four IAEA Nuclear Security Series guidance publications and three additional technical publications provide guidance on information and computer security. The guidance can be used as the basis for the development of national computer security frameworks, including national strategies, as well as for computer security regulations and training.

A key principle of the IAEA's guidance is to preserve the critical functions at nuclear facilities by protecting information and computer-based systems to maintain a safe and secure environment for both the facilities and the materials. This is achieved by developing a computer security programme (see page 6); identifying nuclear security functions; using risk management to determine the potential consequences of compromised security; defining the level of computer security required for sensitive digital assets; and implementing a graded approach and defence in depth concepts in computer security. These elements should be designed and implemented in a way to prevent compromise, and to help increase the operator's ability to detect and respond to intrusions as well as to mitigate the potential impact of cyberattacks.

Upon countries' requests, the IAEA offers various training opportunities to a range of audiences. These audiences include

competent authorities, operators, vendors and other entities that may have responsibilities for computer security implementation. They could also benefit from the IAEA's expertise in conducting computer security exercises as part of the nuclear security programme.

In addition, four e-learning courses on computer security are freely accessible and available in Arabic, Chinese, English, French, Russian and Spanish on the IAEA's Cyber Learning Platform for Network Education and Training, and can be accessed by registration or via a NUCLEUS account. An innovative, new virtualized training platform will also be available soon (see page 12).

In parallel, the IAEA supports national or regional computer security exercises as part of its efforts to raise awareness of the threat of cyberattacks, and their potential impact on nuclear security. The exercises feature different scenarios in which sensitive information and computer-based systems are targeted directly or indirectly as part of an attack on both physical protection and electronic systems (see page 16).

Research complements the IAEA's computer security activities, mainly through the well-established mechanism of coordinated research projects. Coordinated research projects have been launched in recent years to advance the efforts of the global research community in information and computer security and increase the readiness for addressing emerging challenges and risks (see page 18).

What does the future hold?

The IAEA's computer security programme for nuclear security is constantly evolving. The reliance of small modular reactors and advanced reactors on advanced technologies and digital instrumentation, the anticipated impact of AI and the emergence of virtualized learning environments present challenges and areas for expanded support to States (see page 14).

"We are witnessing an increasingly heightened awareness of the potential or actual implications for nuclear safety and security among countries, regulatory bodies, operators and other stakeholders," said Buglova. "The anticipated significant growth in the use of peaceful nuclear applications, specifically nuclear power programmes, makes it imperative to consider information and computer security as an integral part of nuclear security."

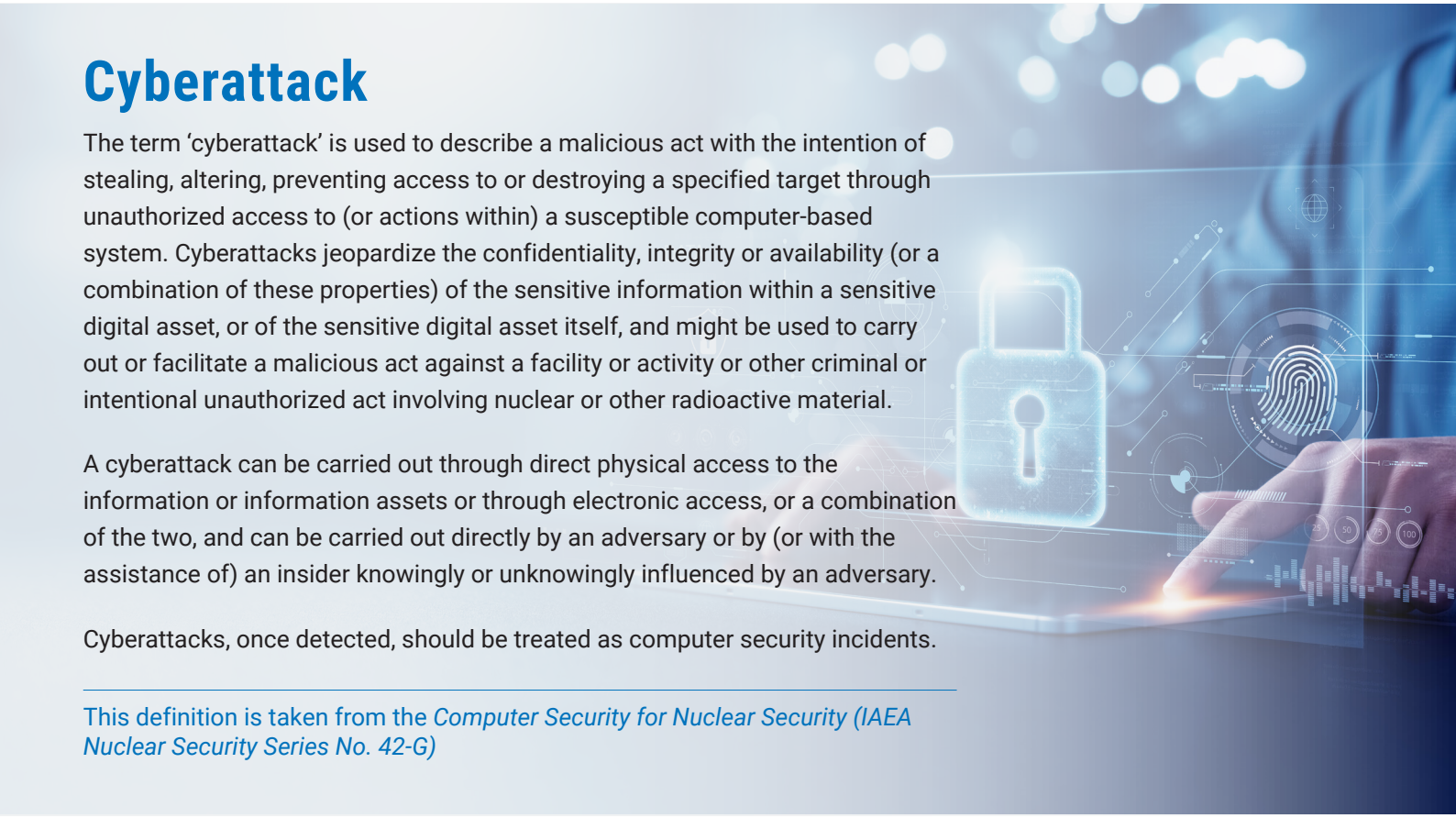
Cyberattack

The term 'cyberattack' is used to describe a malicious act with the intention of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible computer-based system. Cyberattacks jeopardize the confidentiality, integrity or availability (or a combination of these properties) of the sensitive information within a sensitive digital asset, or of the sensitive digital asset itself, and might be used to carry out or facilitate a malicious act against a facility or activity or other criminal or intentional unauthorized act involving nuclear or other radioactive material.

A cyberattack can be carried out through direct physical access to the information or information assets or through electronic access, or a combination of the two, and can be carried out directly by an adversary or by (or with the assistance of) an insider knowingly or unknowingly influenced by an adversary.

Cyberattacks, once detected, should be treated as computer security incidents.

This definition is taken from the *Computer Security for Nuclear Security (IAEA Nuclear Security Series No. 42-G)*



What goes into making a computer security programme

By Vasiliki Tafili and Trent Nelson

Facilities handling nuclear material or other radioactive material, and undertaking associated activities, are critical infrastructure which require high levels of safety and security. By taking a comprehensive and proactive approach to computer security, organizations can protect the sensitive information assets and computer-based systems in these facilities against compromise. The foundation of the IAEA-recommended approach to computer security lies in States establishing requirements for national strategy or policy; and enabling confidentiality and the protection of sensitive information and computing systems related to physical protection, nuclear safety, and nuclear material accounting and control. These requirements can also take the form of national regulations that provide for the development and implementation of a computer security programme (CSP)*.

A CSP is an overarching framework that includes key elements of an effective plan for implementing computer security policies and procedures that will be used throughout the lifetime of a nuclear facility or facility with radioactive sources. It aims to protect sensitive information assets and computer-based systems critical to maintaining safety and security functions from cyberthreats in order to mitigate the impact of cyberattacks.

National strategy

A comprehensive and effective computer security strategy requires a systematic approach that integrates various elements, including regulations, programmes, security protective measures and response capabilities to sustain national nuclear security regimes.

Regulations

Effective regulations provide a legal framework for protecting sensitive computer-based systems and ensure that organizations have established CSPs with the proper controls in place.

Key elements of CSPs:

Roles and responsibilities

Organizational roles and responsibilities with accountability are vital for effective management, especially in the case of critical infrastructure. Awareness of the organizational hierarchy and clear lines of authority and reporting structure are necessary to instill efficient and effective collaboration and synergy within CSPs.

Risk, vulnerability and compliance management

Computer security risk management involves evaluating vulnerabilities and potential consequences of sensitive digital assets and computer-based systems to implement computer security controls using a graded approach to defend against cyberattacks. The level of security measures applied should be commensurate with the level of risk associated with the information and/or computer-based systems being protected. By considering the consequence of the vulnerability or threat, organizations can determine the level of security measures needed to mitigate the risk.

Security design and management

Computer security design is a critical aspect of protecting against cyberthreats. Fundamental design principles include a graded approach and defence in depth, where multiple layers of zoned security controls are implemented to prevent and mitigate attacks. Requirements for security must also be incorporated throughout the system development life cycle including third-party organizations being governed by clear policies and agreements to ensure security measures are consistent and effective.

Digital assets management

Effective computer security relies on a systematic process to identify a comprehensive list of all facility functions, assets, and systems including sensitive digital assets that are essential to protect nuclear operations or to maintain safe and secure use of nuclear and other radioactive material. Such a list also provides data flow and interdependencies that are significant to the organization to support access controls, backups and other security measures to protect these assets from sabotage or theft.

Security procedures

Operational nuclear security policies and procedures provide the direction with accountability to prevent of theft, sabotage, or unauthorized use of nuclear material and facilities. These policies ensure that access to sensitive information and assets is tightly controlled, and that individuals with access are screened and trained appropriately.

Personnel management

Trustworthiness, awareness, and training are critical for personnel management in the nuclear industry. Evaluations of trustworthiness should be conducted to ensure that personnel are reliable, competent, and free from any conflicts of interest that could compromise safety or security. Maintaining qualified and trustworthy personnel is critical to ensure nuclear safety and security.

**More details are included in IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities.*

Beyond physical protection

How the International Physical Protection Advisory Service (IPPAS) facilitates the enhancement of computer security

By Vasiliki Tafili

For almost thirty years, the IAEA's International Physical Protection Advisory Service (IPPAS) has been used by countries for peer review to ensure the physical protection of all types of facilities where nuclear and other radioactive materials are used, including nuclear power plants and hospital radiotherapy units. However, owing to advances in technology, digital systems are now at the heart of operations for these facilities. This has led to many new nuclear security challenges.

"Physical protection against the theft, sabotage or unauthorized use of nuclear and other radioactive material cannot be ensured without computer security measures. By inviting an IPPAS mission, countries can benefit from advice on what can be improved, and how."

— Heather Looney, Head, Nuclear Security of Materials and Facilities Section, Division of Nuclear Security, IAEA

In response to the real threat of cyberattacks on facilities, including nuclear facilities, information and computer security for physical protection was added to the scope of IPPAS in 2012. Since then, countries have increasingly requested this module as part of the IPPAS review, in order to support their work in counteracting cybersecurity threats.

As a core component of the IAEA's nuclear security programme, IPPAS is an advisory service that reviews a country's existing practices against relevant international instruments and IAEA nuclear security guidance. It assists countries, upon request, in strengthening their national nuclear security regimes, systems and measures by providing advice on implementing international legal instruments.

"Twenty-seven years after the first IPPAS mission, the service has evolved to address modern challenges and needs," said Heather Looney, Head of the Nuclear Security of Materials and Facilities Section at the IAEA's Division of Nuclear Security. "Physical protection against the theft, sabotage or unauthorized use of nuclear and other radioactive material cannot be ensured without computer security measures. By inviting an IPPAS mission, countries can benefit from advice on what can be improved, and how," she added.

IPPAS follows a modular approach and offers five modules, which cover the following: a national review of the nuclear security regime for nuclear material and nuclear facilities; a review of security systems and measures at nuclear facilities; a review of the transport security for material; a review of the security of radioactive material, associated facilities and activities; and a review on information and computer security. In total, 97 IPPAS missions have been conducted to date since the first one in 1996, and 22 countries have requested the inclusion of the information and computer security module in the IPPAS review.

What should a country expect during the information and computer security assessment?

As a first step, an IPPAS team of international nuclear security experts examines how national policies relating to information and computer security programmes have been set up and managed. The team will then look at the legislative and regulatory framework by comparing the procedures and practices in place in the country with the obligations specified under the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment, as well as with the guidance provided in relevant IAEA Nuclear Security Series publications. In this way, they are able to determine whether countries have the necessary policies and procedures in place to enable adequate computer security in critical nuclear and radiological facilities.

At the facility level, the computer security review will look at computer security management, computer security programme (See page 6), access controls, defensive computer security architecture, and the detection of and response to computer security events. The team may also assess cross-cutting areas, such as risk management, graded approaches, nuclear security culture and human resource management.

Japan hosted an IPPAS mission and its follow-up mission in 2015 and 2018, respectively. "It was a valuable experience

Since 1996, the IAEA's International Physical Protection Advisory Service (IPPAS) has been helping countries to identify ways to strengthen the protection of nuclear materials and facilities. (Photo: IAEA)

for Japan to review the current status of computer security measures and to promote their enhancement based on the reviewers' suggestions," said Hiroyuki Sugawara, Director for International Nuclear Security in the Division of Nuclear Security at Japan's Nuclear Regulation Authority (NRA). "In response to the IPPAS findings, we decided to strengthen the computer security measures and increase the number of inspectors with expertise in the field. In addition, the NRA incorporated computer security threats in its national threat assessment and required licensees to take robust computer security measures, as well as to enhance the content of their computer security plans by incorporating countermeasures against cyberattacks."

In France, following an IPPAS mission in 2018, the visibility of computer security was strengthened in the national nuclear security framework. "The IPPAS mission required a strong commitment from the various stakeholders giving the opportunity for France to consolidate its nuclear security regime and to stimulate its implementation," said Frédéric Boën, Computer Security Project Leader in the Ministry of Energy Transition, Defense and Security Directorate, Nuclear Security Office. "The staff dedicated to computer security was increased and regulatory guidelines were established in line with the international standards and the IAEA nuclear security guidance."

The IAEA has maintained the IPPAS Good Practices Database since 2016 to share the findings of such missions with the international nuclear security community, thus enhancing the impact of the assistance offered by the IAEA to countries around the world. "Maintaining this database and sharing such examples extends the benefits of IPPAS missions beyond the host country to the international nuclear security community, and multiplies the impact of the assistance offered by the IAEA to its Member States," said Looney.

The majority of the State-level good practices relate to nuclear security management, which provides the foundation for computer security and coordination. In addition, there are 40 good practices relating to computer security both at State and facility level that are accessible for IAEA Member States through designated points of contact.

The IAEA continues to support countries in enhancing their national nuclear security regimes; demand from countries to receive IPPAS missions in 2023 and in 2024 remains high.

IAEA assists African countries in developing computer security regulations

By Andrea Rahandini

Africa's demand for radioisotopes is expected to grow in the coming years as more countries scale up their peaceful use of nuclear technology. Increasing rates of cancer have led to greater demand for radiotherapy, radiology, and nuclear medicine. Reliance on nuclear applications for industry, agriculture, and science has grown. This has created a demand for a heightened production of radioisotopes in research reactors. These essential reactors operate on computer-based systems which could be vulnerable to cyber-attacks. Like nuclear power plants, research reactors are nuclear facilities which require similar protection plans to prevent, mitigate and respond to potential malicious attacks. Protecting all types of nuclear facilities from such potential attacks is an essential element of the safe and secure use of nuclear technology in Africa.

The course helped us to develop and implement a computer security programme in order to protect the facility's sensitive information, and sensitive digital assets vulnerable to cyber-attacks."

—Nadia M. Nawwar, Computer Engineer, Radioisotope Production Facility, Egyptian Atomic Energy Authority

Working to counter these threats, many countries in Africa are learning from experience in Egypt, Ghana and Nigeria, each of which owns and operates a nuclear research reactor. With the support of the IAEA, these three countries are developing and strengthening computer security regulations and implementing programmes to properly secure their facilities against malicious computer-based acts that could potentially have an impact on the nuclear security and safety of the facilities.

"Computer security continues to grow in importance as digital technologies and computer-based systems are integrated in nuclear safety, nuclear security, and operational aspects of nuclear and other radioactive material facilities and operations," said Trent Nelson, Senior Information and Computer Security Officer at the IAEA's Division of Nuclear Security. "The IAEA works with countries in Africa to develop, review and enhance computer security regulations."

In Egypt, the IAEA works with the Egyptian Nuclear and Radiological Regulatory Authority (ENRRA) to review existing computer security regulations and address potential gaps in regulatory aspects. A national training course was organized in 2022 to develop national capacities for conducting computer security inspections in nuclear facilities. Using the IAEA Nuclear Security guidance and techniques available to inspectors, the course equipped the participants with the knowledge and practical expertise to better assess the effectiveness of computer security at nuclear and radiological facilities.

Nadia M. Nawwar, computer engineer at the Radioisotope Production Facility (RPF) in the Egyptian Atomic Energy Authority (EAEA), was one of the 22 participants in this course. "I learned how the regulatory body performs computer security inspections and what are the necessary computer security arrangements that the operator needs to have in place," she said. "Since taking part in the course, we have been able to review and validate the Computer Security Regulation Elements more effectively. The course helped us to develop and implement a computer security programme in order to protect the facility's sensitive information, and sensitive digital assets vulnerable to cyber-attacks."

In Ghana, the IAEA conducted an expert mission in April 2023 to assess the Ghana Nuclear Regulatory Authority's (GNRA) current national computer security regulations and inspections programme.

"The development of computer security in Ghana posed several challenges, including the absence of local technical knowledge on the subject matter, the merging of the legal issues and technical know-how, and how to manage the resources required," said Nelson Kodzotse Agbemava, Team Leader

of the Nuclear Cyber Security Section of GNRA. “During the regulatory development process, expert review support was sought from the IAEA and other countries to ensure a comprehensive and systematic approach to computer security.”

Similarly, the IAEA also conducted an expert mission in Nigeria in October 2022. “The need for an effective legislative and regulatory framework for computer security was identified in 2019 by the IAEA-led Integrated Nuclear Security Support Plan (INSSP) review in the country,” said Ethel Ofoegbu, Chief Regulatory Officer from the Nigerian Nuclear Regulatory Authority (NNRA). “Consequently, the IAEA assessed the national computer security regulations, identified gaps and provided necessary advice. One of the outcomes was the development of the draft Nigerian Computer Security Regulations for Nuclear and Radiological Facilities and Activities.” Currently, Nigeria is reviewing the draft regulations and is planning a training course on computer inspections.

Taking into consideration the growing number of assistance requests from countries, the IAEA is developing a technical document to help countries establish the key elements of computer security regulations. The IAEA is also ready to assist many more countries draft regulations in the area of computer security when the IAEA Computer Security Regulation Elements Drafting School is launched in August 2023. The School aims to help multiple countries simultaneously develop their specific national computer security regulations, rather than the IAEA assisting individual countries one at a time. After the initial workshop in August, the School will be organized semi-annually across all regions. Together, participants will have the opportunity to draft their national strategy for computer security - the regulatory foundation of a robust computer security programme.

An IAEA Computer Security Regulation Elements Drafting School will be launched in August 2023, with the aim of helping countries develop their national computer security regulations.

Innovation in virtual computer security training for nuclear and radiological facilities

By Anjarika Strohal

The omnipresent and ever-increasing digital technology trends of today are quickly and significantly changing our lives. Today's critical infrastructures, which include nuclear power and other peaceful uses of nuclear technology, are heavily reliant on digital technologies for their smooth and reliable operation. The promises of rapidly evolving new technologies, such as artificial intelligence, for solving problems and improving digitally controlled operations will likely be helpful in improving nuclear applications. As such, they are being used and considered today in advanced reactor designs.

Unfortunately, while these digital technologies do bring many benefits, they may also introduce many potential and unknown vulnerabilities. This is due to the ever-present threat of cyber intrusions or malicious cyberattacks on nuclear facilities that might exploit these same technologies.

The number and range of increasingly sophisticated cyberattacks have created urgent demand within the nuclear industry for computer security training for nuclear and radiological facilities. In order to help meet this demand, the IAEA has developed a series of training courses on topics from computer security fundamentals to more advanced computer security for instrumentation and control systems.

In delivering these customized, sophisticated and complex training courses, which feature hands-on experiential learning, the IAEA identified the need for a simple online platform that could standardize the curriculum and allow for its broader and more universal use by training entities — without in-person IAEA assistance. The COVID-19 pandemic travel restrictions and widespread use of virtual technologies further highlighted this need and accelerated the development of the platform.

The virtual training tool, which is called 'Learners', aims to provide flexible and engaging computer security training courses to the nuclear community by offering training materials and the experience of hands-on exercises delivered in a virtual environment. Participants need only a computer and a reliable internet connection to access all necessary course materials. "The new platform is expected to play a pivotal role in improving computer security awareness and training for nuclear security, building a stronger community of experts, and helping to enhance safety and security in nuclear facilities and those associated with radioactive material," said Elena Buglova, Director of the IAEA Division of Nuclear Security.

From June 2023, the IAEA will make the Learners platform available globally in order to enhance computer security at nuclear facilities, as well as at facilities and for activities involving radioactive sources.

Computer Security Training
and other activities

- **194** Total number of events
- **120** Total States supported
- **2676** Total participants
- **3** Coordinated Research Projects
- **14** Expert meetings
- **24** Training courses
- **12** Technical meeting or workshops
- **10** Webinars
- **66** Supporting consultancy meetings (Training development, guidance, preparatory meetings)

The Austrian Institute of Technology (AIT) — an IAEA Collaborating Centre for information and computer security for nuclear security — partnered with the IAEA to create the Learners platform.

"The virtual learning environment offers immense value to increase operational as well as strategic capabilities by supporting various training purposes," said Helmut Leopold, Head of the Center for Digital Safety and Security at the AIT. "By simulating real environments, the platform enables learners to acquire practical skills and experience that are essential for effective nuclear security management."

Learning to enhance computer security

The IAEA Learners platform is available on request to enhance nuclear security training. The platform is designed to be user-friendly for an international audience and offers multilingual support. It has various features, such as guided exercises, immediate feedback, presentation integration and multiscreen support. These make the platform adaptable and accessible for use by training organizations and direct users.

Learners is designed as a platform for the development, delivery and use of interactive simulated environments, and has been built using open-source technologies. Additional modules include standardized approaches to computing platforms, infrastructure provisioning and software provisioning, which enable easy sharing and knowledge exchange with existing IAEA training providers and other organizations intending to use the platform.

Twelve hands-on exercises have been created and organized into six thematic areas based on the IAEA's nuclear security guidance on computer security. "By using virtualized environments representative of real-world facilities, the Learners platform reinforces practical skills development and is supporting a more equitable access to knowledge and skills," Buglova added.

The Learners platform is one facet of the IAEA's work to raise awareness, strengthen cooperation and provide States with support to address growing cybersecurity threats in the nuclear sector. Capacity-building activities have been offered to over 120 countries in the past five years. Furthermore, tailored support through expert missions; national, regional and international training courses; technical meetings; and webinars have fostered active collaboration, knowledge sharing and skills development. In addition, the IAEA supports countries in organizing large-scale cybersecurity exercises.

A hands-on training and demonstration centre

Moving forward, it is crucial to continue investing in such capacity-building initiatives to ensure the highest standards of nuclear security worldwide. The IAEA's state-of-the-art Nuclear Security Training and Demonstration Centre (NSTDC) will open in the second half of 2023 to help strengthen countries' abilities to tackle nuclear terrorism through hands-on training experiences. The innovative training courses offered at the NSTDC will incorporate topics related to computer security and will include scenarios for cyberattacks that could potentially target nuclear facilities or facilities and activities involving radioactive sources.

"By simulating real environments, the platform enables learners to acquire practical skills and experience that are essential for effective nuclear security management."

— Helmut Leopold, Head, Center for Digital Safety and Security, AIT

How artificial intelligence will change information and computer security in the nuclear world

By Mitchell Hewes

Artificial intelligence (AI) and machine learning technologies could potentially revolutionize the world, ushering in unprecedented progress and innovation by transforming how we create, consume and use information. As AI technologies become increasingly sophisticated, they will transform industries, streamline processes and may even impact how we live our lives. The nuclear sector is no exception, and the benefits of AI can be expected in many processes and operations in nuclear and radiological facilities.

"It will not replace the workforce, but rather establish resources and insights that will make early detection and response in computer security realistically achievable."

— Fan Zhang, Assistant Professor, Georgia Institute of Technology, USA

At the same time, AI's rapid advancement also brings with it a multitude of risks. Malicious actors may use AI to launch more advanced and targeted attacks or exploit it to compromise the integrity of networks, systems and sensitive information in nuclear and radiological facilities.

Benefits for information and computer security

The IAEA is preparing for the transformations brought about by AI by fostering international cooperation in the area to ensure all countries can benefit from the opportunities while also preparing to mitigate the risks. Through mechanisms such as Technical Meetings and coordinated research projects (CRPs), the IAEA is supporting the development, awareness and application of AI techniques, as well as countermeasures and defence against malicious actors.

Perhaps the most significant advantage of AI in information and computer security is the reduced reliance on human analysis and intervention. AI-enabled systems can operate 24/7 to monitor networks and systems for threats. By automating these tasks, nuclear security professionals have the time to focus on more strategic tasks and respond more efficiently to incidents when they occur.

"The adaptive learning capabilities of AI can be harnessed to enhance information and computer security by swiftly identifying threats and automatically providing human experts with the information they need to coordinate response activities," said Fan Zhang, an assistant professor at the Georgia Institute of Technology in the United States of America, who participated in a CRP to support research in strengthening computer security. "It will not replace the workforce, but rather establish resources and insights that will make early detection and response in computer security realistically achievable."

By leveraging advanced machine learning algorithms, AI may also help nuclear and radiological facilities sharpen their defences against cyberattacks by identifying anomalous data in computer systems. AI-supported security systems can continuously monitor and analyse vast amounts of data to determine if any activity is anomalous to the facility's normal operation. Cyberattacks may feed fake data to maliciously mislead the operators of nuclear facilities. In this case, AI-supported systems can be harnessed to alert those running a nuclear power plant to even the slightest variation from normal operations. By offering heightened situational awareness, AI also allows for the early detection of criminal actions and prompts the necessary incident response.

Challenges to be addressed

The benefits offered by AI in nuclear and radiological facilities depend greatly on how the AI system has been trained. AI is only as intelligent as the training data it is working with, and it can be manipulated into giving false readings and results if it does not have the correct inputs. This remains a significant barrier to its use for nuclear security.
Even with the recent advancements in AI technology, using it as a replacement for a human is not feasible. Physical protection, material accounting and control and direct measurements — essential activities for ensuring nuclear security — require a human input.

An additional challenge with AI with regard to nuclear security is understanding how and why an AI model has made a particular decision or prediction. "Transparency and explainability —where humans can understand the reasoning behind decisions or predictions made by the AI — are among the most significant problems with AI models. It is often challenging to understand how these models arrive at their conclusions, making it difficult to trust and ensure the integrity of their output," said Scott Purvis, Head of the Information Management Section in the IAEA's Division of Nuclear Security. "This becomes particularly problematic when these models replace sensors providing direct measurements and human experience gained with the unique characteristics of each facility. It becomes impractical to place any assurance in the system's integrity unless there is a prior comprehensive advanced understanding of the AI algorithms to recognize how and why decisions are made."

The IAEA's guidance on computer security for nuclear security includes best practices on human checks and balances to guide facilities' awareness of which processes can be automated by AI and which should continue to have human oversight, at least until the risks of this rapidly developing technology are known. They also provide an essential resource that can enable countries to put important computer security measures in place to detect, prevent and respond to cyberattacks.

Additionally, a CRP was developed by the IAEA to support research in strengthening computer security. Entitled "Enhancing Computer Security Incident Analysis at Nuclear Facilities", the CRP brought together representatives of 13 countries to work on improving computer security capabilities, including AI techniques, at nuclear facilities to detect anomalies indicating targeted cyberattacks.

The race to adopt AI technologies

AI has shown its potential to benefit people who use nuclear technology for peaceful ends. As its use to enhance processes and operations in nuclear and radiological facilities expands, so too must the awareness of the risks associated with its broader adoption. Organizations must maintain a robust computer security programme to assure nuclear security while benefiting from AI.

AI may also help nuclear and radiological facilities sharpen their defences against cyberattacks by identifying anomalous data in computer systems.
(Image: AdobeStock)

Doing so requires a fundamental paradigm shift in how trust and sensitivity is viewed. Every potential point of failure in a system must be considered, even those unrelated to its design. Malicious actors can leverage AI to create more sophisticated malware, automate cyberattacks, exploit biases and vulnerabilities within the models, or bypass security measures by mimicking legitimate user behaviour. This 'arms race' between defenders and attackers will require constant innovation and adaptation.

Greater use of AI technology to enhance computer security measures at nuclear facilities could offer significant benefits, including enhanced threat detection, proactive security measures, reduced reliance on human intervention and improved incident response. By embracing the benefits of AI while addressing its risks, organizations can significantly enhance their computer security in the face of evolving cyberthreats.

How computer security exercises help increase readiness for response to cyberattacks in nuclear security

By Emma Midgley

"It is crucial to develop policies, defined roles and responsibilities, and detailed procedures for a response to computer security incidents before an incident occurs."

— Trent Nelson, Senior Information and Computer Security Officer, Division of Nuclear Security, IAEA

Historically, nuclear facilities have focused on securing their nuclear material against malevolent attacks by putting in place physical protection measures such as guns, guards and gates. These measures are still used to successfully build fortresses around nuclear facilities, preventing theft of nuclear or other radioactive material, sabotage or unauthorized access to control systems. However, in recent decades, the threat of cyberattacks has escalated in our increasingly digital world. Any country, even those with the most advanced nuclear power and research programmes, can be vulnerable to attack. The development of national frameworks for computer security and response against cyberthreats to nuclear facilities have become necessary. Through large-scale exercises, the IAEA assists countries in improving their protection against cyberattacks and helps them improve their detection of and response strategies to cyberattacks against nuclear facilities.

The IAEA has developed computer security exercises for nuclear power plants and radiological facilities, which have been carried out at a national level around the world. These exercises enable countries to practise and prepare their response to the worst-case scenario of a breach of cybersecurity at a nuclear facility. The theoretical scenarios can pinpoint weaknesses in policies, procedures and processes; and identify gaps that need to be filled through mitigation techniques, capacity building and/or organizational change. As well as assisting States in carrying out large-scale exercises to test computer security at nuclear facilities, the IAEA's nuclear security guidance on computer security also provide an essential resource that can enable countries to put important computer security measures in place to detect, prevent and respond to cyberattacks.

"It is crucial to develop policies, defined roles and responsibilities, and detailed procedures for a response to computer security incidents before an incident occurs," said Trent Nelson, Senior Information and Computer Security Officer in the IAEA's Division of Nuclear Security. "That is where the IAEA can assist in many aspects: from exercises and guidance, to sharing best practices and procedures to ensure effective communication and robust security protection."

Factors that make nuclear facilities vulnerable to cyberattacks include people, the complexity of the supply chain and sensitive information shared among multiple stakeholders who use the computer-based systems that support nuclear functions.

"Consider an attack that compromises a supplier and falsifies a work order, causing a trusted technician with authorized access to make a subtly incorrect action," said Trent Nelson. "This is just one way malicious actors could find ways to bypass security systems."

An important element in reducing the potential impact of any cyberattack is awareness and effective communication between stakeholders, as any one of these groups, or individuals within these groups, may be targeted by malicious actors. There are four key players when it comes to the defence of nuclear facilities: the regulatory body; the operator of the facility; technical support organizations (computer security incident response teams (CSIRTs) and/or computer security operations centres); and third-party organizations, such as vendors and support organizations. Carrying out exercises is a good way to test communications, reporting and notifications between stakeholders, and to verify and validate the safety and security of organizational structures.

An important element in reducing the potential impact of any cyberattack is awareness and effective communication between stakeholders.
(Image: AdobeStock)

While in an ideal scenario cyber attackers would find it impossible to penetrate computer security systems at nuclear facilities, the evolving nature of malicious actors, and the fallibility of human nature, means it is almost impossible to predict how the next large-scale attack will unfold. Therefore, the timely detection of attacks is key. In a recent exercise in Slovenia, a theoretical cyberattack helped to verify and validate detection and response capabilities to defend against cyberattacks.

"Computer security is not a project or a process, but rather a lifelong journey that requires continuous effort, attention and practice," said Samo Tomažič, Head of the Cyber Security Division of the Slovenian Nuclear Safety Administration. "Exercises such as the one carried out in Slovenia enable all relevant entities in the nuclear sector to assess how robust their incident response plans are in the event of a successful cyberattack."

In the case of a serious computer security incident, which could potentially contribute to a nuclear safety or security event, a CSIRT should be involved, in addition to the usual stakeholders at a nuclear facility. Such an incident could entail, for example, the violation of security policies or security procedures; impacts on sensitive digital assets or systems; or the loss of sensitive information and control of critical functions for nuclear safety.

In this case, once a computer security incident or compromise is identified, the CSIRT works with the stakeholders of the facility to investigate the incident, gather forensic data, analyse what happened and where, and assist in containing and eradicating the intrusion to help operators bring the nuclear facility back online. At the end of the response, computer forensics evidence is gathered to aid any criminal investigation into the attack, and to ensure effective information sharing to further strengthen computer security measures at the nuclear facility in the future.

In the Slovenia exercise, the detection of cyberattacks was essential to be able to respond to this theoretical security incident and test and validate incident response procedures. These exercises support the testing of the relationship between safety, security and emergency preparedness, and strengthen nuclear security regimes by identifying potential weaknesses and developing necessary changes to improve their overall preparedness for potential cyber-security threats. Additionally, these exercises provide an opportunity to test national and international communication channels for notifications and reporting. Overall, conducting computer security exercises regularly is an important aspect of maintaining the security of nuclear facilities.

Improving computer security anomaly detection techniques through coordinated research projects

By Rodney Busquim e Silva and Andrea Rahandini

Identifying anomalies in the operations of computer systems that control critical safety and security functions calls for extensive expertise, and the actions required need to be tested, analysed and amended in order to be robust.

"Anomaly detection plays an important part in early assessment of possible threats targeting the computer-based systems at nuclear and radiological facilities," said Scott Purvis, Head of the Information Management Section in the IAEA's Division of Nuclear Security. "Usually, the anomaly detection techniques are based on artificial intelligence applications such as machine learning, statistics-based, knowledge-based methods or other technologies," he said. Such technologies are used to identify deviations from expected network communications or process measurements which can be the first indicator that a computer system's defenses have been bypassed by an intruder, and can provide real-time detection of cyberattacks.

These technologies are important because a highly capable malicious actor may introduce malware that compromises the safety or security functions of a digital system while falsifying data from sensors and indicators sent to an operator. This means that the operator may be unaware of any malicious activity taking place and will initially react based on what is displayed in the control room, potentially being misled into taking the incorrect action. Only through the automated detection of the smallest anomalies in such a cyberattack could an operator be correctly informed.

To address this important area of work and other computer security challenges, the IAEA launched a specific coordinated research project (CRP) in 2016.

Research and development through CRPs are an indispensable part of the IAEA's activities in computer security for nuclear security. These projects produce a body of research and actionable conclusions that complement the IAEA's ongoing efforts to enhance countries' capabilities in the prevention, detection of, response to, and recovery after computer security incidents that have the potential to directly or indirectly impact the safety and security of nuclear and radiological facilities.

"Adversaries are becoming more sophisticated, and their cyber capabilities present increasing challenges in developing anomaly detection tools," said Purvis. "The development of anomaly detection techniques requires access to realistic and physically consistent network and plant process data to train and test the detection models."

"We developed and used the ANS to generate a repository of data for training our machine learning models and to evaluate their efficiency. The IAEA CRP brought together international partners to conduct research and created new knowledge in this area."

— Ricardo Marques, Professor, Polytechnic School, University of São Paulo, Brazil

Cyberattack scenario to build capacity

The 2016 CRP, entitled "Enhancing Computer Security Incident Analysis at Nuclear Facilities", produced significant results, such as enabling further research into targeted tools and techniques that had previously been impossible to investigate without the risk of exposing sensitive information from nuclear and radiological facilities.

The CRP team, consisting of researchers from 13 countries and 17 organizations, developed a fictitious facility referred to as the 'Asherah' nuclear power plant (NPP), and a simulator (ANS) was developed by the University of São Paulo based on this facility. Together, they developed realistic cyberattack scenarios within a nuclear facility. These cyberattack scenarios have made it possible to explore and assess the effectiveness of computer security measures, as well as the potential operational consequences of a digital asset being compromised. Additionally, the team worked on data collection and analysis and the development and testing of techniques for detecting cyberattacks.

"We developed and used the ANS to generate a repository of data for training our machine learning models and to evaluate their

A simulator was developed by the University of São Paulo based on a fictitious facility referred to as the 'Asherah' nuclear power plant. (Photo: IAEA)

efficiency. The IAEA CRP brought together international partners to conduct research and created new knowledge in this area," said Ricardo Marques, a professor at the Polytechnic School of the University of São Paulo in Brazil. The cooperation between the CRP participants was essential to validate the work done."

Additionally, the CRP outcomes have been used for ongoing education and training involving a large number of graduate students and researchers in varying disciplines. This has further enhanced research and efforts made with the aim of continuously improving computer security at nuclear and radiological facilities.

"Part of my research as a PhD student has been conducted using the ANS and its Human Machine Interface (HMI), an interface that allows a user to observe and communicate with the simulator, developed within the IAEA CRP," said Si Wen, a PhD student from Tsinghua University in China. "I conducted research on anomaly detection techniques, and the ANS was essential to produce the necessary data to train and evaluate a detection algorithm developed for NPPs. Without the collaboration among all participating institutes, and the tools developed by the CRP team, it would be impossible to conduct my PhD research on cybersecurity of NPP digital systems," she added.

The CRP outcomes — the ANS, tools and guidance — are available to interested research institutes around the world. They can be obtained by submitting to the IAEA, through the relevant national authority, a request form available on the IAEA's Nuclear Security Information Portal (NUSEC).

More recently, in 2023, the IAEA launched a new CRP entitled "Enhancing Computer Security for Radiation Detection Systems" to investigate methodologies and techniques to improve computer security of radiation detection equipment. The research projects planned under the new CRP, with 12 participating organizations (including national laboratories, universities and national researcher institutes) from 11 countries, will address the use of emerging digital technologies, such as cloud computing, and continue to explore and develop innovative anomaly detection techniques.

Securing digital technologies of the next generation of nuclear reactors

By Joanne Liou

"The need to exchange information may introduce pathways that can be exploited by cybercriminals and therefore require robust cybersecurity considerations applied to the communication infrastructure."

— Mike St. John-Green, Computer Security Expert, UK

All innovations bring potential benefits that could transform industries, but they also bring potential risks. In the nuclear field, advanced nuclear reactors, including small modular reactors (SMRs), are incorporating innovative technologies, particularly digital technologies that yield novel solutions.

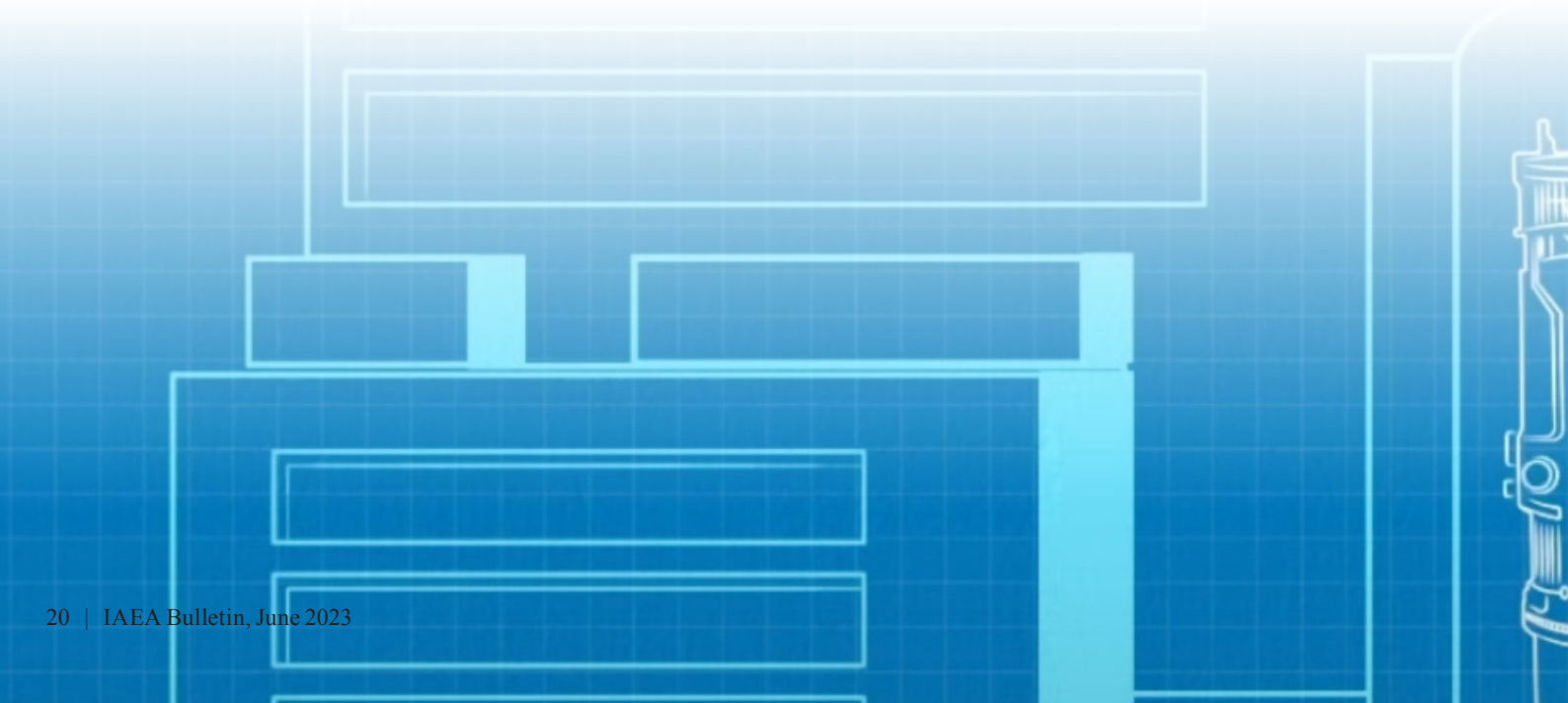
There is growing interest in SMRs. These advanced nuclear reactors have a limited power capacity — typically up to 300 MW(e) per unit, which is about one third of the generating capacity of traditional nuclear power reactors. However, the use of cutting-edge digital technology in these new reactors brings new challenges in terms of nuclear safety and security. There are more than 80 SMR designs and concepts in various stages of development around the world.

"One challenge for deploying SMRs is how to accelerate the development of their technology and demonstrate their level of readiness while maintaining compliance with nuclear safety and security standards," said Rodney Busquim e Silva, Information Technology Security Officer at the IAEA. "This reinforces the need for digital instrumentation and control and computer security solutions to be considered and maintained during the SMR life cycle."

Computer-based solutions and challenges

The innovative designs of SMRs rely on digital instrumentation and control (I&C) systems that enable their innovative features. The increased digital technologies needed for automation, remote supervisory control and maintenance, along with other novel features, highlight the need for computer-based solutions.

Some SMRs are designed for nuclear power deployment in isolated areas and for a reduced number of on-site staff, which may result in the need for constant and reliable remote monitoring. Given the design of digital I&C systems, the application of computer security measures should be a prerequisite for secure communication between the SMR site and a support centre. "The need to exchange information may introduce pathways that can be exploited by cybercriminals and therefore require robust cybersecurity considerations applied to the communication infrastructure," said Mike St. John-Green, a computer security expert based in the United Kingdom. "The confidentiality, availability and integrity of information must be protected for remote operations to ensure the safe and reliable operation of SMRs and associated infrastructure."



Artificial intelligence (AI) and machine learning (ML) also support the operations of SMRs. AI refers to technologies that produce systems capable of tracking complex problems, while ML technologies learn how to complete a particular task based on data. By combining digital simulations of nuclear facilities and monitoring control systems with AI systems, the nuclear industry seeks to optimize complex functions, which could increase operational efficiency. These benefits do, however, come with the potential for cyberattacks. For example, the software-based algorithms needed for AI and ML rely on databases that could be manipulated to cause erroneous AI decision making.

"These systems may be subject to code injection, for example, feeding them intentionally with corrupt data, during the development process, delivery or software installation. The challenge overall is how to produce sufficient transparency of the AI/ML algorithms. The acceptable use of AI/ML must be clearly defined with acceptable levels of risk," said Si Wen, a PhD student from Tsinghua University in China.

Security by design

Experts agree that the computer security of nuclear facilities must be considered from the outset. This proactive approach, known as security by design, draws on best practices and lessons learned from experience, and implements a 'by design' concept that is also applied to nuclear safety, safeguards and decommissioning.

Computer security by design aims to reduce security risks at the source through an approach that considers systematic and consistent security through all phases in the lifetime of the facility or process.

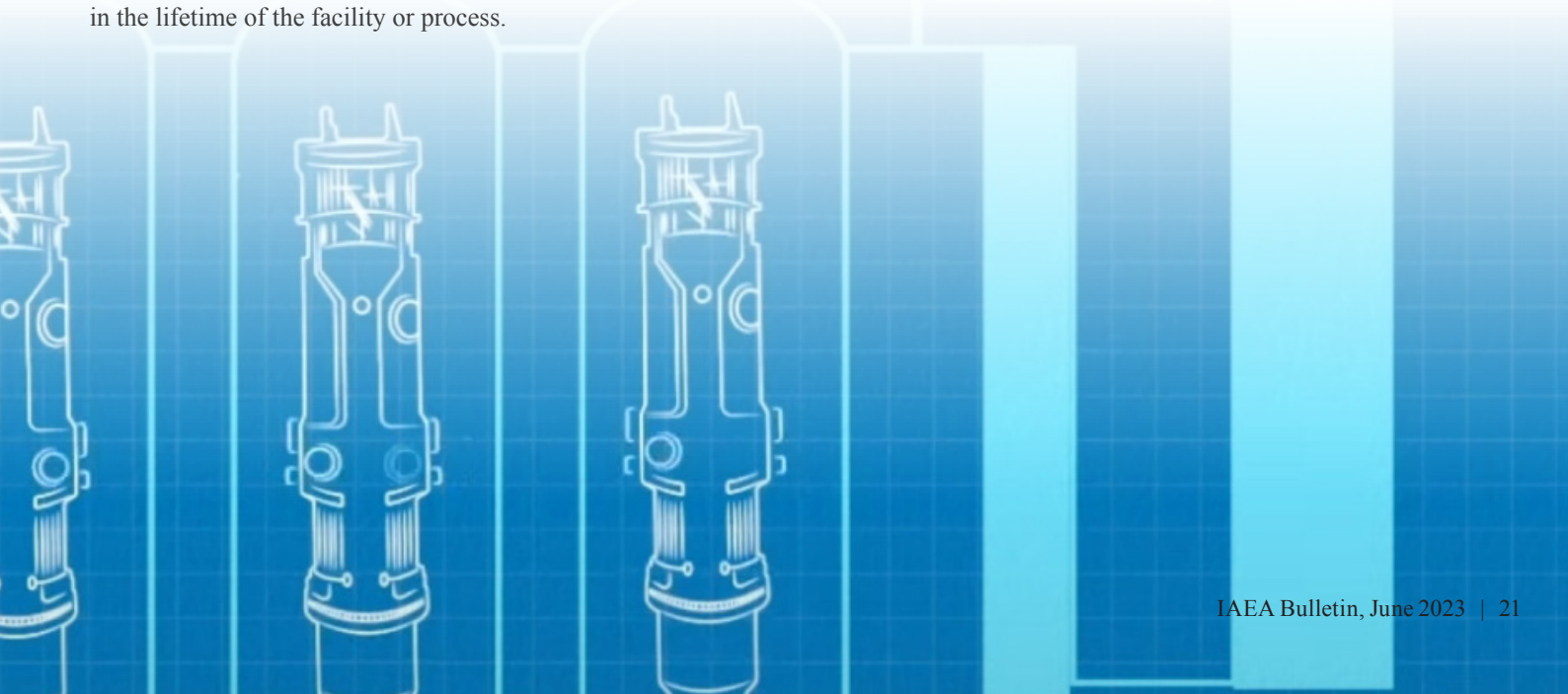
"Computer security measures need to be considered and maintained during the entire SMR lifecycle, from design to operation to decommissioning," Busquim e Silva said. "When security, including cybersecurity, is considered from the outset, facility developers can make design choices that will make facilities safer and more secure, efficient and cost-effective."

The role of the IAEA

The IAEA connects experts from nuclear and other organizations to discuss and identify computer security related issues and challenges related to the technological and operational characteristics of SMRs. For example, in February 2022, the IAEA hosted a Technical Meeting on I&C systems and computer security for SMRs to foster cooperation and to facilitate information exchange among international experts. Participants agreed that there is a need to harmonize national approaches and regulations to make the international market for SMRs viable. "The I&C solutions on standardized SMRs open a whole new technical field. The increasing automation needed for new modes of operation, and the extensive use of digital systems, call for computer security measures and engineering solutions from the design level to guarantee safe and secure plant operation," said Jorge Casanova, who attended the meeting as a representative of the Nuclear Regulatory Authority in Argentina.

In March 2023, the IAEA also conducted a workshop to further explore the development of technical capabilities related to computer security and I&C for SMRs. Furthermore, the IAEA plans to launch a coordinated research project on the topic in 2024.

There are more than 80 SMR designs and concepts in various stages of development around the world.



Enhancing computer security for nuclear safety and security

By Lydie Evrard
IAEA Deputy Director General and Head, Department of Nuclear Safety and Security

Nuclear safety and nuclear security share the same objective and vision: to protect individuals, societies and the environment from the potential harmful effects of ionizing radiation. Though the activities that address nuclear safety and nuclear security are different, it is essential to establish a well-coordinated approach to managing their interface. It is important to ensure that relevant measures are implemented in a manner that capitalizes on opportunities that may be available for mutual enhancement — without compromising either safety or security.

It is well known that in nuclear and radiological facilities physical security systems and measures are necessary to protect equipment, systems and devices — typically intended to maintain nuclear safety — from a deliberate act of sabotage that could potentially lead to a release with radiological consequences. Typically, in older designs and applications, safety systems needed to be protected with only physical protection measures. However, the ubiquitous and ever-increasing technology trends of today are significantly increasing the role of the digital systems in the efficiency of operations at nuclear and radiological facilities, especially associated with those responsible for important facility functions, such as instrumentation and control systems, including those used both for safety and security.

The security of these systems requires stringent vigilance to identify vulnerabilities and deter unauthorized access to digital control systems that may result in compromised safety or security functions. In this regard, computer security is becoming increasingly important for the interplay between safety and security, and is being addressed as part of other key areas that include the regulatory infrastructure; engineering provisions in the design and construction of nuclear installations;

controls on access to nuclear installations; the categorization of radioactive sources; the management of radioactive sources and radioactive material, including spent fuel and radioactive waste products; the detection and recovery of uncontrolled sources; and emergency response and contingency plans.

At a national level, policymakers need to consider nuclear security and nuclear safety together when preparing the regulations on computer security. Clear allocation of responsibilities, leadership and risk management are the foundations of the safety and security interface and are equally important for the implementation of effective computer security measures. At the same time, computer security is intrinsically a global challenge.

In this context, the importance of international cooperation and the central role of the IAEA are widely recognized. The interface between nuclear safety and nuclear security is highlighted in IAEA safety standards and nuclear security guidance. For about a decade now, the IAEA has been developing and offering countries a comprehensive suite of assistance in the technical area of information and computer security, supporting them in taking effective measures against cyberattacks that could potentially impact nuclear security. In addition, the IAEA provides support in establishing synergies between nuclear safety and nuclear security systems and measures to ensure that actions taken in the two fields complement rather than compromise each other.

Looking ahead, technological advancements will further increase the importance of robust computer security for nuclear safety and security at the State and facility levels. Rapidly evolving technologies such as artificial intelligence are promising in terms of solving some problems and improving digitally controlled operations. At the same time, they present new challenges that need to be addressed. Similarly, wireless and automation technologies are being considered and used today in advanced nuclear reactor designs such as small modular reactors and microreactors. As cyberthreats are constantly and rapidly evolving, IAEA support for Member States' needs for enhancing computer security for nuclear safety and security requires agility to keep abreast of all the new opportunities and challenges of these novel technologies in order to provide the most efficient standards, best practices, training and guidelines. This is what the IAEA Department of Nuclear Safety continuously strives for.

At a national level, policymakers need to consider nuclear security and nuclear safety together when preparing the regulations on computer security.

— Lydie Evrard, Deputy Director General and Head, Department of Nuclear Safety and Security, IAEA

Countering threats in an increasingly digitized world

By Wolfgang Picot

In May 2022, the Austrian Institute of Technology (AIT) became the first IAEA Collaborating Centre for information and computer security for nuclear security. The AIT provides support for international and regional training courses and exercises in computer security for nuclear facilities and activities, develops technical demonstration modules for enhancing awareness about cyberthreats, and contributes to the development of training materials for the new Nuclear Security Training and Demonstration Centre at Seibersdorf. To better understand this cooperation, we talked to Helmut Leopold, Head of the Center for Digital Safety and Security at the AIT.

Q: What are the emerging risks and threats in computer security in general?

A: Many modern digital devices today are being built with more extensive networks in mind. Many of them need access to the Internet to function. Every software development includes potential errors that can lead to vulnerabilities. Poorly protected interfaces and users acting irresponsibly increase the number of security threats to the operation of information technology (IT) systems. Attackers exploit the vulnerabilities of digital systems in order to gain access.

Attack methods and tools develop in line with the development of digital innovation processes. Software for hackers is now readily available on the Internet, making attacks easier — even for less qualified attackers. We are confronted with a diverse cyberattack ecosystem driven by organized crime, economic and industrial espionage, and cyberterrorism.

Today, therefore, a broad spectrum of cyberattacks threatens users, companies and authorities, and can attack the digital infrastructure of entire States in conjunction with targeted disinformation campaigns, shaking the foundations of our societies.

Q: Does the nuclear industry face the same challenges?

A: Businesses and individual consumers primarily use data-driven and communication-oriented Information Technology (IT). By contrast, production facilities and critical infrastructures use so-called Operational Technology (OT) that monitors and controls the behaviours and outcomes of defined production processes. OT has traditionally been much less interconnected than IT, however, with the progression of technology, the two fields have converged, and OT software and devices are increasingly being plugged into broader networks.

"We have been working closely with our colleagues at the IAEA to develop training modules, demonstrations and exercises for the NSTDC."

— Helmut Leopold, Head, Center for Digital Safety and Security, AIT

This development is problematic, as cybersecurity awareness is less widespread in OT than in IT.

Thus, these new threats to IT security become relevant for the OT of industrial production and critical infrastructure. This also becomes increasingly relevant for the nuclear industry, which traditionally had a conservative approach and kept control systems isolated.

Q: What activities does the AIT conduct to enhance cybersecurity in nuclear security?

A: The AIT research programme scrutinizes how evolving threat scenarios could impact OT systems and aims to develop know-how and new solutions to increase the resilience of critical infrastructures against cyberattacks. This work is the basis for developing new global security standards, certification procedures for critical system elements and new system architectures to embed solid cybersecurity measures into OT systems from the start of their design.

The AIT also offers comprehensive training and education to prepare against cybersecurity attacks. In complex simulations of 'virtualized' IT systems, so-called 'cyber ranges', users, system developers, operating personnel and government representatives react to realistic cyberattack scenarios. Such simulations are crucial to ensuring resilient IT and OT systems that can effectively fend off cyberthreats.

Q: What are the advantages of the virtual learning environment developed by the AIT and the IAEA?

A: Practical experience is the most effective learning process. The AIT and the IAEA developed a 'cyber range' that offers the creation of 'digital twins' of existing critical digital infrastructures, and that also offers training in highly realistic application scenarios.

Here users from government and industry can evaluate and test the effectiveness of protection mechanisms and business processes.

Experiences from the 'cyber range' support the establishment of sustainable defensive capabilities of public and private organizations alike.

Q: Besides virtual training, how does the AIT's work and expertise in computer security advance nuclear security?

A: We can help to defend against attackers, for example, by developing software to monitor "edge" devices that typically link organizations' internal networks to the Internet. Attackers often use these devices as system entry points before they do damage.

We use our experience in anomaly detection to train analysis software that monitors edge devices typically used in a particular type of nuclear facility.

Such a software can set off an alarm or take countermeasures if a device is acting in a strange way. As a result, operators can swiftly detect and deter cyberattacks before they can do significant harm.

Q: One year ago, the AIT was designated as the IAEA's first Collaborating Centre in computer security for nuclear security and remains the only such Centre today. What does this mean for the AIT's work?

A: We are incredibly proud of our designation as a Collaborating Centre and continue to support the delivery of a regional training course on computer security for instrumentation and control systems in the nuclear sector. The course was held twice in 2022, using some of the outcomes from our joint venture to develop a virtual learning platform.

We have also participated in activities on computer security in developing small modular reactors.

Currently, we are assisting the IAEA in preparations for the 2023 International Conference on Computer Security in the Nuclear World: Security for Safety, where we will perform demonstrations of our virtual training platform, chair panel sessions and present papers that are related to our research in the sector, and more.

Q: What is the AIT's involvement at the Nuclear Security Training and Demonstration Centre (NSTDC)?

A: We have been working closely with our colleagues at the IAEA to develop training modules, demonstrations and exercises for the NSTDC. We incorporate computer security modules into the training courses associated with the physical protection of nuclear and other radioactive materials, and also those associated with the detection and response to nuclear and other radioactive material out of regulatory control. This arrangement seeks to reinforce the concept of computer security as an integral and inseparable element of nuclear security.

How international collaboration keeps the world safe from cyberthreats

Tighe Smith is the Convenor of IEC SC45A WGA9. He has been appointed by a committee to lead the working group A9, which deals with cyber security, at the International Electrotechnical Commission (IEC). The IEC is a global not-for-profit organization that develops international standards for the design, construction and operation of electrical equipment, including that used in nuclear power plants. Founded in 1906, the IEC brings together more than 170 countries and publishes 10 000 IEC International Standards.

The nuclear industry faces a significant challenge in maintaining computer security owing to the widespread use of digital devices. This trend is evident in everyday life, where smart fridges, lighting and other devices controlled remotely via cloud computing have become commonplace. Many systems at nuclear facilities, which previously would not have had any digital components, now have digital elements. Their computational power, reprogrammable nature and ability to interconnect delivers unequalled efficiency in the support of operations, nuclear safety and nuclear security.

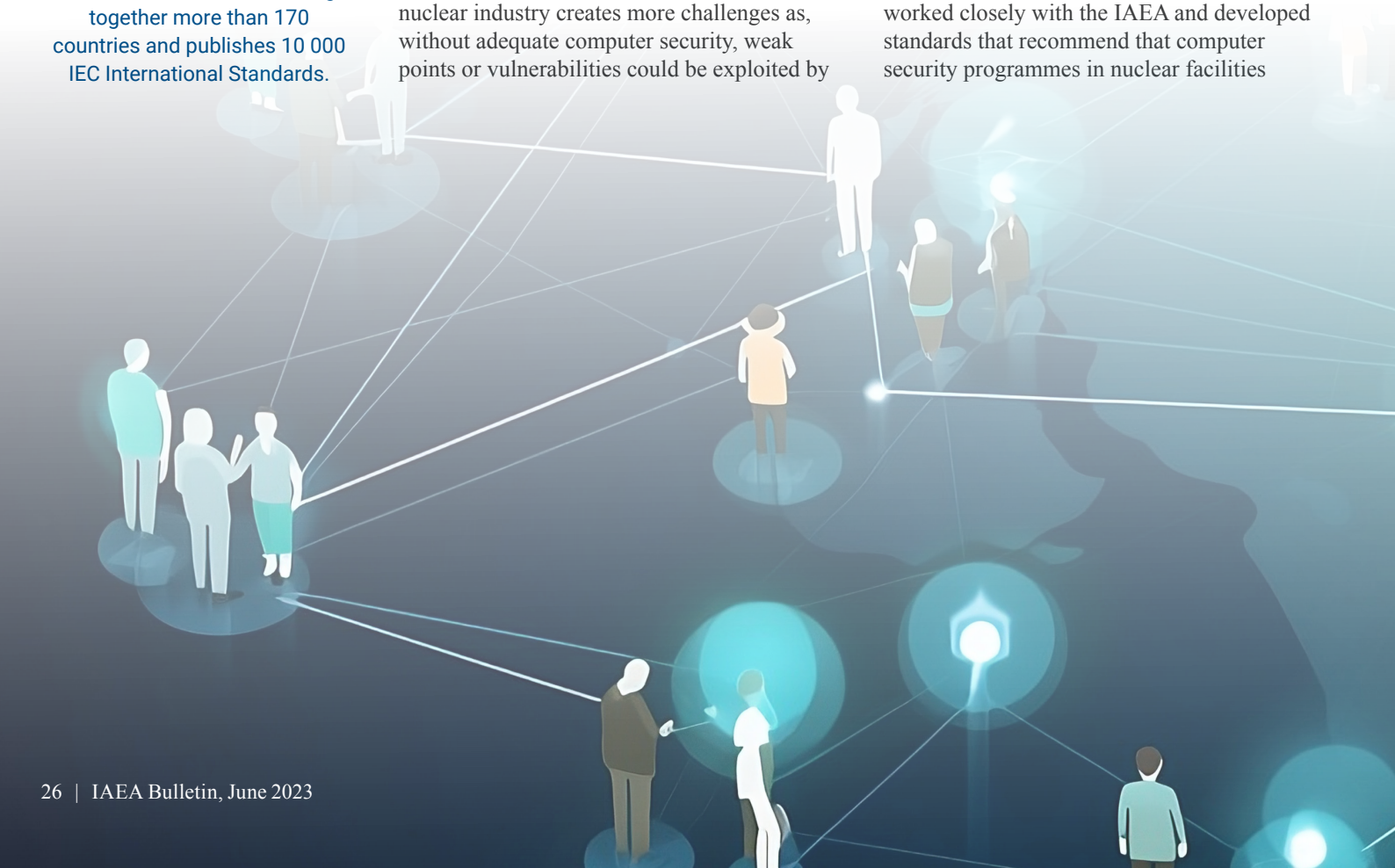
Small modular reactors and other new reactor designs are being developed in a digital-first world with an even more widespread use of computer systems than in previous designs. They may be designed to operate remotely or even autonomously, utilizing computer network infrastructure to communicate with a central operator. This approach can enable operators and automated systems to analyse large amounts of data to increase the operational efficiency of the nuclear facility.

However, this digital modernization of the nuclear industry creates more challenges as, without adequate computer security, weak points or vulnerabilities could be exploited by malicious actors as part of an attack against one of these facilities.

In order to address the challenges posed by the rapidly evolving digital technology landscape in nuclear facilities, and the need to support harmonized approaches between countries and facilities, the IEC has adopted a consequence-based and risk-informed approach aligned with the information and computer security guidance within the IAEA Nuclear Security Series (NSS). Rather than a prescriptive approach, we advise a graded approach, enabling organizations to determine the level of control required for a product or process based on the potential consequences of a cyberattack. For instance, the first step in a computer security programme is to review the functions of the nuclear facility, assess their impact on safety and security, and determine the appropriate level of security requirements.

Prevention, detection and mitigation

Predicting how cyberattacks will evolve in the future is challenging, so the IEC has worked closely with the IAEA and developed standards that recommend that computer security programmes in nuclear facilities



focus on detection, response and recovery, in addition to prevention. Even if elements of a cyberattack are successful, there should be mechanisms in place to restore and ensure the correct performance of the necessary functions to guarantee that safety and security are not compromised.

The rapid digitalization of our world, along with the growth of artificial intelligence and machine learning, can make computer security at nuclear facilities seem daunting. International collaboration is crucial in order to continue the safe and secure operation of these facilities, despite such challenges. For over half a century, the IAEA, the international community and the nuclear industry have collaborated on standardization to support the safety and security of peaceful nuclear technology. With global issues such as climate change and energy security becoming more pressing, many countries are looking to new and innovative nuclear technology as a way to generate low-carbon energy, making standardization even more important in maintaining the safety and security of nuclear facilities.

Collaboration in the nuclear world

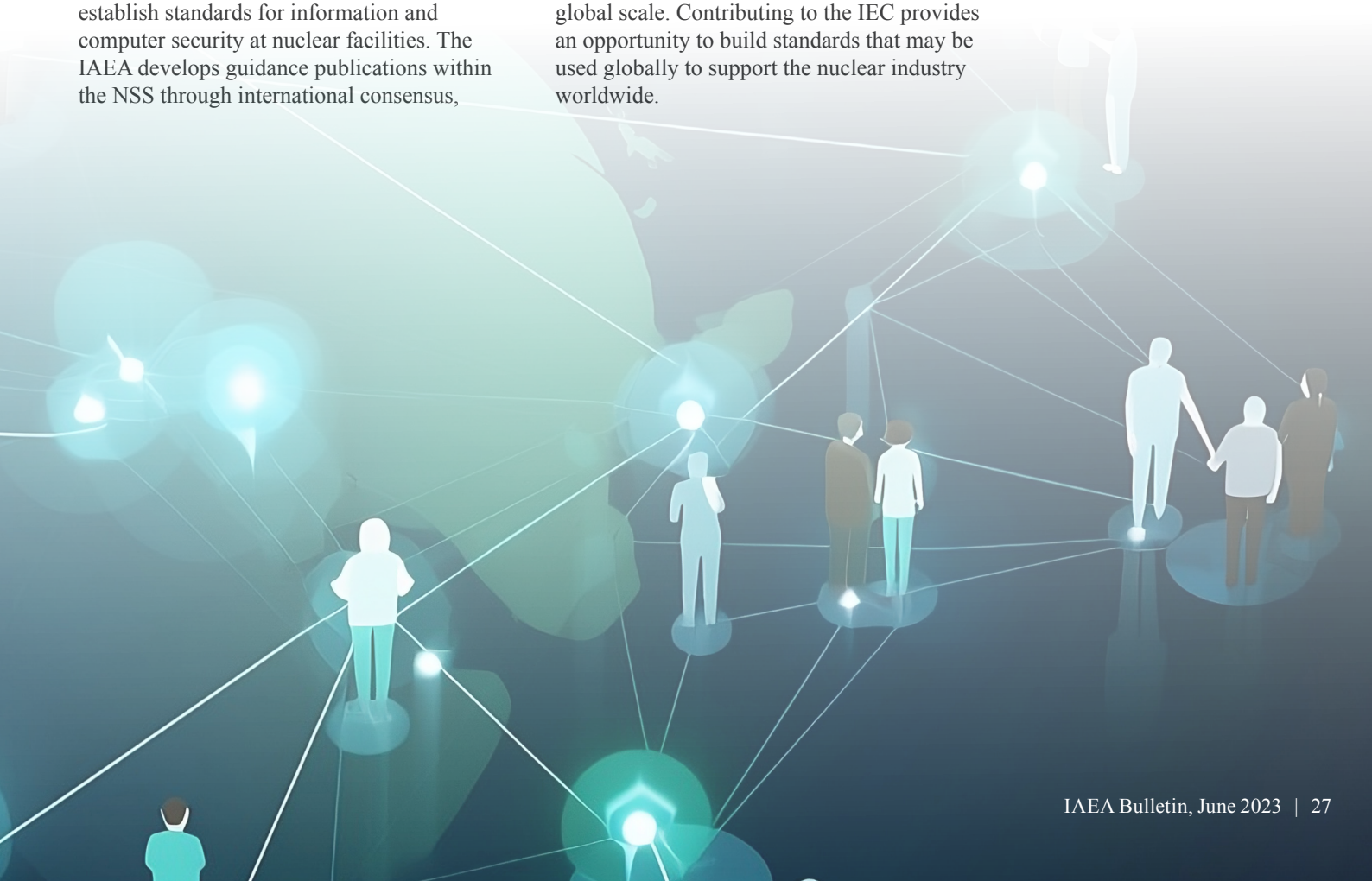
The IAEA and the IEC are essential contributors to the international effort to establish standards for information and computer security at nuclear facilities. The IAEA develops guidance publications within the NSS through international consensus, outlining concepts and norms for ensuring information and computer security as fundamental elements in achieving nuclear security objectives. The NSS provides guidance on organizing State resources and preparing industry regulations and concepts for implementing a cyber-informed engineering approach in nuclear facilities.

As an international standards organization that promotes best practices and knowledge sharing, the IEC works closely with the IAEA. Under the Memorandum of Understanding between the IEC and IAEA, scientists and experts working with the IEC develop standards and technical reports on implementing IAEA guidance through specific programmatic and engineering requirements. These requirements can be leveraged in the design and development of current and future digital systems, which can be certified against regulatory models aligned with IAEA guidance. Experts representing the nuclear industry's experience in implementing IEC standards can then support the development of future iterations of IAEA guidance.

Scientists and experts contribute to the work of the IEC on a voluntary basis, and more volunteers are always welcome. The community of computer security experts in the nuclear field is relatively small, even on a global scale. Contributing to the IEC provides an opportunity to build standards that may be used globally to support the nuclear industry worldwide.

"With global issues such as climate change and energy security becoming more pressing, many countries are looking to new and innovative nuclear technology as a way to generate low-carbon energy, making standardization even more important in maintaining the safety and security of nuclear facilities."

— Tighe Smith, IEC



IAEA Code of Conduct

20 years of progress in safety and security of radioactive sources

Speakers at the side event 'Gender equity and inclusion, and the Code of Conduct on Safety and Security of Radioactive Sources: 20 years of progress'. (Photo: W. Wawrzuta/IAEA)

More than 270 legal and technical experts from 128 countries and 4 international organizations convened in Vienna, Austria in May 2023, to review progress achieved in the safety and security of radioactive sources and address areas in need of improvement.

Radioactive sources play an indispensable role in many domains. In medicine, they help treat cancer. In agriculture, they allow scientists to develop improved crop varieties to adapt to climate change and address food security. In art and archaeology, they help to preserve priceless cultural heritage. But these sources must be handled with proper safety and security measures.

To help countries tackle risks and protect people and the environment from accidental radiation exposure or intentional unauthorized acts involving radioactive sources, the IAEA developed the Code of Conduct on the Safety and Security of Radioactive Sources, which was approved in 2003 by the IAEA Board of Governors and is marking its 20th anniversary this year.

"Twenty years have passed since the approval of the Code of Conduct, and we are making steady progress in improving the safety and security of radioactive sources around the world," said IAEA Director General Rafael Mariano Grossi at the opening session of the Open-Ended Meeting of Technical and Legal Experts for Sharing Information on States' Implementation of the Code of Conduct on the Safety and Security of Radioactive Sources. "But further work must be done to achieve even greater political commitment and to share global best practices for the sustainable, safe and secure management of these sources."

Spanning five days, the meeting served as a platform for global experts to exchange information on national implementation practices of the Code of Conduct and its two supplementary Guidance documents. Such meetings take place every three years, enabling countries to share experiences, exchange lessons learned, and identify existing and future challenges in the implementation of the Code.

Throughout the week, the participants delved into diverse topics, including the evolution of nuclear safety and security, legal aspects, international cooperation, future development and the impact of the Code of Conduct. Discussions addressed challenges and priorities related to the establishment of the appropriate regulatory framework for the safety and security of radioactive sources, their life cycle management, their import and export regulations and how these sources should be managed when they are declared as disused. Crucially, the meeting offered the participants the opportunity to share their respective approaches to effectively implementing the provisions of the Code of Conduct.

Essential guidance for a safe and secure future

Speaking at the opening event, the Co-Chair of the meeting, Ramzi Jammal, Executive Vice-President and Chief Regulatory Operations Officer at the Canadian Nuclear Safety Commission (CNSC), emphasized that the implementation of the Code of Conduct is essential in ensuring the protection of the environment, the public and workers. "Our ultimate goal is to ensure the overall safety and security of radioactive sources during their complete life cycle to avert accidental radiation exposure and prevent radioactive sources from being used with malicious intent. This is a collaborative, ongoing effort."

In introducing a special session on the history of the Code, Theresa Clark, a Deputy Division Director at the US Nuclear Regulatory Commission, also addressed attendees as Co-Chair: "In reflecting on, and in celebration of, these twenty years, we wanted to achieve a common understanding of the background of the Code from the legal and technical perspective, so we can share experiences, best practices and learn from each other to improve the implementation of the Code globally."

The Code of Conduct details how countries can ensure the safety and security of radioactive sources from their initial production to final disposal. It contains international considerations and offers recommendations on the development, harmonization and implementation of national policies, laws and regulations, as well as on cooperation between countries. Although it is a legally non-binding instrument, 146 states have expressed their political support for implementing the Code's provisions since its approval by the Board of Governors in 2003.

The Code of Conduct is supplemented by two Guidance documents. The Guidance on the Import and Export of Radioactive Sources addresses roles and responsibilities in ensuring safe and secure import and export of radioactive sources. The Guidance on the Management of Disused Radioactive Sources provides guidance on the management of disused sources, delineating end-of-life management options such as recycling and reuse, long-term storage and disposal, and return to supplier. This Guidance also encourages the establishment of a national policy and strategy for the management of disused sources.

"The Code of Conduct and its Guidance documents bring tangible benefits to national and international radiation safety and nuclear security, enabling to take full advantage of radioactive sources for a sustainable future," concluded Co-Chair Aayda Ahmed Al Shehhi, Director of Radiation Safety at the UAE Federal Authority for Nuclear Regulation (FANR).

The IAEA works and cooperates closely with countries to ensure the harmonized, safe and secure management of radioactive sources. It supports them in implementing the principles of the Code and provides extensive assistance in developing strategies and action plans for implementing the Code; improving licensing, inspection, enforcement and management systems; and strengthening the capacity of national regulatory bodies in line with IAEA safety standards, nuclear security guidance and international best practices.

Strengthening diversity and inclusion in the nuclear field

On the margins of the meeting, a side event entitled "Gender equity and inclusion, and the Code of Conduct on Safety and Security of Radioactive Sources: 20 years of progress", was hosted by the CNSC. It brought together 120 participants to discuss ways of promoting and strengthening women's participation in the nuclear field — including in nuclear safety and security — and providing equal opportunities to all individuals, regardless of gender.

"Having diverse representation at the table contributes to an increase in questioning attitudes, which in turn leads to a stronger safety culture in the organization. Gender equity is not solely a woman's issue but it is a societal issue to be addressed by all." said Rumina Velshi, President and Chief Executive Officer of the CNSC, adding that the growing demand for human resources makes it imperative to ensure greater opportunities are available for women in the nuclear field.

"Nuclear safety and security rely on a questioning and learning attitude, openness for constructive feedback and the capacity to combine different views and mobilize different expertise. Diversity, including gender diversity, is a true asset in this regard. We are stronger and more efficient when we embrace diversity and encourage our staff to voice their opinion," said Lydie Evrard, IAEA Deputy Director General and Head of the Department of Nuclear Safety and Security, during the event.

Margaret Doane, IAEA Deputy Director General and Head of the Department of Management, said that "enhancing the participation of women and people from diverse backgrounds in nuclear-related sectors is vital to any organization." She highlighted the IAEA's initiatives on improving gender equality, including the Marie Skłodowska-Curie Fellowship Programme and the Lise Meitner Programme, aimed at bringing more women into the nuclear field.

Christer Viktorsson, Director General of the FANR, gave his perspective on the topic: "FANR has focused activities to promote gender equality. Leadership commitment and support are vital, including surveys on how we can improve inclusiveness and fair treatment of all staff. It is equally important to have appropriate framework and effective implementation that are inclusive."

— By Artem Vlasov

Arabic-speaking countries discuss nuclear security plans

Participants at a regional meeting held recently in Tunisia shared their experiences in developing and implementing an INSSP. (Photo: Z. Hassan/IAEA and AAEA)

Member countries of the Arab Network of Nuclear Regulators (ANNuR) met recently in Tunisia to exchange best practices, challenges and opportunities related to the implementation of nuclear security activities within the framework of their respective Integrated Nuclear Security Support Plans (INSSPs). The meeting highlighted the importance of regional approaches to improve regulatory and operational capacities — approaches which are inherent in the IAEA's nuclear security programme.

"Approaching nuclear security through a regional lens improves international cooperation and facilitates the implementation of the IAEA's nuclear security programme," said Elena Buglova, Director of the IAEA's Division of Nuclear Security. "Cooperation with regional networks like ANNuR further strengthens the effectiveness of the INSSP support mechanism, creating opportunities to identify and discuss common needs and challenges among countries of geographic proximity or countries with the same language."

At the meeting, 28 participants from 14 countries provided information on the implementation of their national INSSPs. Particular areas of focus included activities related to legislative and regulatory frameworks for nuclear security; national threat and risk assessments; physical protection regimes; detection of criminal and unauthorized acts involving nuclear or other radioactive material out of regulatory control (MORC); response to nuclear security events involving MORC; and sustainment of national nuclear security regimes.

Lebanon is currently one of the countries using the INSSP as a mechanism to strengthen its national nuclear security infrastructure. "The workshop allowed us to share our national experience in implementing the INSSP and to discuss the nuclear security challenges in our countries as well as the possible ways to address them," said Hassan Basat, Section Head responsible for authorization, inspection and regulations at the Lebanese Atomic Energy Commission. "The most important outcome was the identification of INSSP common priority areas that need to be further enhanced among the ANNuR members."

Currently, 19 out of 22 ANNuR members have an approved INSSP. Globally, 92 countries have approved INSSPs.

"At a regional level, we share borders, as well as specific challenges," said Shaima Khalid AlJanahi, Head of the Physical Analysis Unit, Radiation Protection Directorate, Supreme Council for the Environment of Bahrain. "The workshop has enabled sharing experience and knowledge that hopefully will be followed by solid actions to improve and strengthen nuclear security in the region."

The meeting was hosted by the Arab Atomic Energy Agency (AAEA) and was supported financially by the European Union.

The INSSP support mechanism

The IAEA helps countries, upon request, to develop an INSSP, which provides the framework for a systematic and comprehensive approach to identifying and prioritizing national nuclear security needs and establishing a plan for implementing nuclear security improvements at the national level. The INSSP process is complemented by a voluntary self-assessment tool available to interested countries through the Nuclear Security Information Portal (NUSEC).

The INSSP and its associated implementation plan enables countries to address their most pressing needs, and to identify areas that can be addressed nationally and others where assistance from the international community needs to be sought.

Once the needs of each country have been identified, the IAEA can start to build the foundations for targeted assistance, such as that provided by its International Physical Protection Advisory Service (IPPAS) and the International Nuclear Security Advisory Service (INSServ) missions.

IAEA–ANNuR cooperation

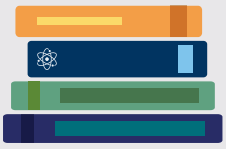
The ANNuR is a regional network established in 2010 under the IAEA Global Nuclear Safety and Security Network (GNSSN). The ANNuR fosters, enhances, strengthens and harmonizes radiation protection and nuclear safety and security regulatory infrastructure frameworks in its participating countries, and serves as a forum for the sharing and exchange of regulatory experiences and practices.

— Vasiliki Tafili

IAEA Publications free online

download here

www.iaea.org/books



To order a book, write to:
sales.publications@iaea.org

DOWNLOAD

Security of Nuclear Information

and other IAEA publications on

computer security in the nuclear world

www.iaea.org/bulletin/64-2

Read this and other editions of the IAEA Bulletin online at
www.iaea.org/bulletin

For more information on the IAEA and its work, visit
www.iaea.org

or follow us on

ISSN 0020-6067 23-01968