Zeitschrift für Friedens- und Konfliktforschung
https://doi.org/10.1007/s42597-024-00126-1

ARTICLE

Nuclear safeguards during crises: three scenarios of restricted access to nuclear interim storage facilities

Leonardo Bandarra · Stefan Böschen · Andreas Dürholt · René Geiser · Malte Göttsche · Sophie Kretzschmar · Irmgard Niemeyer · Linda Ostermann · Lukas Rademacher · Julian Schäfer

Received: 26 February 2024 / Revised: 24 July 2024 / Accepted: 24 August 2024
© The Author(s) 2024

Abstract Safeguards by the International Atomic Energy Agency (IAEA) play a pivotal role in preventing the proliferation of nuclear weapons. Over the years, the IAEA's safeguards system has adapted to technological advancements and changing political landscapes, making it more resilient and flexible. This adaption is not only the result of programmes aiming at preparing and foreseeing future challenges in the nuclear field but also the result of several crises that have occurred over the last decades, including attempts to break non-proliferation commitments and limited access to facilities. The aim of this article is to explore what could be done in an event of unavoidable crises, with a focus on interim nuclear storage facilities where the continuity of knowledge is broken, and a quick and relatively reliable response is needed. We conducted a scenario-based workshop with multidisciplinary experts with different backgrounds working in the area of peace and conflict research. The workshop simulated three scenarios: (1) a terrorist occupation, (2) a flood, and (3) a mismatch of information following a coup d'état. This workshop revealed insights

Leonardo Bandarra
Institut für Politikwissenschaft, Universität Duisburg-Essen, Duisburg, Germany

Stefan Böschen · ✉ Linda Ostermann · Julian Schäfer
HumTec, RWTH Aachen University, Aachen, Germany
E-Mail: linda.ostermann@humtec.rwth-aachen.de

Andreas Dürholt · René Geiser
Institut für Politische Wissenschaft, RWTH Aachen University, Aachen, Germany

Sophie Kretzschmar · Lukas Rademacher
Nuclear Verification and Disarmament, RWTH Aachen University, Aachen, Germany

Irmgard Niemeyer
Forschungszentrum Jülich, Jülich, Germany

Malte Göttsche
PRIF – Leibniz-Institut für Friedens- und Konfliktforschung, Frankfurt am Main, Germany

Technische Universität Darmstadt, Darmstadt, Germany

Published online: 26 September 2024

into crisis management strategies, data sampling, and the relevance of formal and informal interpersonal networks.

Keywords Nuclear interim storage facilities · Nuclear safeguards · International Atomic Energy Agency—IAEA · Simulations · Spent nuclear fuel

Nukleare Safeguards in Krisensituationen: drei Szenarien unter eingeschränktem Zugang zu nuklearen Zwischenlagern

Zusammenfassung Die Safeguards der Internationale Atomenergie-Organisation (IAEO) spielen eine zentrale Rolle bei der Verhinderung der Verbreitung von Kernwaffen. Im Laufe der Jahre hat sich das Safeguards-System der IAEO an den technologischen Fortschritt und die sich verändernde politische Landschaft angepasst, wodurch es widerstandsfähiger und flexibler geworden ist. Diese Anpassung ist nicht nur das Ergebnis von Programmen, die darauf abzielen, künftige Herausforderungen im Nuklearbereich vorzubereiten und vorherzusehen, sondern auch das Ergebnis mehrerer Krisen, die in den letzten Jahrzehnten aufgetreten sind, darunter Versuche, Nichtverbreitungsverpflichtungen zu brechen und den Zugang zu Anlagen zu beschränken. In diesem Artikel soll untersucht werden, was im Falle unvermeidlicher Krisen getan werden könnte, wobei der Schwerpunkt auf nuklearen Zwischenlagern liegt, bei denen die Kontinuität des Wissens unterbrochen ist und eine schnelle und relativ zuverlässige Reaktion erforderlich ist. Wir haben einen szenariobasierten Workshop mit im Bereich der Friedens- und Konfliktforschung tätigen Expert:Innen unterschiedlicher disziplinärer Hintergründe durchgeführt. Der Workshop simulierte drei Szenarien: (1) eine terroristische Besetzung, (2) eine Überschwemmung und (3) ein Informationsdefizit nach einem Staatsstreich. Der Workshop brachte Erkenntnisse über Krisenmanagementstrategien, Datenerfassung und die Bedeutung formeller und informeller zwischenmenschlicher Netzwerke.

Schlüsselwörter Nukleare Zwischenlager · Nukleare Safeguards · Internationale Atomenergie-Organisation – IAEO · Simulationen · Abgebrannter Kernbrennstoff

Safeguards are a crucial pillar in ensuring effective non-proliferation—that is, efforts to prevent the spread of nuclear weapons to new countries. They comprise a set of technical measures applied to nuclear facilities[1], such as nuclear power plants and nuclear interim storage facilities, to ensure that relevant fissile material (e.g., uranium and plutonium) is not diverted for non-peaceful purposes. The central organisation conducting nuclear safeguards is the International Atomic Energy Agency (IAEA; henceforth, "the Agency"), created in 1957 with the "dual mandate" to promote the

[1] According to the IAEA Glossary, a nuclear facility is the structure involved in "all sources of ionising radiation, all radioactive waste management activities, transport of radioactive material and any other practice or circumstances in which people may be subject to exposure to radiation from naturally occurring or artificial sources" (IAEA 2018, p. 93).

peaceful application of nuclear energy (Roehrlich 2022) and to ensure that states are "living up to [their] international commitments not to use nuclear programmes for nuclear-weapon purposes" (IAEA 2014). Over its almost seventy years of existence, the IAEA's safeguards system has been applied to countries around the world, and in that process, it has shown flexibility in incorporating technological changes and adjusting to changes in the political landscape (Ikonomou 2021; Weichselbraun 2020; Rockwood 2013; Seaborg and Loeb 1993).

The first models of nuclear inspections were developed "from scratch" in 1961 (Grümm 1987, p. 29), covering specific items and reactor types (up to 100 megawatts). Over the 1960s and 1970s, the scope of safeguards expanded from items to facilities. The first modern document to inform safeguards agreements was INFCIRC/153 (corrected) of 1972, which guides "comprehensive safeguards agreements" and defines a standard minimum procedure for all IAEA member states (ISCN 2016; Rockwood 2013). With the discovery of a clandestine nuclear weapon programme in Iraq in 1991 and North Korea in 1993, the Agency redefined its procedures for verification, and the Board of Governors (the political and decision-making body of the Agency) approved the so-called "Model Additional Protocol", under which States must inform the Agency about all parts of its nuclear fuel cycle, including mining, processing and waste management (Cooley 2020; Pilat 2021; Rosenthal and Stern 2019). The IAEA is also provided with short-notice access to all buildings on a site and may request additional information on relevant development activities. In addition to continuous adaptation in areas such as digital image transmission or unattended verification systems (Pellaud 1991) for the implementation of safeguards, there is a need to be able to address future challenges and improve preparedness for the unavoidable. For that, the Agency created dialogue formats with Member States, academia, industry, and other relevant stakeholders. An example of such efforts is the IAEA Safeguards Symposium, which occurs every four years.[2]

However, there is always an open space for unavoidable critical events, and specific methods are needed to explore the room for manoeuvring. This article contributes to those efforts by shedding light on possible crisis situations. To study how the IAEA can perform safeguards activities for a facility impacted by a crisis, we focused on interim storage facilities for spent fuel and high-level radioactive waste (henceforth nuclear interim storage facilities). They represent an increasingly important type of nuclear facility, as they will also remain under safeguards in countries that have or had nuclear reactors at some point in their history. This article uses a scenario-based workshop to examine *how the Agency can act in unavoidable crises*[3] that *affect interim nuclear storage facilities* where *on-site inspections are impossible*, breaking the continuity of knowledge and *requiring a fast and relatively reliable response.* It contributes, therefore, to the current debates both around the

[2] More information can be found under https://www.iaea.org/topics/assistance-for-states/safeguards-symposium. Accessed on 05 February 2024.

[3] "Unavoidable crises" denote disruptive events that cannot be prevented, despite efforts to mitigate or avoid them. Unavoidable crises could be foreseen, and efforts could be made to prepare for them, should they happen.

resilience of nuclear safeguards and crisis management. The debates are multifaceted and include discussions on how to adapt to technological advances and political changes (Ahn et al. 2017; Kumar 2023; Roth et al. 2024). Our paper examines how the Agency can possibly operate effectively in scenarios where knowledge continuity is disrupted, requiring rapid and reliable responses. The crisis scenarios include (1) a terrorist occupation of a nuclear storage facility, (2) a flood, and (3) a mismatch of information after a coup d'état.

This article is divided into three parts. In the first part, we briefly describe IAEA inspections in interim storage facilities, with their specificities. In the second part, we briefly define the general setting of our workshop exercises, justify decisions, and define the structure we applied to the simulation settings. The third part discusses the results and conclusions of the workshop, which are further summarised and organised in the conclusion. We also describe the main "takeaways" and conclusions of the workshop in Table 2 in the third part of this article. These conclusions may serve as food for thought for the Agency to effectively respond to crisis scenarios.

1 IAEA inspections in interim storage facilities

Nuclear storage facilities play a crucial role in the nuclear fuel cycle. With the increased global focus on nuclear energy to reduce carbon emissions and the almost complete absence of geological repositories to permanently store high-level waste in the foreseeable future, these facilities will continue to be safeguards-relevant. Spent fuel is bound to remain in nuclear interim storage facilities for decades to come, even in States that have made commitments to phase out nuclear energy until its final disposal in a geological repository. More specifically, these storage facilities contain closed and sealed casks, often more than six meters high, loaded with spent fuel elements and high-level radioactive waste (e.g., CASTOR® type or similar). The elements are first removed from the reactor core and then cooled in a spent fuel pond for approximately 5 years. Thereafter, they are loaded underwater into a storage cask. Once loading is completed, the spent fuel cask is lifted out of the water and dried until a certain drying criterion is reached. The loaded cask will then be closed, sealed, and transported from the reactor to the storage facility (Aymanns et al. 2017).

Most nuclear interim storage facilities are outdoor buildings surrounded by fences and a protection area. The relocation of casks to nuclear storage facilities can be a challenging endeavour, especially when the storage area is near full capacity. The design and size of the casks usually complicate easy or frequent movement in the facility. Space limitations may also prevent the straightforward movement of casks, potentially necessitating the shifting of all casks located in front of the target cask. Interim storage facilities are access-controlled according to on-site safety and security requirements so that only certain personnel and vehicles can enter the facility. Accredited IAEA inspectors need access authorisation for the controlled area, which is given by the country's regulatory authority (IAEA 2020).

Safeguard measures within interim nuclear storage facilities serve to enable the IAEA to detect unauthorised diversion of nuclear materials and thereby act as a deterrent against such actions (Fischer et al. 2022; Rauf 2016). The storage hall with the spent fuel casks is constantly monitored by surveillance cameras, which save the data to local storage and/or send the data to the responsible national or regional safeguards authority, who then submits these data to the IAEA headquarters (Aymanns et al. 2017). The casks are closed with passive or (less frequently) active seals that indicate whether a cask has been opened. The facility operators keep records of the inventory and associated changes, which are shared with national (or regional) regulators such as Euratom or national nuclear energy authorities. IAEA inspectors visit such facilities on a regular basis to carry out inspections. They verify a certain number of seals, some of which are replaced, depending on their type. Inspectors also verify inventory reports, count and identify the casks in the storage hall, and, if necessary, collect the storage data of the cameras. The activities performed in the cask storage hall are also optimised to minimise the duration of stay due to the radiation in the area.

2 The "Darmstadt simulation": design and scenarios

To assess the three scenarios (1. a terrorist occupation, 2. a flood, 3. a mismatch of information), we conducted an in-person scenario-based workshop following a "world café" format. The world café approach, as described mainly by Juanita Brown, is a "technique [that] was developed specifically to facilitate knowledge exchange" (Prewitt 2011, p. 189) in a group setting. In short cycles, participants engage in a structured exchange of individual experiences and knowledge to find a shared "collective and more valuable" (Prewitt 2011, p. 190) understanding or new ideas. The participants are mixed in every round, meaning that they do not stay in a single group but rather discuss in different compositions to gather a maximum of exchange between the participants and their very own knowledge and experiences.

Following this described world café format, and with respect to the World Café Foundation's description of the methodology as well as its seven "World Café Design Principles" (see The World Café Community Foundation (n. d. a, b)), we conducted our workshop through structured synchronous discussion rounds with randomised groups of peace and conflict experts from the natural and social sciences. Those experts were drawn from participants at the conference *Science—Peace—Security '23* held between 20 and 22 September 2023 in Darmstadt, Germany (henceforth, we call it the "Darmstadt Simulation"). Overall, our workshop had 18 participants, 10 of whom were women and 8 of whom were men. Most of those participants worked as researchers at universities and think tanks in Europe, and all of them either had or were pursuing a PhD. The exercise was instructed by an interdisciplinary team of seven VeSPoTec researchers at the doctoral and post-doctoral levels.

Prior to the simulation, all participants were sent a booklet with general terms and concepts associated with nuclear verification and inspections. On the simulation day, they were first briefed with general information on what nuclear safeguards are and how they are conducted in interim nuclear storage facilities. All participants were instructed about their roles and expectations: they were to be part of an "ad hoc interdisciplinary advisory group" charged with writing a report to the IAEA

Director General with possible pathways the Agency could follow to overcome the immediate lack of access to the storage facility. In that exercise, participants were asked to think specifically about safeguards, that is, how to assess whether nuclear material has been or could have been diverted from its peaceful purposes.

Under the "world café" methodology, each participant was then given a list with a random order of scenarios they should follow for different discussion rounds (e.g., round 1: flood; round 2: occupation; round 3: misinformation). We opt for this participant-mixing procedure to reduce the influence of previous socialisation effects among participants in the activity (to avoid situations of like-mindedness) and to have a maximum of knowledge exchange, as described above. We briefed all participants together on the details of all three scenarios, and then they were divided into separate tables to discuss each scenario. They changed tables for every discussion round (every twenty minutes), following the random pre-set order. In each discussion round, participants were given a different question for discussion. The first round focused on collecting safeguards data. Here, participants were asked (1) *what information and information sources the IAEA should consider* for each scenario and (2) *which information would be most valuable* to the *Agency.* Then, the participants were asked to change tables, and a new set of questions was asked. The second round was centred around interpreting the information and drawing conclusions. Participants were asked (1) *what information and sources of information were more and less useful for verification purposes,* (2) to *rank the information and sources* gathered from the previous group, and (3) to determine *what was missing* from that list. After a new change in groups, the third round addressed the safeguards regime, and the participants were briefed on the discussions from the first two rounds and asked *what the IAEA could do to make the safeguards regime more resilient and prepared* for situations of unavoidable crises.

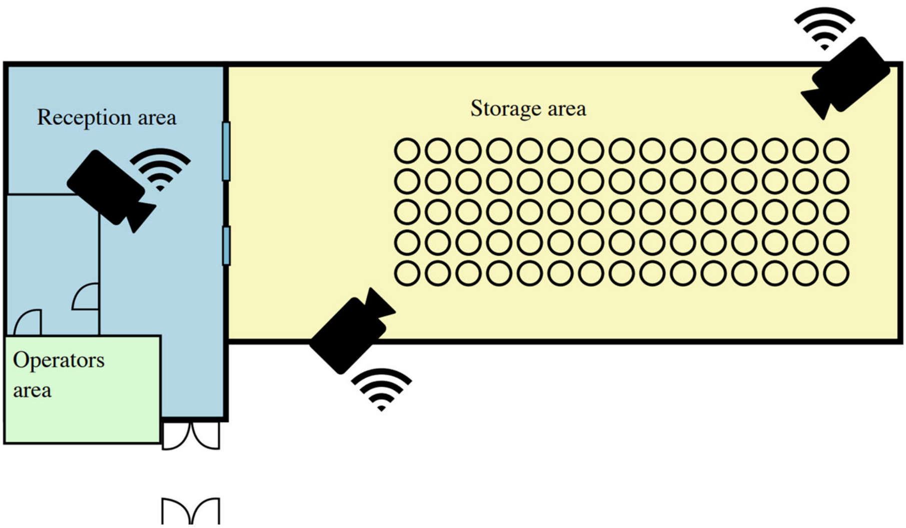

Fig. 1 Building Plan for an Interim Nuclear Storage Facility. Source: VeSPoTec, based on a chart by BASE. Bundesamt für die Sicherheit der nuklearen Entsorgung (BASE): https://www.base.bund.de/DE/themen/ne/zwischenlager/bauweise_zwl/bauweise-zwl_node.html (retrieved 9th February 2024)

Audio recording was not feasible during the exercise. Nonetheless, multiple methods were employed to gather information. First, participants documented and structured their group's scenario dialogue outcomes on posters, which were later collected. In addition, multiple VeSPoTec representatives were designated notetakers for each group. Finally, another VeSPoTec member was assigned to monitor the group interactions, noting any unusual patterns or dynamics. Post-exercise, all collected data were triangulated between all VeSPoTec members to obtain a comprehensive picture of the discussion.

For the workshop, we defined a setting of a regular interim storage facility in a non-nuclear-weapon State that is a member of the Nuclear Non-Proliferation Treaty and that has a Comprehensive Safeguards Agreement with an Additional Protocol with the IAEA in force. The fictitious facility contained 75 dry casks and had the capacity to store 100. These casks contained spent fuel elements from a nuclear reactor located close to the facility. We based our workshop on a storage facility with a typical design (Aymanns et al. 2017), as illustrated in Fig. 1 below. This figure was shared with participants in the "Darmstadt Simulation" and was used in all three crisis scenarios.

We developed three scenarios of possible crises involving safeguards implementation in nuclear storage facilities: (1) a terrorist occupation of a nuclear storage facility in the fictitious country of Plutopia, (2) a flood that harmed communications in the fictious country of Northern Urania, and (3) a mismatch of information after a coup d'état in the fictious country of Atomika. These cases were designed based on general political trends and global shifts in international systems, as foreseen by specialised literature (Kohler 2021; MOD 2018). These trends include the possible

Table 1 Key Aspects of Three Scenarios

	1. Terrorist Occupation	2. Flood	3. Misinformation
IAEA inspector's access to the facility	Not possible	Not possible	Not possible
Regulator's (state) access to the facility	Not possible	Restricted	Possible (but the IAEA has no contact with regulator)
Source of the crisis	External occupation of facility	Environmental catastrophe	"Leak" of information or "misinformation" campaign
Nature of the crisis	A hostile group may have diverted nuclear material	Restricted physical and virtual access to the facility and danger of losing data (e.g., books)	Misleading or mismatching information
Means to assess compliance (technology, physical material, etc.)	No access to traditional means (on-site verification or remote access)	Restricted access to means and possible loss of sources for future inspections	Official means of assessing information show evidence that is contested by unofficial means. There is no certainty to confirm which means to rely on
Nature of the risk	Diversion of nuclear material	Loss of information to assess peaceful commitments	Diversion of nuclear material

growing role of non-state actors in global politics, including those with non-peaceful intentions such as terrorist organisations; the increased frequency of natural disasters (such as floods) due to climate change; the possible resurgence of domestic instability, particularly in "fragile" states; and the emergence of social media and new technologies as key sources of social instability. It should also be noted that our scenarios are limited to safeguards and do not address general nuclear safety and security concerns.

These scenarios represent unavoidable situations that fall beyond the realm of control, and they present challenges that make on-site inspections impossible in the short term. We also chose different countries for each scenario to isolate those cases from each other. Table 1 shows the main aspects of each of the three scenarios and how they differ from each other. In all scenarios, IAEA inspectors do not have full on-site access to nuclear facilities and are therefore bound to find ways around those limits. Each scenario will be explored in more detail in the next section of this article.

Scenario 1 (Occupation): Terrorist Occupation in Plutopia. The first scenario occurs one day after a terrorist group with unrealisable demands occupies an interim nuclear storage facility in the fictitious country of Plutopia. The terrorist group had previously attacked critical infrastructure in Plutopia. They have proven to be technologically capable of executing their threats and are known to avoid negotiations. They would simply wait until their demands are fulfilled, which, in our case, is not possible. In the evening, the terrorist group arrived in a heavy transport truck at the interim storage facility, overpowered the security personnel, and forced the staff to grant access to all areas of the facility, including the archives with sensitive information about storage casks and, possibly, the casks themselves. A few hours later, the facility's staff was released from the facility without mobile phones. Since the facility is in an isolated area, they needed a couple of hours to contact local authorities about the occupation. At the time of the scenario simulation, the facility is surrounded by Plutopia's army forces, and access to the road is blocked. The terrorists switched off the IAEA cameras, which were used to provide remote monitoring of the facility, and they issued threats via social media to open the casks and remove the nuclear material. According to the State's intelligence service, those threats should be taken seriously, and in an extreme situation, they may even destroy the facility as a whole. They buttress their threats by sharing a video on social media where they show how they cut a seal from a dry cask. It is unclear whether the heavy transport truck left the site and returned during the first hours of the occupation.

Scenario 2 (Flood): Flood in Northern Urania. The second scenario consisted of a severe flood in the fictitious country of Northern Urania, which also affected an interim storage facility. In that scenario, the facility was not structurally damaged, but water leaked into the building, and the staff is currently busy cleaning up the office rooms and repairing the outer fence around the facility. The roads around the facility are partially destroyed. Northern Urania's airports are being shut down, and its government notified the Agency that inspections could not be carried out for at least six months due to rebuilding efforts in the country. The operation staff are in the facility and can be reached by mobile phones. However, due to the destruction of infrastructure, power connections are not very stable, and data transmission from remote monitoring systems is limited. Northern Urania has stable governing institutions and is a nuclear "newcomer" that has already developed reasonable expertise in the nuclear field.

Scenario 3 (Misinformation): Mismatching Information after Coup d'État in Atomika. The third scenario pictured an abrupt change in regime after a successful coup d'état in Atomika. The new ruling elite closed all borders while forming a new government, leading to an unstable and unpredictable situation. There is also no clear contact point with the new administration, which renders on-site inspections impossible. All communication of the new government has been reduced to a minimum. The new ruling elite claims that this is only a temporary situation and that the new government will behave cooperatively in the future. During the coup d'état, all systems in the country, including remote camera monitoring at the country's only interim nuclear storage facility, were cut off for approximately three hours. Moreover, several pictures and videos were suddenly reported by reliable mainstream media channels showing two spent fuel casks being loaded onto a truck and taken away from an interim storage facility. After three hours, the Agency has recovered access to remote monitoring in the facility, and the camera footage does not show any signs that casks have been diverted. At this point, contact with the operators of the facility is difficult. However, it is known through informal channels that they are safe and have not recorded any unusual activity.

3 The "ad hoc interdisciplinary advisory group" report: discussions and results

3.1 Discussion round 1—Sampling information and information sources

Terrorist Occupation in Plutopia. In the first round of discussions, participants in the "Darmstadt Simulation" suggested considering six sources of information, all of which would be gathered by the Agency itself due to the absolute lack of cooperation with the facility occupiers: (1) satellite imagery (e.g., activity in the loading bay of the facility); (2) social media searches for suspicious observations (e.g., videos or photos of heavy trucks or casks); (3) venues and local traffic surveillance cameras if they exist; (4) interviews with the released staff to clarify if they were forced to move casks or if such a movement is possible; (5) interviews with experts on terrorism to collect more information on the terrorist's motives; and (6) inquiring with the truck company for the specifications or the hiring information of the truck.

Flood in Northern Urania. Participants suggested considering the following sources of information, divided into five strategies. The first strategy involved communication and cooperation with the operators of the facility, which included (1) comparing cask ID (identification codes) lists, (2) conducting random sampling of cask positions, (3) sending local camera monitoring or radiation monitoring data from the facility via available means of communication, and (4) sending photos or videos of the casks via mobile phones. The second strategy involved communicating with State authorities from Northern Urania, including (5) asking for access to traffic surveillance data from the areas surrounding the facility and (6) checking the current road (access) status. The third strategy was open-source data collection, including (7) satellite imagery and (8) social media searches. Fourth, the participants suggested (9) observing and thereby evaluating the State's true intentions behind negotiations about the postponement of annual safeguards inspections and (10) evaluating past relations with Northern Urania and previous reports provided since the last on-site inspections. The last strategy was to establish a standing ad hoc group to assess the situation and mediate an agreement for restored access to the facility.

Mismatching Information after Coup d'État in Atomika. The first round of discussions centred on how to ensure that available data are reliable and may serve as a source for knowing what was, *de facto,* happening in the storage facility. General consent was obtained to avoid assuming that nuclear storage casks were indeed diverted. Much thought has been given to (a) how to verify the authenticity of available information (i.e., the images from the cameras on site and the images available in mainstream media) and (b) how to acquire further information that can be used to confirm or reject diversion suspicions. Twelve different activities were mentioned from where to obtain information, namely, (1) repeatedly verifying images and videos to detect fake news and deep fakes; (2) monitoring traffic/street images around the facility; (3) confirming changes in satellite images; (4) tracking GPS signals from trucks and casks (if applicable); (5) scrutinising changes in software or hardware used in the facility related to facility management, involving cloud storage services, video chat apps, antivirus systems, etc.; (6) establishing informal contacts within the country; (7) engaging informal networks of retired agents with country-specific inspection experience to assess media images; (8) scouring social networks for images from local residents or individuals connected to the facility; (9) analysing historical cases of movement of people and material inside storage facilities to identify patterns; (10) mapping potential destinations and pathways for transported casks; (11) researching the new government's key figures, their roles, and ideologies; and (12) monitoring activity at the Atomikan borders and communicating with neighbouring countries to track potential cask movements during or after the coup.

3.2 Discussion round 2: prioritising information sources

Terrorist Occupation in Plutopia. During the subsequent discussion phase, the participants prioritized data gathered from satellite imagery (depending on the weather), interviews with former employees, and observations from local sites and surveillance equipment as the primary and most critical sources of information. Meanwhile, insights from social media and communications with the transportation company were deemed important but of secondary priority.

Flood in Northern Urania. The information sources regarded as most important included satellite imagery, radiation monitoring data, photos and videos provided by facility staff, and information relevant to assessing Northern Urania's intentions and cooperativeness. The participants deemed social media information potentially unreliable and noted limitations in trying to monitor the country's facilities in a situation of public mobilisation. Furthermore, the participants pointed out that excessive demands on operators or excessive questioning of the State's intentions could erode trust between the parties.

Mismatching Information after Coup d'État in Atomika. The main takeaway of this discussion was that it would not be advisable to rank all activities on a "one by one" basis but rather to define three layers of priority, each one covering activities that should be conducted "immediately", "as soon as possible", or "if needed". The first layer of priority ("immediately") addressed the most reliable sources of information that should be obtained immediately. Taken from the list above, these include (1) "image-checking" from the cameras in the facility, (3) satellite images, (7) contacting informal networks of people in the country, and (12) border checks. Based on those sources, the Agency may be able to identify which hypothesis (i.e., diversion or non-diversion of a cask) is most likely. The second layer of information ("as soon as possible") included "less reliable" information that is advisable only to consider once the first preliminary conclusions are reached. The second-layer sources included (2) checking traffic and street images, (7) contacting informal networks with people who have experience with the country, (4) GPS signals, and (10) mapping potential destinations to diverted casks. The third layer of information ("if needed") covered sources that should be consulted at a later moment, pending the availability of time and resources. Third-layer sources include (5) past changes to hardware and software in the facility, (8) social networks and open-source information, and (11) information about the new government ("who is in charge").

3.3 Discussion round 3: increasing resilience

Terrorist Occupation in Plutopia. In the third round of discussions, participants were tasked to think about suggestions for improving the IAEA's safeguards resilience, including adding technical measures, as participants identified the lack of redundant remote technology throughout the interim storage facility as the greatest shortcoming. If the cameras fail, they are technically blind. Such additional technical measures could include (1) (remote) monitoring of the cranes to assess when and how cranes are moved, (2) equipping the casks with tracking devices, (3) placing scales under the casks that could issue alerts when they are being moved, or (4) using robotic devices and drones to monitor plant perimeters and facilitate labour-saving on-site inspection. In terms of existing technical measures, satellite imagery was seen as the most important source of information, which could be linked to the presence of satellite experts among the participants. Even if the images were not conclusive (e.g., due to cloud cover or other technical problems), frequent satellite imagery would help to monitor movement around the facility. During the discussions, participants further highlighted that IAEA verification efforts in this scenario would require intensive contact and cooperation at multiple levels, including the State and local authorities in Plutopia. In such future cases, open channels for such communication should be established as quickly and efficiently as possible.

Flood in Northern Urania. In the third round of discussions, participants identified a range of technical, institutional, and cooperative measures that could be pursued to make the IAEA safeguards regime more resilient. Technical measures included (1) establishing alternative data connections for existing surveillance equipment, potentially via satellite links, and (2) expanding the use of sensors, such as cameras, radiation monitoring devices, floor scales, and drones, for more comprehensive monitoring. Institutional means included (3) increasing the budget to increase the IAEA's capabilities, (4) providing additional funding for research, and (5) (if not already done) revising regulations for the geographical location of interim storage facilities. Finally, cooperation measures, deemed the most important for increasing resilience, included (6) integrating efforts with other emergency teams—associated with the IAEA or not—, (7) training facility operators on safeguards awareness and crisis management and (8) developing clear crisis guidelines at both the facility and State level (i.e., increasing preparedness).

Mismatching Information after Coup d'État in Atomika. The participants' discussion on how to enhance the safeguards regime's resilience was centred around two keywords, namely, "triangulation" and "redundancy". "Redundancy" emphasises the importance of multiple information sources for verification that give the same information, and those sources could be confirmed ("triangulated") with each other. Specific suggestions included (1) ensuring remote sensing throughout all process stages, including access points such as doors and throughout all relevant facility areas; (2) establishing a standing crisis committee with high-ranking personnel of the Agency and external advisors of diverse expertise, ready for immediate deployment; (3) incorporating physical redundancies at various process stages, including cask identification; (4) equipping casks with GPS trackers and possible identification markers such as large QR codes, facilitating media image verification; (5) strengthening resilience in taking into account transportation activities; and (6) harnessing new technology, such as drones, to enhance verification efforts in collaboration with other actors.

4 Safeguards during crisis: implications and conclusions

This article contributed to the discussions on nuclear safeguards by exploring possible ways to conduct safeguards in situations of unavoidable crises in nuclear interim storage facilities, where the continuity of knowledge is broken due to the lack of access to the facility. We assessed such crises in a scenario-based workshop (the "Darmstadt Simulation"), which was conducted in a conference session of the *Science—Peace—Security '23* with the conference participants. By inviting such an interdisciplinary group of scholars with broad expertise, our goal was to start the dialogue and promote out-of-the-box thinking, profiting from more diverse perspectives. We sought to explore as many options for building resilience as possible, which might be beneficial to the Agency's preparedness in future unavoidable crises. Additionally, by analysing three different scenarios isolated from each other, we could identify sources of information that were not case-specific and came up in every scenario, which could provide possible choices of where to focus energy and financial resources. Nonetheless, a future exercise would benefit from the presence of at least some verification experts other than the organisers.

It is relevant to note that some participants leaned toward strengthening the resilience of the already existing safeguards regime by adopting a broader approach

Table 2 Summary of Main Sources of Information and Resilience Measures

	1. Terrorist Occupation in Plutopia	2. Flood in Northern Urania	3. Mismatching Information After Coup D'état in Atomika
Shared non-case specific sources of information (more important)	Satellite imagery Facility staff (interviews/contact) Image data (authenticated and checking for fake news or deep fakes)		
Shared non-case specific sources of information (less important)	Social media data Traffic/street imagery Former facility staff (interviews/contact)		
Case specific sources of information (more important)	Data on truck movements (e.g., provided by the truck company) International and local authorities	Cask ID (identification codes) lists Random samples of cask positions to check for specific IDs Local camera monitoring or radiation monitoring via available means of communication Photos or videos of the casks (sent via mobile phone)	Informal networks of people in the country Border checks
Case specific sources of information measures (less important)	Terrorist experts	Evaluation of the country's past relations with the Agency Reassessment previous reports provided since the last on-site inspections	Informal networks of people who have experience with the country Map of potential destinations of the diverted casks Hardware and software for verification

Table 2 (Continued)

	1. Terrorist Occupation in Plutopia	2. Flood in Northern Urania	3. Mismatching Information After Coup D'état in Atomika
Shared non-case specific future resilience and preparedness measures	Increase multilevel cooperation on a local and international level		
	Attaching tracking devices to the casks		
	Developing clear crisis guidelines both at the facility and State level		
	Expanding the use of additional sensors (increasing redundancy) including tracking devices		
	Strengthening resilience in verifying transportation activities		
Case Specific future resilience and preparedness measures	Establishing common crane protocols Placing scales underneath under all the casks to detect potential movement	Establishing alternative data connections for existing surveillance equipment	Emphasising remote sensing throughout all nuclear process stages Equipping, casks with GPS trackers and possible identification markers like large QR codes Harnessing new technology, like drones, and old technologies like Geiger counters, to enhance verification efforts in collaboration with other actors
"Take out"	The lack of remote data transmission throughout the interim storage facility was the biggest shortcoming	Excessive questioning of the State's intentions could erode the trust relations with personnel on the ground	In the absence of new sources, verifying and confirming existing data, and contacting existing networks of individuals becomes increasingly important

that would consider establishing social connections and multiple channels of communication with the facilities, together with a conscious and justified establishment of additional data sources: data sources that were already in use and available for the Agency, such as satellite images (Rutkowski and Niemeyer 2020; Pabian et al. 2020) and radiation monitoring of sealed casks (Tarvainen et al. 1997; Williamson and Preston 2020), were deemed most valuable in the scenarios—as asked in the guiding question of Round 2. In summary, however, participants followed an inherently holistic approach to evaluate all the scenarios, which considered both traditional data assessment techniques and associated non-traditional methods (e.g., social media sources and fact-checking mechanisms). Such flexibility to integrate available sources beyond the traditional options available to safeguard inspectors should be more relevant in the future.

Table 2 summarises the main topics that arose in the discussions among the peace and conflict scholars and experts in the "Darmstadt Simulation" and indicates the sources of information that were suggested by participants in all three scenarios. Those include not only technical sources such as the use of satellite images (e.g., to monitor the streets and access to the storage facility) or, even if on a smaller scale and with many reservations, social media analyses; they also highlighted the importance of social sources such as contacts with relevant personnel on the ground. Table 2 also indicates the need to tailor specific answers for each scenario. In scenario 1 (occupation), for example, consulting with terrorist experts outside the IAEA was deemed a relevant way forward, as it would enable safeguards inspectors and analysts to define how to approach the facility without negotiating with the terrorists directly. In another example, discussions in scenario 3 (misinformation) also suggested the relevance of keeping track of broader political developments that could change the course of verification activities. Such a tracking process may also be achieved by maintaining frequent contact with relevant stakeholders, who can support the evaluation of the usefulness, limits and opportunities of new challenges that safeguards may face. Such networks may provide a relevant source of information and avoid situations that may erode trust between the Agency and relevant stakeholders.

As also established in the literature (Jorant 2020; Amaldi 1991; Drayer et al. 1990), participants in the simulation highlighted the cruciality of managing and providing redundant data or data sources that can be used to ensure consistent verification assessments when on-site inspections are not possible (redundancy principle). These findings indicate the need to approach crises in a holistic way and to rely on multiple sources that complement and strengthen each other. It also shows, however, the need to rank data appropriately according to their robustness, transparency, traceability, and technical soundness. In that regard, for example, most third-party sources, including social media data, were deemed less reliable than direct sources, such as interviews with local facility staff and distance radiation measurements.

Overall, the results of the "Darmstadt Simulation" highlighted the need for addressing safeguards in crisis situations under a broad approach that considers not only technical but also societal and political aspects. Participants were, in general, quite immersed in the scenario settings and embraced the premises previously set in the three narratives. This immersion, which was pointed out by participants in a feedback discussion after the simulation, facilitated broad discussions, allowing for different approaches that surpassed the scope of the specific scenarios. The world café method proved to be a useful tool for actively engaging different experts in a casual environment without judgement and motivating them to bring their expertise to the table in a playful manner. That most of the participants did not have a background in IAEA verification activities, allowed for creative ideas “outside the box”. However, a possible improvement for the next step is to explore how realistic and practical the proposed ideas are. This would entail consulting with verification experts from various fields, such as technology, politics, and law, to carefully assess the potential difficulties and dangers but also potentials associated with them.

As the global community continues to grapple with the delicate balance between harnessing nuclear energy for peaceful purposes and preventing its diversion towards military purposes, the IAEA’s preparedness to ensure its safeguards mission in unavoidable crises in interim nuclear storage facilities becomes increasingly crucial, as those facilities become more present in all countries that possess or once have possessed nuclear technology. Such effort requires not only continued updating to keep track of current technological developments but also a holistic approach to verification and openness to new sources of information—without, of course, losing track of the technical robustness and traceability of those sources and being mindful of limiting intrusiveness. Such studies should include frequent contact with stakeholders in academia and research who can support and evaluate the usefulness, limits and opportunities of new approaches to address new challenges safeguards may face. Last, it is also important that the IAEA and other verification agencies maintain information sources and social networks that endure and can be easily retrieved if an unavoidable crisis occurs.

Acknowledgements The authors thank the organisers of the Science—Peace—Security ‘23 Conference (SPS) for their support, which made this simulation possible. We also thank Lena Herholz and Pia Stickeler for organisation and logistical support in the preparation for the simulation, as well as the Nuclear Verification and Disarmament Group of the RWTH Aachen University, particularly Benjamin Jung and Max Schalz, for their participation in a mock simulation. Previous versions of this article were read and commented on by Katharina Aymanns and Kim Westerich-Fellner. Their comments and suggestions helped to improve this article considerably. We would also like to thank the editors of the Zeitschrift für Friedens- und Konfliktforschung and the anonymous reviewers for their time and suggestions.

Funding This article research is funded by the German Ministry of Education and Research (BMBF), grant number 01UG2210A (VeSPoTec).

Author Contribution L. Bandarra: Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Visualization, Writing: Original Draft Preparation, Writing: Review & Editing; S. Böschen: Funding Acquisition, Project Administration, Supervision, Commenting; A. Dürholt: Conceptualization, Data Curation, Investigation; R. Geiser: Conceptualization, Data Curation, Investigation; M. Göttsche: Conceptualization, Funding Acquisition, Investigation, Project Administration, Supervision, Writing: Review & Editing; S. Kretzschmar: Conceptualization, Data Curation, Investigation, Methodology, Formal Analysis, Project Administration, Writing: Review & Editing; I. Niemeyer: Funding Acquisition, Project Administration, Supervision, Commenting; L. Ostermann: Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Writing: Review & Editing; L. Rademacher: Conceptualization, Data Curation, Investigation; J. Schäfer: Conceptualization, Data Curation, Investigation, Formal Analysis, Methodology, Project Administration, Writing: Review & Editing.

Funding Open Access funding enabled and organized by Projekt DEAL.

Conflict of interest L. Bandarra, S. Böschen, A. Dürholt, R. Geiser, M. Göttsche, S. Kretzschmar, I. Niemeyer, L. Ostermann, L. Rademacher and J. Schäfer declare that they have no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Ahn, Joonhong, Franck Guarnieri, and Kazuo. Furuta. 2017. *Resilience: a new paradigm of nuclear safety*. Cham: Springer International.

Amaldi, Edoardo. 1991. The future use of redundant weapon-grade material. In *Reducing Nuclear Arsenals*, ed. Carlo Schaerf, David Carlton, 79–95. London: Palgrave Macmillan.

Aymanns, Katharina, Arnold Rezniczek, Astrid Jussofie, and Irmgard Niemeyer. 2017. Sealing systems in German spent fuel storage facilities. *ESARDA Bulletin* (55):39-43.

Cooley, Jill N. 2020. The evolution of safeguards. In *Nuclear non-proliferation and arms control verification*, ed. I. Niemeyer, M. Dreicer, and G. Stein, 27–41. Cham: Springer International.

Drayer, Darryl D., Cecil S. Sonnier, Dennis L. Mangan, and Frank Walford. 1990. Redundant and independent containment and surveillance systems. Sandia Report SAND-90-0806. https://www.osti.gov/biblio/5758246.

Fischer, David, Paul C. Szasz, and Josef Goldblat. 2022. *Safeguarding the Atom: A Critical Appraisal*. London: Routledge.

Grümm, Hans. 1987. IAEA Safeguards: Milestones in Development & Implementation. *IAEA Bulletin* (3):29-34. https://www.iaea.org/sites/default/files/29303452934.pdf.

IAEA. 2014. IAEA Safeguards Overview. Text. July 7, 2014. https://www.iaea.org/publications/factsheets/iaea-safeguards-overview.

IAEA. 2018. IAEA Nuclear Safety and Security Glossary. International Atomic Energy Agency. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf.

IAEA. 2020. Storage of Spent Nuclear Fuel: Specific Safety Guide. No. SSG-15 (Rev. 1). International Atomic Energy Agency. https://www-pub.iaea.org/MTCD/Publications/PDF/P1882_web.pdf.

Ikonomou, Pantelis F. 2021. *Global nuclear developments: insights from a former IAEA nuclear inspector*. Cham: Springer.

ISCN (Integrated Support Center for Nuclear Nonproliferation and Nuclear Security). 2016. Handbook of international nuclear safeguards. Tokai-mura, Japan: Japan Atomic Energy Agency. http://www.jaea.go.jp/04/iscn/archive/ssac/ISCN%20SSAC%20handbook.pdf.

Jorant, Caroline. 2020. Adapting non-proliferation approaches to a changing world: a European expert's viewpoint. In *International Cooperation for Enhancing Nuclear Safety, Security, Safeguards and Non-Proliferation,* ed. Luciano Maiani, Raymond Jeanloz, Micah Lowenthal, Wolfango Plastino, 123-132. Cham: Springer.

Kohler, Kevin. 2021. *Risk and Resilience Report: Strategic Foresight, Knowledge, Tools, and Methods for the Future*. Zürich: Center for Security Studies (CSS), ETH Zürich. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/505468/2/RR-Reports-2021-StrategicForesight.pdf.

Kumar, Rajesh. 2023. Building resilience against nuclear disaster. In *International Handbook of Disaster Research*, ed. Amita Singh, 257–272. Singapore: Springer Singapore.

MOD. 2018. Global Strategic Trends: The Future Starts Today - Sixth Edition. London: Ministry of Defence.

Pabian, F.V., G. Renda, R. Jungwirth, L.K. Kim, E. Wolfart, G.G.M. Cojazzi, and W.A. Janssens. 2020. Commercial satellite imagery: an evolving tool in the non-proliferation verification and monitoring Toolkit. In *Nuclear non-proliferation and arms control verification*, ed. Irmgard Niemeyer, Mona Dreicer, Gotthard Stein, 351–371. Cham: Springer International.

Pellaud, Bruno 1991. Safeguards in transition: Status, challenges, and opportunities: Political and technological developments are strongly influencing the IAEA's system for verifying the peaceful uses of nuclear energy. IAEA Bulletin 36(3):2–7. https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull36-3/36303480208.pdf.

Pilat, Joseph F. 2021. *The International Atomic Energy Agency: Historical Reflections, Current Challenges, and Future Prospects*. London: Routledge.

Prewitt, Vana 2011. Working in the café: lessons in group dialogue. *The Learning Organization* 18(3):189–202.

Rauf, Tariq. 2016. The general framework of IAEA safeguards. In *Nuclear Non-Proliferation in International Law, Vol. II - Verification and compliance*, ed. Jonathan L. Black-Branch, Dieter Fleck, 11–21. The Hague: T.M.C. Asser Press.

Rockwood, Laura 2013. *Legal framework for IAEA safeguards*. Vienna: International Atomic Energy Agency.

Roehrlich, Elisabeth. 2022. *Inspectors for Peace: A History of the International Atomic Energy Agency.* Baltimore, MD: Johns Hopkins University Press.

Rosenthal, Michael, and Warren M. Stern. 2019. *Deterring Nuclear Proliferation: The Importance of IAEA Safeguards*. Upton, NY: Brookhaven National Laboratory. https://www.osti.gov/servlets/purl/1525379.

Roth, Nickolas, Ross Matzkin-Bridger, and Jessica Bufford. 2024. Nuclear facilities in times of crisis. NTI Paper. Washington, DC: Nuclear Threat Initiative. https://www.nti.org/wp-content/uploads/2024/06/NTI_Paper_FITOC_FINAL_060724.pdf.

Rutkowski, Joshua, and Irmgard Niemeyer. 2020. Remote sensing data processing and analysis techniques for nuclear non-proliferation. In *Nuclear non-proliferation and arms control verification*, ed. Irmgard Niemeyer, Mona Dreicer, Gotthard Stein, 339–350. Cham: Springer International.

Seaborg, Glenn T., and Benjamin S. Loeb. 1993. *The Atomic Energy Commission Under Nixon: Adjusting to Troubled Times*. New York: Palgrave Macmillan.

Tarvainen, Matti, Ferenc Lévai, Timothy E. Valentine, Mark Abhold, and Bruce Moran. 1997. NDA techniques for spent fuel verification and radiation monitoring. Report on activities 6a and 6b of task JNT C799 (SAGOR). Finnish support programme to the IAEA safeguards. Helsinki: Radiation and Nuclear Safety Authority (STUK). https://www.osti.gov/etdeweb/biblio/599096.

The World Café Foundation. n.d. a. Design Principles. The World Café Foundation. https://theworldcafe.com/key-concepts-resources/design-principles/. Accessed 13 June 2024.

The World Café Foundation. n.d. b. World Cafe Method. The World Café Foundation. https://theworldcafe.com/key-concepts-resources/world-cafe-method/. Accessed 13 June 2024.

Weichselbraun, Anna. 2020. From Accountants to Detectives: How Nuclear Safeguards Inspectors Make Knowledge at the International Atomic Energy Agency. *PoLAR: Political and Legal Anthropology Review* 43(1):120–135.

Williamson, Martin, and Jeffrey Preston. 2020. Radiation detectors and instrumentation. In *Nuclear non-proliferation and arms control verification*, ed. Irmgard Niemeyer, Mona Dreicer, Gotthard Stein, 249–264. Cham: Springer International.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.