CYBER NUCLEAR FORUM AUTUMN 2025 MEETING

Amsterdam, the Netherlands. 07-10 September 2025

Summary

From 7–10 September 2025, the Cyber Nuclear Forum (CNF) held its Autumn meeting in Amsterdam, the Netherlands, bringing together 25 members and 6 external experts to exchange knowledge and reflect on pressing nuclear cyber security issues. The agenda featured high-level discussions on geopolitical developments beyond the nuclear sector, supply chain security, and the role of public–private partnerships in strengthening cybersecurity. Participants engaged in topical working groups on insider threats, artificial intelligence, and governance, while also sharing operational experience on remote access for maintenance and cybersecurity in decommissioning. The meeting concluded with a site visit to the NRG PALLAS facilities in Petten, including tours of the High Flux Reactor, Hot Cell Laboratories, the PALLAS construction site, and the Decommissioning and Waste Treatment facility offering members unique insights into nuclear projects. The event underlined the importance of trust, collaboration, and diversity in the CNF community, while highlighting future priorities for 2026.

Update on CNF Status and Strategic Plan

Mr. Anno Keizer of Urenco Nederland B.V., the Netherlands, and Chair of the CNF Steering Committee (SC), welcomed participants and provided a brief overview of the Forum and its recent activities. He also presented the CNF action plan for 2026. Mr. Todd Warnell of Bruce Power, Canada, and Vice Chair of the CNF SC, then outlined the objectives and agenda of the Autumn meeting.

Participants reflected on the Forum's identity, value proposition, and future direction. Discussions highlighted the importance of CNF maintaining its distinctiveness by fostering trust among members, focusing on operators' needs, and ensuring tangible benefits from participation. The meeting also underscored the need to enhance geographical and gender diversity, noting the limited representation of women in cyber roles and the importance of broader outreach, particularly to major operators in the United States and Asia. Participants also highlighted the necessity of clear differentiation between Forum members and participants in CNF activities, as well as the potential for special events to engage vendors and industry leaders. Funding was again identified as critical to sustaining CNF activities, with calls for imaginative approaches to securing support. Furthermore, participants discussed the need for stronger interaction with the next generation of cyber professionals, harmonisation of job functions, and developing an annual general assembly to consolidate CNF's role as a unique and trusted platform. Finally, it was agreed that CNF activities will be highlighted during the upcoming IAEA cyber security conference (Cybercon26) that will be held in Vienna, Austria in May 2026. It was suggested to organise a dinner or side event for CNF members during the conference.

Session 1: Developments Beyond Nuclear

Session 1 was designed to provide participants with the opportunity to hear perspectives and experiences from outside the nuclear sector. It was organised first to better understand the recent and upcoming evolutions of the geopolitical landscape and assess their impacts on cyber security matters. The session was also an opportunity to listen to the lessons learned from implementing cyber security measures in the aviation sector and discuss the process for the nuclear industry to benefit from the experience of other critical infrastructures.

Developments beyond nuclear - Geopolitical changes at the world stage by Koen Aartsma (Programme Lead, Security Unit, Clingendael Research Institute, The Netherlands)

Mr. Aartsma provided an overview of major geopolitical shifts shaping today's security environment. He highlighted the intensifying great power rivalry between the United States and China, Russia's continued ability to avoid isolation, and the growing role of middle powers and the Global South through multi-alignment strategies. He stressed that the world is entering a transitional era, marked by accelerating climate change, rapid technological advancements, and increasing conflict potential through both conventional and hybrid means. Mr. Aartsma also pointed to the renewed importance of hard power, the geopoliticization of the economy, and the centrality of cyber operations as tools of influence and plausible deniability.

During the follow-up discussions, participants agreed that the world is changing rather quickly, is becoming less predictable, and that relationships between countries were evolving towards much more transactional relationships and that identifying reliable and trustworthy partners was becoming more complex. They believed that such changes would impact cyber threats, in particular the capabilities of adversaries, which may include States and their proxies. It was agreed that cyber matters can be a force multiplier for certain physical threats. Participants highlighted the need for developing competencies amongst the workforce as a foundation for effective and resilient cyber security arrangements. Participants mentioned the fact that organizations are usually well prepared for mitigating traditional cyber threats but are not that well prepared to counter disinformation. Participants finally highlighted the challenges in protecting data and providing operation and business departments with the information they need to optimise their work. In certain instance, it seems to be better to give access to an environment you control, instead of sending data to the person who needs to access it.

International security collaboration in the air transportation industry by Patricia Damen (Vice President Security, KLM Royal Dutch Airlines, The Netherlands)

Ms. Damen outlined the multifaceted security challenges faced by the aviation sector, ranging from terrorism and insider threats to cyber and subversive crime. She explained how international cooperation is facilitated through frameworks such as the International Civil Aviation Organisation (ICAO), the International Air Transport Association (IATA), and the European Union Aviation Safety Agency (EASA), supported by national regulators. Ms. Damen highlighted the importance of established mechanisms such as passenger and baggage screening, intelligence sharing, and harmonized standards, while also addressing the impact of new EU regulations (NIS2, CER, and EASA Part-IS) on the industry. She emphasized the growing need for cyber threat intelligence sharing, the development of global standards, and public–private partnerships to enhance resilience. Her conclusion underscored that in airline security there is no competition—only collective responsibility—and called for strengthened partnerships, investment in technology, and the continuous adaptation of standards to meet emerging threats.

Answering questions from the audience, Ms. Damen highlighted the strength of collaboration between security airlines, in particular through well-established quick and simple communication channels (e.g., Signal) with other partner airlines in case of emergencies, and offered some examples when information is shared. She indicated that laws and regulations related to privacy and data protection were sometimes a barrier to exchange of security-related information (e.g., when people misbehave in a plane) with other airlines (even when law enforcement is engaged). Ms. Damen also highlighted the role of technologies in support of cyber security and stressed the benefit of integrating AI into security applications. She also praised the collaboration between aviation security stakeholders but regretted the too high number of regulators and regulations involved in the security process.

Session 2: Supply Chain Security

Session 2 was designed to specifically review and discuss cybersecurity matters in the supply chain. A case study was presented to highlight the importance of cyber security culture and response mechanisms in case of supply chain compromise. The session also provided an opportunity to discuss experiences and lessons learned by operators developing supply chain cyber security programmes.

Partner Incident Response by Tomas Nystrom (Information Management and Systems Director, WANO)

Mr. Nystrom started his presentation by reminding the group of the mission of his organization, the World Association of Nuclear Operators (WANO), and how WANO has been established as a global organization dedicated to maximizing the safety and reliability of nuclear power plants through mutual support, benchmarking, and the exchange of best practices. He then described a phishing incident that occurred through one of their trusted suppliers and shared with the group some of the main learning points. Amongst others, Mr. Nystrom highlighted the challenges in identifying and requiring necessary cyber security expectations in contracts with service providers, especially with small or long-term partners. He also stressed the importance of having effective incident response processes in place, including a clear definition of roles and responsibilities during an incident and escalation routes which are known to staff and partners.

Developing an information security supply chain programme by Andrew Haslam (Head of Governance, Risk, Compliance & Security, Urenco, UK)

Mr. Haslam first described Urenco and its role as a supplier to the global civil nuclear industry. He then explained how Urenco supports the 2022 - 2027 UK Civil Nuclear Cyber Strategy (CNCS), in particular when it relates to supply chain matters, and how Urenco, alongside other UK stakeholders, follows good practice developed by the UK National Cyber Security Centre (NCSC). Mr. Haslam then provided an overview of the Urenco supply chain approach and highlighted some of the challenges and opportunities arising from implementing supply chain security arrangements. In the final part of his presentation, Mr. Haslam presented a research project on artificial intelligence, risk and assurance to be jointly implemented by Urenco and King's College London from 2025 to 2029. He indicated that they were looking for industry partners who would be willing to collaborate with them on this important project.

Building on the presentations, participants stressed the importance of supplier audits and of establishing minimum standards through contracts. They discussed scope, process and frequency of security audits of suppliers. It was agreed that audits should follow a graded (risk) approach and might be used to educate suppliers. Participants stressed the challenges in assessing legacy suppliers and putting high expectations on small organizations. Participants discussed incident response matters and highlighted the need to involve more people than just cyber security specialists (e.g., procurement people and the legal department). It was mentioned that some nuclear organizations have thousands of suppliers and that they need to allocate significant resources to manage suppliers' incidents. Participants felt that the supply chain risks were very credible and that threat actors would target the supply chain to infiltrate a target organization (e.g., by compromising a digital tool used in confidence). It was also clear that the insider risk through the supply chain was real and that organizations had to develop and implement tight preventive and protective measures. Participants identified the timely sharing of experience as essential pillar to effective supply chain security.

External Presentations

In order to broaden the scope of the discussions and foster further exchanges amongst participants, two experts from the National Cyber Security Centre (NCSC) of the Netherlands were invited to present selected initiatives and activities of their organization.

Building Digital Trust - Public Private Partnership to Strengthen Cybersecurity by Mischa Coulier (Senior Relationship Manager, National Cyber Security Centre, The Netherlands)

Mr. Coulier presented first the mission of the NCSC, which is as an advisory organization, to increase the digital resilience of Dutch society, with the vision of a safe, open and stable information society. He then described the main tasks and global positioning of the NCSC amongst key governmental stakeholders, including direct links to the counter-terrorism national coordinator or the Prime Minister, when necessary. Mr. Coulier provided the group with further information on the role of NCSC leading Information Sharing and Analysis Centers (ISACs) and creating trusted, sector-specific environments for companies, including for those from the nuclear industry, to share sensitive information about cybersecurity threats, vulnerabilities, and lessons learned to collectively improve their digital resilience. Mr. Coulier concluded his presentation by providing a number of examples of public private partnerships, including the development of information security networks, cyber intelligence and cyber capacity building opportunities.

During the follow-up discussion, participants indicated that they had established similar organizations in their countries. It was agreed that building trusted environments to support national and international sharing of information and experience was essential.

Knowledge is power – NATO Summit 25 and Cybersecurity in The Netherlands by Erik-Jan Roggekamp (Senior Relationship Manager, National Cyber Security Centre, The Netherlands)

Mr. Roggekamp delivered a presentation describing the role of his organization, the NCSC, in supporting the preparation and organization of the NATO Summit organised in June 2025 in the Hague in the Netherlands. He started his presentation by reminding the group of the Nuclear Security Summit organised in the Netherlands in 2014, which was the last major nuclear-related international event organised in the country. He then indicated how the NATO summit held in Vilnius, Lithuania in 2023 and the Olympic Games in Paris, France in 2024 provided crucial information for designing security arrangements for the 2025 NATO summit in the Hague. From the experience gained from previous major event, it became clear to them that they would be subject to cyber-attacks and disinformation campaigns. They knew that incidents would happen. Mr. Roggekamp also explained how his organization, the NCSC, structured itself to prepare for the Summit. He then described some the situations and challenges actually faced by his country during the Summit itself and how the NCSC supported an effective response to them. In his conclusion, Mr. Roggekamp reiterated the importance of the public and private sectors to work together in cybersecurity, of consolidating and implementing lessons learned from past experience, and of developing flexible and reactive cyber security strategies.

Answering questions from the audience, Mr. Roggekamp indicated that interactions with other Dutch stakeholders was facilitated by the use of multiple already-established confidential channels. He also indicated that since they were monitoring and collecting many information, they were identifying a lot of possible issues and that their challenge was to identify the relevant ones and to decide what information needed to be kept confidential and which one need to be transferred to selected organizations or the public. Overall, the NCSC has the feeling that they have significantly improved their communication practices and that these improvements are sustainable.

Session 3: Topical CNF Working Groups

Session 3 was designed to offer an opportunity to the participants to discuss in further details the following topics during break-out groups: Insider Threat, Artificial Intelligence and Governance. The working group discussion were respectively led by Brad Stephenson (Southern Nuclear, USA), Donald Dudenhoeffer (ENEC Operations, UAE) and Tom Wilson (Southern Nuclear, USA).

Some of the key take-aways of the WGs are summarised below:

Insider threat

- A lot of materials on the topic already exist.
- It is important to focus on what really works.
- A first task could be to review existing publications (e.g., IAEA, WINS, others) and build on them.
- Innovative thinking and approaches will bring added value.
- Discussions should cover both physical and cyber insiders, and focus on gaps, if any.
- Constant monitoring of people and activities is very effective but challenging.
- Insider threat reviews could focus on anomalies.

Artificial Intelligence

- Not really a new topic. AI technologies have been proposed for use in nuclear facilities since the 1980's. Advancements in hardware, software and data accessibility has significantly enhanced the feasibility of implementing AI in practice.
- Nuclear facilities should proceed with caution, and it is recommended that organizations initially attempt pilot AI projects in non-critical systems. AI is not the solution to everything, but it can provide benefit for addressing certain complex problem spaces.
- Initial discussions should cover prerequisites for the successful adoption of this technology and address the concerns nuclear operators may have using it.
- It will be important to stay abreast of on-going international activities, especially those conducted by the IAEA, on AI and nuclear security.
- An abstract will be submitted for presentation at Cybercon26. The proposed paper will address nuclear industry concerns and cybersecurity-related challenges associated with the use of AI.

Governance

- Many materials on the topic also exist in this area. We need to develop something valuable to CNF members. It will have to be specific to the nuclear industry and its regulator.
- It could be around corporate policies, management and culture (e.g., Governance, Risk, and Compliance framework). It could address some of the usual challenges from a governance perspective (e.g., Corporate CISO vs Facility CISO as part of licensing and plant management. Who is accountable? Who has authority?).
- It should provide some guidance for Board and Executive engagement.
- It could include some guidance for a CISO on how to train a successor.

It was agreed that the WGs represent one of the pillars of CNF sustainability and that efforts should be conducted to keep momentum in-between CNF events. The frequency and exact process of each WG meeting remain to be determined. It was nevertheless agreed that each WG can follow their own ways. WG leads may engage their members and overall CNF members through various means, including surveys. The exact outputs of the WGs still need to be agreed but could take the form of reports to be produced by Spring 2026.

Session 4: Sharing Operational Experience

Remote access for maintenance by Paul van der Ploeg (NRG PALLAS, The Netherlands) and Jelmer van der Neut (Urenco Nederland, The Netherlands)

Mr. van der Ploeg and Mr. van der Neut moderated a discussion on managing the risk of remote access for maintenance. This interactive session was built around a fictional facility which requires various levels and types of maintenance activities for diverse systems. The discussions focused on the maintenance of selected elements of the physical security system. The initial questions to be addressed included "Why do you need remote maintenance" and "What is the risk impact?". In support of the discussion, Mr. van der Ploeg and Mr. van der Neut presented a selection of cyber security international standards and facilitated the group discussion along 8 steps of IEC62443 with a systematic review of people, process and technologies involved in the process. They concluded their session by exploring how remote maintenance practices and threats may evolve in the future.

During the session, participants raised the following points:

- A couple of IEC standards are missing (missing from where) (IEC 62645; IEC 63096. They are specific to the nuclear sector).
- Monitoring and maintenance channels and practices need to be separated.
- It is challenging to know, after a maintenance operation, if a parameter has been modified. Do you verify every line of the software?
- Some participants expressed preference for changes done on-site. Even if you cannot fully control what people are doing behind their laptops, at least, you know the guys doing the changes.
- Portable media devices, such as contractor laptops remain the largest infection vector for OT systems at nuclear facilities. Portable device and mobile media management programs should be used to tightly control and minimize any portable device and mobile media used in the plant. This often requires a joint effort between cyber security and the physical protection team.
- As the digital footprint of nuclear facilities grow, so does the ongoing challenge of maintaining a full and accurate digital asset inventory.
- Many suppliers are required to work on a platform/environment owned by the facility.

  Ownership is not shifted. Access rights are evolutive.
- Prepare a risk register. Let the operational units be accountable.
- There is growing convergence between IT and OT. While technically similar and potentially relying on some of the same digital components, cyber security strategies between OT and IT are different for a number of key reasons. The main reason being the need to maintain production functions on a 24/7 basis.
- Staff competence and turnover is an issue.
- Will we be moving towards full cloud-based services? If yes, it will minimise the difference between on-site and off-site accesses.
- Remote maintenance for GEN III, GEN IV, and SMRs are very different.
- Equipment outside the nuclear island might be more interesting targets for impacting a nuclear power plant.

Lessons learned implementing cyber security measures during decommissioning by Michael Mosler and Thomas Walter (Preussen Elektra, Germany)

Mr. Mosler and Mr. Walter explained first how security needs and regulatory requirements were evolving during the decommissioning process. In particular, they described the changing IT paradigm and the need for significant rebuilding of the IT systems. They also presented some of the challenges arising during the decommissioning process, including developing new IT security concepts, maintaining a high level of cyber security awareness amongst the workforce, adapting to a new working environment. Mr. Mosler and Mr. Walter concluded their presentation by illustrating the challenges faced during the removal of the steam generator.

During the follow-up discussions, participants highlighted the following issues:

- Changes in the workforce pose strong security challenges (a lot of new staff; less familiarity with the facility; different awareness and culture, in particular in term of security).
- In many instances, regulations for facilities under decommissioning are the same than for operating facilities. However, some new, dedicated ones have been already issued or are under development.
- As many radioactive materials remain (e.g., highly activated filters), radiation protection matters are more complex during decommissioning than during construction. These materials bring new security risks.
- Decommissioning companies are not always aware of nuclear requirements.
- Dismantling and decommissioning matters are not really included into the new build projects.

Preparing the NRG PALLAS Visits

Cyber security organization at NRG and Pallas by Paul van der Ploeg and Ruud Koning (IT manager, NRG PALLAS, The Netherlands)

Mr. van der Ploeg and Mr. Koning started their presentation by providing a description of the High Flux Reactor (HFR) and of the upcoming Pallas reactor, of their importance for the Netherlands and the world, in particular for isotope production, and a timeline of their construction and operation. They then presented the cybersecurity challenges that the Pallas reactor will face all along its life cycle and discussed how such challenges may be addressed, or not, during the design and construction process. Mr. van der Ploeg and Mr. Koning offered some opportunities to improve cyber security by design by developing modular cybersecurity systems that can be replaced or upgraded without redesigning the entire reactor, implementing a layered defence strategy through multiple levels of monitoring, detection, and containment, or building digital twins to simulate both physical processes and potential cyberattacks before construction. They concluded their presentation by stressing the fact that flexibility, modularity, and a culture of continuous adaptation is a prerequisite to success.

Introduction to the NRG Pallas visit by Roel Krol (Manager Corporate Security, NRG PALLAS, The Netherlands)

Mr. Krol provided the group with the global overview of NRG Pallas presenting the main activities of the organization developing and delivering nuclear medicine products and contributing to energy solutions. He presented the various facilities of NRG Pallas (HFR, various laboratories, waste treatment facilities, etc.) as part of the Petten Energy & Health Campus. In the area of medical radioisotopes, Mr. Krol described the essential role of NRG Pallas in producing such isotopes and developing innovative products and use. He also detailed NRG Pallas consultancy and research and development activities on technologies for nuclear energy conversion. Mr. Krol concluded his presentation by providing the group with more details on the timeline of construction of the new Pallas research reactor and related on-site nuclear infrastructure, including field laboratories and a nuclear health centre.

NRG PALLAS Visit

The meeting concluded with a site visit to the NRG PALLAS facilities in Petten, including tours of the High Flux Reactor, Hot Cell Laboratories, the PALLAS construction site, and the Decommissioning and Waste Treatment facility offering members unique insights into ongoing projects.

After the visit, participants were offered an opportunity to provide their feedback on the organization and conduct of the Autumn meeting. They reported a high level of satisfaction and offered suggestions for improvement in a couple of areas. Overall, participants indicated that the Autumn meeting was a success. In particular, they valued networking opportunities and the topical discussions they had during the event. Participants expressed very high level of satisfaction with the site visit. For the next events, they recommended, amongst others, to focus on challenges faced by nuclear operators and on possible solutions.