

CYBER
NUCLEAR
FORUM

A Global Initiative
to Protect Nuclear
Facilities from
Cyberattacks

CNF Newsletter June 2026



INTERVIEW: My Path to Nuclear Cybersecurity - Michael Mosler from PreussenElektra, Germany

SPOTLIGHT: Working Groups Drive Progress on Key Cybersecurity Challenges

REPORTS: Two successful CNF events organized this Spring

UPCOMING EVENT: CNF Autumn 2026 Meeting

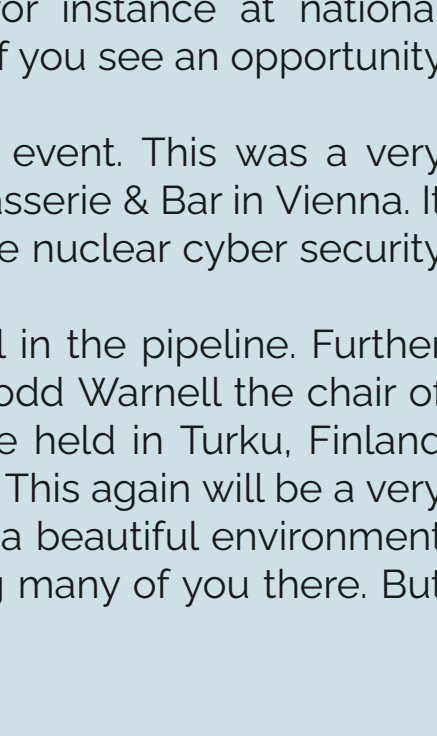
A Message from our Steering Committee Chair

Welcome to the second CNF newsletter in 2026. We have successfully met some important milestones already in this year. And we still have some nice plans in our pipeline for the second half of this year, of which the in-person CNF Autumn meeting 2026 is the major one. As organisation we are in a decent shape. Membership is gradually growing as planned and funding for this year is assured. We have held a very interesting online CNF Spring 2026 event on which you will read more further down in the newsletter. Furthermore, the CNF was present at the IAEA CyberCon26 in more than one way.

During CyberCon26 I presented as CNF chair on what the CNF is and wants to achieve. Besides explaining that, the main aim of that presentation was to further raise membership. Since we now have that presentation available, I could also give that presentation to other fora if you think that makes sense, for instance at national meetings of nuclear cyber security professionals. Let me know if you see an opportunity for that.

Moreover, during CyberCon26 we held our yearly CNF social event. This was a very lively and memorable drinks and dinner meeting at Veranda Brasserie & Bar in Vienna. It was an excellent opportunity to meet old and new friends in the nuclear cyber security world.

Looking forward, the in-person CNF Autumn 2026 Event is still in the pipeline. Further down in this newsletter you will read an update on that from Todd Warnell the chair of the organising committee for that event. Spoiler alert: it will be held in Turku, Finland from 2 to 5 November 2026. Note that already in your agendas! This again will be a very lively event, with a lot of interaction, with inspiring speakers, in a beautiful environment and with an interesting site visit. I am looking forward to seeing many of you there. But first, enjoy this second CNF newsletter in 2026.



Anno Keizer
URENCO, Netherlands

Your experience builds our shared resilience

We're preparing the next edition of our community newsletter, and we'd love to highlight the insights, projects, and experiences of our members. We invite you to share your stories, upcoming events and recent articles. This is your opportunity to contribute and connect with the wider community. Please email any contributions for considerations to [Luka Cekic](#).

Stay connected with CNF

The Cyber Nuclear Forum relies on the active participation and support of its members. As part of our ongoing efforts to update the membership database, we have decided to request all previous participants in CNF activities to indicate they wish to remain Forum members.

VISIT OUR WEBSITE

If you haven't already, here is how to confirm your CNF Membership

If you wish to remain a Forum member, here is the process to follow:

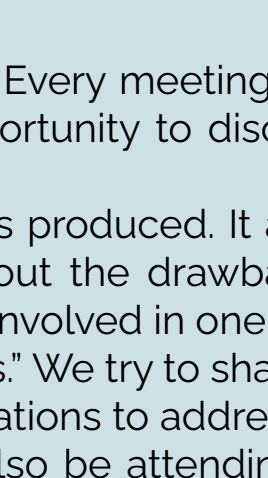
1. Fill out the [online membership form](#) with your personal details, organisational affiliation, job title and a short description of your professional background and its relevance to the Forum. Please note that you will be requested to upload a short CV.
2. Once submitted, your application will be reviewed by the CNF Steering Committee to ensure it aligns with CNF's membership criteria (i.e., cybersecurity specialists employed by companies holding a nuclear licence; nuclear research organisations; contractors upon recommendation of the nuclear operator they are working with).
3. After the review, you will receive a confirmation of membership or a follow-up message if any additional information is needed.

If you have any questions or encounter difficulties with the form, please contact [Luka Cekic](#) directly.

APPLY FOR MEMBERSHIP

My Path to Nuclear Cybersecurity - Michael Mosler from PreussenElektra, Germany_

Here's my take: It's much easier to recruit an I&C engineer for cybersecurity than it is to get IT professionals to engage with I&C technology. But we need a combination of both skill sets to build the capabilities needed to protect our systems. Why do I think that? Why am I writing about it? What's behind it? In short: It's my story. It's my path to cybersecurity. It's my way of thinking about security. And that's how I contribute to CNF, by sharing this knowledge.



Michael Mosler
PreussenElektra GmbH

I have been a member of the CNF since the 2022 spring meeting. Every meeting since then, whether virtual or in-person, has provided an excellent opportunity to discuss a wide range of topics in an atmosphere of trust. In my opinion, this trust is one of the best outcomes the forum has produced. It allows you to consult directly with experts from around the world without the drawback of having to withhold too many details about your problem. I am also involved in one of the CNF's working groups, which focuses on the topic of 'insider threats.' We try to share our collective knowledge and develop best practices and recommendations to address this constantly evolving threat. If you'd like to discuss this further, I'll also be attending this year's CNF fall meeting.

Who am I? My name is Michael, and I entered the nuclear energy industry in Germany in 1999. I worked in the control systems department for over a decade and was responsible for the maintenance and optimization of several control systems at nuclear power plants in Germany. While working in the control systems department, I studied at a university of applied sciences (Electrical Engineering and Industrial Engineering). After graduating, I transitioned to a role as an on-site IT security officer. After a few years, I am now also responsible for physical security and serve as deputy head of the security department.

Based on this wide-ranging personal experience, I can say that it is much easier to understand the necessity of protecting control systems from cyber threats than it would be without the background knowledge of the variety of systems required to keep a nuclear power plant running. When I speak with people who have only a direct IT background, it is much more complicated to help them understand the interdependencies of the individual systems.

Currently, all nuclear power plants in Germany are permanently shut down; on-site, we have removed all fissile material from one of the units and have already successfully dismantled the pressure vessel in the other unit. We have established a complete dismantling facility to carry out all these tasks to high standards and with optimized material flows.

In many decommissioning processes, such as the dismantling of large plant components or the decontamination and clearance of buildings, we are implementing new systems that rely heavily on IT and OT. Cybersecurity therefore plays a crucial role and is essential to ensuring that decommissioning proceeds on schedule and within budget.

I am happy to share my experience and knowledge in the field of decommissioning with other operators, as it is important to ensure security even during the decommissioning.

Spotlight: Working Groups Drive Progress on Key Cybersecurity Challenges_

CNF's Working Groups continue to play a vital role in advancing collaboration and knowledge-sharing on some of the most pressing issues in nuclear cybersecurity. Focusing on Governance, Insider Threats, and Artificial Intelligence (AI), the groups provide a trusted forum for practical discussions, thought leadership, and the development of guidance and best practices.

The Governance Working Group has made significant progress on a charter-style document designed to support the Forum's future structure and operations. The paper, which was shared with members ahead of the meeting, represents an important step toward formalizing CNF's governance framework.

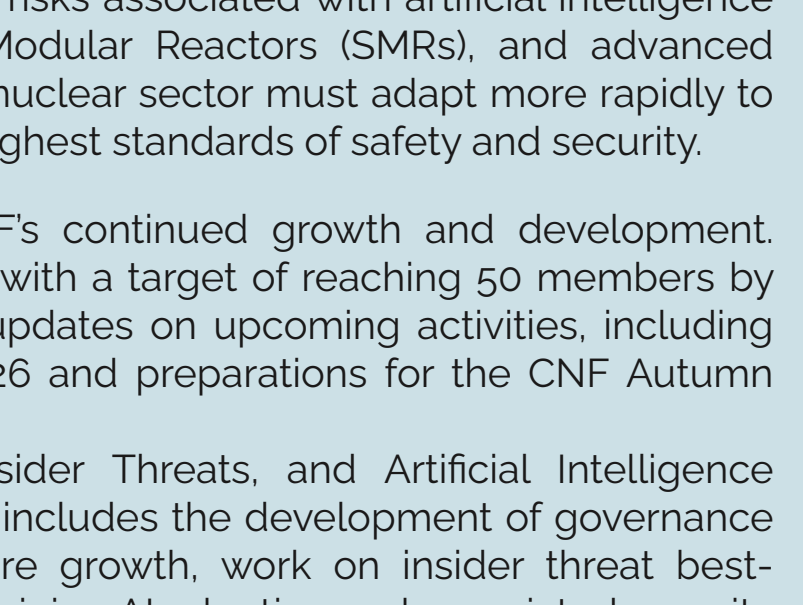
The Insider Threat Working Group is developing guidance materials and reviewing existing approaches to insider threat management from both the nuclear and non-nuclear sectors. The goal is to establish a best-practices framework that reflects the operational realities of nuclear organizations.

Meanwhile, the Artificial Intelligence Working Group is examining both the opportunities and risks associated with AI in nuclear facilities. Building on the results of a member survey, the group has developed a paper exploring security considerations related to AI applications. While many organizations are already using AI for research, reporting, and data analysis, concerns around data protection, information leakage, and the handling of sensitive data remain key challenges.

Together, the Working Groups demonstrate the value of expert collaboration in addressing emerging cybersecurity issues and strengthening security across the nuclear sector.

CNF Spring 2026 Meeting Explores AI, SMRs, and the Future of Nuclear Cybersecurity_

The CNF Spring 2026 Meeting brought together around 30 cybersecurity professionals and nuclear industry experts from around the world for two days of virtual discussions on the evolving cyber challenges facing the nuclear sector. A major theme throughout the meeting was the impact of emerging technologies on nuclear cybersecurity.



Presentations explored the opportunities and risks associated with artificial intelligence (AI), advanced digital technologies, Small Modular Reactors (SMRs), and advanced reactor designs. Participants agreed that the nuclear sector must adapt more rapidly to technological change while maintaining the highest standards of safety and security.

The meeting opened with updates on CNF's continued growth and development. Membership has increased to 34 individuals, with a target of reaching 50 members by the end of 2026. Participants also received updates on upcoming activities, including the Forum's engagement at IAEA CyberCon26 and preparations for the CNF Autumn Meeting in Finland.

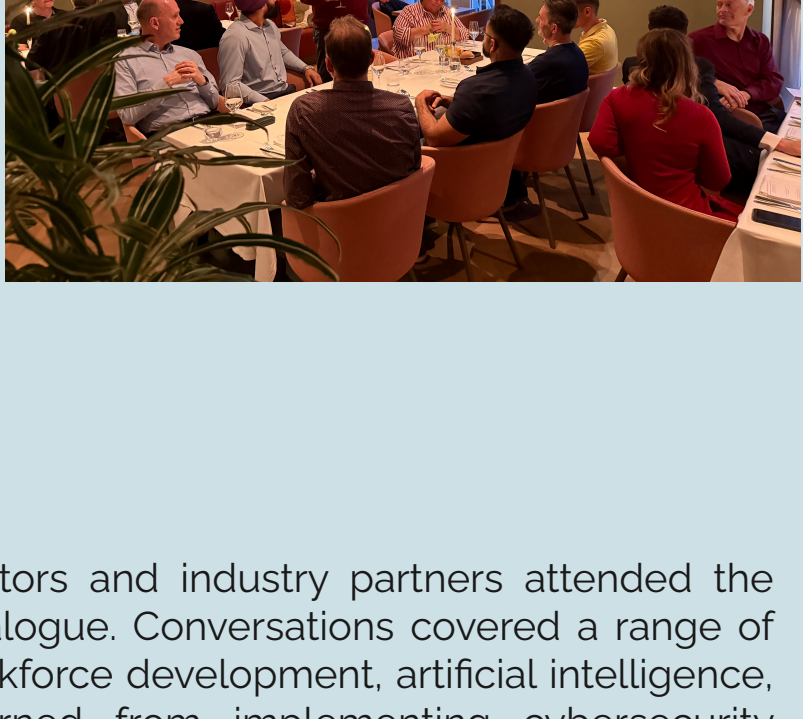
CNF's Working Groups on Governance, Insider Threats, and Artificial Intelligence reported on their ongoing activities. Progress includes the development of governance documentation to support the Forum's future growth, work on insider threat best-practice guidance, and a member survey examining AI adoption and associated security concerns within the nuclear sector.

Expert presentations highlighted how organizations are beginning to implement AI applications while maintaining strict governance and cybersecurity controls. Discussions also focused on the increasing importance of cybersecurity-by-design principles for advanced reactors and SMRs, which rely heavily on digital technologies and interconnected systems. Speakers emphasized that cybersecurity must be integrated from the earliest stages of design, engineering, and procurement to ensure long-term resilience.

The meeting concluded with an interactive discussion on future priorities for the Forum. Participants highlighted the value of trusted international collaboration and operational experience sharing in addressing emerging threats. Feedback from attendees was overwhelmingly positive, with participants particularly appreciating the practical discussions on AI, operational technology security, and advanced nuclear technologies.

CNF Social Event during IAEA CyberCon26

On the margins of IAEA CyberCon 2026, the Cyber Nuclear Forum (CNF) hosted a social networking event that brought together approximately 20 CNF member and invited guests from across the nuclear cybersecurity community. The gathering provided an informal setting for participants to strengthen professional relationships, exchange experiences, and continue discussions initiated during the conference. The event reflected one of the core strengths of the Forum: fostering a trusted international network of practitioners committed to advancing cybersecurity across the nuclear sector.



Representatives from various nuclear operators and industry partners attended the event, creating valuable opportunities for dialogue. Conversations covered a range of topics, including emerging cyber threats, workforce development, artificial intelligence, insider threat mitigation, and lessons learned from implementing cybersecurity programmes in nuclear facilities.

The evening also served as an opportunity to welcome new participants to the CNF community and highlight upcoming Forum activities, including working group initiatives and future meetings. Participants emphasized the importance of maintaining strong professional connections and trusted channels for information exchange as cyber challenges continue to evolve.

The event once again demonstrated the value of the CNF network in bringing together experts from around the world and reinforcing collaboration beyond formal meeting settings.

CNF Autumn 2026 Meeting_

Turku, Finland | 2-5 November 2026



The Cyber Nuclear Forum Autumn 2026 Meeting will convene leading cybersecurity and nuclear operations experts from around the world to advance knowledge-sharing, discuss evolving cyber risks, and promote resilient practices for securing nuclear facilities. Following the successful Autumn 2025 Meeting, this high-level gathering will feature expert presentations, interactive sessions, and peer exchanges on critical topics including threat landscapes, artificial intelligence, governance, operational intelligence, and emerging technologies.

Participants will have the opportunity to engage with global practitioners, contribute to working group discussions, and explore real-world approaches to addressing cyber challenges unique to the nuclear sector. As with previous events, the Autumn Meeting aims to strengthen professional networks and support collaborative learning across industry and technical domains. Details on the venue, dates, and agenda will be shared once confirmed.

The location of this years Autumn Meeting is Turku, Finland. Furthermore, a visit to a nuclear facility is planned as part of this event - probably the deep geological disposal facility in Olkiluoto.

REGISTER HERE

[View in browser](#)