

CNF Newsletter December 2025

INTERVIEW:

Todd Warnell on Resilient Cybersecurity

SPOTLIGHT:

Progress of the CNF Working Group on Artificial Intelligence

UPCOMING EVENT:

CNF Participation at IAEA CyberCon26

WINS WORKSHOP:

Role of Advanced Tech in Nuclear Cybersecurity

A Message from our Committee Steering Chair

It is an honour and a privilege to present to you the first Cyber Nuclear Forum Newsletter. As part of our efforts to further strengthen relations between the Cyber Nuclear Forum and its members and participants, this quarterly newsletter will share the latest developments from the CNF community as well as updates about our future plans.



Anno Keizer
URENCO, Netherlands

In this edition, you'll find a retrospective of our achievements in 2025, an update on the progress of the CNF Working Group on AI and a personal introduction to our vice-chair, Todd Warnell.

I would like to thank all Forum participants for their contributions throughout 2025 and wish you a wonderful and joyful holiday season and a happy new year.

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.

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 CNF. 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.



Progress Made & Priorities Ahead

Looking back at 2025, one of the milestones achieved by the CNF Steering Committee was the launch of the **CNF website**. Establishing this online presence enables potential members and financial sponsors to read who we are and what we do. The CNF getting a "face" in this manner is really a fundamental improvement. The CNF Spring Event marked significant discussions about the direction in which the CNF should develop and how the membership and funding processes could be made more professional and structured.

The CNF Autumn Event was also a major highlight. The participants' interesting and interactive presentations made our meeting in Amsterdam a success. The event was topped off with a site visit to the NRG-Palls nuclear facility in the north of the Netherlands. Participants had the opportunity to visit the operational HFR research reactor and the construction site of the new Pallas reactor for production of medical isotopes as well as various other locations.

We also launched three **CNF Working Groups** to allow members to stay in touch between the Spring and Autumn events and discuss current topics like artificial intelligence, insider threats and governance.

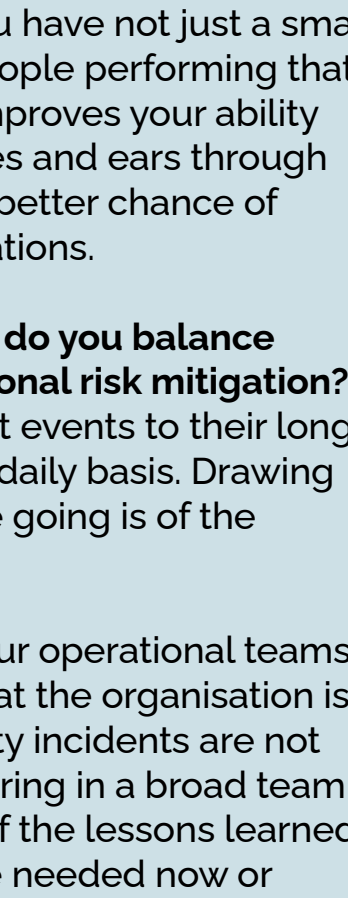
Last but not least, our new quarterly newsletter will provide another avenue for communication with and among our members. Please let us know what you think of the CNF newsletter and don't hesitate to propose topics or content for future editions. Looking ahead to 2026, we'll again organise our two biannual events, and we look forward to announcing additional activities to serve our Cyber Nuclear Forum community.

Building Resilient Cyber Governance

Todd Warnell is the Chief Information Security Officer at Bruce Power. He took on that position in 2023, when information security was made a standalone division. Previously he led the entire CIO organisation.

Over his more than 25-year career in technology and data, he has focused on driving major technology and process changes, recognising the central role of security to effective operations. "Security is at the core of ensuring everything works well and reliably together," he said.

He serves as Vice-Chair of the CNF, which gives him a platform to share his expertise and enthusiasm for the dynamic field of security. "I love to solve ever-evolving problems, and change is constant in security. Challenges and techniques are always evolving, and new ones are constantly emerging."



Todd Warnell
Bruce Power, Canada

In this interview, Todd shared his insights about strategies for strengthening cybersecurity governance, building broad organisational support for cybersecurity, and the role of the CNF in assisting its members and enhancing cybersecurity across critical infrastructure.

What is the role of cybersecurity governance in supporting a holistic approach to nuclear security?

Cybersecurity can no longer be treated as a standalone or separate security domain. In any nuclear organisation, cybersecurity needs to be thought of and treated as a core part of safe, reliable operations. Highly skilled technologists and cybersecurity experts have a specialised skillset, but they're not working in a silo. They're enabling the operations of the organisation.

When you frame it that way and demystify cybersecurity, it encourages more people to be involved. The cybersecurity department is a core part of enabling reliable operations, so embedding that mindset as part of the safety and security culture within an organisation really helps to drive broad acceptance, promote senior executive buy-in to its importance, and ensure that it becomes a core conversation both with senior executive teams and operational teams across the organisation, as well as with the Board of Directors.

How do you define effective cybersecurity governance within an organisation and in a sector as critical and regulated as nuclear energy?

My number one measure of effectiveness is the broadness of who is talking about and inquiring about cybersecurity. When our CEO asks our suppliers how they're performing on their overall cybersecurity programme and business reliability avenues, that demonstrates an effective cybersecurity programme. It shows that leaders don't just turn to the CISO; they don't just turn to the head of cybersecurity or information security. Cybersecurity should be indoctrinated in the way we operate the business.

The next characteristic is a pervasive culture where cybersecurity is propagated and performed by distributed line leaders. Cybersecurity is not the responsibility of a central single organisation; it needs to involve functional performance lines like engineering, maintenance, and nuclear security. The cybersecurity team should provide effective central support and oversight that drives cybersecurity work.

What governance structures do you find are most effective to ensure that cyber risk is treated as an enterprise-wide strategic issue?

If cybersecurity governance structures are highly centralised and highly specialised, then it becomes seen as the cybersecurity team's responsibility alone. A highly distributed performance organisation, where many lines of business are involved in the day-to-day work around cybersecurity, signals an effective governance model. For example, a design engineer should know that their role is to harden an asset based on its classification or requirement.

That's the most effective means of delivering a cybersecurity programme that sustains and becomes a driver of excellence because then you have not just a small specialised team, but potentially hundreds or thousands of people performing that work on a day-to-day basis, which improves your resilience, improves your ability to come up with novel solutions, and fundamentally act as eyes and ears through the nuclear security lens. A broad workforce provides a much better chance of detecting and responding to any anomalous or abnormal situations.

When leading a cyber and information security division, how do you balance between long-term governance maturity and urgent operational risk mitigation?

The leader in those spaces must always be connecting current events to their long-term vision. The threat landscape itself changes on an almost daily basis. Drawing the connection between what's happening now to where we're going is of the utmost importance.

When an event or a scenario unfolds, you respond to it and your operational teams help to triage, recover and respond. You need to make sure that the organisation is aware of what's happening so that they know that cybersecurity incidents are not just a hypothetical, that these events do happen. You should bring in a broad team of stakeholders to understand that situation and also as part of the lessons learned. How does that situation tie into either new capabilities that are needed now or capabilities within your long-term vision that may need to be accelerated or pulled forward?

It is always a balancing act. The role of senior security leadership is to espouse that vision of where we're going and why we're going there, but also checking and adjusting based on the events that are happening or unfolding in your business.

How does collaboration with international colleagues through CNF help to support your work?

First and foremost, knowing one another and learning from each other is vitally important from a global operating perspective. The nuclear sector operates as a global family. While not everything can be shared, such as details of a security event, openness in sharing operational experience is a core part of the culture.

The Cyber Nuclear Forum brings together a close community of trusted security professionals that are facing similar threats. Understanding how they address those events and their long-term vision is an exceptional resource and is essential to driving best practices and excellence. A broader perspective allows you to calibrate your approach in line with others' experience.

How do you envision international collaboration evolving over the next decade, especially for critical infrastructure protection?

Candially, as the world's geopolitical landscape becomes a bit more complex and a bit more challenging, the necessity for collaboration between friendly allied and trusted nations continues to be of growing importance. That's a bit counterintuitive to the broader perspective of global information sharing in the nuclear sector. Not all aspects of security can be shared with everyone or every nation, so we need to find the right balance of true geopolitical allies and move forward together.

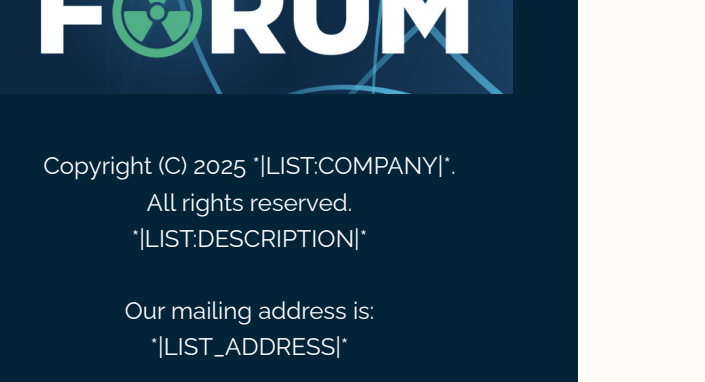
Potential splits in that dynamic will probably be the single biggest driver of change over the next decade. There's always going to be a drive for openness, transparency and fostering a larger circle of trust, but there are forces and geopolitical posturing that none of us control in our day-to-day jobs. Adjusting accordingly as that unfolds will probably be the single biggest impact for us over the next decade.

How do you see the role of the nuclear sector in leading cybersecurity and resilience among critical infrastructure more widely?

Cyber and information security leaders have a mandate to look beyond their organisation and their sector and fundamentally drive the conversation around critical infrastructure and resilience.

As nuclear operators, we have an important mission. We have a culture and a history around emerging and maturing cybersecurity practices that has been built over decades. That background provides a level of expectation and positions us to support other industries. We can share our experience, advocate and help to point out the path forward for broader critical infrastructure. Taking on a leadership role and evangelising for resilience across sectors in one's nation and around the world will be fundamental to making the world a safer, more resilient place. We are always so focused on our own organisations, but we as nuclear operators have a platform that we can build upon to lift others up.

The CNF adds to and bolsters that leadership position. It's not just one CSO speaking about it, but an international cooperative group driving that message together. It may be an emerging mandate for us. Of course, we're still in the formation phase of the CNF and fostering that community around nuclear, but we can also change and evolve that message to share how we drive – and have driven – cyber maturity in our important mission so others can also follow in that same path. This can absolutely be a growth opportunity for us internationally.



Since the CNF meeting in September and the inaugural meeting of the Artificial Intelligence Working Group, the team has made a strong start.

We've completed the CNF AI survey and extend our sincere thanks to all participants! The findings highlight the primary concerns and challenges associated with implementing AI in nuclear facilities. Across responses, data-related issues — particularly those involving security and accuracy — emerged as the dominant themes. These results will be examined in greater detail in a forthcoming paper.

The abstract, titled Nuclear Industry Security Concerns for the Application of AI at Nuclear Facilities, was submitted for the IAEA International Conference on Computer Security in the Nuclear World: Securing the Future (CyberCon26). Formal confirmation of acceptance is pending. Contributions from the AIWG team for the associated full paper would be greatly appreciated.

Actions and Requests

- Currently only a chairman has been assigned to the AIWG. We are seeking a co-chair to assist in coordinating the group. If you are interested, please contact donald.dudenhoeffler@enecprogram.ae
- A virtual meeting of the AIWG is planned for January 2026. Stay tuned for details on the exact time and date.

IAEA CyberCon26

International Conference on Computer Security in the Nuclear World: Securing the Future

Vienna, Austria | 11-15 May 2026



We hope to see you at the IAEA's upcoming International Conference on Computer Security in the Nuclear World: Securing the Future!

Many CNF members will be participating, and the CNF AI Working Group is contributing a paper on *Nuclear Industry Security Concerns for the Application of AI at Nuclear Facilities*.

We encourage you to register if you haven't already. More details can be found on the [IAEA event page](#).

We'll organise a side event for CNF members in conjunction with the conference, so [let us know if you'll be attending](#) CyberCon26.



The World Institute for Nuclear Security is hosting an interactive workshop for cybersecurity professionals in the nuclear sector to explore how advanced technologies can enhance cyber resilience.

The event will provide participants with practical insights into integrating AI, machine learning, automation, behavioural analytics, zero trust frameworks, SOAR, and cloud-native platforms into nuclear cybersecurity programmes.

Participants will have the opportunity to:

- Understand the cyber threat landscape for nuclear facilities, including OT-targeted attacks and supply chain risks
- Examine how advanced technologies can improve detection, response, and risk management
- Review cybersecurity frameworks and assess their applicability to nuclear environments
- Learn from real-world case studies and lessons shared by nuclear and critical infrastructure experts
- Identify immediate steps to strengthen organisational and national cybersecurity programmes

Around 40 participants will be invited, including representatives from nuclear operating organisations, regulators, technology vendors, academia, law enforcement, and other critical infrastructure sectors.

There is no attendance fee for this event. Participants are expected to cover their own travel and accommodation expenses, as no funding is available to support these costs.

More information is available on the event page