

CNF Newsletter September 2026



LOOKING
AHEAD:
Help Shape
CNF's Planning
for 2027 and
Beyond

MEMBER
SPOTLIGHT:
Cyber Threats,
Risks & Dad Jokes
with Audrey
Crowe

PROGRESS AND
PRIORITIES:
Updates from
the CNF Working
Groups

UPCOMING
EVENT:
Preview of the
CNF Autumn
2026 Meeting

A Message from our Steering Committee Chair

Time flies. We are already in the third quarter of 2026, a year that has not been business as usual.

The cyber landscape is changing fast and fundamentally. The geopolitical landscape has become more unstable, with full-out kinetic-, hybrid- and cyber war spreading further and impacting countries that seemingly are not directly involved.

The result has been a profound shift in cyber sabotage risk that seems unlikely to disappear anytime soon.

2026 has also seen a technical transformation in cyber threats. AI models are finding vulnerabilities and developing exploits at a speed far exceeding the previous capabilities of human attackers. Even more worrying is that recently two agentic AI models, of the companies Anthropic and Open AI, escaped their guard-railed sandboxes and successfully hacked into other companies without human intervention. Companies need to organise their cyber defences to be flexible and agile enough to keep pace as AI models are quickly developing as threat actors. Many companies have not yet reached the elevated level of cybersecurity maturity needed to effectively protect against this AI threat.

At the same time, regulators are responding to these developments with additional legislation and strengthened regulation. While this is understandable, it puts an additional workload on the already-stretched cybersecurity teams at nuclear facilities.

Against this backdrop, collaboration matters more than ever. As you navigate these challenges, we remind you that the CNF offers opportunities to collaborate and combine efforts with your nuclear cybersecurity peers. While your agenda may be full, investing the time to connect with your peers will pay off.

We hope you enjoy this newsletter and take the opportunity to get involved in CNF activities throughout the year. You can contribute through our Working Groups, join our upcoming events, and stay connected through our quarterly newsletters.

We would also welcome your input as we shape CNF's activities for 2027, as outlined below.

Anno Keizer
URENCO, Netherlands

What would *you* like CNF to focus on next year?

CNF aims to be an organisation that helps you do your job more effectively, so we are keen to hear your suggestions.

In 2027, we are planning a two-day virtual meeting in March and a four-day in-person event in September. We also aim to hold a social event alongside a conference or international exercise. We invite you to share your ideas, proposals and wishes for these gatherings.

We also invite your suggestions for additional working groups as well as entirely new initiatives such as collaboration with training institutions, establishing a CNF mentorship program, or more. For instance, a small group of forum members is in the process of developing a voluntary peer review process.

If you have an idea, please don't hesitate to reach out. Just drop me an email (anno.keizer@uranco.com) or give me a call (+31 622 808 823)!

Cyber Threats, Risks & Dad Jokes with Audrey Crowe

What is a hacker's favourite season?
Phishing season.

Now that we've cleared the bar for terrible cybersecurity humour, let me introduce myself.

I am Audrey Crowe, Program Manager for the National Security & Critical Infrastructure Research Directorate at Canadian Nuclear Laboratories (CNL). I joined the CNF at the end of 2025 following a recommendation from a fellow Canadian colleague that you all know well, Todd Warnell, and I am delighted to connect with this community.

My career has taken me across the nuclear, defence, and cybersecurity sectors, where I've spent nearly two decades working to understand and address complex security challenges. Today, my work focuses on research and advisory support in cybersecurity governance, risks and compliance, insider threat management, and the impacts of the spicy geopolitical developments on national security and the nuclear threat landscape.

What fascinates me most is how interconnected nuclear security really is. Cybersecurity, physical protection, personnel trustworthiness, supply chain security, and safeguards are often managed separately, even though the threats rarely fall neatly into single boxes. In my view, true resilience starts with bringing those pieces together and treating security as a single, integrated, system. I owe much of this perspective to our dearly missed colleague Scott Hilts and his "grand unified security theory". His ideas continue to inspire my doctoral research, which focused on developing comprehensive operational tools to increase insider threat management maturity across the nuclear enterprise.

One of the things that drew me to CNF was the opportunity to connect with a trusted community of nuclear cybersecurity professionals. I see CNF as a way to ensure our research remains grounded in reality and focused on solving real-world problems. I look forward to drawing on your experience and insights to help identify and prioritize the cybersecurity challenges facing our sector. Full disclosure: I am not magic and I cannot make more money appear in your cybersecurity budgets. But I can arm you with the right data and evidence to make a strong case, and I can ensure our research efforts are focused on developing practical and relevant solutions that address the needs of our community.

I look forward to collaborating, sharing ideas, and contributing research that can make a meaningful difference for the security and resilience of our sector. And if all else fails, I am happy to provide you with a steady supply of cybersecurity dad jokes.

One more for the road:

Why don't cybersecurity professionals like nature?
Because there are too many bugs

See you all in November!

Audrey Crowe
Canadian Nuclear
Laboratories

Updates from the CNF Working Groups

Insider Threat
The Insider Threat Working Group conducted its first virtual meeting in August with participants from Canada, Germany, and the United States. The participants highlighted best practices from their organization as well as sharing information about resources they found valuable. The outcomes will contribute to the creation of an insider threat guidance overview document that will be presented at the upcoming Autumn CNF event.

Governance
The Governance Working Group is drafting a document on best practices for critical infrastructure companies to engage with the nuclear regulator on cybersecurity governance. The guidelines suggest shifting away from technical reporting to clear, business-aware communications that address cyber risk in plain language and within the wider context. They also look at the importance of dialogue and collaboration.

AI
The next virtual meeting of the AI Working Group will take place on 22 September at 15:00 CEST. Dr. Sarah Case Lackner, Senior Fellow at the Vienna Center for Disarmament and Non-Proliferation (VCDNP), will join as a guest speaker, discussing her recent research on the intersection of frontier AI models and nuclear security.

The AI Working Group is also beginning a new initiative to develop a set of high-level principles for secure-AI-by-design for nuclear facilities. These principles are meant to guide organizations in designing, building and implementing AI applications in nuclear facilities.

If you'd like to take part in any Working Group activities, please contact [Pierre Legoux](#).

Preview of CNF Autumn 2026 Meeting

 Turku, Finland |  1-5 November 2026

Planning is well underway for the 2026 CNF Autumn Event, taking place 1-5 November in the old city of Turku, Finland!

The interactive agenda will provide opportunities to share experience and insights with their expert peers from around the world as well as networking and a technical visit to Onkalo Spent Nuclear Fuel Repository.

Planned sessions include:

- **Threat landscape:** Cyber threat developments with an extra twist from Finland's geopolitical location
- **Managing regulatory expectation:** Complying to new legislation in response to threat of state sponsored sabotage
- **National perspective:** The Finnish nuclear industry and its approach to cybersecurity
- **Advanced technologies for cybersecurity:** Mobile devices, connectivity and AI in OT environments
- **Exercising cybersecurity arrangements:** Finnish cyber range facilities and Finnish cyber reserve construction

Space is limited, so secure your place today!

REGISTER HERE

Confirm, Connect and Take Part in the Community

If you haven't confirmed your CNF membership yet, please complete the following steps:

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 [Pierre Legoux](#) directly.

APPLY FOR MEMBERSHIP

[View in browser](#)

CYBER
NUCLEAR
FORUM

Copyright (C) 2026 World Institute for Nuclear Security.
All rights reserved.

Want to change how you receive these emails?
You can [update your preferences](#) or [unsubscribe](#)