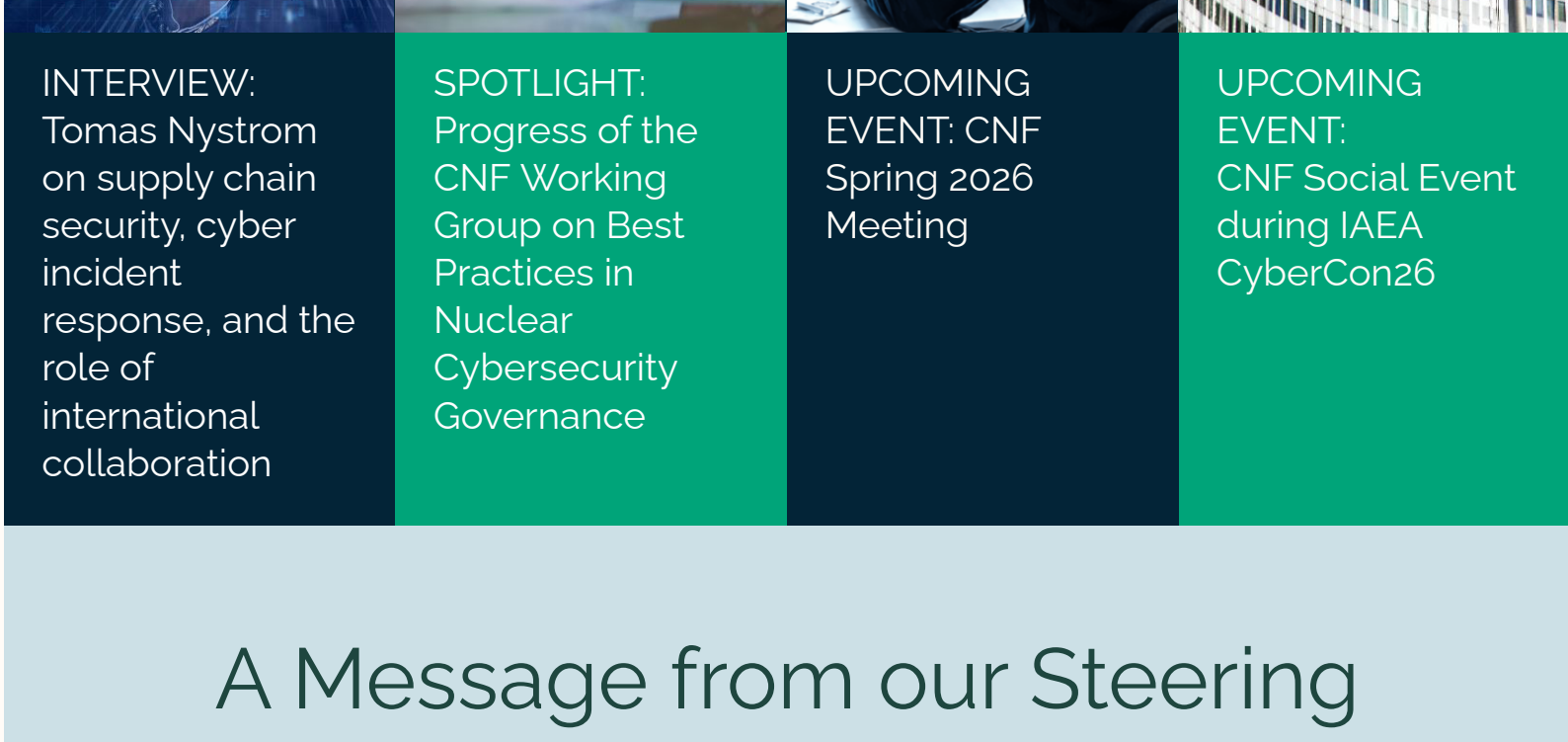


CNF Newsletter March 2026



INTERVIEW:
Tomas Nystrom
on supply chain
security, cyber
incident
response, and the
role of
international
collaboration

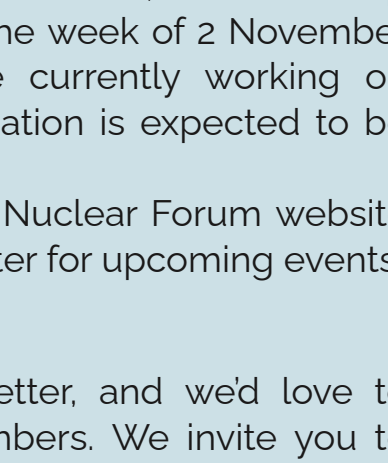
SPOTLIGHT:
Progress of the
CNF Working
Group on Best
Practices in
Nuclear
Cybersecurity
Governance

**UPCOMING
EVENT:** CNF
Spring 2026
Meeting

**UPCOMING
EVENT:**
CNF Social Event
during IAEA
CyberCon26

A Message from our Steering
Committee Chair

On behalf of the CNF Steering Committee, I would like to wish you a warm welcome to the quarter 1 2026 CNF Newsletter. We have been working hard to deliver interesting and valuable activities for our members and the broader community of nuclear cybersecurity specialists in 2026. We hope you will enjoy and benefit from your membership or simply value being part of some of our activities. First, I would like to thank all of you who have reconfirmed their membership. We value your engagement and support. We encourage others who want to join our community and contribute to our programme of work to apply for membership.



Anno Keizer
URENCO, Netherlands

Looking at upcoming CNF activities, I have the pleasure to inform you that the online CNF Spring 2026 event is scheduled for 28–29 April 2026. The first day, which will be restricted to CNF members will provide an opportunity to discuss CNF mission and activities and will provide participants with a deep dive into the topic of Artificial Intelligence, building on the work carried out by the CNF AI Working Group. On the day 2, a broader community of cybersecurity practitioners will be invited to join and to discuss cyber security matters for SMRs and advanced reactors.

On 13 May 2026, during IAEA CyberCon 2026 in Vienna, Austria, we will organise an evening social gathering for CNF members who are attending the conference. In addition, the CNF will deliver a presentation during the event to further increase the Forum's visibility and expand our membership.

Later in the year there will be many more developments and activities, but I will keep those for the next newsletter. In the meantime, please mark the week of 2 November in your diaries. Although not yet fully confirmed, we are currently working on organising the CNF Autumn event during that week. The location is expected to be somewhere in Europe or Asia.

For now, please enjoy this Newsletter and do visit the Cyber Nuclear Forum website from time to time to stay updated on our activities and to register for upcoming events.

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.

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:

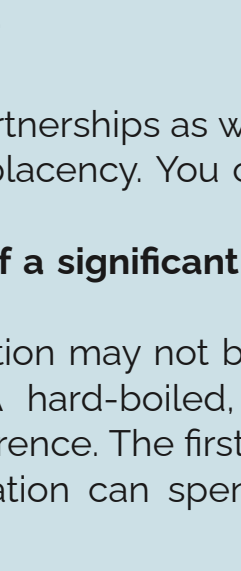
1. Fill out the **online membership form** with your personal details, organisational affiliation, job title, and a short description of your professional background and its relevance to CNF. Please note that you will be requested to upload a short CV.
2. Once submitted, your application will be reviewed 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.

[APPLY FOR MEMBERSHIP](#)

Supply Chain Security, Cyber Incident
Response, and the Role of
International Collaboration

Tomas Nystrom has worked for Fortum, an energy company in the Nordics, for more than 25 years. With experience in IT infrastructure and corporate security, he became the director of nuclear IT in the company in 2016. He is currently on a two-year secondment to WANO, where he is serving as the global IT director.



Tomas Nystrom
WANO

In this interview, he shared his perspective on supply chain security, cyber incident response, and the role of international collaboration.

What practical steps can operators take to improve supply chain security without creating excessive administrative burden?

I think you can't totally get rid of the administrative burden; some is always necessary.

Not only related to cybersecurity, but a good example of how you can be more cost-effective is an industry-driven initiative between nuclear companies in the Nordics around supplier audits and certifications. You save a lot of administrative burden if one company does the supplier audit and shares it, rather than five or ten companies having to do supplier audits. In practice, it's actually a document management system that is shared between the parties, and they have direct access to supplier audits and audit reports.

Maybe the model could be something that the Cyber Nuclear Forum (CNF) could host or run, but cybersecurity is challenging as sharing that information is sensitive. If I buy something, do an audit on it and find some vulnerabilities, that information is often too sensitive to share. CNF is a really good example of where this kind of trusted relationship forms over time. With those relationships, you could maybe share this information. It always takes time to build trust. It's usually quite person dependent, but CNF is the only example that I know of in the cyber world where it works.

How can organisations effectively approach cybersecurity requirements in their contracts, especially with small or long-term partners?

I have seen a lot of potential partners struggle with the requirements, especially the small ones. Applying the same procurement process rules to everyone makes sense, water flows to the lowest point. But the really small players struggle a lot with that process and the administrative burden. I've seen it result in smaller vendors not even bidding because they can't cope with the time and cost involved.

I think the solution is not to have lighter requirements for small vendors or for long-term partners; it wouldn't make sense for small vendors to have lower cybersecurity requirements. That would open an attack vector. To approach it more effectively, one option could be AI tools to pinpoint the requirements better. The requirements set in the nuclear world are often so complex that it's becoming difficult for a human being to comprehend everything. That was one of the first areas where we applied AI tools to manage requirements at my home company already 10 years ago.

You need to be quite vigilant about complacency in long-term partnerships as well. It's a good thing to have long partnerships, but it can also risk complacency. You can be tempted to be less strict.

How should organisations prioritise actions in the first hours of a significant cyber event?

First of all, incidents happen quite rarely, and your own organisation may not be very comfortable or used to running a significant cyber event. A hard-boiled, really experienced major incident manager (MIM) can make a huge difference. The first hours are usually the most critical ones. A less experienced organisation can spend five hours just to get organised and then the situation is still a mess.

Using a security operations centre might be a good quick win. They don't make the decisions, but they run and manage the incident professionally. It's maybe a bit of a big company luxury, but it makes a huge difference.

It is also very, very important to exercise and train. Nuclear companies are usually quite good at emergency training, but that doesn't necessarily always flow down to IT, OT and cyber organisations.

Another challenge is the architectural differences between IT and OT. For a long time, everyone saw IT and OT as quite different. OT had its proprietary stuff, and it wasn't real computers, but today it's almost the same so it actually would make sense to combine it more.

Many times, totally separate organisations run them. IT is more centralised and corporate wide and OT is more site specific. This kind of differentiation might make it more challenging to connect the dots if it's a combined cyberattack or if you see problems both in IT and OT and maybe also a physical attack at the same time. They usually also have different monitoring systems. It might be air-gapped systems or OT might have a SCADA model that runs several plants. You might use satellite or other networking to run it all and it might not be connected to IT systems.

The remedy is probably combined exercises and trainings. And maybe most importantly, aligning the incident management process between those possibly separate organisations.

How do established emergency procedures apply in response to a cybersecurity incident?

At plants, cybersecurity is often part of the security arrangements.

Cyber is actually a fantastic area to integrate into other parts because it's so broad. Many times, you can actually leverage the cyber side to influence more broadly because cyber is everywhere. For example, you can leverage IT and OT through cyber because they need to comply with cybersecurity requirements. I might have difficulties influencing the OT side, but I can do it through cyber. It can be a good tool to be influential in your organisation. It's a useful framework.

What governance structures do you find are most effective for ensuring accountability for cyber resilience across these extended enterprise networks?

Nuclear facilities are generally owned by an enterprise. I see this everywhere I go. Nuclear is an island and if the corporate side doesn't understand nuclear you run into problems or friction. But like with cyber, you need to elevate it to the top. Nuclear

needs to be at the top level in the enterprise governance structure. And it's usually not; nuclear has been kept as its own island, separate from enterprise governance. If the top level doesn't take the requirements into account, then you run into all kinds of trouble with your regulator on data handling or sensitivity. But if you elevate the nuclear to the top of the structure, then it's sort of built in and you can take into account the nuclear requirements. The same thing with cyber: I think cyber should be at the top. If you report through some strange structures, through HR or finance or whatever, it's not the same, so elevate it to the top.

What makes cross-industry and international cooperation particularly important for addressing cyber threats to nuclear facilities?

As an example, WANO was created after the Chernobyl accident in Ukraine. Organisations thought the ultimate cause of the accident was insufficient collaboration and information sharing. They created this global non-profit information sharing organisation.

I think that's important because no one can or should stand alone. When you don't collaborate, you think you know everything. You are in a silo just because you haven't seen anything else. Personally, before I went to work for WANO in London, I had done a lot of international cooperation through CNF and many other groups. I still noticed that I was quite siloed, which can be a bit dangerous. I saw how things were done differently, and that they were better in many ways. That shows the true value of international cooperation and also the value of diversity.

The most important thing in my career has been networking. And with information sharing, it may be a cliché but the more you share, the more you get, even if you don't realise it right away. It takes a lot of effort and a long time to really, truly build these global networks.

Some people hold back and don't share what they know, especially within companies, but that's the worst thing that you could do.

How can collaboration through CNF enhance visibility of evolving supply chain risks or cyber risks?

CNF has helped me a lot. I wouldn't have met the connections I did through CNF in any other way. But CNF is not that cutting edge. It is quite good for more strategic and long-term mitigation of evolving risks. It's fantastic to have this sort of sandbox where you can discuss and test ideas. But I see potential for another, more active side as well.

CNF Working Group Spotlight - Best
Practices in Nuclear Cybersecurity
Governance

Following the 2025 Cyber Nuclear Forum (CNF) meeting in Amsterdam, a cross-section of CNF members from multiple sectors and regions agreed to collaborate on drafting best practices for nuclear cybersecurity governance. The

objective of this effort is to provide a high-level set of governance principles that can be broadly applied across the global nuclear sector, supporting both CNF participants and the wider community.

Tom Wilson (Southern Company), Tomas Nystrom (WANO), and Thomas Walter (PreussenElektra) committed to drafting initial guidance across three foundational areas of nuclear cybersecurity governance: **Board Engagement**, **Executive Engagement**, and **The Role of Regulation and Standards in Nuclear Cybersecurity**. Additional contributions were provided by Jelmer Van der Neut (URENCO) and Bert Cuyppers (SCJ CEN), with broader CNF members invited to participate. Early discussions also benefited from the insights of Don Dudenhoeffer and Nathan Faith.

Drawing on experience across the U.S., European, and Middle Eastern nuclear cybersecurity landscapes, the team has completed a first draft of **Board Engagement Best Practices**, along with proposed outlines for the remaining two governance areas. These documents establish a framework for further refinement and development with input from the larger CNF community.

The working group welcomes continued feedback from all CNF members and looks forward to advancing the drafts toward a consolidated best-practices document for presentation at the next in-person CNF meeting in 2026.

CNF Spring 2026 Meeting

Online | 28-29 April 2026



The CNF is pleased to announce its 2026 Spring Meeting to be held online on 28–29 April 2026, from 15:00 to 17:15 CEST on both days.

Day 1 will be restricted to CNF Members and will open with administrative updates including membership, funding and priorities for the remainder of 2026. Furthermore, CNF working groups on governance, insider threat, and artificial intelligence will provide an overview of ongoing collaborative efforts.

The day will continue with a focused session on the integration of advanced technologies – such as AI, 5G, IIoT, and quantum – at nuclear facilities. Presentations and discussions will explore practical applications, cybersecurity concerns, regulatory status, and operator experience, including insights from recent WINS work on advanced technologies.

On Day 2, invited guests will join the CNF members for forward-looking presentations addressing topics such as advanced reactors and SMRs, the nuclear renaissance, workforce challenges, geopolitical developments, and emerging threats.

[REGISTER HERE](#)

CNF Social Event during
IAEA CyberCon26

Vienna, Austria | 13 May 2026



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

We are planning an informal evening gathering intended to complement the conference programme by providing a relaxed environment for participants to connect, exchange ideas, and strengthen professional relationships beyond the formal sessions.

This social event will bring together members of the CNF community and CyberCon participants for an evening of networking and conversation in a convivial setting. Details regarding the venue, timing, and participation arrangements will be shared once confirmed.

In case you have any questions, please contact [Luka Cekic](#).

[REGISTER HERE](#)

[View in browser](#)