Cybercation Forum 2025
Event Report

AI, Cybersecurity, and Nordic Resilience

Cyber Security Nordic 2025

4 November 2025, Helsinki

Baltic Sea Region Youth Forum (CBSS)

Prepared by:

Justus Ferdinand August

November 2025

Executive Summary

On 4 November 2025, I represented the Baltic Sea Region Youth Forum at the Cybercation Forum at Cyber Security Nordic in Helsinki. The event focused on AI-driven cybersecurity threats, Nordic readiness in light of Russia-linked activity, and the pipeline for developing cyber talent across the region.

Representing CBSS/BSRYF, this report documents observations from panels and discussions with Nordic thought leaders, researchers, technologists, and policymakers. The dominant narrative centered on talent attraction and retention through lighter taxation, better study conditions, and competitive compensation. While valid, this approach overlooks structural requirements for regional competitiveness.

The core observation: talent pipelines alone will not position Northern Europe as a global AI and cybersecurity hub. Achieving resilience requires infrastructure investment—data centers, expanded energy capacity, and treating compute resources as security infrastructure rather than commercial afterthought.

Contents

Executive Summary **1**

1 Event Overview **3**

1.1 Context and Positioning 3

1.2 Participants and Scope 3

2 Representation and Engagement **4**

2.1 BSRYF Participation 4

2.2 Engagement Approach 4

2.3 Network Development 4

3 Key Themes and Discussions **5**

3.1 Talent Attraction and Retention 5

3.2 Education Pipeline 5

3.3 Russia-Linked Threat Activity 5

3.4 AI Integration in Cybersecurity 6

4 Strategic Observations **7**

4.1 Talent Is Necessary But Insufficient 7

4.2 Infrastructure as Security Requirement 7

4.3 Data Center Development 7

4.4 Energy Capacity Expansion 8
4.5 Structural vs. Incremental Approaches 8

5 Follow-Up Actions **9**
5.1 Continued Dialogue with SANS EMEA 9
5.2 BSRYF Policy Development 9
5.3 Network Maintenance 9

Conclusion **10**

1 Event Overview

1.1 Context and Positioning

The Cybercation Forum positioned itself as a platform for educators, experts, and industry stakeholders to address AI-driven cybersecurity threats and build the next generation of cyber talent for a resilient Nordic digital society. The forum ran alongside Cyber Security Nordic at Messukeskus, Helsinki, on 4 November 2025.

A hands-on component—the Telia Cybercation Challenge finals—took place concurrently at the same venue, demonstrating the direct link between education initiatives and practitioner capacity development.

1.2 Participants and Scope

The forum convened:

- Cybersecurity educators from Nordic institutions
- Industry security professionals and threat researchers
- Technology company representatives
- Policy advisors and government officials
- Academic researchers focused on AI and security

Geographic scope centered on the Nordic countries, with particular attention to coordinated responses to Russia-linked cyber threats and the region's capacity to develop indigenous AI and cybersecurity capabilities.

2 Representation and Engagement

2.1 BSRYF Participation

I represented the Baltic Sea Region Youth Forum and Council of the Baltic Sea States at the forum, introducing BSRYF's youth-focused policy work to attendees unfamiliar with the organization's mandate. The representation emphasized BSRYF's role in developing next-generation perspectives on regional cooperation, technology policy, and security coordination.

2.2 Engagement Approach

My participation consisted primarily of observation and targeted intervention through panel questions. Two specific questions drove deeper discussion:

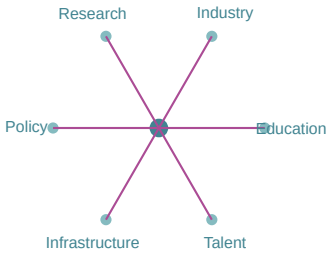
1. What concrete measures would position Northern Europe as a global hub for AI and cybersecurity development?
2. What specific protections for critical services are feasible given documented Russian cyber activity?

These interventions shifted discussion from abstract concerns toward implementation requirements and resource allocation decisions.

2.3 Network Development

Substantive conversations occurred with multiple stakeholders:

- **Christofer Bjelvenius**, Country Manager Sweden at SANS EMEA: Discussion of infrastructure requirements for AI security capacity, particularly compute and energy dependencies. Follow-up planned.
- Nordic cybersecurity researchers exploring threat modeling for AI systems
- Policy advisors working on cross-border security coordination
- Industry representatives evaluating talent pipeline effectiveness



Nordic Cyber Hub

3 Key Themes and Discussions

3.1 Talent Attraction and Retention

The prevailing narrative emphasized human capital development and retention strategies:

- Lighter individual taxation for technology professionals
- Improved study conditions and research funding for cybersecurity programs
- Competitive salary structures and bonus packages aligned with private sector expectations
- Streamlined pathways from education to employment in critical infrastructure protection

Panel consensus held that Nordic countries face disadvantages recruiting and retaining top-tier cybersecurity talent compared to US tech hubs and emerging Asian centers.

3.2 Education Pipeline

Discussion focused on the Telia Cybercation Challenge as a model for practical skills development:

- Hands-on competition format providing real-world experience
- Direct pathway from academic study to industry placement
- Assessment of technical capabilities under realistic constraints
- Bridge between theoretical cybersecurity education and operational demands

The challenge finals, running concurrently with the forum, illustrated the integration of education initiatives with measurable skill validation.

3.3 Russia-Linked Threat Activity

Multiple panels addressed documented cyber operations targeting Nordic infrastructure:

- Persistent reconnaissance of critical services
- Targeting of energy infrastructure and supply chain dependencies
- Influence operations leveraging AI-generated content
- Coordination between state actors and criminal organizations

Discussions acknowledged threat sophistication but offered limited concrete defensive measures beyond awareness and information sharing frameworks.

3.4 AI Integration in Cybersecurity

AI emerged as both opportunity and vulnerability:

- Defensive applications: automated threat detection, pattern recognition in network traffic, vulnerability scanning at scale
- Offensive concerns: AI-enhanced social engineering, automated exploit generation, adversarial attacks on AI systems
- Capability gap: Nordic countries' defensive AI capabilities lag threat actor offensive innovation

4 Strategic Observations

4.1 Talent Is Necessary But Insufficient

The forum's emphasis on talent pipeline development reflects genuine needs but incomplete strategic analysis. Attracting cybersecurity professionals requires more than competitive compensation:

- Access to cutting-edge infrastructure (compute resources, research facilities, operational environments)
- Participation in significant problems (regional security challenges create opportunity for meaningful work)
- Professional development pathways (exposure to advanced threat landscapes and defensive requirements)
- Ecosystem density (critical mass of expertise enabling knowledge exchange and career mobility)

Focusing exclusively on tax incentives and salary structures ignores these foundational requirements.

4.2 Infrastructure as Security Requirement

A critical gap in forum discussions: treating cybersecurity capacity as separate from computational infrastructure. Reality connects them:

- AI-powered threat detection requires substantial compute resources
- Security research and vulnerability analysis demand high-performance computing
- Defensive capabilities depend on training AI models on threat data at scale
- Energy constraints limit deployment of computationally intensive security measures

Northern Europe cannot achieve cybersecurity leadership without addressing these dependencies.

4.3 Data Center Development

The region possesses natural advantages for data center infrastructure:

- Cold climate reducing cooling costs by 30-40%
- Access to renewable baseload energy (Nordic hydropower, potential nuclear capacity)
- Geographic position between European and Asian markets
- Political stability and rule of law
- High digital literacy and technical workforce baseline

Leveraging these advantages requires deliberate policy choices, not market drift.

4.4 Energy Capacity Expansion

Current energy constraints directly limit cybersecurity capabilities:

- High energy costs make large-scale AI security operations economically unviable
- Limited capacity prevents deployment of computationally intensive defensive systems
- Dependence on imported energy creates strategic vulnerability
- Competition for power between general economic activity and security infrastructure

Expanding energy generation and reducing costs should be framed as security investment, not merely economic development.

4.5 Structural vs. Incremental Approaches

Forum discussions gravitated toward incremental improvements within existing frameworks. Missing perspective: structural changes enabling step-function capability increases.

Incremental approaches:

- Adjust tax rates by 2-5%
- Increase university cybersecurity program funding
- Create additional professional development programs
- Strengthen information sharing between agencies

Structural approaches:

- Build massive compute infrastructure treating it as security asset
- Expand energy generation specifically for high-value technology applications
- Create regulatory environment optimized for rapid security innovation deployment
- Integrate cybersecurity requirements into all critical infrastructure from design phase

Both matter, but forums like Cybercation underweight structural thinking.

5 Follow-Up Actions

5.1 Continued Dialogue with SANS EMEA

Christofer Bjelvenius, Country Manager Sweden at SANS EMEA, expressed interest in infrastructure-security connections. Planned follow-up:

- Deeper discussion of compute requirements for modern cybersecurity operations
- Analysis of energy dependencies in AI-powered defense systems
- Potential collaboration on regional capability assessment
- Exploration of BSRYF involvement in Nordic cybersecurity education initiatives

5.2 BSRYF Policy Development

Insights from Cybercation inform BSRYF's ongoing work:

- Integration of cybersecurity perspectives into AI policy recommendations
- Emphasis on infrastructure requirements in technology strategy documents
- Youth perspective on security-infrastructure connections often absent from expert discussions
- Potential workshop or report connecting AI development, energy policy, and regional security

5.3 Network Maintenance

Connections established with Nordic researchers, policymakers, and industry representatives provide foundation for ongoing engagement. BSRYF can serve as bridge between youth perspectives and expert communities in future security and technology forums.

Conclusion

The Cybercation Forum 2025 effectively highlighted Nordic cybersecurity challenges and education initiatives. However, the dominant narrative—talent attraction through tax incentives and improved study conditions—addresses symptoms rather than structural requirements.

Three observations frame a more complete approach:

1. **Talent requires infrastructure** to be effective. Cybersecurity professionals need access to compute resources, energy capacity, and research environments. Tax breaks without infrastructure investment yields limited results.
2. **Security and computation are inseparable** in modern threat landscapes. AI-powered defense requires massive computational resources. Treating data centers and energy infrastructure as security assets, not commercial afterthoughts, changes strategic calculus.
3. **Structural changes enable capability jumps** that incremental improvements cannot match. Northern Europe's natural advantages—cold climate, renewable energy, stability—create opportunity for leadership if policy choices deliberately exploit them.

BSRYF's continued engagement in these discussions brings youth perspectives and cross-sectoral thinking often absent from specialized forums. The connections established at Cybercation provide foundation for deeper collaboration on infrastructure-security linkages.

Contact Information

Justus Ferdinand August
justus.august@icloud.com

Baltic Sea Region Youth Forum
Council of the Baltic Sea States (CBSS)