Connect4Cyber ECCC 1-3

Erik Hieta-aho, PhD
Research Team Leader
Advanced Cybersecurity and Cryptography

Sustainable growth with research and development

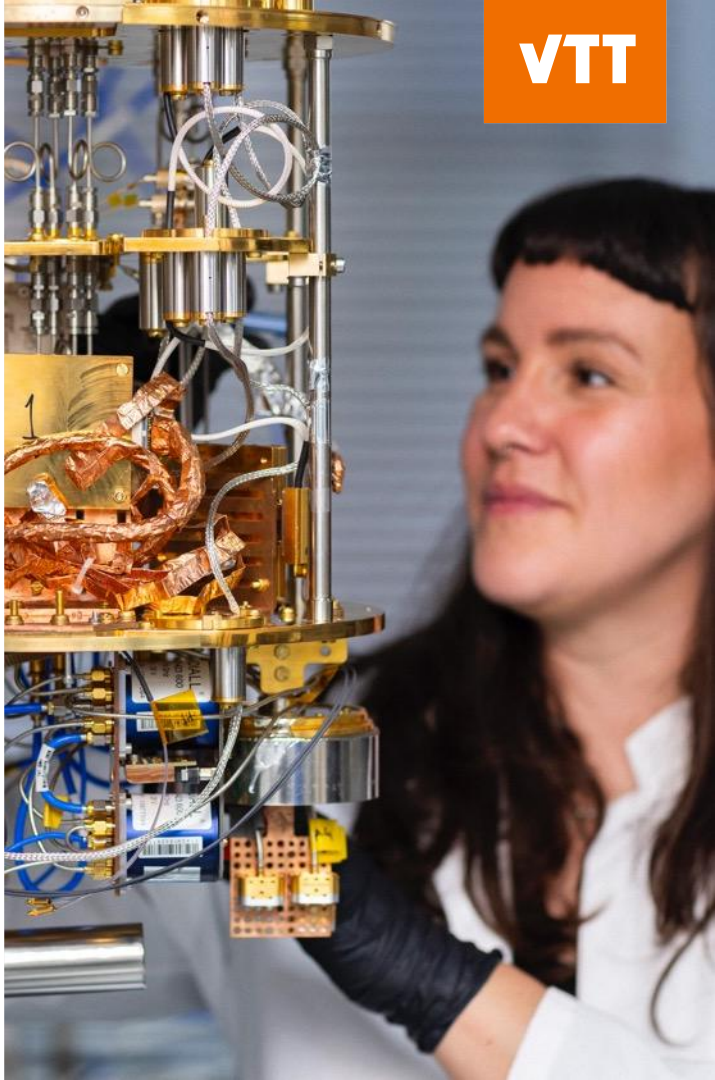
VTT is a visionary research, development and innovation partner for businesses and society and one of Europe's leading research organisations.

We bring together people, businesses, science and technology to solve the world’s biggest challenges and create sustainable growth, jobs and well-being.

2,390
employees

1,100
customers

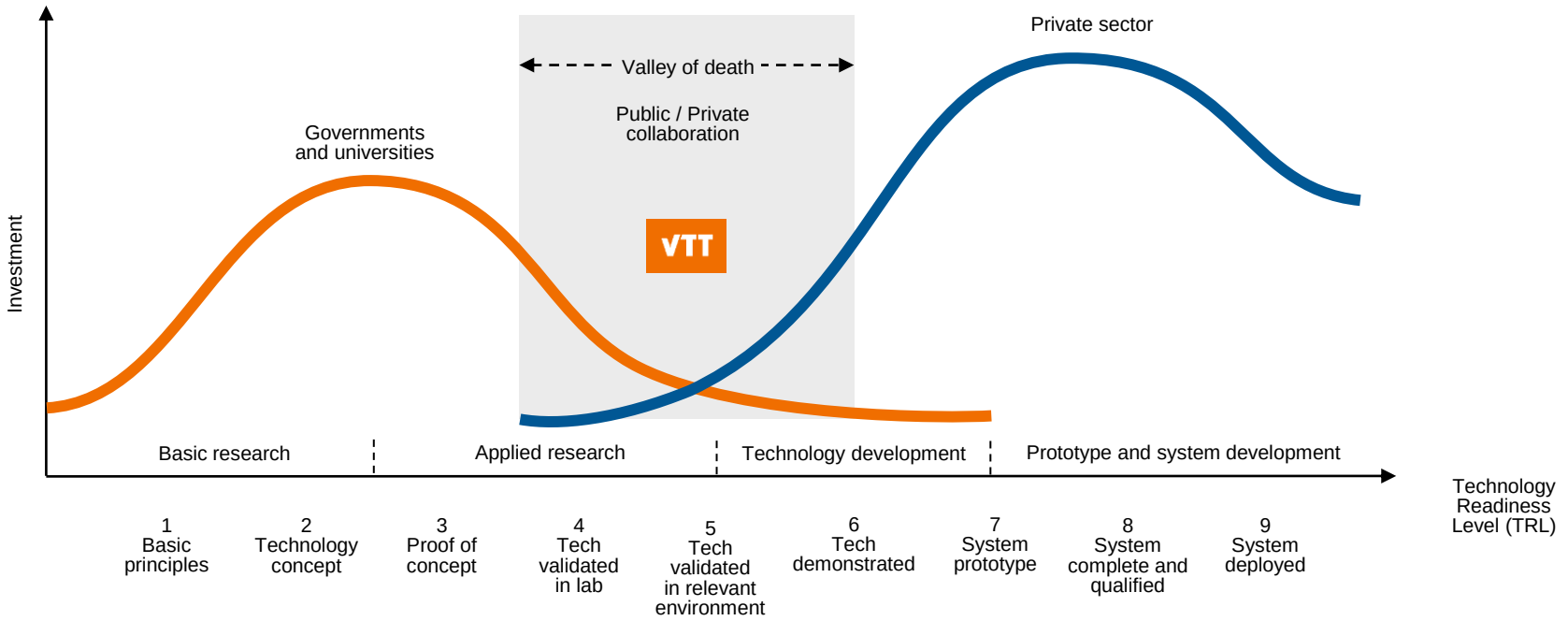
296 M€
operating income



At VTT, we've been creating hope through research for 80 years. By combining multidisciplinary research expertise with cutting-edge technologies, we help create radical change and sustainable breakthroughs.

Thinking *beyond the obvious*, we unlock new solutions.

We help our customers turn science into practical innovations



Advanced Cybersecurity and Cryptography Research Team

Advanced Cybersecurity and Cryptography

- 18 researchers
  - Cryptographers
  - Cybersecurity experts
- **Cryptography experts**
  - Privacy enhancing technologies
    - Digital Credentials/VCs
    - FHE
    - PUFs etc
  - PQC and QKD expertise
    - Implementation testing
    - Crypto-agility
    - Cryptography inventories
    - Hardware security testing

- **Cybersecurity experts**
  - 5G/6G Network Security
    - ORAN Security Orchestration
  - AI and Cybersecurity Research
    - AI optimization of network management
    - Security of AI implementation
  - Platform Security
    - Confidential computing
    - Pen testing
    - Hardware security

ECCC-1 - Approaches and tools for security in software and hardware development and assessment

Interested in joining a consortium

- Hardware testing and implementation
- Security testing methodologies, including formal verification approaches and AI-driven security testing methodologies;
- PQC hardware implementation testing
- Side-channel analysis and Fault Injection testing

ECCC-2 SecureAI Enhancing the Security, Privacy and Robustness of AI Models and Systems

Uncertainty Quantification for AI Security and Robustness

- **Uncertainty/Confidence Quantification (in LLMs):**
  - Distance between "correct answer" distribution and the LLM output distribution in a given task.
  - Sources of uncertainty:
    - Aleatoric: imperfectness of task specifications
    - Epistemic: model insufficiency, inherent LLM stochasticity (operational uncertainty)
- **Use cases:**
  - Hallucination detection
  - Early stopping during reasoning (resource efficiency + reliability)
  - Adversarial prompt detection
- **Technological readiness:**
- High readiness level, lower risk
- Black-box analysis of dynamic systems: Universal application but not universal results
- Research challenge: Finding model specific UQ proxies

Alternatives

- **Training Data Attribution:**
  - Analysis of inner dynamics of models
  - Estimating the impact of individual data points on model behaviour
  - Continuation of our work
  - Lesser technological readiness, more innovation.
  - Results more generalizable
  - **Use cases:** Poison detection, outlier detection, data intervention for, e.g. robustness
- **AI Safety and Security in feature space:**
  - Sub-circuit attribution for model behaviour
  - Sub-space identification for unsafe, insecure behaviour
  - Part of my near-future interests
  - Better technological readiness than TDA,
  - But still needs research.
  - **Use cases:** run-time jailbreak detection and mitigation, robustness

ECCC-3 Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

Possible partner

- We are interested in consortia that are focused upon the formal verification aspects of the call:

- Formal verification tools, improved High-Assurance Cryptographic Software (HACS) approaches and their integration in software workflows, to provide strong security guarantees in post-quantum migration, and enable streamlined evidence-based evaluation of secure systems that use cryptography.

- We have expertise and interest in supporting a proposal involving formal verification tools.