

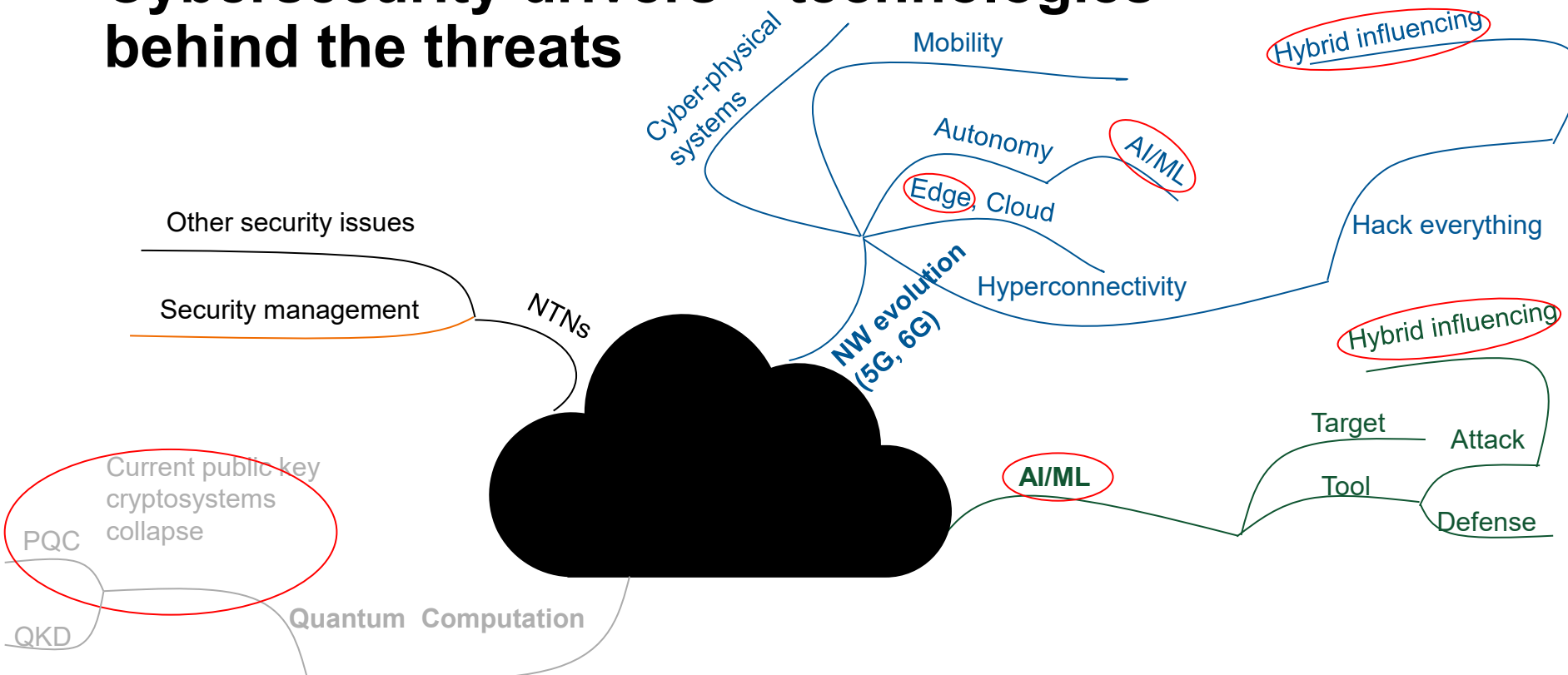
The VTT logo consists of the letters 'VTT' in a white, bold, sans-serif font, centered within an orange square. The background of the slide features a repeating pattern of stylized, interlocking shapes in orange, blue, white, and black, creating a sense of depth and movement.

VTT

Cybersecurity hot topics 2025 and beyond

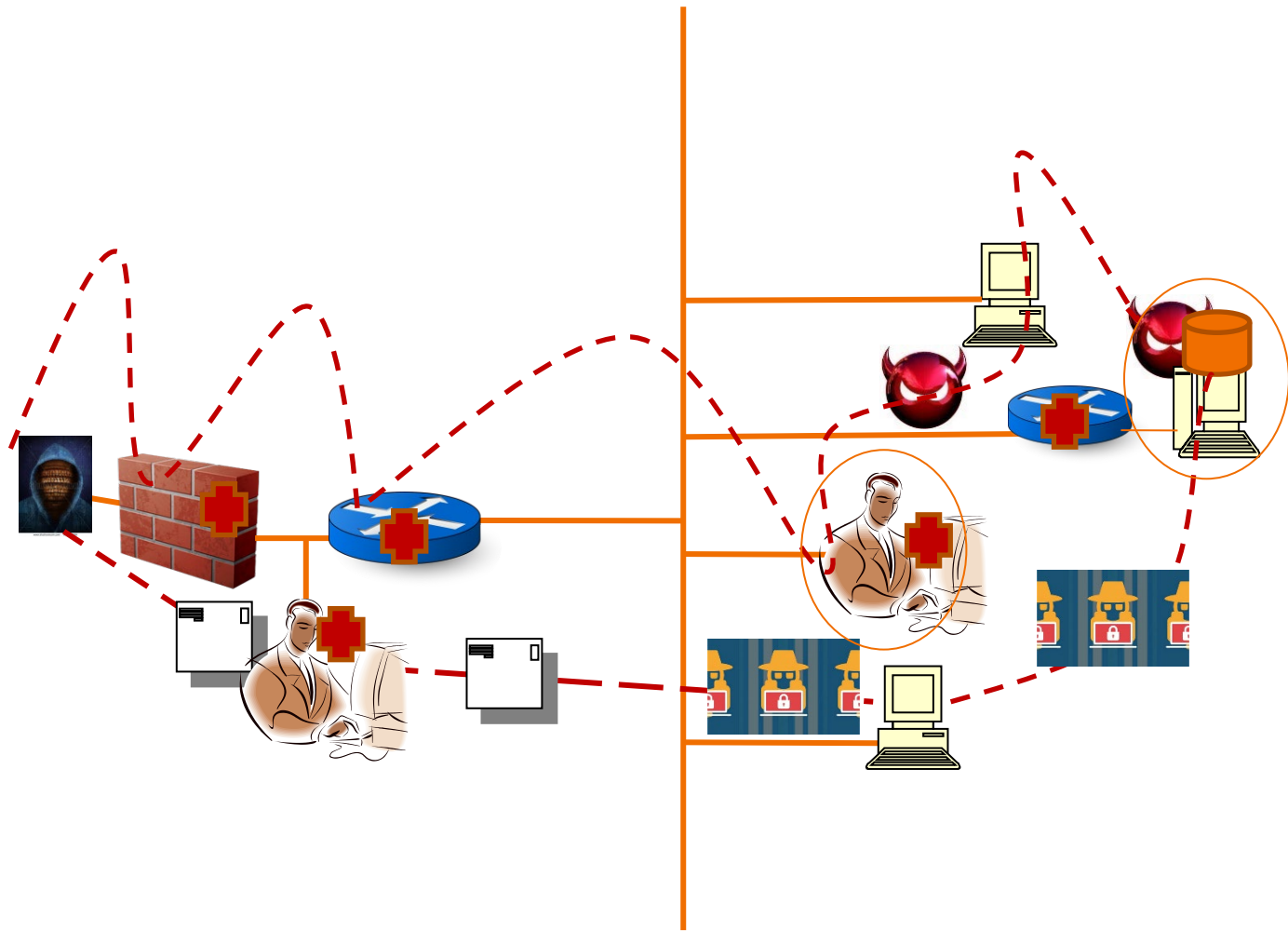
05/06/2024 VTT – beyond the obvious

Cybersecurity drivers – technologies behind the threats



Attacker's viewpoint





Examples of Smart City attack surface

- Traffic control systems
- Smart street lighting
- Public Data – openness increases cyber risks
- Mobile applications
- Cloud and Edge



- All smart grids, e.g.,: power grids, water treatment and distribution
- Mobile cyber systems like cars and public transport
- Cameras and sensors
- Location-based Services

The left side of the slide features a complex, repeating geometric pattern. It is composed of interlocking shapes that create a 3D effect, resembling a grid of rounded cubes or a woven fabric. The colors are various shades of blue, from light to dark, and white, set against a dark blue background.

Cybersecurity & some disruptive technologies

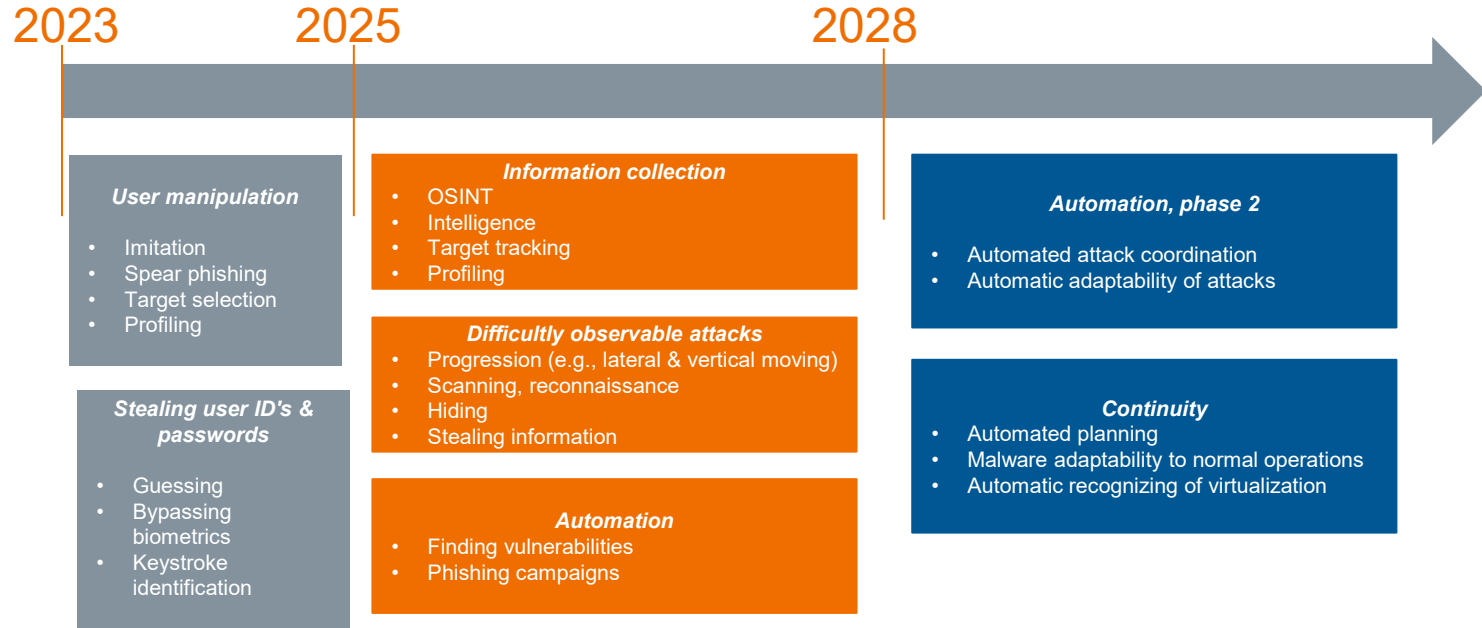
Examples of AI/ML in cyberdefense

- Intrusion Detection Systems (IDS)
- Malware Analysis
- Phishing Detection
- Network Behavior Analysis
- User Behavior Analytics (UBA)
- Threat Intelligence
- Log management & SIEM
- Forensics & incident response



AI assisted cyberattacks

reference: Traficom, *Tekoälyn mahdollistamat kyberhyökkäykset*



Computational problems that quantum computing can tackle

Some examples of mathematical problem types that could be solved more efficiently with quantum computers

1. Simulations
2. Optimization algorithms
3. **Unstructured-data search algorithms**
4. **Factoring large numbers**





OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

- Is the system a high value asset based on organizational requirements?
- What is the system protecting (e.g. key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
- What other systems does the system communicate with?
- To what extent does the system share information with federal entities?
- To what extent does the system share information with other entities outside of your organization?
- Does the system support a critical infrastructure sector?
- How long does the data need to be protected?

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.



2021-2023

Inventory and prioritize systems



2024

NIST post-quantum cryptography standard published



2024-2030

Transition of systems to NIST post-quantum cryptography standard



2030

Cryptographically relevant quantum computer potentially available

bey⁰nd

the obvious

Dr. Petri Puhakainen
Cybersecurity Lead
petri.puhakainen@vtt.fi