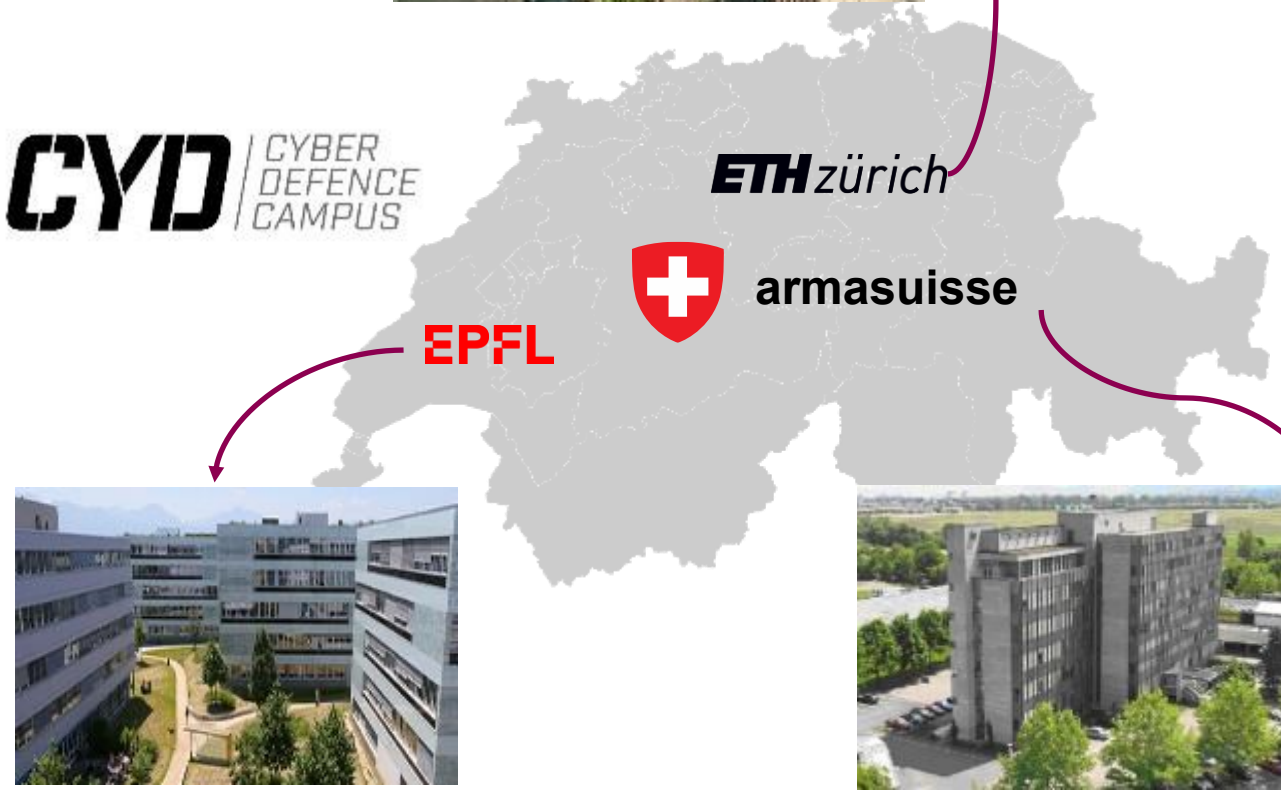
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Technology Monitoring – Track 5, Part 1

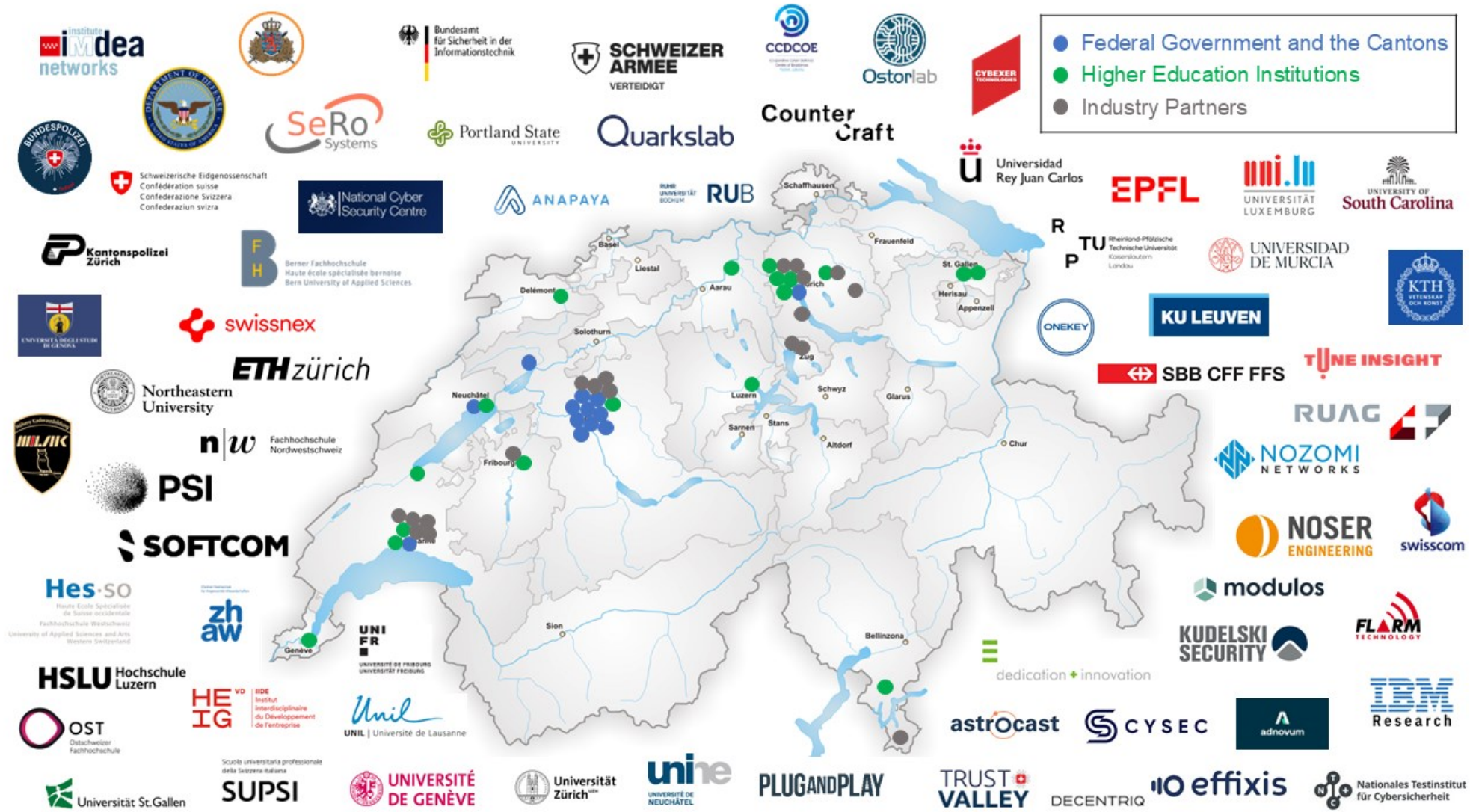
Dr. Julian Jang-Jaccard, Valentin Mulder & Dr. Alain Mermoud
Cyber Alp Retreat, June 19, 2025

Cyber-Defence Campus

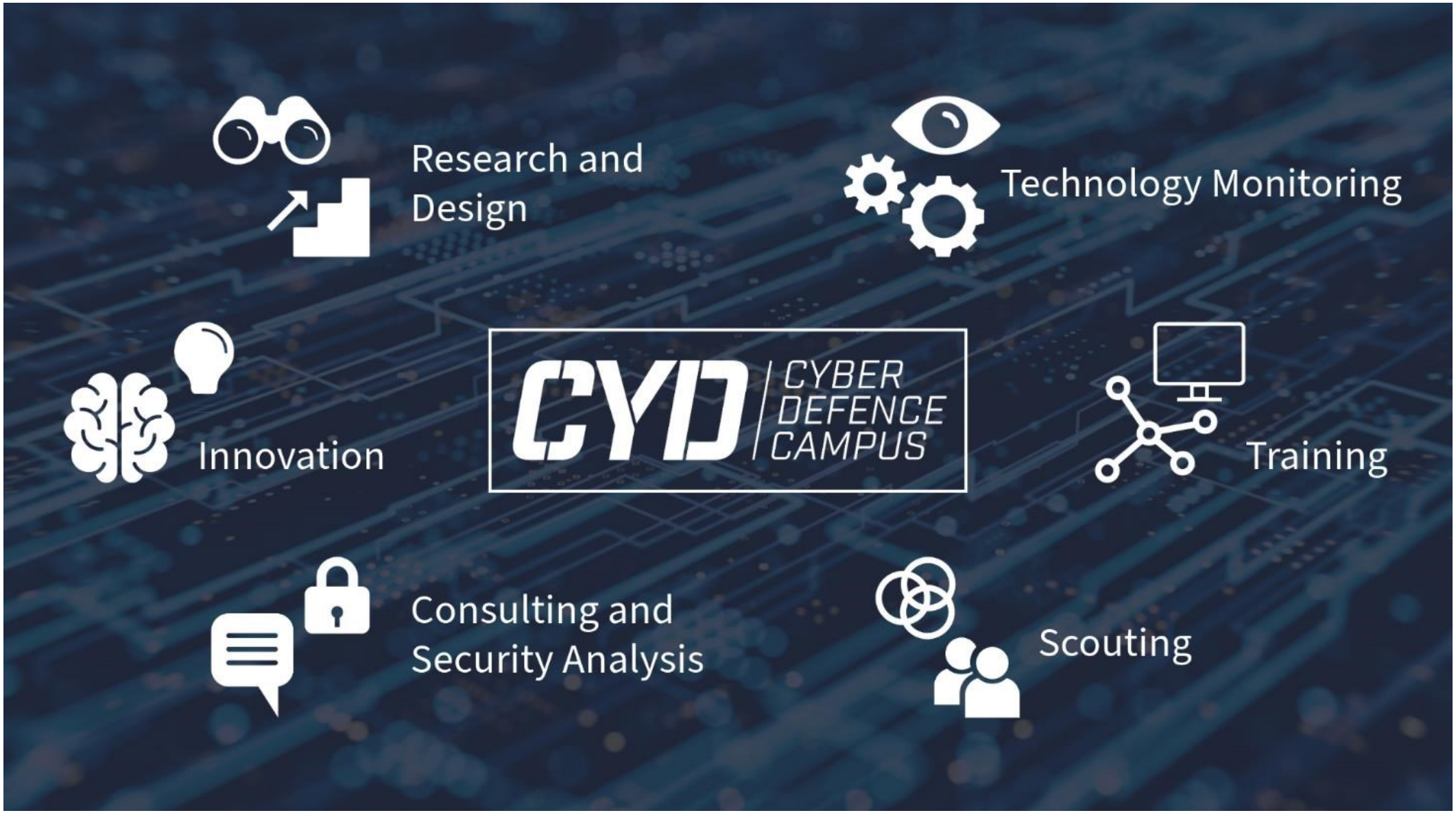


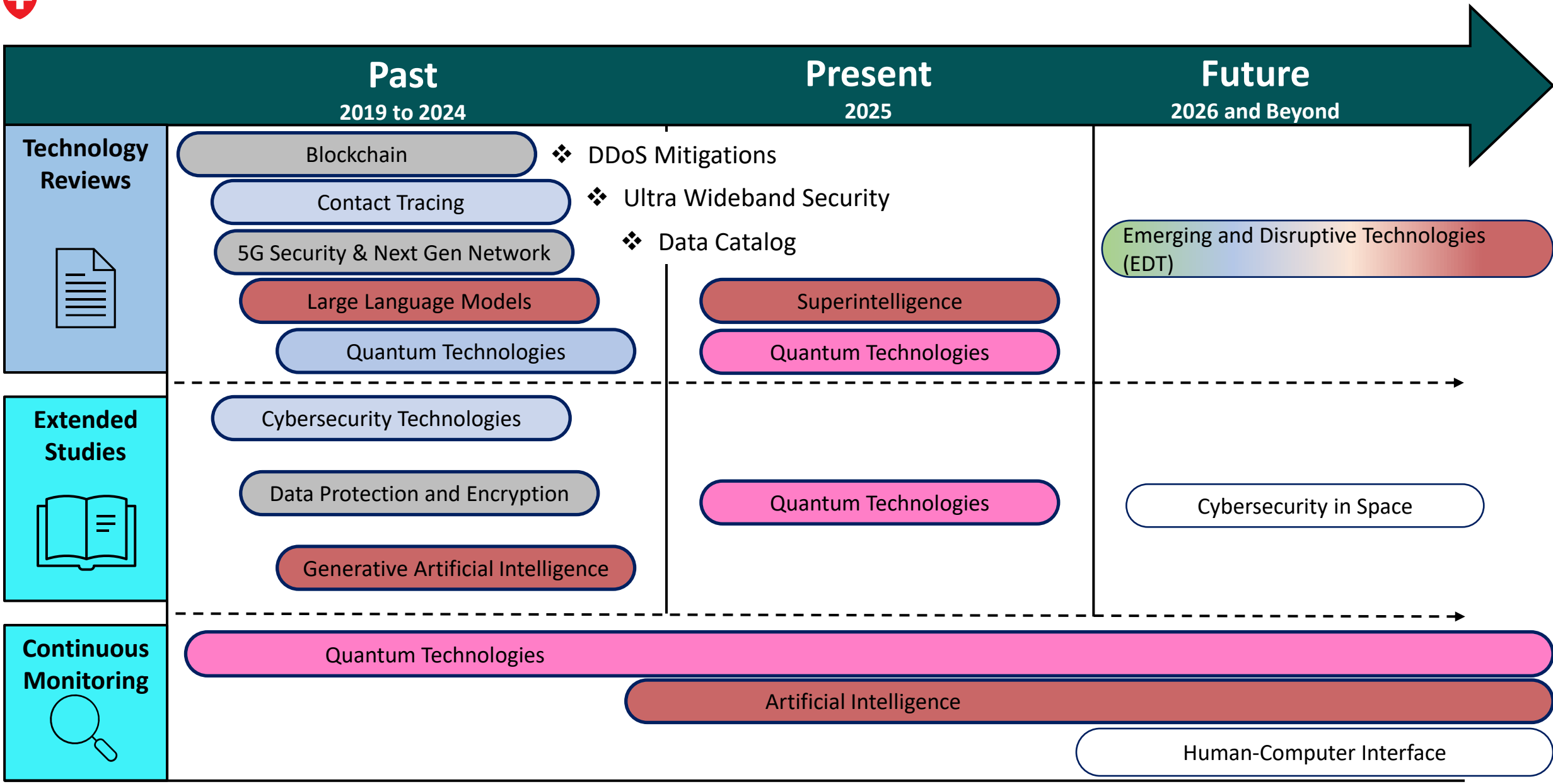
- ✓ Founded in **2019** as a part of **Swiss Federal Office for Defense Procurement armasuisse**, DDPS
- ✓ 3 locations, 4 teams with 40+ employees
- ✓ 5 laboratories with tools and resources
- ✓ 250+ completed university internships & student research projects
- ✓ 250+ scientific publications
- ✓ 60+ collaboration partners

Our Partners



Key Activities




Past
2019 to 2024
Present
2025
Future
2026 and Beyond
Technology Reviews
Blockchain
Contact Tracing
5G Security & Next Gen Network
Large Language Models
Quantum Technologies
DDoS Mitigations
Ultra Wideband Security
Data Catalog
Superintelligence
Quantum Technologies
Emerging and Disruptive Technologies (EDT)
Extended Studies
Cybersecurity Technologies
Data Protection and Encryption
Generative Artificial Intelligence
Quantum Technologies
Cybersecurity in Space
Continuous Monitoring
Quantum Technologies
Artificial Intelligence
Human-Computer Interface

Today's Program

Quantum Topics

TM Methodologies & Analysis

Thursday, June 19: Technology Monitoring (TM) – track 5 chair: Julian Jang-Jaccard		
0830 – 0845	Welcome and Opening	Julian Jang-Jaccard (CYD Campus)
0845 – 0900	**Quantum Technologies: Trends and Implications for Cyberdefence**	Julian Jang-Jaccard (CYD Campus), Philippe Caroff (EPFL, QSE)
0900 – 0930	**Expert Technology Assessment on Quantum Computing and Photonics Device**	Cornelius Hempel (PSI)
0930 – 1000	**Exploration of Miniature Quantum Sensor for Cyberdefense Applications**	Clément Javerzac (FHNW)
1000 – 1030	Coffee break with Aerospace & Transport Security track and Generative AI track	
1030 – 1050	**Trends Analysis at Swisscom: Ventures, Silicon Valley Outpost, QKD PoC, Central Innovation Funnel**	Martin Lechmann (Swisscom Ventures)
1050 – 1110	**Dynamic Network Modeling for Quantum TM**	Jean-Marie Le Goff (CERN / Dtangle)
1110 – 1130	**Leveraging Embedding and Graph Neural Networks (GNNs) for TM**	Paul Bagourd (CYD Campus)
1130 – 11:50	**Multi-Agent Reinforcement Learning (MARL) in Cyber Security**	Christoph Landolt (OST)
1150 – 1200	Wrap-up	Julian Jang-Jaccard (CYD Campus)
1200 – 1400	Lunch	

(upcoming book announcement) Quantum Technologies: Trends and Implications for Cyber Defense

Editors: Julian Jang-Jaccard, Philippe Caroff, Evan Blezinger, Valentin Mulder, Alain Mermoud, Vincent Lenders

At a Glance

40+

Expert Contributors

Leading researchers and practitioners from academia, government, and industry

22

Core Chapters

Comprehensive coverage of quantum computing, communication, and strategy

1000+

Citations

Extensive references to current research and authoritative sources

Single-blind peer review process with both external and internal reviewers

[Quantum Technologies: Trends and Implications for Cyber Defence: Jang-Jaccard, Julian, Caroff, Philippe, Blezinger, Evan, Mulder, Valentin, Mermoud, Alain, Lenders, Vincent: 9783031907265: Amazon.com: Books]

Topics Covered (Quantified)

- Goal: To explore how quantum tech impacts cyber defense.
- Total Chapters: 22 core chapters + summaries + forewords
- Major Topics:
  - 9 in Quantum Computing
  - 8 in Quantum Communication & Cryptography
  - 5 in Quantum Ecosystem & Strategy
- Additional Sections:
  - Glossary (3 pages)
  - References (extensive, >1000 citations across chapters)

Quantum Computing: Hardware Platforms and Algorithms

Superconducting Qubits

- Leverages Josephson junctions operated at cryogenic temperatures.
- Advantages include fast gate operations and established fabrication techniques.
- Used by IBM, Google, and Rigetti.

Trapped Ions

- Utilizes electromagnetically suspended charged atoms.
- Benefits include long coherence times and high-fidelity operations. Pursued by IonQ, Quantinuum

Neutral Atoms

- Employs optical tweezers to position uncharged atoms.
- Offers natural scalability and reconfigurability.
- Developed by QuEra and Pasqal.

Semiconductor Spins

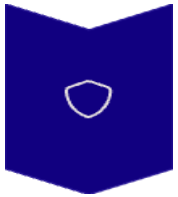
- Based on electron or nuclear spins in semiconductor materials. Promises compatibility with existing microelectronics manufacturing.
- Pursued by Intel and quantum startups.

- Current research emphasizes quantrum error control focusing on control, mitigation, and correction (e.g.,Zero Noise Extrapolation)
- Some exploration of quantum-enhanced ML and its security benefit – theoretical stage.

Quantum Communication & Cryptography

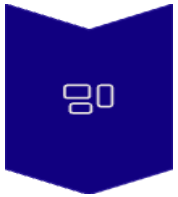
Quantum Key Distribution (QKD)

Leverages quantum properties to create theoretically unhackable encryption keys. Current limitations include distance constraints and implementation vulnerabilities.



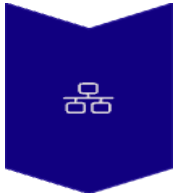
Post-Quantum Cryptography (PQC)

Mathematical approaches resistant to quantum attacks. NIST standardization process advancing with lattice-based and hash-based candidates.



Quantum Random Number Generators (QRNG)

Harnesses quantum indeterminacy for true randomness. Critical for strengthening cryptographic protocols against predictive attacks.



Quantum Networks

Enables distributed quantum computing and long-distance secure communication. Requires quantum repeaters to overcome current distance limitations.

- A significant **debate** continues regarding the optimal deployment strategy: **hardware-based quantum communication systems (QKD)** vs **software-based post-quantum cryptographic (PQC)** algorithms.
- Each approach offers distinct advantages in terms of security guarantees, implementation costs, and integration with existing infrastructure.

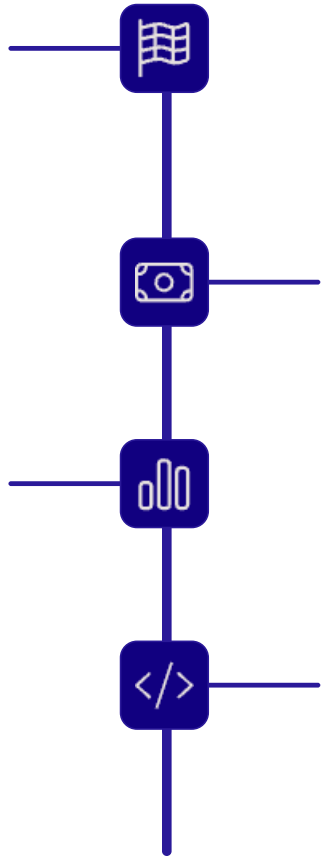
Global Ecosystem & Investment Landscape

National Quantum Strategies

Analysis of governmental initiatives across major economies including the US National Quantum Initiative, EU Quantum Flagship, and China's quantum programs.

Bibliometric Analysis

Quantitative assessment of research output, citation patterns, and international collaborations, revealing knowledge concentration and diffusion dynamics.



Investment Trends

Detailed breakdown of venture capital, corporate, and public funding flows into quantum technologies, identifying emerging hotspots and priority applications.

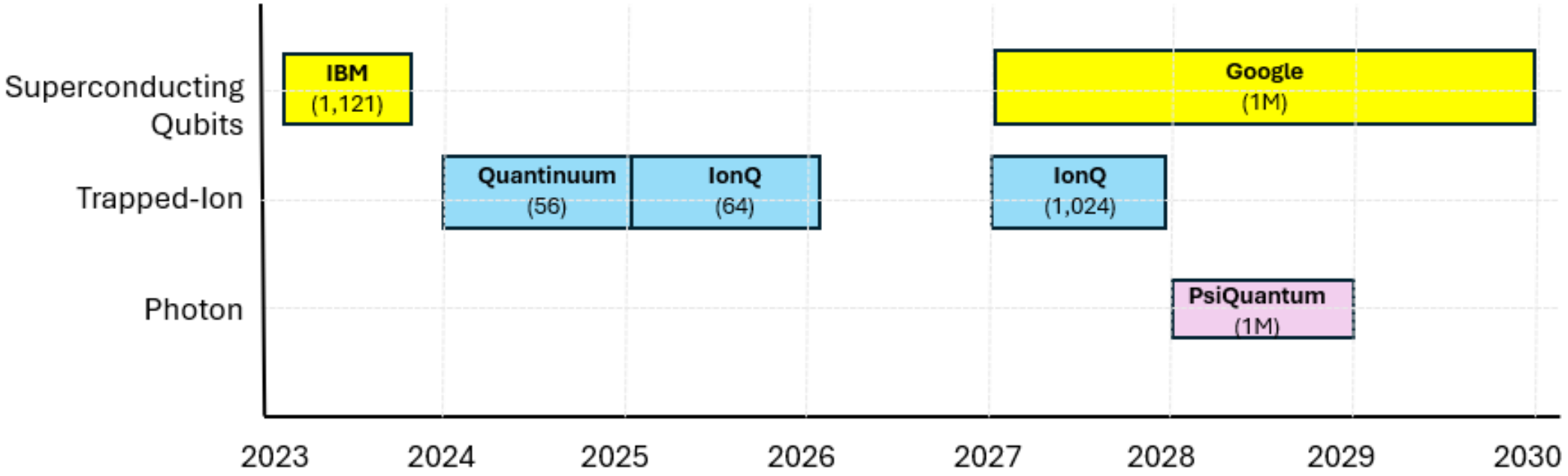
Software Repository Analysis

Examination of open-source quantum software development trends, highlighting the democratization of quantum programming tools.

A dedicated chapter examines Switzerland's quantum ecosystem as a case study, analyzing its unique combination of academic excellence, industrial partnerships, and strategic government support.

Recent **Major** Quantum Announcement and Their Implications

Quantum Computing Roadmap Timeline



- Note here the number of qubits are based on **Physical qubits**
- At this stage, 1 logical qubit requires about 100 ~ 1,000 qubits.

arxiv Publication: May 21, 2025

- RSA-2024: a common standard used for securing online data (e.g., online banking)
- It's a sharp decrease from 2019 announcement : 20 million qubits under 8 hours

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

craig.gidney@gmail.com
Google Quantum AI, Santa Barbara, California 93117, USA

(May 21, 2025)

Abstract

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

https://arxiv.org/html/2505.15917v1

Quotes from the paper

“Despite the dramatic reduction in required resources, the threat remains hypothetical. … Pushing the requirement below the one-million-qubit mark would be significantly harder given current methods”

“Looking forward, I agree with the initial public draft of the NIST internal report on the transition to post-quantum cryptography standards [nist2024]: vulnerable systems should be deprecated after 2030 and disallowed after 2035. Not because I expect sufficiently large quantum computers to exist by 2030, because I prefer security to not be contingent on progress being slow”

IBM’s Announcement: May 30, 2025

How IBM will build the world's first large-scale, fault-tolerant quantum computer

With two new research papers and an updated quantum roadmap, IBM® lays out a clear, rigorous, comprehensive framework for realizing a large-scale, fault-tolerant quantum computer by 2029.

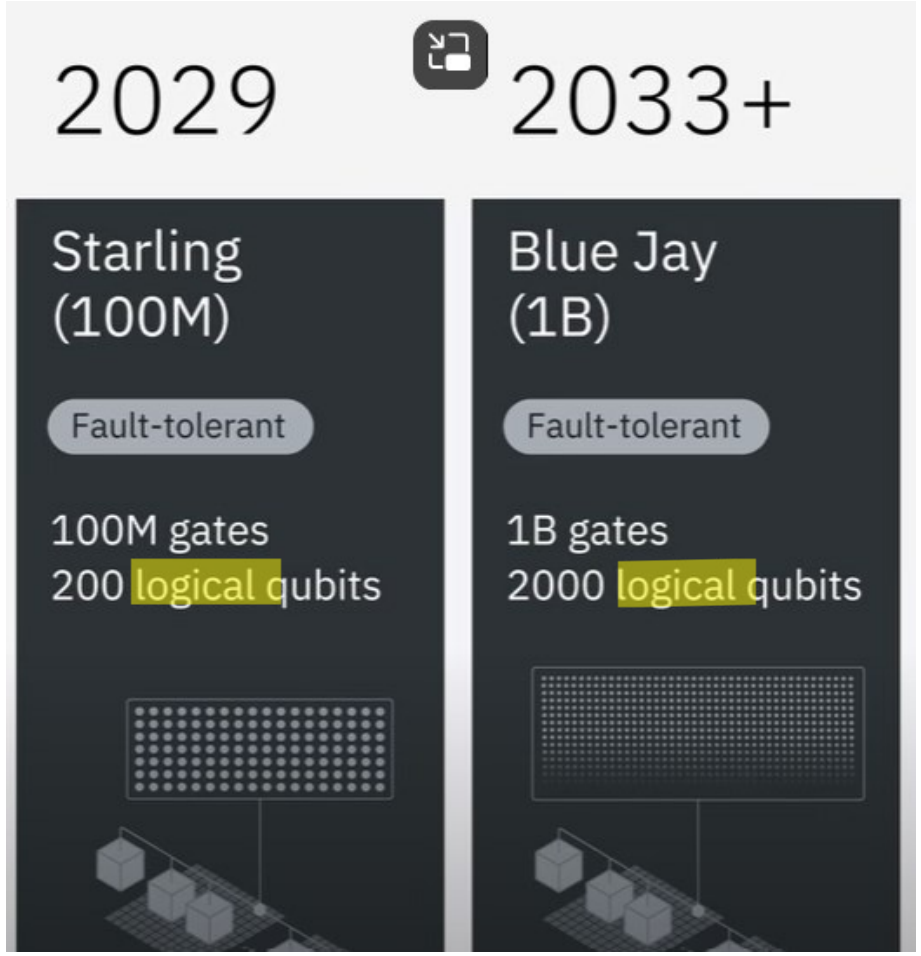
A rendering of Starling, a large-scale fault-tolerant quantum computer IBM plans to build by 2028.

“ *By 2029, we will deliver IBM Quantum Starling — a large-scale, fault-tolerant quantum computer capable of running quantum circuits comprising 100 million quantum gates on* ***200 logical qubits***” (IBM)

Changes from 2024 Roadmap

- 👉 The 2025-2028 platform changes its name from Flamingo to Nighthawk
- 👉 The targets for qubit counts are reduced from 156 qubits in Flamingo to 120 qubits in Nighthawk
- 👉 Where Flamingo stated fixed figures of maximum qubit counts when connecting multiple processors (1092 qubits by 2025 with no growth until after 2028), Nighthawk scales from 120 qubits (no multiprocessor) in 2025 to reach "up to" 120*9=1080 qubits in 2027 and 2028.
- 👉 The maximum number of gates per circuit are not changed between both roadmaps.
- 👉 The 2029 goal for the Starling platform remains unchanged at 200 qubits with 100M gates, although Starling species them as "**logical qubits**".
- 👉 The 2033+ goal for BlueJay remains at 2000 qubits with 1B gates.

New IBM Roadmap Updates



From; IBM's Vision For A Large-Scale Fault-Tolerant Quantum Computer By 2029

- Qubit Count: Gap between Physical qubit to Logical qubit reduced
  - Before (2024): 1 logical qubit = 200 ~ 300 physical qubits
  - Now (2025): 1 lq = 24 pq
- Other important measures:
  - error rates: from (two-gate) 10^{-4} to 10^{-23}
  - clock speed: from 70 mu(microsecond) to 1 mu
  - qubit connectivity?
  - 1 million qubit race still far away?

Wrap-up

Time	Monday (16.06)	Tuesday (17.06)	Wednesday (18.06)	Thursday (19.06)	Friday (20.06)
From 7.00 am	Breakfast	Breakfast	Breakfast	Breakfast	Breakfast
8.30 am - 12.00 pm	Track 1: Cyber Security Chair: Bernhard Tellenbach Track 2: Cyber Data Technologies Chair: Gérôme Bovet	Track 1: Cyber Security Chair: Bernhard Tellenbach Track 2: Cyber Data Technologies Chair: Gérôme Bovet	Track 3: Aerospace & Transport Security Chair: Martin Strohmeier Track 4: Generative AI Chair: Ljiljana Dolamic	Track 3: Aerospace & Transport Security Chair: Martin Strohmeier Track 4: Generative AI Chair: Ljiljana Dolamic Track 5: Technology Monitoring Chair: Alain Mermoud	Track 5: Technology Monitoring Chair: Alain Mermoud
12.00 pm	Lunch	Lunch	Lunch	Lunch	Lunch
2.00 pm - 5.30 pm	Tour of the Avalanche Research Institute Hike with two guides	Track 1: Cyber Security Chair: Bernhard Tellenbach Track 2: Cyber Data Technologies Chair: Gérôme Bovet	Tour of the Monstein brewery Hike with two guides	Archery on the Schatzalp Hike with two guides	Departure
From 6.00 pm	Apéro	Welcome/Farewell Apéro	Welcome/Farewell Apéro	Welcome/Farewell Apéro	
From 7.00 pm	Dinner	Dinner	Dinner	Dinner	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYD | CYBER DEFENCE CAMPUS

Cyber Alp Retreat 2026

Save the date!
31.08. to 04.09.

Thank You and Farewell Vincent

Follow us on...

LinkedIn

Website

cydcampus.admin.ch

CYD | CYBER DEFENCE CAMPUS