ALLIANZ
DIGITALE SICHERHEIT
SCHWEIZ

Cybersecurity, AI, and Quantum Seminar:

Washington, New York and Boston, USA, 20 April 2024 – 27 April 2024

The Cybersecurity, AI and Quantum Seminar of the Alliance Digital Security Switzerland (ADSS) with the support of the Swiss Confederation, the Permanent Mission of Switzerland to the United Nations, Switzerland Global Enterprise, InfoSec Global, Amazon Web Services, Samsung, Cisco, Swiss Cyber Institute and cyberunity brought a delegation of representatives from politics, business, and academia to Washington, D.C., New York, and Boston from April 20 to 27, 2024. The seminar offered an in-depth look at the culture of innovation and the driving forces behind the cybersecurity, AI, and quantum ecosystems in the United States.

Andreas Kaelin, the leader of ADSS and the seminar, emphasized that the Swiss information and communication technology (ICT) sector, which currently ranks as the seventh largest pillar of the Swiss economy, requires significant additional investments to fulfill its potential and importance.

National Councillor Franz Grüter, President of the Alliance Digital Security Switzerland, agreed and confirmed that Switzerland can benefit greatly from collaborating with the U.S. ecosystem.

How can Switzerland benefit from collaborating with the U.S. ecosystem? The following is a summary of insights gained from the seminar programme, highlighting several ways in which Switzerland can collaborate with its U.S. counterparts.

“Don’t miss the train.” – The digital revolution is gaining momentum

At the historic Watergate Hotel in Washington D.C., Swiss Ambassador to the United States Jacques Pitteloud opened the seminar with a powerful proclamation: "The 21st century will be American." He emphasized that the U.S. is at the forefront of the digital revolution, bolstered by significant investments from the Chip and Science Act and the Inflation Reduction Act. While a few European countries – such as, the UK, Germany, Sweden, the Netherlands, Denmark, and Switzerland – are making serious investments, the U.S. remains the leader.

The United States is Switzerland's top destination for foreign direct investment, surpassing Germany, France, Italy, and the UK combined, with $300 billion in direct investment. Switzerland, the seventh-largest foreign investor in the U.S., is also a valuable partner, providing essential technology for U.S. spacecraft and micro-engines. Pitteloud urged Switzerland to seize the opportunity to intensify cooperation with the U.S. as the digital revolution gains momentum.

US and Switzerland are «Academic Superpowers»

In the U.S., institutions like MIT drive innovation through cutting-edge research and strong industry collaborations, attracting top talent, venture capital, and technological breakthroughs, solidifying the U.S.'s global tech dominance. Similarly, ETH Zurich and EPFL Lausanne are central to Switzerland's tech ecosystem. According to Martin Vetterli, President of EPFL, and Joël Mesot, President of ETH, these are the only universities outside the U.S. and UK in the global top 10. Renowned for world-class research and practical innovation, they have attracted $2 billion in venture capital over the past two years, half of Switzerland's total venture capital investment.

Multinational companies like AWS, Cisco, Samsung, Google, Microsoft, IBM, Nvidia, and Disney have a significant presence in Switzerland, creating jobs and driving technological advances through substantial R&D investments. Many of these initiatives are led by former ETH and EPFL students who have established company branches in Switzerland. The universities also contribute to climate change, public health, and education innovations. In 2023, they launched the Swiss AI initiative to position Switzerland as a leading hub for transparent and reliable AI development. With a supercomputer featuring 10,000 Nvidia GPUs, they support world-class research. Jacques Pitteloud asserts that without the scientific prowess of ETH and EPFL and the skilled Swiss workforce, Switzerland would be "just another normal country."

Despite their important contributions to Switzerland's future prosperity, ETH and EPFL are reaching their limits. Martin Vetterli noted that, for the first time in Swiss public university history (excluding medical schools), EPFL will cap the number of first-year students. Additionally, Serge Frech, director of ICT-Berufsbildung Schweiz, predicts a shortage of 38,700 ICT professionals in Switzerland by 2030, potentially costing the economy CHF 30 billion.

The U.S. Government actively subsidizes innovation

The U.S. government actively promotes and subsidizes innovation, driving advancements across various sectors. Executive orders on AI, quantum computing, and cybersecurity, along with initiatives like the Chip and Science Act and the Inflation Reduction Act, boost clean energy, semiconductors, AI, quantum computing, cybersecurity, healthcare, and biotechnology. These policies provide substantial funding, attract talent, and encourage foreign investment.

Switzerland’s Role as a Neutral, Bridge Builder

Our delegation was honoured to be invited by H.E. Ambassador Pascale Baeriswyl to the Permanent Mission of Switzerland to the United Nations in New York. Ambassador Baeriswyl emphasized the importance of the UN Charter, which focuses on economic development, human rights, and peace and security. Despite the Charter, the world faces 110 armed conflicts and 114 million refugees, leading to global destabilization. Today, the Security Council is struggling with leadership, trust, and truth, exacerbated by misinformation and violations of international law. Geopolitical tensions frequently hinder the adoption of constructive resolutions.

Switzerland, with its neutral, bridge-building role, can make a difference in international law, build trust, and engage civil society. Switzerland's four priorities for the Security Council, defined by the Federal Council, are sustainable peace, protection of civilians, climate security, and effectiveness and transparency. An important aspect of this agenda is AI for Good, including co-hosting the AI for Good summit in Geneva, the Digital Dilemmas initiative with the ICRC, and mitigating the risks of deep fakes with EPFL.

In technology diplomacy, Switzerland's neutral stance is deeply rooted in its humanitarian tradition and commitment to international law and human rights. Geneva hosts one of the world's leading digital governance hubs, where over 50% of global discussions on digital governance occur. These discussions focus on the societal impact of technology, emphasizing a human-centered approach. This approach, described by Microsoft President Brad Smith as the "spirit of Geneva," bridges the gap between people and technology and underscores Switzerland's role in fostering a balanced and inclusive digital future.

Geopolitical dynamics have intensified the demand for data

Data is the new oil, AI is the new refinery, and top AI models require the best data, making data a crucial geopolitical asset. Don D'Amico, Founder and CEO of the Glacier Network, highlighted that anti-privacy governments collect vast amounts of data, giving China an edge in AI advancements, while the U.S. excels in AI tools. Europe, with stringent privacy regulations, struggles to balance innovation with data protection, resulting in a $4 billion market for Commercially Available Data (CAI), with 45% of its revenue from the U.S.

Doug Levin, Executive Fellow at Harvard Business School, noted that new data centers are emerging globally at a rate of one every three days, driven by AI demands. This trend towards cloud-based computing poses challenges, such as increased energy consumption. The current U.S. grid infrastructure cannot support the surge in AI demands, prompting companies like Amazon and Google to establish data centers abroad, marking a significant shift in AI adoption and infrastructure.

The Rise of Generative AI

Doug Levin highlights significant shifts in AI, particularly towards generative AI and Large Language Models (LLMs), which enhance language processing tasks. In March 2023, OpenAI released GPT-4, marking a major advancement with enhanced human-like reasoning, as noted by Abhi Yadav, MIT alumni and HBS mentor.

Despite the praise, GPT-4's release also highlighted ongoing limitations and ethical concerns. Abhi Yadav pointed out issues with information accuracy and hallucinations, leading to biased outputs. Leila Elmergawi, Senior Advisor at the U.S. Department of State, mentioned that AI applications, even with good intentions, can cause harm. For instance, AI introduced in courts to reduce bail decision times ended up reinforcing biases. Thus, ethical considerations are crucial in AI development.

Emerging technologies like LLMs, knowledge graphs, and autonomous agents promise to transform raw data into actionable insights, leading to decision intelligence. Dr. Francesca Lazzeri from Microsoft emphasized the importance of building LLM applications responsibly, assessing harm, bias, and quality in context. Abhi Yadav predicts that open-source AI software like Lama3 will surpass closed-source models like OpenAI for specialized, country-specific cases.

Another challenge is the escalating threat activity in the AI landscape. Doug Levin noted that cybercriminals, hackers, state-sponsored actors, and insider threats are using AI for malicious activities, such as automated social engineering, deepfakes, intelligent malware, adversarial attacks, and spear phishing. However, AI also offers positive developments in cybersecurity, enhancing security mechanisms and threat detection. In the future, AI will enable more proactive cybersecurity measures, predictive analytics, and greater integration into cloud services and IoT devices.

“AI for good requires a united, purpose-driven approach”

Mark Minevich, author and President of Going Global Ventures, believes AI can tackle humanity's biggest challenges, such as healthcare, education, and climate change. He emphasizes that AI should go beyond corporate and national interests to address global issues. An inclusive innovation ecosystem, involving governance, industry, NGOs, and academia, is crucial for achieving a sustainable and just future. Minevich urges policymakers, investors, entrepreneurs, and leaders to focus on broader societal impacts.

Minevich highlights the U.S. as a global AI superpower, attracting 75% of the world's top AI talent and leading in venture capital. Frank Michaud, Principal Engineer at Cisco Switzerland, notes that 61% of notable AI models come from U.S. institutions, compared to 21% from the EU and 15% from China, underscoring the importance of U.S. leadership. However, Switzerland shows reluctance in adopting new AI programs.

Leila Elmergawi, who led the first UN General Assembly resolution on AI, notes the increased importance of AI governance, especially since the rise of generative AI like ChatGPT in late 2022. Countries worldwide are trying to regulate AI, sometimes excessively hindering innovation or inadequately putting everyone at risk. Elmergawi stresses that poor AI governance in one country affects the entire world. The U.S. approach balances regulation and innovation, gaining voluntary buy-in from AI companies. In October 2023, the Biden administration issued an executive order for federal agencies to create guidelines for safe AI development. A UN resolution on trustworthy AI for sustainable development was agreed upon by all 193 countries in March 2024, highlighting global collaboration.

However, robust and standardized evaluations for LLM responsibility are lacking. Michaud cites the Stanford Artificial Intelligence Index 2024, which found a significant lack of standardization in responsible AI reporting. Leading developers test their models against different benchmarks, complicating risk comparisons. The number of AI regulations in the U.S. has increased sharply, from one in 2016 to 25 in 2023, with a 56.3% increase in AI-related regulations last year alone.

Quantum computing has the potential to outperform our current computing model

“it’s just a matter of scaling”. For many, the word “quantum” conjures thoughts of science fiction. However, Dr. Vladimir Soukharev, Vice President of Cryptographic Research and Development at InfoSec Global, emphasizes that scaling is the main challenge. Quantum computing represents a monumental shift from binary bits to quantum bits («qubits»), which can store and process vastly more information, enabling unprecedented computational speeds. In 2019, Google achieved quantum supremacy, demonstrating quantum computers' ability to outperform classical ones in specific tasks. The challenge now lies in scaling this capability, which promises significant advancements in machine learning, AI, and other fields.

Urgency of Transition to Post-Quantum Cryptography (PQC)

Nick Polk (Branch Director for Federal Cybersecurity at The White House), Aaron Kemp (Director of Technology Risk at KPMG US), and Dr. Soukharev agree on the significant risks of delaying the transition to PQC. Robert Roggenmoser, Founder and CEO of Securosys, likens it to a black swan event: rapid and potentially devastating. Once quantum computers become widely available, data not protected by quantum-resistant algorithms will be vulnerable. PQC involves developing cryptographic algorithms that quantum computers cannot break. Adversaries may adopt a "harvest now, decrypt later" strategy, collecting encrypted data today to decrypt it using quantum computers in the future. The migration to PQC is complex and time-consuming, potentially taking up to 14 years. Hardware transitions could take even longer.

Proactive Adaptation to Quantum Legislation

Despite the urgency, most organizations are unprepared for the quantum era due to a lack of legislative frameworks. Aaron Kemp highlights the gap between the rapid pace of quantum innovation and the slow legislative process, risking sensitive data exposure. He urges businesses to proactively adapt to PQC innovations, which will help avoid future compliance risks and provide an early mover advantage. Dr. Soukharev suggests leveraging developing guidelines and standards, such as NIST SP 1800-38 B&C and the CNSA 2.0 timeline, to facilitate a smooth transition to PQC.

Insights from the White House's PQC Migration

According to Nick Polk, the key migration precepts include a comprehensive and ongoing cryptographic inventory as the key baseline to a successful migration. He agrees, that the threat of “record-now-decrypt-later attacks” must be addressed by starting the migration to PQC before quantum computing is known to be operational. Agencies must prioritize systems and data for PQC migration and identify systems that will not be able to support PQC algorithms as early as possible. From the transition within the U.S. government, he learnt, that it is an iterative migration process requiring continuous updates and refinements. Interoperability across various systems is a major challenge. Further, according to Nick Polk, it is vital that all departments adopt the same level of cryptography to avoid vulnerabilities. He strongly advised not to adopt different types of encryptions.

Increasing Complexity of the Digital World

Elaine Maison, Senior VP at Cisco, notes the digital world's growing complexity with 46 billion IoT devices expected to generate 67 zettabytes of data, and 750 million new applications by 2025. This expanding landscape is predicted to cost $10 trillion in global cybercrime, increasing cyber incident risks. Timothy Sherman, VP/CTO at Cisco, highlights that only 9% of Swiss companies are at a mature level of cybersecurity readiness according to Cisco's 2024 index.

Current Cyber Threats

Joe Marshall, Senior Security Strategist at Cisco Talos, a major cyber threat unit collaborating with NATO, UN, Europol, Interpol, and the FBI, provided insights into the cyber threat landscape. In Q4 2023, the top threats were ransomware, post-compromise activity, and phishing. Attackers increasingly target large companies with potential insurance coverage, especially in manufacturing and education sectors due to their vulnerabilities. Healthcare institutions are also high-priority targets, with attacks sometimes leading to fatalities.

Ransomware was the most significant threat, with the main initial access vector being exploits in public-facing applications. Key weaknesses include the lack of multi-factor authentication (MFA) and unpatched or misconfigured systems. Critical infrastructure, such as communications, energy, transportation, and water systems, also faces advanced persistent threats like the Volt Typhoon attack on U.S. infrastructure. State-sponsored hacker groups, particularly from China, pose serious risks. Marshall advises focusing on resilience, being honest about risks, preparing for the worst, and ensuring robust cybersecurity fundamentals.

Digital Sovereignty and Resilience

Sean Roche, Director of National Security at AWS, emphasized that true digital resilience goes beyond control and recovery. While sovereignty and political considerations are important, resilience involves creating systems that continuously operate and adapt during failures. This includes backing up critical data and having active standby systems in the cloud. For instance, Ukraine quickly moved to cloud services for resilience at the start of the Russian invasion, highlighting the importance of adaptable digital infrastructure.

Addressing the Lack of Transparency in Software

Frank Michaud highlights a significant shift within Cisco towards emphasizing security during the development phase, rather than just the production phase. This transition is crucial, as demonstrated by past attacks such as the Heartbleed bug (2014), the SolarWinds breach (2020), and the log4j vulnerability (2021). The rise in open-source software use adds complexity due to its lack of transparency.

To address this, the White House issued the Executive Order on Improving the Nation’s Cybersecurity in 2021, requiring software vendors supplying the U.S. government to provide a Software Bill of Materials (SBOM). This SBOM tracks all components and third-party software used, allowing immediate identification and mitigation of vulnerabilities.

Similarly, the EU Cyber Resilience Act mandates cybersecurity requirements for hardware and software products throughout their lifecycle. This legal framework ensures that manufacturers design secure products, maintain their security with patches, demonstrate their security measures, and remain accountable for them.

Shift from On-Premises to Efficient Cloud Computing. Amazon Web Services (AWS), founded in 2006, hosted our delegation at their impressive facilities in Arlington. AWS was a pioneer in the cloud business. According to Peter Ronchetti, head of the public sector and managing board member at AWS, the cloud offers superior speed, quality, resilience, and cost-efficiency compared to traditional on-premises solutions.

One of President Joe Biden's initial actions was signing an executive order to improve national cybersecurity, including measures to move federal data and services to secure cloud environments and adopt a zero-trust architecture. Sean Roche highlighted these initiatives.

The shift from on-premises to cloud computing is gaining momentum, with significant potential. While 90% of data is still stored in local data centers, all new applications are typically built for the cloud, according to Ronchetti. AWS's fully encrypted cloud is five times more energy-efficient than standard data centers and is powered entirely by renewable energy. AWS, with the highest market share in cloud computing, believes this shift is the future.

Space Networking: The Next Big Thing

Space networking is poised to revolutionize global communication by providing high-speed internet and real-time data services worldwide. Don Brown, Head of Global Government at Amazon Project Kuiper, announced that Amazon Kuiper will deploy 3,232 low Earth orbit satellites with over 500 global gateways, delivering unparalleled broadband internet access. This significant advancement is imminent, with the satellite industry set to expand into a mass market driven by governments and companies like Amazon. Full coverage in Switzerland is expected by April 2026, ensuring no service gaps.

Space networking will transform how we communicate, access information, and monitor our planet. It promises enhanced climate monitoring, real-time observations, improved weather forecasting, secure communication, better disaster management, increased agricultural productivity, climate research, environmental protection, and the prediction of climate-sensitive diseases. According to Amazon, these satellites will feature unprecedented end-to-end security.

Switzerland plays a crucial role in this development. The U.S. relies on Swiss technology for satellite deployment, specifically using dispensers designed and produced by Beyond Gravity, headquartered in Zurich.

Conclusion

The Cybersecurity, AI, and Quantum Seminar that took place in Washington, New York and Boston from 20 April to 27 April 2024 underscored the U.S.'s leadership in the digital revolution, promoting technologies like climate tech, semiconductors, AI, quantum computing, and cybersecurity. Switzerland, fueled by its strong academic institutions (ETH Zurich and EPFL Lausanne in particular), is poised to play a significant role in this revolution. These universities drive technological advancements, attract talent, and foster industry collaborations, though limiting student numbers at EPFL may have opportunity costs.

AI holds immense potential for solving critical issues in healthcare, education, and climate change, but its implementation must be context-specific to avoid harm. Mitigation measures are essential to balance innovation with safety. Quantum computing is set to transform industries, and organizations should urgently migrate to Post-Quantum Cryptography to safeguard data.

Switzerland's cybersecurity maturity is low, and the digital world's growing complexity increases cyberattack risks. Strengthening AI-based cybersecurity measures is crucial. As a neutral bridge-builder, Switzerland can facilitate global tech diplomacy, ensuring balanced regulation and innovation. Continuous investment in R&D, tech diplomacy, and U.S.-Swiss relations is vital for Switzerland's future prosperity.

Author: *Pascal Schöni, ICPRO GmbH*