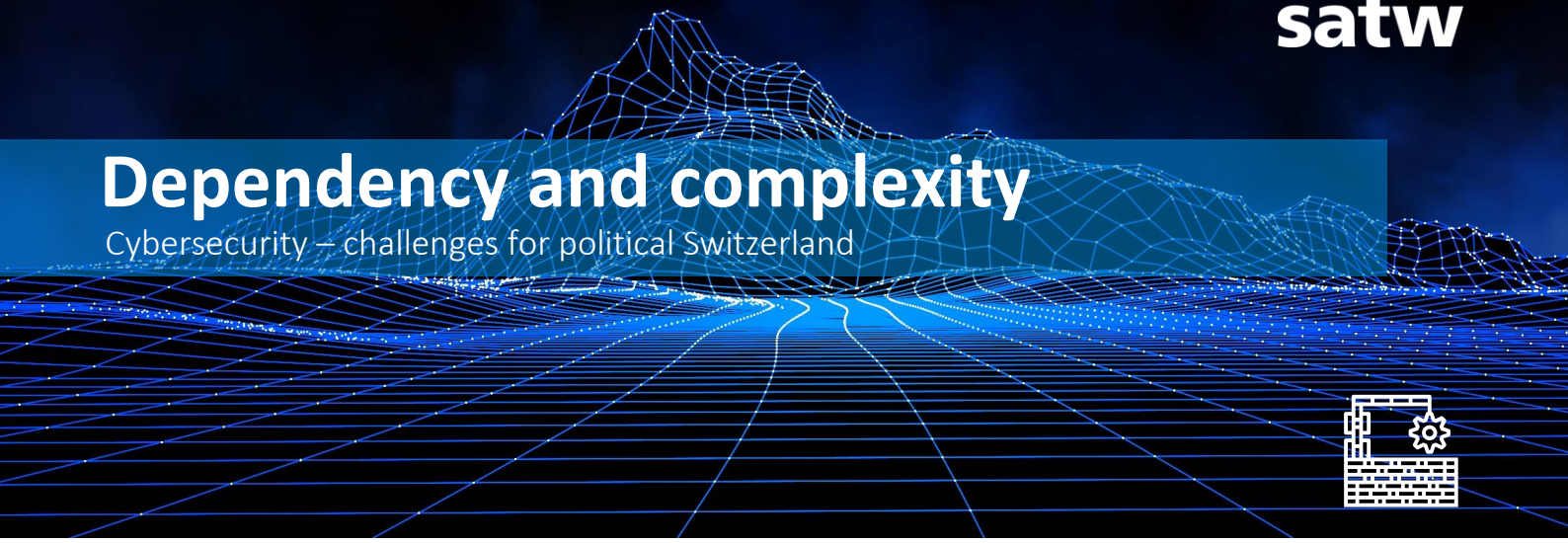
satw

Dependency and complexity

Cybersecurity – challenges for political Switzerland



State of the art

Our society and economy have become critically reliant on a variety of digital infrastructures. We depend on the steady availability of connectivity and the correct functioning of countless technologies and services that we no longer directly control. Distant events can have instant, long lasting, and serious local effects. Cascading network effects today present a much larger risk to the whole economy than any time before in history.

The financial crisis of 2007 was a teachable moment about the obscure and under-appreciated risks of highly interconnected and interdependent systems. We have only increased our dependencies since then.

The ongoing digitalization and trends towards connecting everything increase efficiency as well as the consequences of a chance occurrence, malfunction, misconfigurations, malicious attack, political power play, or sanctions. Switzerland currently runs the risk of creating critical dependencies and issues through the premature use and, in some cases, uncontrolled procurement and deployment of digital products and services. Such issues will only become manifest in the long term (or in a crisis) and can then only be corrected at huge expense and effort.

Recommendations

1. Embrace the digitalization, but invest into understanding the key risks and make conscious decisions about critical investments.
2. The government, organizations, and individuals must consciously evaluate critical dependencies in their cyber infrastructure and actively balance optimization (efficiency, short term gains) vs. resiliency (keeping redundancy, long term survival) and respective costs.
3. Assume failure and plan accordingly. Critical function for society and business must withstand outages to a given degree. Redundancies must be planned for, communicated, financed, implemented and tested.
4. «Plan for the difficult whilst it is easy. Act on the large while it's minute. The most difficult things in the world begin with things that are easy.» - Laozi (Lao Tzu), 600 BC

Challenges

Ignorance concerning the level of security and the increasing dependencies within and amongst the infrastructures lead to critical threats as digitalization progresses.[1] Tight coupling, complexity, and increasing dependencies on few and dominant players, services, technologies, and infrastructures result in a huge accumulation of critical risks in the digital society. Things are objectively getting more complicated, coupled, and interdependent at super linear rate.

- **Connectivity & Network**: Services and devices require continued communication and network availability. Most of the infrastructure is out of our direct control, outages cripple critical functionality.
- **Hardware & Software**: A few dominant software and hardware products from even fewer manufactures are absolutely critical for the functioning across industries. Vulnerabilities, correct functioning, and lock-in effect result in availability, business, privacy, and resiliency challenges.
- **Protocols**: Dependency on small set of Internet protocols and their provisioning infrastructure increase risk of cascading effects across industries.[2]
- **Cloud, Cloud Provider & Service Models**: An increasing number of online or cloud driven services paired with continued pressure to migrate to subscription models increase dependencies on network and service provider availability. Less than ten cloud providers from just two countries provide the majority of the worlds Internet business. Small outages result in increasing damages, huge and increasing accumulation of systemic risk.[3]

Cryptography: A few dominant cryptographical methods and their implementations back almost all security guarantees in the digital world. Huge systemic exposure to yet unknown vulnerabilities in the math, implementation, or sudden advances in Quantum computing.

- **Legacy**: Products and services can no longer run in isolation without continued connectivity or support from the manufacturer throughout the whole service life. Critical risk by premature failure of vendor or provider (bankruptcy, forced obsolescence, sanction).
- **Political**: High concentration of dominant manufacturers and infrastructures in just a few countries. Control of the digital infrastructure has become a proxy for political power, since countries can easily reach across borders to disrupt real-world systems. The diffusion of the Internet into the physical world radically escalates governance concerns around privacy, discrimination, human safety, democracy, and national security.[4]

[1] Reference to Cyber Security "Wake-Up Calls" - https://ctovision.com/reference-cyber-security-wake-calls/
[2] How the Dyn DDoS attack unfolded - https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html
[3] Adobe is cutting off users in Venezuela due to US sanctions - https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions
[4] The Internet in Everything: Freedom and Security in a World with No Off Switch - https://www.amazon.com/Internet-Everything-Freedom-Security-Switch/dp/0300233078

Need for action

Switzerland requires a solid identity that covers companies, citizens, and foreign nationals with work permits, and offers a level of trust comparable to the Swiss passport. The legislation required must be established and the infrastructure set up.verything is connected and gets more complex. We can no longer operate in isolation and effective and sustainable measures for the protection and availability of products and infrastructures go beyond the securing of individual systems. After the financial crisis of 2008, economists developed the notion «too big to fail» when describing financial firms whose failure would have catastrophic implications for the economy that it would be irresponsible to allow them to become insolvent.

We have to identify and assess «to critical to fail» infrastructures of the digitalization and develop strategies to minimize dependencies, protect these infrastructures, and increase resiliency of the digital society and industry. We should consider doing this before a crisis hit.

Understanding and Taming Complexity

Complexity in systems and infrastructures leads to increased vulnerabilities, failures, errors, human confusion and difficulty of recovering from an issue[5]. We need to favor simple and consistent architectures, designs, and implementations to avoid unnecessary complexity and dependencies. Prediction, complete testing, and modeling of all states is not possible is such systems, we therefore must assume and account for failures and compromise and design that systems fail safe and secure. The only thing that ever-yielded real security gains was *controlling complexity*.[6]

[5] Flash Crash - https://en.wikipedia.org/wiki/Flash_crash

[6] Security, Moore's law, and the anomaly of cheap complexity, Thomas Dullien - https://rule11.tech/papers/2018-complexitysecuritysec-dullien.pdf

References

- Systemic Risk in the Broad Economy - www.rand.org/t/RR4185
- Globally networked risks and how to respond, Dirk Helbing - http://adaptation.ei.columbia.edu/files/2018/09/nature12047.pdf
- The Precautionary Principle - https://www.fooledbyrandomness.com/PrecautionaryPrinciple.html
- Whitepapger Supply Chain Security, ICT Switzerland - https://ictswitzerland.ch/en/white-paper-supply-chain-security

Contact

Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-challenges

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020