Cyber threats - how great is the danger and how well are the state, the economy and society protected against them?

Summary Report | 11th SSF Security Talk on October 17, 2022, Hotel Schweizerhof, Bern

How are the EU and other European countries dealing with the growing cyber threat? How is Switzerland responding to it? Where does the DDPS's "Cyber Strategy 2021-2024" stand? How can our critical infrastructures be protected? How can the state, the economy and society protect themselves against cyber threats?

These and other central questions were discussed by renowned experts at the 11th SSF Security Talk in Bern. The 120 interested participants received first-hand information. The event started with input speeches by **Dr. Stefanie Frey** (Managing Director Deutor Cyber Security Solutions GmbH, Advisory Group ENISA), **Colonel i Gst Robert Flück** (Project Command Cyber, Swiss Army) and **Dr. Peter Friedli** (Head of Defence AWK Group). This was followed by an exciting panel with **Florian Schütz** (Delegate of the Swiss Confederation for Cyber Security), **Dr. Jörg Mäder** (National Councillor GLP/ZH, freelance programmer), **Alexandra Arni** (Head of ICT, Swiss Bankers Association, Vice President Swiss FS-CSC) and **Dr. Urs Loher** (CEO Thales Suisse SA). The SFF Security Talk was moderated by **Fredy Müller** (Managing Director SFF).

The experts basically agreed that **cyber threats affect everyone** and therefore **cooperation** across all levels is necessary to counter the growing threat. However, the event also made clear that we are still far from understanding the **cyber threat in all its facets and taking the necessary measures**.

Cyber threats - "We know the enemy, but we do not know how to fight him and protect ourselves"

Dr. Stefanie Frey, Managing Director of Deutor Cyber Security GmbH, kicked off the presentation. Right at the beginning, she stated that although cyber is talked about everywhere nowadays, most people do not have a clear idea of what cyber exactly means. Three observations related to the term cyber need to be underscored, she said: "Cyber is a **means to an end**, not an end in itself; One should not speak of cyber war, but rather of **cyber "in war"**; and cybersecurity is **not just IT security**, there are many other organizational and strategic components involved."

Frey then highlighted the current **trend of cyber attack growth**. This strong growth, she said, poses a major problem. Every year, she said, the number of crimes doubles and, in addition, a **very high number of unreported cases** must be taken into account. The damage to the German economy, for example, is estimated at 223 billion euros for 2020 alone. According to the study, nine out of ten German companies were victims of cyber attacks in the same year. This damage is not sustainable!

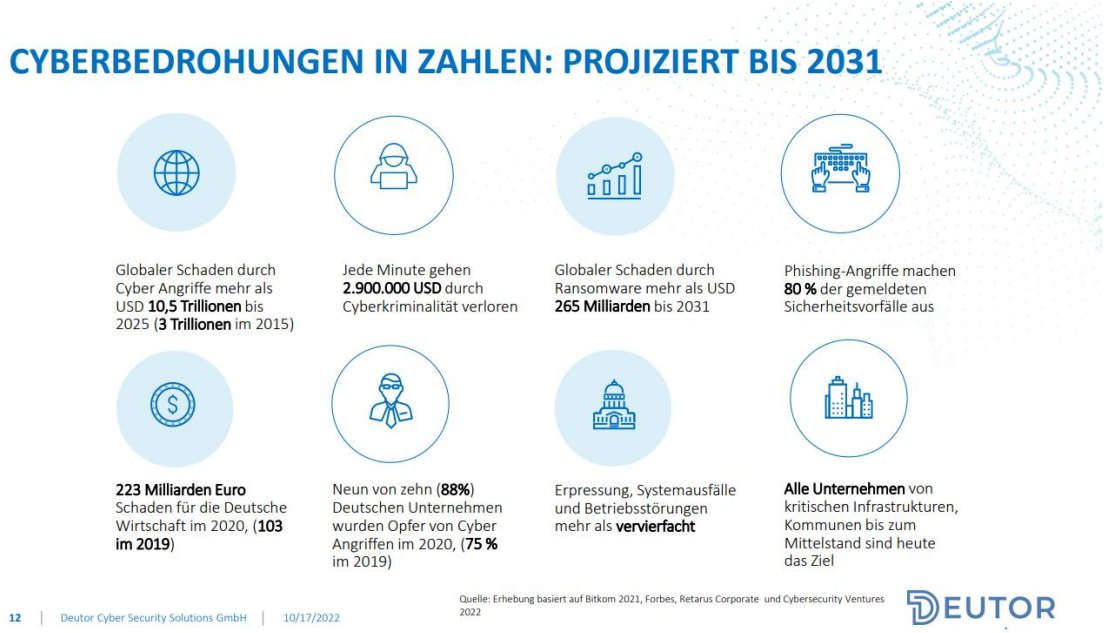

Figure 1: The numbers speak for themselves: cyber threats are already causing enormous damage, and the problem will become even more acute in the future.

The question is why the damage caused by cybercrime is so great. The answer is relatively simple: "We are fighting an **enemy that we know, but we don't know how to fight it** because we don't analyze the problem enough and we are looking for solutions to a **problem that we haven't studied enough**. That is why it would first be important for us to understand what solutions protect us against cybercrime."

Frey went on to point out that everything is automated and digitized today, but that this is **very dangerous without sufficient security**. For example, she said, weapons systems are being networked without enough thought being given to security. Cyber is therefore not always a good idea, but only with a **good team and enough money** to be able to **take all the necessary security aspects into account**. "It needs digitization with security and with intelligence."

"...we must learn to think like the perpetrators..."

For a better overview of the various facets of the problem, Frey then went into a bit more detail about the **different cyber threat types** of cybercrime, espionage, subversion and sabotage. "There is really a **lot of money** to be made in cybercrime! There are **smart people** at work who will do anything for money, are **highly motivated** and unfortunately, far too often succeed." The motivation, however, is not always readily apparent, she said. In one case from the healthcare sector, for example, which she had followed herself, the issue was the disclosure of patient data. However, the perpetrator never collected the promised extortion money, which has triggered speculations about the perpetrators and their motives. Another case she mentioned, which again involved personal data, concerned the Conti Group. The case showed that companies are often **too unaware of their own IT infrastructure and its security vulnerabilities**. "But if the perpetrators are able to find and exploit existing vulnerabilities, we would also **have to know about them and eliminate them**. There's **no excuse** there: If the perpetrators can do it, so can we!" In the case of critical infrastructure, she said, sabotage via cyberattacks more often comes into play.

©Daniel Saxer (iOf App, Defence & Security News)

Frey then addressed important **problems** in connection with **combating** cyber threats. "We would have to **learn to think like the perpetrators**." If a company becomes the victim of a cyber-attack, any shame or concealment is wrong. However, there is often the problem that many things are imposed from the top down, such as data protection legislation, which often complicates things. It would be **better** to develop and improve data security in a **bottom-up process**.

For Dr. Frey, it is clear that a **comprehensive risk assessment** should be standard for every decision in the cyber area. After all, in every training course today, one learns how a threat situation can be compiled together with a vulnerability analysis into a risk assessment, which should be used as the **basis for decisions**. "This would **also be possible in the cyber area**, but no one is doing it yet! We need to learn to live this sequence: first we analyze our **cyber threat situation**, then our **cyber vulnerabilities**, and this together allows us to identify our **risk profile** and take targeted actions to **eliminate our cyber vulnerabilities."**

In addition, we should think like suspected perpetrators who are considering a cyberattack on our company or person. "A lot could be gained by this **critical questioning** of our cyber hardware and software." But that would take time and money, not digitizing everything and everyone without pause. Cyber security is a key challenge for every company, every country and even every individual. But the threat is being analysed incorrectly, which explains the boom in cybercrime, which urgently needs to be curbed. Otherwise, the situation will not improve; quite the opposite.

"The Swiss Armed Forces Cyber Command will be ready for action in 2024!"

As the second speaker, **Colonel i Gst Robert Flück** gave an insight into how the **Swiss Army** is preparing for cyber threats. In particular, he highlighted the creation of the **Cyber Battalion 42**, which is expected to be fully operational **by 2024** and will play an important role in the fight against cyber threats.

First, Flück informed about the two basic tasks of the army in the cyber domain: "In order to ensure its operational capability and freedom of action at all times and across all situations, the army is permanently able to **recognize cyber threats**, to **protect** itself against attacks and to **defend** against them. In case of conflict, it is also able to **support military actions with cyber actions**."

He then went into more detail about the Army's cyber organization. A distinction should be made, he said, between ICT system control, detection & defense, situation & operations, ICT system operations and intelligence gathering & effects.

©Daniel Saxer (iOf App, Defence & Security News)

In concrete terms, **five fields of action** would be taken care of by the **Cyber Command** in the future: Firstly, this would be **self-protection**, secondly, the alignment from IT service provider to **military command**, the creation of the prerequisites for the **digitization of the Armed Forces**, electronic **combat and cyber operations**, as well as the ability to cooperate and support in the **Swiss Security Network**.

The Cyber Command is to be fully operational from 2024 and will continue to develop thereafter. To this end, the **training of personnel** is currently playing a key role. In a rigorous selection process, IT specialists are chosen who, after 42 weeks of training, will serve in various militia functions in the Cyber Command.

©VBS

Figure 2: "Cyber is a People's Business" - Accordingly, the training of Command Cybers personnel takes a central role in the Army's fight against cyber threats.

This leads to a **mutual gain**, he said. "On the one hand, the individuals concerned benefit in their **civilian area** of operations from their **cyber experience in the Armed Forces**, and the Armed Forces benefit from top-trained operational forces."

Flück further added that the Cyber Command can only function well if it can benefit from **cooperation** with various fields, such as in cryptology. Further, he said, Cyber Command could **provide subsidiary support to civil authorities** when civil authorities' resources are exhausted or unavailable and commercial service providers are not available to the required extent or in a timely manner.

Flück then presented the timeline and organizational structure of the Kommando Cyber project in more detail. The initialization phase started in 2021, followed by conceptualization in 2022 and realization in 2023. Finally, the **introduction of the Cyber Command is to follow** in 2024 and it is to be **continuously developed** in the future. In the organizational structure, the "long-term development" element and the "militia operational element" should be emphasized. In connection with cyber, it is very important to be able to look a long time into the future and to recognize trends at an early stage. The militia system also allows cyber capabilities from the civilian world to be brought into the armed forces and further developed there, which is of great benefit to both the armed forces and society.

In summary, cyber is primarily a **people's business** - "it needs **people**, IT experts, who can recognize and deal with cyber threats. Furthermore, a **suitable organization is needed within the armed forces**. This role is being played by the **Cyber Battalion 42**, which is currently being set up. Finally, we are at the beginning of a development to **renew the Swiss Armed Forces and to align them with modern requirements.**

"Too little attention is being paid to the increasing convergence between IT and OT".

The third speaker was **Dr. Peter Friedli, Head of Defence, AWK Group**, who opened **the picture from known IT threats to threats in the area of Operational Technologies**. Threats in the information space or in IT ("Information Technology") are ubiquitous and generally known, he said. One example is the well-known phishing, i.e. the stealing of passwords in order to infiltrate the computers of other people and companies and cause them financial and other damage. **In addition to IT, however, there is also OT**, or "operational technology," which includes the **hardware and software used to monitor and control** physical processes, devices and infrastructures. The manufacturing industry, but also systems in the medical sector, in traffic control, energy supply or water treatment are dependent on OT. However, the main focus is on operational security, availability and production cycles. With **increasing convergence between IT and OT**, however, there are also significant risks for OT. "With the growing digitization of OT, the opportunities for **cyberattacks are also increasing in OT**." The continuously more powerful and more complex infrastructure means that interrelationships are becoming increasingly difficult to grasp. Accordingly, it is also becoming more difficult to predict how a risk in one place will conjugate through the entire web of interconnected elements.

©Daniel Saxer (iOf App, Defence & Security News)

Cases of industrial companies being paralyzed via cyberattacks or power supply failures are becoming more frequent, and in the healthcare sector in particular, such cyberattacks can put lives at risk. "What are we finding, though? **In OT, there is often not enough awareness of security risks**. **Known best practices from IT are not used in OT**, he said, and a **complete end-to-end view** of the value chain

is lacking. IT and OT are separated in many companies, although they are increasingly converging with the growing digitization of production processes. "

Figure 3: IT and OT are converging more and more - but many are not yet sufficiently aware of the associated risk.

Particularly in energy distribution, it can be seen that there are **not enough protective measures** in place against possible cyber-attacks." Interestingly, however, there is no correlation between the size of the energy distributors and the cyber maturity, i.e. the expansion of the protective mechanisms.

Fortunately, there are also best practices in the area of OT security. On the one hand, OT security is also based on early risk identification, where all related elements and the associated risks should be analyzed. In this context, a deep understanding of the interfaces between IT and OT is also important. Furthermore, this is also achieved through the involvement of suppliers and manufacturers, as well as through staff training and careful operation of the systems.

In conclusion, there were **four key messages** Friedli wanted the audience to take away: **cyber threats also exist in the physical domain** and pose a major risk; with increasing digitization, attack vectors are also multiplying; **OT and IT are converging**; operational security is **not guaranteed** for many critical infrastructures and therefore poses a weighty risk; and OT security and supply chain security close major security gaps - and must always **involve manufacturers, service providers and operators**. "So a lot needs to be done to improve OT Security and protect against potential cyberattacks."

"Let's think more in terms of opportunities than risks" - The Panel

Three very informative presentations were followed by the panel discussion. At the beginning, moderator **Fredy Müller** divided the discussion into three areas: On the one hand, the **military-civilian area**, on the other hand, the question of how **industry** is dealing with the problem and finally, how **politics** is taking a stand on these issues. For the opening question, he turned to **Florian Schütz, the federal government's delegate for cybersecurity**, and wanted to know what his key learnings from the last 20 years in cyber were. For Schütz, it was clear that the relevance of the topic has clearly increased. However, this should not surprise anyone due to increasing digitalization and networking. Unfortunately, society has so far paid too little attention in the political discussion and at the management level to the fact that this is a technical issue. Therefore, he said, it is a mistake **not to promote professionals to the management level.** "After all, you don't have a CFO who doesn't know anything about finance" Schütz added to illustrate his point. Yet, he said, there is **great potential** due to the excellent education in Switzerland. **Schütz also noted that history repeats itself:** "Aviation and cars were also new once, and you first had to figure out how to handle them. Here, however, we can say that we have recognized the development. We're moving forward, we still have room for improvement but we're not quite that bad."

The moderator then turned to **Dr. Jörg Mäder, freelance programmer and National Councillor GLP/ZH**, to ask how this issue was perceived in the Federal Parliament. Mäder confirmed that cyber is indeed a topic in politics, but **not to the extent that would be desirable.** So far, Digitisation has been seen more as a **means to an end**. People want to use IT, but no one wants to think too much about the risks.

Alexandra Arni, Head of ICT at the Swiss Bankers Association and Vice President of the Swiss FS-CSC, emphasized that the banking and finance sector was one of the first industries to recognize the importance of cyber. Arni explained that banks have always been a **popular and strong target of cyberattacks**.

Cyber has also long been an issue in the military sector or defense industry, **Dr. Urs Loher, CEO of Thales Suisse SA**, emphasized, saying that he thought it was wrong for everything to be presented as more complex today. **In the past, too, information had to be protected, but today it simply happens on a different level**, which many people no longer fully understand: "We have to come back and simplify things so that people understand what we're doing again." It's about protecting information and who has access to what, he said. That principle has not changed, he said.

Cyberattacks on companies a lucrative source of revenue

Moderator Fredy Müller mentioned that **cybercrime today generates more money than drug trafficking** worldwide. Therefore, he wanted to know from **Florian Schütz** whether one should put oneself more into the perspective of the perpetrators. Schütz replied that the experts already understand very well how the perpetrators work. They want to get **maximum return with minimum effort.** Organized cybercrime is often structured **like a company with regional or global divisions**, he said. Operations are often carried out from Africa because there is a lot of talent and a small labor market there. Support, on the other hand, is more likely to be found in northern Europe because many languages are spoken there. This understanding can be built upon, but one has to keep at it. That's why Switzerland has the NDB and law enforcement. But of course there would always be room for improvement in the **situation picture**.

Müller is addressing **Jörg Mäder**, who is a **board member of the Digital Society**. There are many hobbyists and developers there, but the security aspect is often forgotten. **Jörg Mäder** replied that,

due to the **Internet of Things**, physical boundaries no longer guarantee security, as everything can be networked together. As long as the tinkering is only done for fun, the potential for damage is small. However, if they are to be used **for productive systems**, it becomes more difficult. However, awareness in this area is now very high and security standards exist. You simply have to stick to them and follow and implement **regular patches and update**s.

©Daniel Saxer (iOf App, Defence & Security News)

Cyber-attacks in the everyday life of a company

This led Fredy Müller to ask **Urs Loher** how Thales deals with cyber-attacks. He confirmed that **Thales was even attacked almost daily**. The only thing is that they have managed to get through so far. For a defense company, security is of course very important, as it is directly related to the credibility of the company. A great deal is invested in operational security. However, one is never 100% secure. The moderator therefore wanted to know why the inhibition threshold to talk about cyber-attacks was so high. Loher also sees this phenomenon as a major crux: everyone wants to settle such attacks quietly. However, this is the wrong approach. Within a group, the exchange functions excellently, **but between the groups and also with the authorities, there is probably too little communication.**

Alexandra Arni then explained that the Swiss FS-CSC was therefore in the **process of setting up a crisis organization that would be deployed in the event of a bank attack**. Arni illustrated the importance of this organization with an example: "If a systemically important bank were to be hit by a DDoS attack, this would have an impact on the entire payment traffic in Switzerland and thus on the entire national economy. In such a case, a stringent crisis organization is needed, which can then use the policies that are now being developed to decide how the systems can be brought back up as quickly as possible." In such a case, customers would of course also have to be informed accordingly from the point at which the bank ceased to function. This **communication** strategy is now being worked out in the still very young **Swiss FS-CSC**, he said.

"A Clear allocation of competences is essential"

Companies like Zalando are regularly threatened by cyberattacks too, Fredy Müller mentioned, and therefore asked **Florian Schütz**, as the former person in charge **at Zalando**, how the **online** retailer dealt with it. Schütz explained that attacks were a daily occurrence at Zalando. Some attacks resulted in business interruptions, which caused five-digit damages in minutes. Therefore, **quick decisions** and a **clear assignment of competences** are elementary in cyber defense. Schütz then emphasized that risks can also give rise to **new opportunities**. As an example, he cited a case in which a form was set up on the website for "blocked" customers so that they could still place their order. This resulted in **market intelligence** and new marketing ideas and the costs for such security measures are also no longer such a big issue.In view of the great importance of rapid crisis management in the event of cyber-attacks, Fredy Müller wanted to know from **Alexandra Arni** whether the Swiss FS-CSC had already prepared a logbook for such cases and whether **crisis scenarios were also actively practiced**. Arni confirmed that it is elementary that **operational cyber exercises** take place for such cases and that all those involved know their roles very well and act accordingly.

In response to the question of whether there are also cyber risk precautions in the Federal Palace, National Councilor **Jörg Mäder** explained that the Federal Palace is "unfortunately" still relatively well positioned, as **digitization is not yet that far advanced**. In an emergency, he said, one could fall back on tried-and-tested methods such as vote counters to keep parliament running. However, it seems to him much more important to talk more about such incidents and risks. "It's like an STD: It affects a lot of people, but they don't know about each other, although that's precisely what would help. To be able to cleanly defend against attacks, you have to know your opponent, and the more cases that are known, the better this would be." However, Mäder continued, **the reality is the opposite**. You don't want to lose your reputation, but if the worst comes to the worst, you don't want to be alone.

What to do in case of a cyber-attack?

What happens in the event of a specific cyberattack on a company? Should one call the National Cyber Security Center (NCSC) or the federal cyber delegate directly? **Florian Schütz** explained the **division of responsibilities of the federal government**, which many companies are not aware of. In the case of a criminal act, which, depending on the statistics, accounts for about 95% of cases, **law enforcement** is responsible. In the case of sabotage, the Federal Intelligence Service **(FIS)** takes over. Any incident can be reported to the NCSC. The NCSC provides first aid and informs the right partners. In this context, Schütz criticized that the current **distinction between critical and non-critical infrastructure** makes less and less sense. Rather, a distinction should be made between the economy and the population and only then classified according to criticality. In principle, he therefore recommends **always involving the police** in cases of criminal offences. The NCSC would then still act as **technical support**. In the case of sabotage, the NCSC then provides the FIS primarily with analyses. The follow-up question was how to deal with **ransom demands**. Schütz made it clear that **ransoms should never be paid**, as this would only support the machinations of the attackers. However, it is important to get help. The police can often negotiate with perpetrators and thus gain valuable time. One point, however, was particularly important to Schütz: "Actually, we are talking about the wrong time. In the event of an attack, I'm already too late. You could also build the system safely, then we wouldn't have to discuss it. Believe me: you wouldn't cross a bridge either, which is built as insecurely as many IT systems are." For Florian Schütz, IT is therefore clearly an engineering discipline. That's where the focus should be and less on attack and defense. **Jörg Mäder** added and emphasized that it is important to have a strategy for a quick shutdown and restart of systems. There is definitely a need for higher awareness there.

Special cyber defense systems for armies and states

Fredy Müller wanted to know from Urs Loher what systems Thales builds to **provide states and also armies with the necessary security - also in the cloud area.** Loher made it clear that Thales builds systems in such a way that **they make life as difficult as possible for an attacker** if they have already been able to penetrate the system. The goal and first priority, of course, is to **prevent attackers from getting into systems in the first place**, he said. This is supported by building separate systems and working with firewalls or protection mechanisms of an operational nature, such as restricting access rights. This also requires **regular updates** to close possible gaps. Loher explains that cryptography also plays a central role. Here, Thales is a leader in the protection and encryption of data, data transmission and cloud solutions for countries or NATO. Investments are already being made in these areas in systems of the future, such as **quantum cryptography**. However, he said, it is important to always use different security channels at the same time and to have two-factor authentication, for example.

"Cybersecurity is a process that requires permanent risk analysis".

Afterwards, moderator Fredy Müller opened the panel discussion to the audience. **Hans-Peter Steffen, a member of the RUAG** management, pointed out that there was a technology race between innovation / total networking and the prevention of misuse. He therefore wanted to know whether there **was another approach** than total control of all life data. As an example, he mentioned predictive policing to better identify future threat situations. **Florian Schütz** replied that one must always weigh up **security and freedom** and that both are only possible to a limited extent. For him, however, it is quite clear that we must get away from the idea that security is a state. Security, including cyber security, is **rather a process** that requires a **permanent risk analysis**. In his opinion, a social credit system like the one in China would not be compatible with our understanding of values. In this context, Schütz also referred to the Federal Constitution, which clearly states in Article 6 that it is not the state that protects you, but that **each person must handle decisions responsibly**. **Jörg Mäder** added that risk assessment is already known from other areas: "You probably also have a front door key and a bicycle key, which are of different quality because the damage event would be of different amount." Mäder also added that in predictive policing, many systems operate with artificial intelligence and this causes further problems.

The next question came from **David Ribeaud, CEO of Helvetia Specialty Markets**. He stated that Helvetia sees two challenges with regard to cyber: on the one hand, prevention is not enough for a resilient Switzerland, and on the other hand, there are **no insurance solutions to cyber threats**. Helvetia therefore proposes that the private insurance industry, with **financial support from the federal government**, develop a prevention-focused support program for companies. However, the companies would only benefit from such support if certain measures were taken to increase cyber security. In response to these remarks, he wanted to know from Florian Schütz what he thought about such an idea. **Florian Schütz** found the idea interesting but was **skeptical about financial support** from the federal government. If the model would be economically interesting, then it should also be financially self-supporting. He would not start directly with the support, but **first develop the model itself** and then **discuss the capital providers in a second phase**.

Jörg Mäder asked Mr. Ribeaud about the situation regarding reinsurance and the assessment of long-term risks. He replied that there was **no reinsurance**, which is why measures had to be scaled back. He drew a comparison with the pandemic, in which the risk was also poorly diversified, which is why the federal government had to step in as a subsidiary Schütz suggested that the question here was actually whether **one should learn to understand the risks better** in order to then be able to quantify them, or whether this was indeed not possible and there was actually a **need for a substitute solution for the omission of insurability**. In the case of the latter, models such as the one proposed by Helvetia could certainly be discussed. He would **not close his mind to the model**, it would just have to be examined carefully.

Another question came from **Yann Schmuki, an employee of the Armed Forces Command Support Base**. He wanted to know from the panel guests how the state and the army can ensure that investments in the cyber sector make sense and guarantee the protection that one wants. In response, **Florian Schütz** pointed to the functions of the private market: "It is a misconception that the state can do everything itself. In the past, the state has therefore increasingly gone in the opposite direction and privatized various areas." The last question from the audience came from **student Yvonne Aregger**, who wanted to know whether there were **any solutions that would lead to "de-digitization"** due to the cyber risks. Urs Loher pointed out that this was similar to supply chains, where there were similar considerations. However, one must think about the trade-off of what such a measure would entail. Perhaps in the future, certain things will no longer be digitized that would otherwise have been digitized. **Florian Schütz** also thinks the **idea is tempting**, but sees a **small error** in thinking about it. Today, in a global market, it is **no longer primarily important to be secure, but to be fast**. There is a **shift in power from states to companies** that operate on global markets. He illustrated this with the example of microchips, whose components are all manufactured elsewhere in the world. Many things can therefore no longer be done manually.

Learnings and takeaways

In the final round, the speakers passed on **important key messages** to the audience. For **Jörg Mäder**, federal awareness campaigns are important, but there needs to be an even **greater focus on training** so that IT and OT can be used properly in the future. **Alexandra Arni** made it clear that **digitalization is here and that it can no longer be reversed**. Therefore, one must learn how to deal with it. In addition, there needs to be an increasing awareness of personal responsibility in the cyber area. Cyber security is not just something for nerds, but must reach all parts of society, right up to the management level. For **Urs Loher**, cyber is much broader than just attacks on IT networks. Just as much effort is needed in building systems and developing measures. The closing words were given to **Florian Schütz**: "Take the nerds with leadership skills and make them leaders, and secondly, let's think more in terms of opportunities than risks, and in terms of taking advantage of those opportunities." The panel closed with this plea. The audience then had the opportunity to discuss many more exciting questions at the aperitif that followed.

©Daniel Saxer (iOf App, Defence & Security News)

We thank our event partners!

helvetia

AWK Group
a member of eraneos group

THALES

bedag

....and our annual partnerships!

spa
Sicherheit & Schutz

LKMD

VSSU