

## Concluding Report: «Critical Infrastructures»

### 2<sup>nd</sup> Network Event of the SWISS SECURITY FORUM, April 10, 2019, Welle 7, Bern

More than 110 people interested in security from business, public authorities, science and civil society discussed the topic of "critical infrastructures" at the sold out network event of the SWISS SECURITY FORUM (SSF) in Bern on April 10, 2019. In two input presentations and a top-class panel discussion with federal representatives and decision-makers from SBB, Swisscom and Migros, possible failures of system-relevant infrastructures and their far-reaching consequences were discussed and a lot of food for thought was provided.

In his introductory remarks, Hans-Jürg Käser, President of the SSF, recalled that Switzerland faces major challenges in the area of critical infrastructures. The population is too passive on this important issue. Security is taken for granted and far too little attention is paid to the risks associated with the Internet or smartphones, for example.

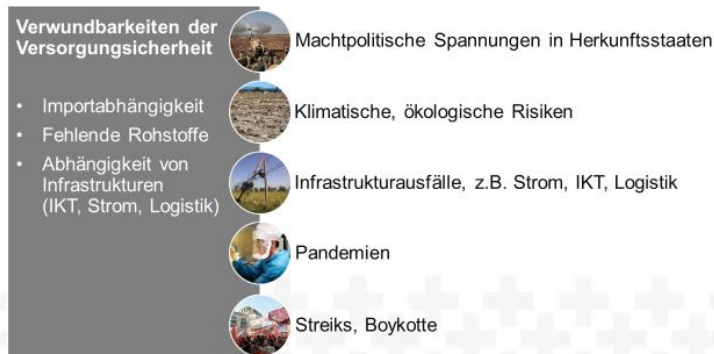
#### **Public-private partnership and the principle of subsidiarity - how does national economic supply work?**

Right at the beginning of his speech, Werner Meier, Delegate of the Federal Council for National Economic Supply (NES), drew attention to the principle of subsidiarity of national economic supply, which is anchored in the Federal Constitution. It is indeed the task of the Federation to ensure the supply of essential goods and services in situations of severe shortage. However, this responsibility is subsidiary, i.e. *only if the economy cannot solve the supply problem itself*. The term "national economic supply" already indicates that the main responsibility lies with the economy - the federal government only supports the economy in fulfilling its mandate within the framework of a public-private partnership.

#### **Modern threats and challenges for national supply**

The NES delegate emphasized that nowadays so-called "*modern threats*" such as import dependency or dependence on information and communication technologies (ICT) are central to national supply. If system-relevant goods and services are no longer available globally due to political tensions, climatic conditions, infrastructure failures or pandemics, this directly affects Switzerland (see Figure 1). The fact that Swiss consumers are hardly affected by crop failures or strikes abroad underscores the functionality of the system in Switzerland. It is a great challenge to take account of the increasingly rapid changes in the market. Thus, the "*prepared measures*" for deficiencies must always be adapted to new market mechanisms by means of an agile organization.

## **Gefährdungen für die Landesversorgung**



Bundesamt für wirtschaftliche Landesversorgung, Bernastrasse 28, 3003 Bern

5

**Figure 1: Threats for national supply**

### Internal federal cooperation as a key factor

The priorities of NES are the areas *energy*, *ICT*, *logistics* and *medicines*. In the ICT area in particular, the creation of minimum standards is essential to strengthen resilience against cyber attacks. Minimum standards are needed so that all links in the chain are of similar strength and the entire process chain cannot be brought to a standstill by an inactive company. However, regulations only make sense if voluntary agreements between companies do not work. In concrete terms, federal measures to strengthen resilience can be divided into the areas of *prevention & early detection*, *supply management* and *demand management* (see Figure 2). Prevention has a very special role to play in preventing crisis situations from occurring in the first place. Werner Meier emphasized that, to this end, work is being carried out cooperatively within the federal administration. The ICT minimum standard of NES is also part of the National Strategy for Switzerland's Protection against Cyber Risks (NCS) and is not limited to operators of critical infrastructures, but can also be used by SMEs.

## **Massnahmen zur Stärkung der Resilienz**



Bundesamt für wirtschaftliche Landesversorgung, Bernastrasse 28, 3003 Bern

7

**Figure 2: Measures to strengthen resilience**

### Migros - a system-relevant retail corporation

Andres Münch, member of the General Directorate of the Federation of Migros Cooperatives, highlighted in the second input presentation the challenges in Swiss national supply from the perspective of a system-relevant retail corporation in the food industry. Migros sells four billion products annually, which corresponds to a fully loaded truck train from Zurich to Pakistan. "When something shakes in our company, it shakes quite intensively throughout Switzerland," said the Migros representative.

### The neglect of emergency stocks

This is precisely why emergency stocks are of high relevance from the point of view of Migros. However, emergency stocks for a week are usually no longer possible today due to the size of the apartments (see Figure 3). An additional difficulty is the change in consumer behavior due to demographic developments: The increasing aging of the population and the rising number of single or two-person households automatically promote the demand for small packages. If instead of a five-kilo pack of carrots a single packed carrot is bought, according to Andreas Münch, this makes stock-keeping enormously difficult.



Figure 3: Recommended emergency stock for a family of four (Andreas Münch, MGB)

### Not all processes can be protected

Using the products milk and poultry as examples, the Migros representative made it clear that the self-sufficient operation of an entire production chain is impossible in the event of a prolonged power outage. It is simply not realistic to protect all processes with emergency generators and at the same time guarantee affordable prices. In an emergency, it is therefore necessary to focus on the absolute core processes of a company. There, for example, the resistance time can be extended with emergency power and the *power drop* can be kept as low as possible. The most important thing, however, is to reduce the *recovery time* - in concrete terms, measures must be taken so that normal operation can

be restored as quickly as possible after a major event. For this purpose, for example, spoilage of goods or the dependence of other systems on these core processes are minimized (see Figure 4).

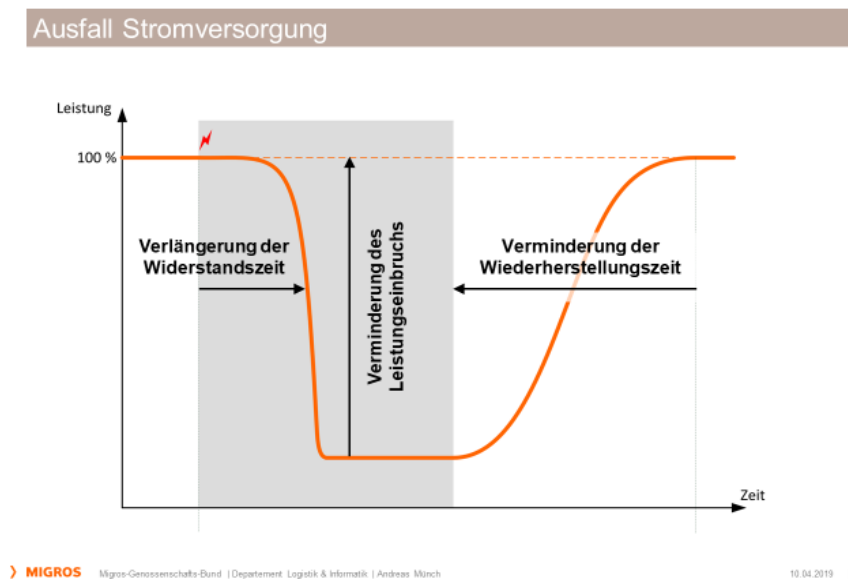


Figure 4: Example power outage

### National Strategy for the Protection of Critical Infrastructures: Out of the Dark

In the following panel discussion, moderated by SSF Managing Director Fredy Müller, the *national strategy for the protection of critical infrastructures (CIP) 2018-2022* was discussed. The national CIP strategy was developed together with operators of critical national infrastructures and contains measures to maintain and improve Switzerland's security of supply. According to Stefan Brem, Head of Risk Foundations and Research Coordination at the Federal Office for Civil Protection (FOCP), it is pleasing that the seven departments, the Federal Chancellery, numerous federal offices, cantons and municipalities, together with operators of critical infrastructures, were able to agree on certain measures. Werner Meier, too, considers it positive that the CIP strategy is bringing a cross-cutting issue to the public in a targeted manner. "It is indispensable to talk about the extraordinary situation even in the normal situation and to try to create trust," said the FONES delegate. The CIP strategy needs all organizations on board - every company, every federal office and every municipality depends on energy and ICT. It is now a matter of informing and sensitizing the economy and the population about the measures taken and messages sent.

### Nothing works without power supply

According to the FOCP, a power outage is one of the most relevant threats to civil protection and the national economic supply in Switzerland. Therefore, electricity is one of the most central areas of critical infrastructure. The flow of energy is the basic prerequisite for the flow of data, goods and payments. Andreas Münch already emphasized in his input presentation that these four areas must always be considered as an integral whole. Werner Meier, in addition to his function in NES, also Head of Corporate Security at Alpiq, stressed this point as well. He also pointed out that a distinction must always be made between blackouts and shortages in the event of infrastructure failures. Blackouts are

usually manageable in terms of time, whereas a power shortage can last for weeks or even months and requires different solutions. In this context, Stefan Brem once again emphasized the need to focus on core processes in crisis situations: "If you try to protect everything, you protect nothing".

### **Security risks in telecommunications are neglected**

The Head of Physical Security and Safety at Swisscom, Dominik Winter, emphasized that Swisscom takes its security responsibility very seriously. Swisscom is aware of the dependence of numerous business-critical processes in the army, blue-light organizations and the economy on the mobile network. At the same time, Dominik Winter emphasized that no provider could guarantee the functioning of its network. "Companies, but also public authorities, have to think carefully about what their *plan B* is if the network should ever stop functioning". FOCP representative Stefan Brem explained that society and the economy want to increase efficiency and avoid redundancies. The flipside of higher efficiency is increased dependencies, which inevitably has a negative effect in the event of a crisis.

Werner Meier used the "All IP" example of digitization to illustrate this problem: "In the past, we used to make phone calls on one channel, transmit data on another channel, listen to the radio on a third channel and watch television on a fourth channel. Today these processes all take place via a single channel". If everything is converged for efficiency reasons, optimization is made for the normal case, while a solution is missing for the crisis situation. Dominik Winter added that every citizen and every company needs a contingency plan to be able to plan in case of a crisis. According to Werner Meier, cooperation is also always required in crisis situations, and all available means must be used to communicate. This includes Polycom, for example, as Stefan Brem added: "The national radio network Polycom enables communication between the fire department, police, civil defense, blue-light organizations and technical companies even in the event of a mobile phone network failure.

### **SBB as responsible system operator**

SBB is also aware of the immense importance of security, says Daniel Schlup, Head of Emergency and Crisis Management at SBB. Safety always comes first - if safety can no longer be guaranteed, SBB must shut down operations. "We see ourselves as the backbone of Switzerland's transport system," the SBB representative said. As the system operator, SBB is responsible for involving other railroad companies and assigning them tasks in the event of a crisis. The SBB have the task of maintaining operations as long as possible - but they cannot protect the entire railroad. If it is no longer possible to maintain operations, instructions from the federal government are required. For example, in the event of an incident, the SBB could be obliged to give priority to freight transport for the national economic supply in the short term. Stefan Brem emphasized the central role of prepared decisions and well-coordinated cooperation to save time in the event of a disaster. The Federal Council is still responsible for strategic decisions in a crisis.

### **Lack of experience with crisis situations in Switzerland**

Switzerland repeatedly simulates crisis events as part of the integrated security exercise, but has little experience to date with real crisis situations of national dimensions. International networking is therefore particularly important. According to Stefan Brem, Switzerland could benefit greatly from foreign experience, particularly in terms of population behavior. This was also underlined by Daniel Schlup, who is in regular contact with foreign experts and can benefit from their valuable experience in crisis situations.

In this context, the question of solidarity among the population is crucial. According to international experience, solidarity is often greater than expected, said Stefan Brem. It is crucial that the state communicates with the population and informs them. In addition to the classic media, this is now also done via the app and Internet platform Alertswiss, which, in addition to the siren alarm, also enables the dissemination of differentiated instructions for action. Daniel Schlup added that Switzerland is very well equipped in terms of security association, coordination and cooperation. However, he did not dare to predict the reaction of the population in the event of a crisis. At the same time, he said, central buzzwords such as "crisis" had to be handled somewhat more cautiously - the train derailment in Lucerne in 2017, for example, was an emergency for SBB, but not a crisis situation.

### **Economic incentives or moral appeals?**

In the course of the final round of questions, further aspects were discussed. Jürg de Spindler, Director of the Association of Swiss Regional Banks, was surprised that in the context of critical infrastructures, moral appeals rather than economic incentives are used as arguments. Werner Meier replied that companies involved in national economic supply are able to deliver longer. This is already an incentive. The incentive of Migros, Andreas Münch added, is the existential pressure to keep the business running as long as possible in order to be able to pay the wages of the more than 100,000 employees on time.

### **The ultimate responsibility lies with the cantons and municipalities**

Diego Ochsner, President of the cantonal authorities responsible for the military, civil protection and civil defence, and head of the Kantonaler Führungsstab of Solothurn, also made an interesting contribution. Ochsner stressed that two levels of federalism had been neglected in the panel discussion because the cantons and municipalities were not represented. Ultimately, it is the cantons and municipalities, not the federal government, that are primarily responsible for civil protection.

### **Cyber security as a core topic**

Former National Councillor Roland F. Borer was surprised that the topic of cyber security was only marginally addressed in the panel discussion. Dominik Winter referred to the great efforts of Swisscom with regard to cyber security. Swisscom has its own highly qualified cyber experts and with its teams, measures and technical resources it fends off around two million cyber attacks every month. The central topic of cyber security will be dealt with in greater depth by the SWISS SECURITY FORUM in another network event at the beginning of 2020, explained Fredy Müller, Managing Director of the SSF.

### **Cooperation and awareness raising are key**

The network event of the SWISS SECURITY FORUM made it clear that Switzerland is preparing for possible failures of critical infrastructures. However, it has a very limited wealth of experience, especially since it has so far (fortunately) been largely spared from crisis situations. The behavior of the population in the event of a supply crisis or shortage of supplies therefore remains a great unknown. SSF Vice President Claudia Hollenstein concluded by saying that it is therefore all the more important to increase public information and awareness. Coordinated cooperation between the federation, the cantons, the municipalities and the economy is equally indispensable.