When blackout is just a click away

Beitrag

_Pierre Kilchenmann, Senior Cyber Security Expert at the Federal Department of Defence, Civil Protection and Sport (DDPS)
_Giorgio Tresoldi, Head of International Relations and Scouting, Cyber-Defence Campus

Published in SMART insights 2023 magazine

The Swiss Armed Forces prepare for attempted hacking by foreign states to protect the nation. Cyber attacks are on the rise, causing severe disruption to society and businesses. So far Switzerland has performed well in Locked Shields, one of the world's most prominent cyber defence exercises. Pierre Kilchenmann, who led the Swiss Blue Team, describes a particular success. Also involved was Giorgio Tresoldi, an expert in innovative cyber defence solutions.

The power is cut. Public transport is at a standstill and medical assistance can't get through. It is a nightmare scenario, but an increasingly frequent reality. Hybrid warfare continues to spread, and cyber attacks on critical infrastructures are growing. They are under multiple threats that go beyond simply disabling the electricity grid. Other dangers include cyber espionage and data theft for the purposes of extortion. Attacks on critical infrastructures can have devastating effects on the population and the business community. They jeopardise the supply of goods and services that are crucial to a functioning society. Particularly sensitive personal data, such as biometric information or criminal records, are also at risk.

In Switzerland, the Federal Council defines what constitutes a critical infrastructure. A total of 10,000 individual buildings and facilities have been designated critical infrastructures. They are divided into nine sectors and 27 sub-sectors.

There are various ways of protecting critical infrastructures with structural, legal or technical measures. All are designed with one thing in mind: to prevent serious outages. And if there were to be an incident, they serve to restore functionality as quickly as possible. The Locked Shields scenario is an opportunity to rehearse the response in the event of such an outage resulting from a cyber attack.

Fictional, yet real: the simulated cyber attack

The Locked Shields exercise simulates a large-scale cyber attack on a NATO member state. During the exercise, experts from the Swiss Armed Forces train alongside teams from 32 other nations in how to defend against such attacks. The incident is fictional, but extremely realistic, encompassing all of the technological and political aspects of cyber defence. The objective is to secure control over your own technical infrastructure.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn organises one of the largest cyber defence exercises in the world. As part of Switzerland's participation, the Cyber-Defence Campus (CYD) forged partnerships with innovative Swiss companies. As a specialist unit within Armasuisse, the Federal Office for Defence Procurement, CYD helps to identify cyber risks at an early stage and trains cyber experts. It selects its alliances strategically in order to provide defence tools that offer the highest level of security. One of these is Airlock Gateway.

Vulnerabilities under attack

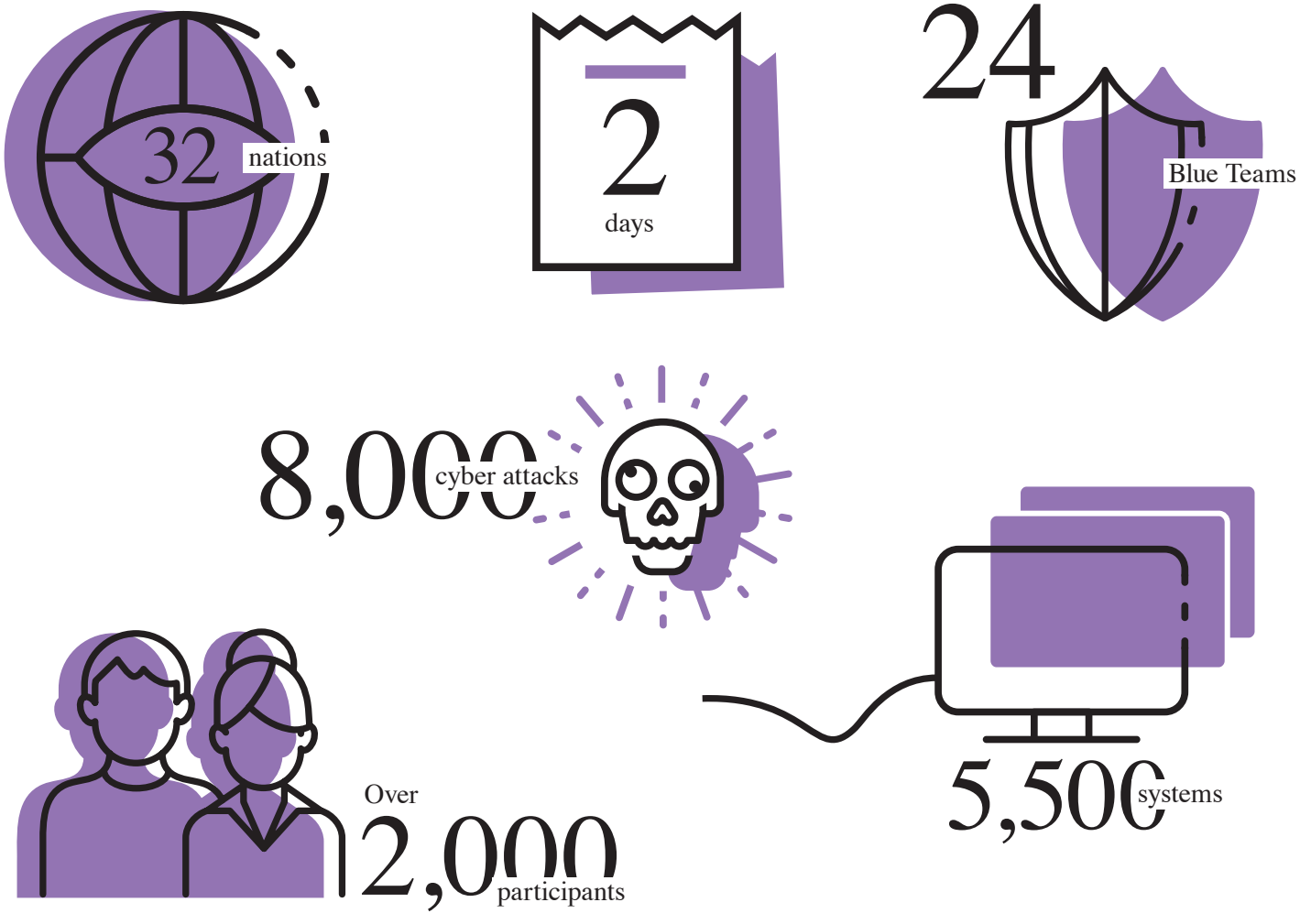
The exercise involves Blue Teams, including the Swiss delegation, supporting and overseeing a country's critical infrastructures. Meanwhile, Red Teams launch attacks in cyberspace to identify and exploit weak points in systems and processes. Blue

Teams must fight off simulated attacks on the fictional nation of Berylia as quickly as possible. Since 2012 the Swiss Armed Forces have regularly participated in the Locked Shield exercise with their own Blue Team.

Good Swiss performance

The exercise covered 40 web applications, countless bugs, false configurations and outdated software. To protect services against attack, they must be updated and errors in the code rectified. But time is tight in a crisis. That's where a central Airlock Gateway helps. It allows all applications to be patched as a group, closing loopholes. It protects business-critical, web-based applications and APIs against attack. Artificial intelligence supported by machine learning guards against new forms of cyber aggression and recognises bots that behave in a different way to normal users. In 2022 the Swiss Blue Team finished among the top ten nations in the exercise, with Airlock Gateway a major factor in their success. Although the attacks became increasingly sophisticated as the exercise progressed, Airlock Gateway was able to handle even the rarest of cases. Airlock will be deployed as part of the Swiss arsenal again for Locked Shields 2023.

_The cyber defence exercise Locked Shields in figures

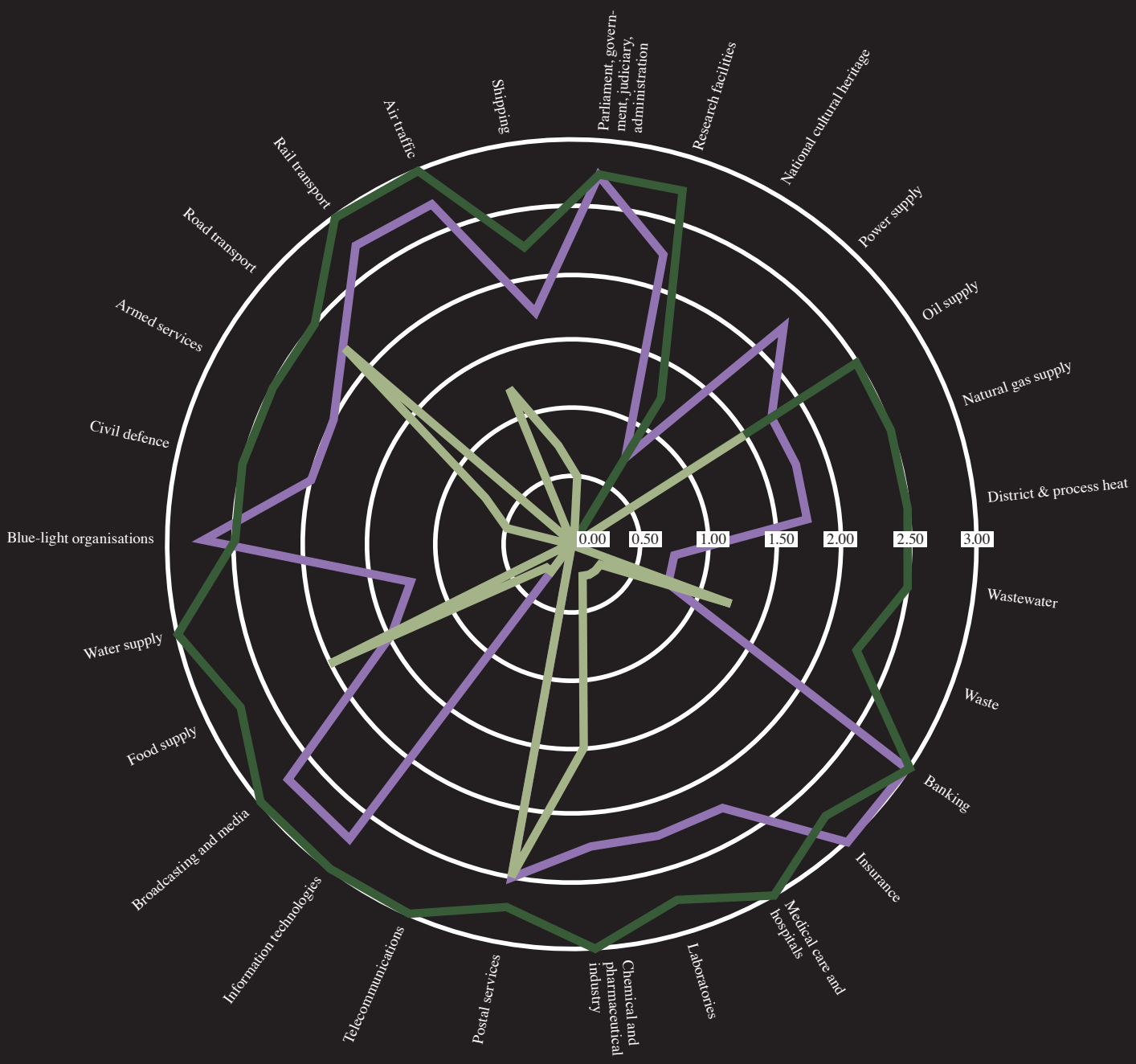


_One outage leads to more

Critical infrastructures in Switzerland comprise nine sectors subdivided into 27 sub-sectors.

If one sub-sector fails, this affects other sub-sectors. So in the event of a disruption or failure of the electricity supply sub-sector, the water supply, banking or chemical and pharmaceutical industries are also massively affected. However, the outage will have hardly any impact on national cultural assets.

Using the example of three sub-sectors, the chart shows how the disruption or outage of one sub-sector would affect another.



- Power supply
- Rail transport
- Telecommunications

0.00 → 3.00

Disruption or outage has no impact on the sub-sector

Disruption or outage has a very heavy impact on the sub-sector

Trust is the best defence

Pierre Kilchenmann is part of the Armed Forces Command Support Organisation (AFCSO), and heads the Swiss Armed Forces' Blue Team for the Locked Shields exercise. He is also Senior Cyber Security Expert at the Federal Department of Defence, Civil Protection and Sport (DDPS). We spoke with him about Locked Shields and about leadership where the rigid military and agile cyber cultures meet.

How important is Locked Shields?
As one of the world's most prominent cyber security exercises, it is incredibly important. It is the perfect opportunity to test an extreme scenario and to establish whether Switzerland would be prepared and functional in the event of a serious incident. In other words, whether our supplies would be sufficient and our people resources ready.

What is the appeal for you?
Working together in an international context towards a common goal makes the exercise extremely valuable and exciting. You get to know professionals from all sorts of fields, whether civilian, military or industrial, and you quickly have to establish a basis of trust with people you've never met before in your life. Security is primarily a matter of trust.

How has the exercise evolved over the years?
It used to have a more military focus. As digitalisation has advanced the technological element has gained in importance, because it is fundamental to critical infrastructures. That's why we work closely with partners such as Swiss Federal Railways (SBB) and Swissgrid, who also simulate scenarios like these. We also train together so that we could provide each other with resource support if necessary. Failure to fine-tune things now would cost us valuable time in an emergency.

What are the biggest challenges with Locked Shields?
It is a multinational competition, so there is a bit of national pride at stake, but it centres on co-operation. The winner isn't the nation with the best defence, but the one that best encourages collaboration with others. For example, if one country finds vulnerabilities, they could affect neighbouring states, so you bring them on board. Cyberspace is highly complex. You might be able to survive precarious situations on your own, but you're unlikely to stabilise them without help.

What were the most important lessons from the 2022 exercise?
Efficient resource planning is always a sticking point, but of course there were also plenty of lessons at the strategic, operational and technical levels. Since the field is getting more and more complex, crisis communications are becoming increasingly important. Is national leadership sufficiently well informed about strategic and political factors that it can answer questions from the media? And can it simplify the cyber jargon so that everyone affected, including members of the public, understands it?

How are these lessons conveyed to stakeholders?
By involving our partners. In 2023 teams from Swissgrid and SBB will be taking part. It's important to them not just to be familiar with the strategic and political level, but also to have first-hand experience of what happens in a serious incident.

The search for security

What success did you enjoy the most?
It was when I realised that, in just three weeks, a bunch of wildly diverse individualists had coalesced into a harmonious, high-performance team. They all left their egos at home, and learned a huge amount from each other as a result. That was the most satisfying thing for me personally.

How do you achieve that?
Strict military-style leadership has its place, but only where necessary. Otherwise you have to adapt to the cyber culture and mindset. It's like being in a special operations team. Although you have anticipated and advance-tested every move down to the minutest detail, reality is always going to throw up new challenges. In the infinity that is cyberspace, it will never be possible to plan every detail. That's why you have to keep moving.

Giorgio Tresoldi is Head of International Relations and Scouting at the Cyber-Defence Campus run by armasuisse Science and Technology, founded in 2019. He was part of the Swiss success in the Locked Shields exercise, as the curator of both the technology and the team, and the coordinator between the armed forces, research and the academic world. He gives us an insight into the process, and his view of where Switzerland stands as a cyber nation.

What does your job entail?
I comb the global market for ground-breaking cyber security solutions that meet the needs of the Federal Department of Defence, Civil Protection and Sport (DDPS) and the federal administration. High levels of security and protection are key here, of course, but it also involves areas such as data science and machine learning.

How does the Locked Shields cyber defence exercise fit in?
We're involved in Locked Shields in numerous respects. We advise the Swiss Armed Forces on technologies that might be relevant to the exercise, and are their procurement channel. We also evaluate potential participants. Our research projects give us a network of distinguished experts in all manner of fields. Locked Shields generates a great deal of data, so we help the team to evaluate it. That's where our huge expertise in data science comes in.

You used Airlock Gateway in the 2022 exercise.
We did. We were interested in using web application and API protection, so we looked around for Swiss suppliers who could provide not only the

“The focus isn’t on where a company comes from, as long as it delivers the best quality.” _Giorgio Tresoldi, Head of International Relations and Scouting, Cyber-Defence Campus

technology, but also an expert who still had a few days’ military service to complete. Ergon offered just that. It was the perfect combination.

How important is the use of Swiss technology?
The supply chain is becoming increasingly problematic for software as for other products. That is why it helps to keep the chain short. It allows better traceability. That’s what makes Swiss technology important.

Does Swiss software protect us better than other products?
I’m not going to make any sweeping statements. There are good and less good software companies everywhere, and Switzerland is no exception. The focus isn’t on where a company comes from, as long as it delivers the best quality. The new procurement law places greater emphasis on sustainability. Here Swiss companies certainly have great potential. Naturally, however, the WTO rules and the applicable procurement legislation are always adhered to.

How do you assess Switzerland’s readiness to fend off a cyber attack?
It’s difficult to answer that in general terms because we’re talking about a broad range of targets, from three-person SMEs in which one person is in charge of IT, to billion franc big pharma. You can’t lump them together. I can only talk about the federal government and armed forces. In my opinion

we are well prepared compared with many countries. But there is always room for improvement.

Where do you think this improvement potential lies?
I think we still have plenty of scope with regard to software that automates certain processes. At the moment we don't have enough people to look at the data and run projects. If we could increase the level of automation, we could achieve more with the same number of staff.

Which areas are most vulnerable to a cyber attack?
There are different levels and sectors here. Financially motivated crime, for example, targets organisations so that they will pay up. In Spain there were attacks on a hospital, and operations had to be postponed. Hacker gangs of course know that a hospital can't just shut down.

You mentioned that most of the staff of the Cyber-Defence Campus are still studying.
Each year we run projects for the DDPS with 30 to 40 students and interns. Many of them are doing their PhDs, so they have a sound academic foundation. What we offer in the context of term papers or master's theses are use cases that are important to Switzerland's cyber defence. It may well be that the students' work is later used by the DDPS or federal government to improve those defences. But the Cyber-Defence Campus isn't just interested in working with the academic world. We also seek out public-private partnerships.

You even offer a Proof of Concept Fellowship, don't you?
Exactly. It is still in its earliest stages. The aim is to develop a product. Nobody has yet completed the fellowship, but I look forward to getting lots of applications from your readers! The best way is to contact us directly at cydcampus@armasuisse.ch. />