Cyber Espionage and Data Security: The West in the Crosshairs?

Summary report | 15th FFS Security Talk on November 22, 2023, Hotel Schweizerhof, Bern

Over the last two decades, the triumphant advance of the Internet and the associated progressive digitalization have created a highly complex cyberspace that has enabled the entire world to be networked. On the one hand, this digital space opens up a multitude of new possibilities, but at the same time it is also extremely dangerous. Hacker attacks on state institutions and companies in the West have increased massively in recent years. This trend has also been clearly evident in Switzerland, as a number of examples over the past year have shown. Private sector players have not been spared either and are increasingly becoming the target of such attacks.

Which sectors and institutions are the focus of such attacks? How can and must authorities, institutions and companies protect their critical data from cyber attacks? How should politicians deal with the threat of cyber espionage and other cyber dangers? What measures are urgent and necessary?

These and other important questions were discussed at the 15th FSS Security Talk in Bern by renowned experts such as **Major General Jürgen Setzer** (Deputy Inspector CIR and CISO, German Armed Forces), **Dr. Myriam Dunn Cavelty** (Senior Lecturer in Security Studies, Center for Security Studies (CCS), ETH Zurich), **Nicolas Mayencourt** (Founder & Global CEO, Dreamlab Technologies), **Franz Grüter** (Chairman of the Board of Directors, green.ch Group; National Councillor SVP, LU) and **Johann Alessandroni** (Head of Information Security Governance, Excellium Services by Thales Group).

Hans-Jürg Käser, President of FORUM SICHERHEIT SCHWEIZ, welcomed the almost 120 participants to the 15th FSS Security Talk with a few introductory words. To accommodate the tight program, however, Major General Setzer immediately began with the first input presentation.

Presentation Major General Jürgen Setzer

Major General Setzer is often asked how he can still sleep at night in his role as Deputy Inspector of Cyber and Information Space and Chief Information Security Officer of the Bundeswehr. His answer is simple: "By being wide awake during the day". The protection of cyber and information space is a top priority in the Bundeswehr. This is why the Bundeswehr's **cyber and information space (CIR)** was established as an **independent military organizational area** in April 2017 and thus elevated to the same level as the **other dimensions of land, air, water and space**.

Cyber and information space as a military operational area

The importance of cyber and information space as a military operational area can be seen very clearly in the current Russian war of aggression against Ukraine, for example. Although reporting is largely focused on the conventional kinetic capabilities of the armed forces, it can nevertheless be seen on a daily basis that **capabilities in cyber and information space** are **an essential component of warfare.** The media in particular functioned as a stage and actor of Russian information warfare, with the overarching goal of breaking the will to defend Ukraine and its allies. Germany, although not a party to the war, was permanently exposed to hybrid influence, whether through information campaigns or cyberattacks, in an attempt to influence political decision-making. The actors included both regular cyber warriors from Russian secret services as well as criminal organizations and groups. It is clear that **state actors like to use non-state actors to carry out attacks and deny responsibility,** which makes it difficult to clearly attribute the incidents, both for Germany and for other countries and allies. Russia's attack on Ukraine and the accompanying cyber attacks also pose a considerable indirect threat to Germany. One example of this is Russia's cyberattack against Viasat's KA-SAT satellite service used by the Ukrainian military, which also affected the operators of wind turbines in Germany, as the remote maintenance of the wind turbines was also carried out via KA-SAT.

A similar importance of cyber and information space in military conflicts can currently be observed in connection with the war between Israel and Hamas. The attack by Hamas terrorists is being accompanied by operations in cyberspace. Important information media such as the Jerusalem Post news agency and an Israeli security information and warning system, which is an essential, life-saving tool for the Israeli population in the face of constant rocket attacks, have already become victims.

Information as a key resource for modern societies and armed forces

On the one hand, such attacks naturally stir up fear and confusion among the population. On the other hand, the aim of these attacks is often to compromise enemy information, as this is a key resource of modern societies and a prerequisite for the operational readiness of the armed forces. Information security, i.e. the successful protection of information transmission, information processing and information storage, is therefore of particular importance. **"Ultimately, information superiority is a prerequisite for decision-making superiority, a prerequisite for effectiveness superiority and, at the end of the day, a prerequisite for the ability of armed forces to win in a conflict**," said the Major General, emphasizing the key role of information.

The Bundeswehr is also the target of attempted attacks in cyberspace on a daily basis. As Chief Information Security Officer, he is pleased to say that none of these attacks have been successful so far. However, you always have to be careful with these statements, because you can never rule out 100% that someone has already penetrated your own system and has not yet been noticed by the protection mechanisms.

These attacks therefore showed that it is important to be alert, innovative and agile at all times and to constantly review and improve one's own security architecture. To this end, four fields of action have been defined: the human factor, concepts and technology, the expansion of the innovation environment and national and international cooperation.

The human factor

The first field of action, the human factor, also represents a very decisive factor in IT security. Firstly, from the perspective of the user: **Over 80% of successful attacks on IT security can be attributed to the unwanted involvement of the user.** The methods used by the perpetrators are diverse. The term social engineering encompasses numerous strategies aimed at influencing and manipulating people and inducing certain behaviors, such as granting access to data and systems and sharing information. Advances in the field of AI have also improved the possibilities of successfully deceiving victims. Everyone present had certainly already received phishing emails, whether on private or business email addresses, some of which looked deceptively genuine. On a positive note, however, it should be noted that awareness among users has generally increased as a result of the attacks in the context of the Russian war of aggression against Ukraine. However, this is still not enough. For this reason, the Bundeswehr is facing up to the real threat situation with self-challenges 7 days a week, 24 hours a day, in order to identify possible weaknesses before they can be exploited by others. This involves attacking oneself with offensive forces, sensitizing employees and increasing their awareness that they are under attack on a daily basis.

However, the **significant increase in demand for cyber security specialists and a growing shortage of skilled workers also posed challenges** and made it necessary to explore new avenues in order to find enough suitable personnel. A particular focus is therefore on training. The Bundeswehr therefore also trains its own personnel, sometimes at its own IT school or at the universities in Hamburg and Munich.

Concepts, technology, innovation and cooperation

The second field of action concerns the concepts and technologies used. The Bundeswehr has information security concepts as standard. These are the basis for all units before they go into action, whether they are deployed in normal crisis management operations, as is currently the case in Mali or Kosovo, or in the context of deterrence or on NATO's eastern flank, for example in Lithuania.

At the same time, the company is also working on new and future concepts and technologies, or the expansion of the innovation environment, the third field of action. **Cyber security is not a static state.** It requires continuous **adaptation** and **further development in** order to keep pace with the **short innovation cycles** experienced in digitalization, including in cyber security. Three aspects are of particular relevance in this context from the point of view of the innovation environment: Effectiveness, demand orientation and agility.

In order to increase effectiveness, an established IT dialog and innovation dialog with partners from industry, such as Bitkom, the industry association of the German information and telecommunications sector, is just as important as with federal and state security authorities or science and research institutions. In addition, there must of course also be a dialog within the armed forces to increase the focus on requirements. In the Bundeswehr, the innovation dialogue relies on an implemented network between those responsible for the digitalization platform, the procurement office and the private sector IT system service providers. This network embodies the key element for **rapid** and **sustainable digital transformation** and will only work if **users**, **developers** and **procurers sit hand in hand in the same boat** and work together from the **outset.**

In addition, the Bundeswehr also has application-leading innovation players. These include the Cyber Innovation Hub as a central focus point for testing marketable solutions from the world of start-ups. In addition, there is the so-called "BWI Forge", which, as a coding force, makes a decisive contribution to the digitalization and automation of the Bundeswehr. A cross-departmental cyber agency has also been set up to promote research projects in the context of cyber security. **"In the cyber area, there is no boundary between internal and external security, which is why the forces for internal and external security must work together to advance their capabilities**," said Major General Setzer, once again emphasizing the need for cross-departmental and cross-level cooperation. This cyber agency was created for this purpose and to provide sufficient scope for the approach of continuous improvement and innovation across internal and external borders. Furthermore, cooperation is also maintained, for example, with the Fraunhofer-Gesellschaft and the two Bundeswehr universities.

"It's not one player on the pitch that determines what happens, but many games together"

The fourth field of action is about national and international cooperation and exercises. Interdepartmental cooperation at national level between research, security authorities and companies is considered to be of crucial importance. The German cyber security strategy also provides clear guidelines for this. The focal point in Germany is the National Cyber Defence Centre. It was implemented back in 2011 under the leadership of the Federal Office for Information Security (BSI). It was the first forum for state cooperation in the context of cyber security. In the years that followed, the focus was on successively developing this forum further and continuously increasing the number of participants. This is important because cyber defense is a team game: "It's not one player on the pitch that determines what happens, but many players together". But one thing is also clear: without

a convincing captain or coach, it won't work. That's why the decision was made to define coordinators. The Bundeswehr always takes on the role of deputy coordinator in order to ensure the transition from peace to war in the coordination committee at all times.

This instance of the National Cyber Defense Center, which was set up as an information coordination and cooperation platform, is therefore making a significant contribution to cyber security, today and now. **The state has a responsibility to be prepared for a digital meltdown before it actually occurs.** Joint exercises by our security authorities, the German armed forces, local authorities, government agencies and KRITIS companies are essential for this, as was the case in September of this year during the cross-state and cross-departmental crisis management exercise LÜKEX. During the simulated nationwide cyberattacks, the primary goal was to maintain state and government functions. Because if these were no longer guaranteed, then chaos would be encouraged. Only through such joint exercises can decisive impulses be created to improve resilience for scenarios that have not yet occurred, but which could happen.

International cooperation

The exchange at a multilateral level is also important. In this context, we are particularly pleased about the close ties with our Swiss partners, for example through the annual meetings of the cyber commanders of the DACH region or joint German-Swiss seminars on command and control information systems and data strategies. Furthermore, the Cyber and Information Space is already looking forward to the visit of the Swiss Cyber Commander and the Chief of Staff Operational Training in Bonn next year.

In addition to this exchange, continuous practice is also one of the prerequisites for effective cyber defense. **There, too, there is a good and sustainable connection with Swiss friends within the framework of "COMMON ROOF".** This is an annually recurring exercise with the aim of practicing the capability development of the DACH nations in operability. Looking to the future, the DACH format also fosters profitable cooperation. As part of the multilateral Cyber Defense Exercise next year, the cyber and emergency response teams will be exercised together in an umbrella format and, as originally planned, also with their Israeli friends.

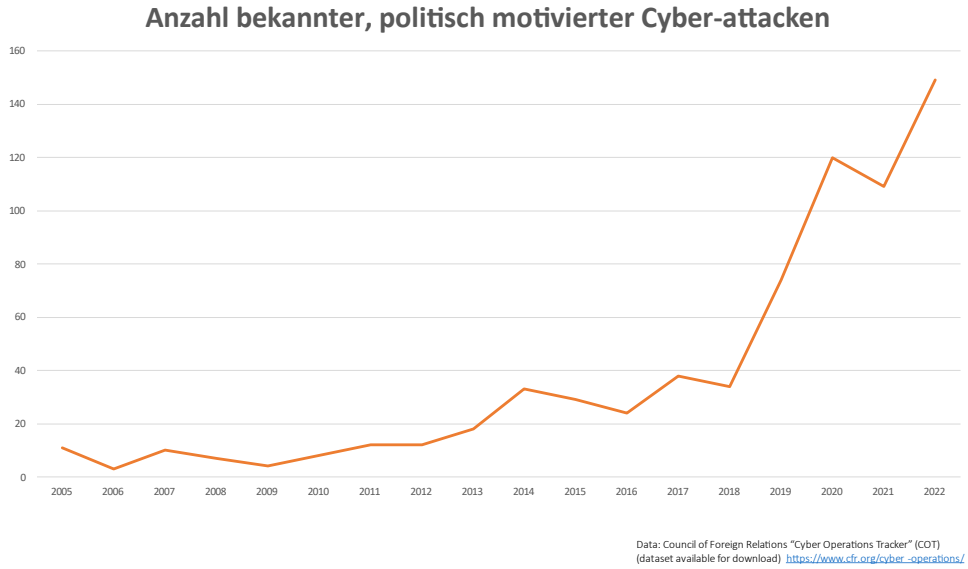
"**Information is the key resource of our modern society and our armed forces.** Protecting it, i.e. cyber information security, is a duty for all of us, Germans and Swiss alike, and at the same time one of the greatest challenges. Let us see this challenge as an opportunity. An opportunity to develop our capabilities together, to protect our countries and to shape our future together."

Presentation Dr. Myriam Dunn Cavelty

The second speaker, Myriam Dunn Cavelty, focused on cyber espionage, which she examined from a scientific perspective. Her aim was to show why we mainly talk about espionage when it comes to state activities in cyberspace and less about other common forms of cyberattacks, which would not require such large capacities.

Increase in politically motivated cyber attacks since 2017 /2018 - cyber espionage at the top

If you look at the data, you can see a massive increase in the number of publicly known, politically motivated cyber attacks around 2017/2018. On the one hand, this increase can be attributed to the development and expansion of capacities in cyberspace after 2010. Nowadays, there are more actors who can carry out such targeted attacks. On the other hand, the increase is also due to the expansion of defense capabilities and the ability to detect such attacks. As already mentioned by Major General Setzer, a lot has been and is being invested in cyber security.



Data: Council of Foreign Relations "Cyber Operations Tracker" (COT)
(dataset available for download) https://www.cfr.org/cyber -operations/

If you now look at the type of attacks, you can see that espionage is at the top of the list with a large majority. Of the known politically motivated attacks, 70-80% are espionage. And this is only the known data. If you take into account the fact that espionage is carried out as covertly as possible, then you can assume that the actual figure is even higher.

Capacities / Configurations / Context - Good reasons for cyber espionage

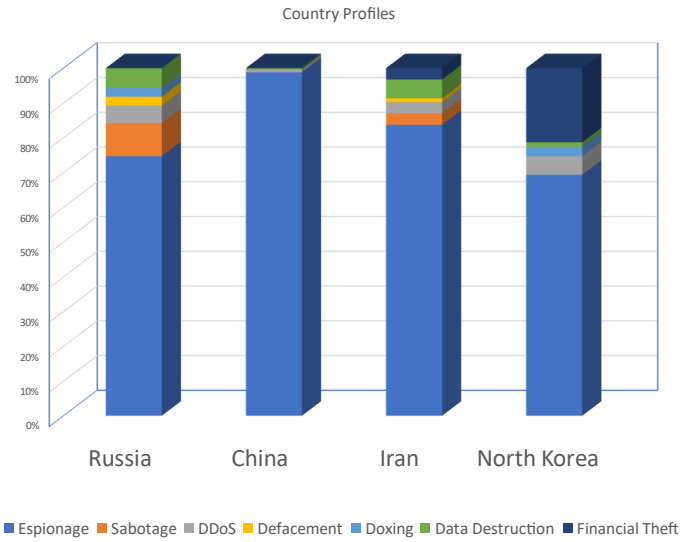
There are three reasons why espionage is so widespread as a state tool in cyberspace: firstly, the aforementioned capacities or, in this context, the so-called **"advanced persistent threats"**, or **APTs** for short. Secondly, the **configurations,** which include the technical properties of systems and the ability to influence them, but also the human factor and its competencies in the cyber area. And finally, the geopolitical context and the concept of **"strategic competition"** explain why cyber espionage makes a lot of sense for states.

Capacities

When addressing the issue of capacity, it must first be understood that there are certain activities in cyberspace that are very difficult to carry out. "The idea of the hacker sitting in the basement and pressing some buttons to create something big has to be removed from people's minds in these cases." This insight is necessary in order to recognize who you are actually up against and what measures can be taken.

Länderprofile

- Seit 2005: 34 Länder führen offensive Cyber-operationen durch
- China, Russland, Iran, Nord Korea verantwortlich für 77% aller Operationen
- Achtung, Visibilität!



If you look at the country profiles of the countries that have carried out cyber operations in the higher segment since 2005, you can see that these are 34 countries. **Approximately 77% of these are** attributable to the **four players Russia, Iran, China and North Korea**, i.e. political rivals of the USA. However, it is important to address the issue of visibility here too. The available data is provided by threat intelligence companies, the majority of which are based in the USA. These companies have spent years building up the capacities and capabilities to record such attacks, while other countries lack these capacities, which means that the scientific data basis is also incomplete.

As mentioned above, espionage accounts for a large proportion of high-end state cyber operations - especially among the USA's main rivals. The units that carry out these espionage activities are also referred to as advanced persistent threats, or APTs for short. They are characterized by highly developed capabilities that last for years and are based on people. In addition to **in-depth technical expertise,** such **cyber operations** are also **very costly**. As a result, **APTs** are **usually state-controlled** and **are interested** in **sensitive, valuable data to make** the effort behind such operations worthwhile.

Configurations

If you look at the configurations that facilitate cyber operations, you realize that attackers need time until vulnerabilities are found and the programs are ready to actually exploit the vulnerabilities found. This usually takes months, if not years. Furthermore, cyber operations are worthwhile if you can and want to operate covertly, which is in line with the requirements of espionage. As access to a network cannot be gained by force, **existing vulnerabilities** and the **ability to remain undetected are important**. If an attacker is discovered in the system, he could lose his entire, expensive and highly developed toolset. Cyber operations are also worthwhile if you are not aiming for high intensity or destruction. It is not easy to precisely time a destructive effect and predict the extent of the effect. This also means that, **from a military point of view,** it makes **little sense to use cyber operations to destroy networks**; instead, **the physical approach makes more sense**. This means that the more intensive the targeted effect and the more complex the operation, the more likely an attacker is to be caught and risk their investment. And finally, cyber operations are worthwhile if their effect does not have to be fully controlled. **Cyber operations take place** in **enemy systems** that are often **not fully known,** which is why the **effects of an operation** cannot usually **be fully tested or predicted**. This often results in the collateral damage that can be observed in many cyber attacks.

If these 4 points are now brought together and we look at what kind of cyber operations are worthwhile in networks with increased security, we are back to espionage.

Context and strategic competition

Finally, the geopolitical context also provides an explanation for the use of cyber espionage as a state tool. It proposes **strategic competition** as a framework that allows us to understand why certain activities in cyberspace can be increasingly observed. Strategic competition is a concept that originated in the USA. This concept is seen as an active **blurring of war and peace, and cyber** operations are again suitable for this. All cyber operations, for example in Ukraine, are deliberately kept below the threshold of war, in a hybrid form between war and peace. Strategic competition is about using all areas of power, which is why it is also suitable as a great power game. It mobilizes very large resources, and if we now return to cyber espionage, the systematic theft of intellectual property, this is again a useful means for states to accumulate a power resource. It is still very difficult to measure the effects and damage of espionage, even from a scientific perspective. However, it is now clear that a **cumulative strategy**, i.e. **repeated, smaller, low-threshold attacks**, is **more profitable** than one **large, destructive attack**. It can therefore be seen that all these factors favor the use of espionage as a state tool in cyberspace.

In conclusion, however, Dr. Dunn Cavelty emphasized that, even though she had spoken primarily about cyber espionage, cyber espionage capabilities are closely linked to capabilities for other types of cyber operations. We must therefore be aware that the **expansion of cyber capabilities that has** been observed in recent years also **increases** the **risk of operations** that have the potential to **significantly disrupt social order.**

Presentation Nicolas Mayencourt

In his input presentation, Nicolas Mayencourt focused on vulnerabilities, i.e. attack surfaces and weaknesses in cyberspace, with the aim of ensuring that these are recognized and acted upon accordingly. Although Switzerland is such a small nation, its innovative strength is impressive and it is

therefore particularly important to him that the dangers and methods of protecting this innovative strength are known.

From the natural to the world 2.0

When dealing with vulnerabilities in cyberspace, it makes sense to first take a look at where we come from: the beautiful, old, natural world that humans have made their own over tens of thousands of years with their unique DNA, their unique intuition and their unique reflexes.

This is all the more astonishing as humans are inferior to animals or their direct ancestors in many respects. For example, they can run less quickly and climb less well. The fact that humans have nevertheless established themselves as the dominant species is due not only to their intuition and exceptional reflexes, but also to two other decisive advantages, which are particularly noticeable when it comes to information: On the one hand, humans have managed to **formalize knowledge**, pass it on over generations and thus **build up** an insane **wealth of knowledge and experience** over hundreds of thousands of years of human evolution. In addition, humans also have the crucial ability to **organize** themselves in **groups on an ad hoc basis**. Swarming behavior is also known in the animal world, for example in birds and fish. However, the difference is: "Humans can organize themselves ad hoc, purpose-, goal- and project-based, in order to create an advantageous outcome together, whether they know each other in advance or not." These abilities have accumulated over the course of evolution and led to the first industrial revolution, which in many ways was the origin and foundation of modern civilization, the new world.

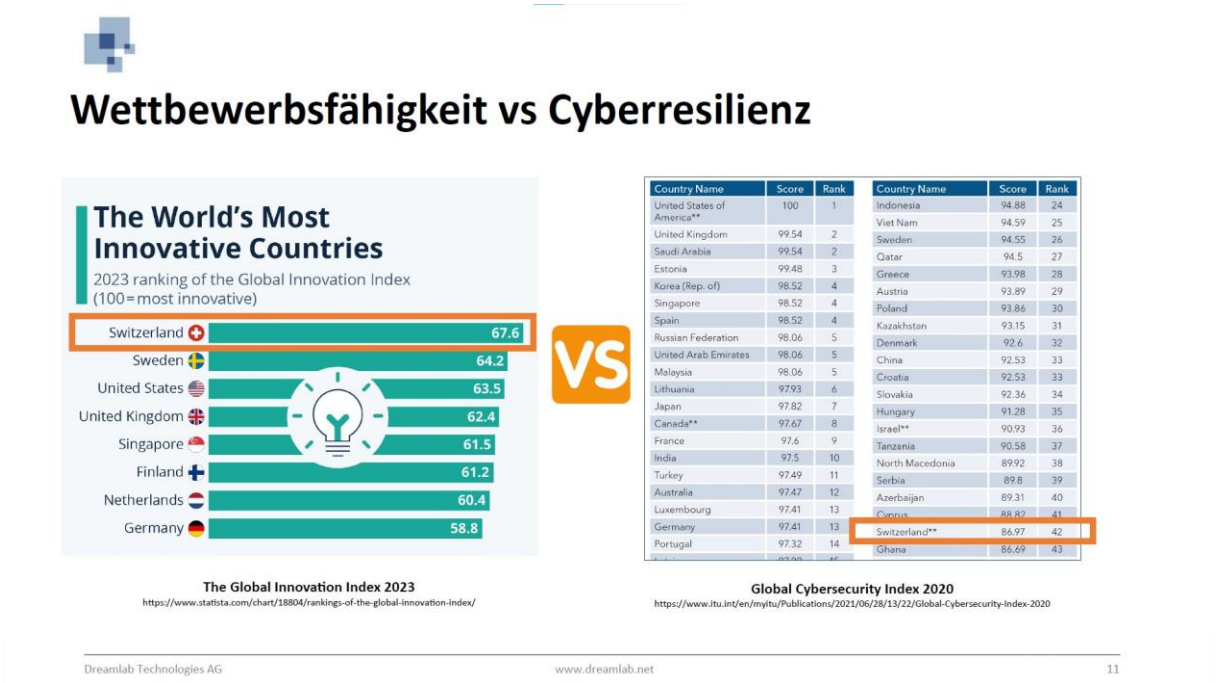
Cyberspace - abstract, omnipresent, dangerous

Humans, with their unique humanity, have thus managed to establish themselves as a winning species in the four dimensions of land, water, air and space. However, World 2.0, or the world he has created, goes even further: in the **third industrial revolution,** humans created a **new, unique, man-made space**: **cyberspace**. The invention of the computer and digital space as well as networking via internet technology and other network technologies enabled him to give free rein to his innovations without

physical limitations and to tackle things that would not be possible in the real world. These developments were characterized by an incredible speed, which still continues today. Within 50 - 70 years, cyberspace has been built up, and today it almost completely permeates and controls the physical dimensions. At the same time, this cyberspace is not tangible for humans, not accessible to the senses. It is omnipresent, invisible and yet controls everything. This construction is unique, wonderful, almost paradoxical, but also extremely dangerous because the dangers and their immediate effects are not directly perceptible. People lack the sensory perception for this - they often only feel the effects when it is already far too late. It is essential to bear this context in mind. People are victims of their own innovations. He has developed a space that is extremely powerful, but in which his human attributes, his intuition and his sensuality no longer apply.

Danger for Switzerland as a center of innovation

This brought him to Switzerland here and now. He noted that, according to various statistics, **Switzerland** is the **most innovative nation in the world.** The reason for its innovative strength can be summarized simply: Switzerland can afford it and has been **systematically investing in research and education** for many years. The result: Switzerland is highly innovative today; it has a strong research and development landscape; it is known for precision and quality as well as its neutrality and independence. However, these characteristics and virtues must also be carefully cultivated in the future.



Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43

In addition to the often very pleasing statistics and indices on Switzerland, however, there are also key figures that should give the Swiss far less pleasure. The **index** of the UN-based **International Telecommunication Union (ITU)** includes a cyber ranking of the cyber-readiness of nations. **Switzerland** is in a rather mediocre **42nd place, and** everyone should be aware that sooner or later this will have an impact on Swiss innovative strength. In today's world, research results are ultimately data that is stored on servers. If these servers cannot be protected, then the results of investments in research and development will flow to other nations. According to Myriam Dunn Cavelty, 80 % of attacks are espionage. That is why it is important to take more care and work more properly in the area of cyber security and to ensure that Switzerland is also in a top 10 position here in order to ultimately protect its innovation location.

Cyber - a global risk cluster

If you look at the cyber threat situation, you realize that it is a global problem. According to the World Economic Forum and many other institutions, there are two major risk clusters facing our world: The first is climate change and the second is cyber. There are various reasons for this. The dangers facing state and non-state actors in cyberspace have already been well highlighted by the previous speakers. However, the effects of this are also primarily of a pecuniary nature. In **2021,** the **cyber losses** reported to insurers amounted **to CHF 5,000 billion**. This is already equivalent to the **GDP of** the **third largest economy** and almost **50 times the damage caused by all natural events**. These are losses and sums that can no longer simply be ignored, but must result in decisive action.

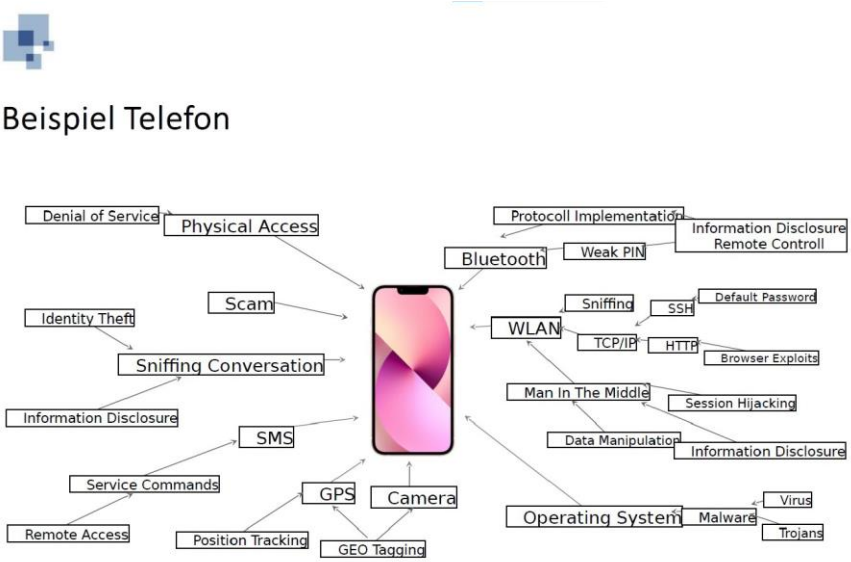
Switzerland is also affected by this. Switzerland is also connected to cyberspace and is not an island of the blessed, separated from the rest of cyberspace. It is assumed that one in three companies in Switzerland will be a victim of cybercrime in 2021 - but the number of unreported cases is likely to be much higher**.**

"As a society as a whole, too little is still being done to ensure adequate protection"

In connection with the enormous extent of damage caused by cyber damage, one point is of great concern to him: "Compared to natural and other dangers, we have greater leverage in cyberspace to protect ourselves and can defend ourselves against attackers." However, many people still lack an **understanding of cyberspace** itself and the associated dangers. Although there has been a strong increase in awareness over the last three years, people still play down their own vulnerability too much, even though anyone can become the target of cyber attacks. As a result, society as a whole is still doing too little to adequately tackle the problem.

Complexity as the enemy of security

However, why protection in cyberspace is so important and difficult in the first place can be illustrated using the example of our cell phones. The original cell phones had a limited feature set with manageable opportunities for attackers to intervene. In recent years, however, the evolution of the cell phone with its unparalleled speed has meant that the feature set of our devices has continuously multiplied and with it the **complexity of the devices and their vulnerabilities**.



IT as a whole has developed in a similar way over the last 20 years. Originally simple systems have virtually exploded in complexity, and **complexity is known to be one of the biggest enemies of security**. Securing systems with this level of complexity is extremely difficult. If this fact had been taken into account more consistently in recent years, we would not be struggling with these enormous amounts of damage today.

In Switzerland, too, we are victims again and again, and this should not be about pointing the finger at someone; instead, such incidents should trigger concern and lead to action. We need to do better, from the government to the media, the economy and society as a whole. If you overcome the sensory hurdle of cyberspace with tools and make it visible, then you can see the sheer mass of vulnerabilities that are publicly known in cyberspace. **"If you leave the safe door open and hang a sign outside on the street, you shouldn't be surprised when data thieves strike mercilessly,**" he said, symbolizing the current situation in Swiss cyberspace.

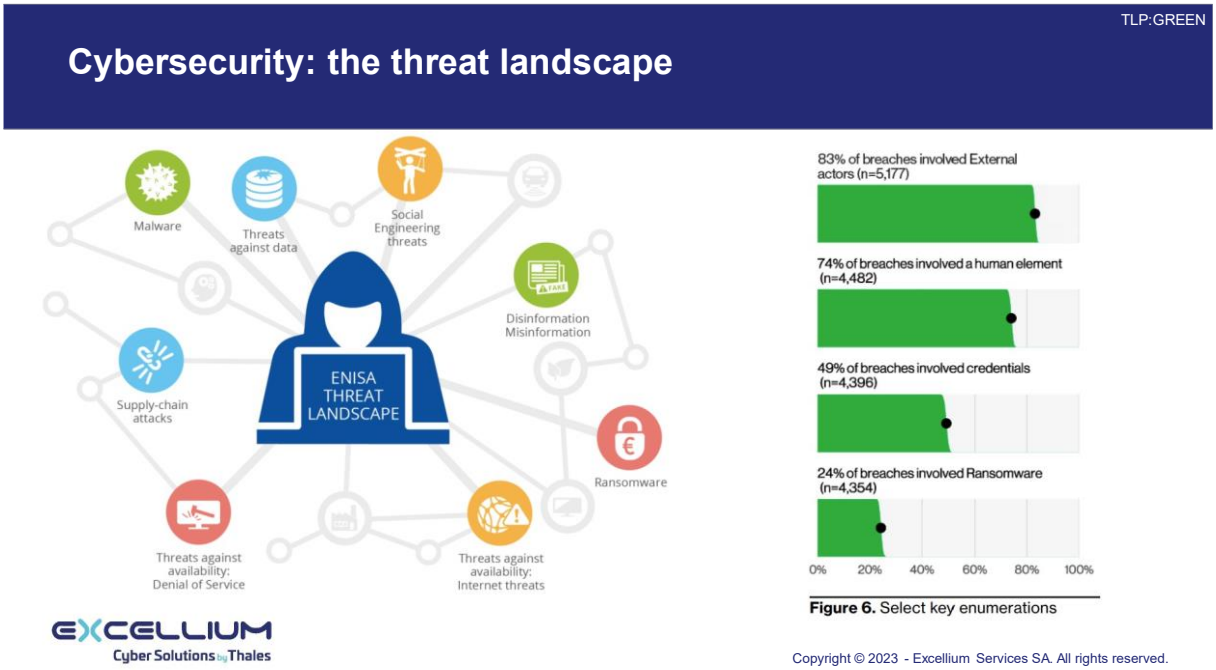
He does not have a conclusive explanation as to how cyberspace could be fully secured, managed and controlled. Perhaps it would help to simply pause for a moment, **analyze** the unchecked **development of the last 20 years in detail** and **treat cyberspace with the necessary respect**, just as is done with physical space - after all, vault doors are not simply left open there either. And last but not least, a start should be made on demystifying the cyber dimension and allowing the unique human characteristics to flow into it.

Presentation Johann Alessandroni

After the valuable previous contributions had provided a good overview of the context of the dangers in cyberspace, Johann Alessandroni showed how cyber security can be organized in practice.

Recognize, use, transfer

When talking about securing information systems, it is first necessary to address where risks exist and how to deal with them. It is not enough just to look at the systems themselves; the **human factor must** also be taken into account as an important factor. Starting with the systems and making them safer is already a major challenge, but finding the right adjustments for people and adapting their behavior is even more difficult. The great importance of the human factor for cyber security is also illustrated by statistics. **74% of cyberattacks in 2020 were linked to the human factor**. For manufacturers of cyber security solutions, this means that the human factor must never be neglected in strategies for securing systems.



Statistics and **information** are generally important for understanding the **threat situation in cyberspace**, but even more important is how the findings can be used to improve cyber security. The statistics show, for example, that attacks have increased significantly in recent years and that cyber espionage is the preferred method at state level. The question now is how these findings can be transferred to other levels, such as the non-governmental level, in order to provide better protection. Another example of this is the observations made during the war in Ukraine. The physical war began in February 2022. However, cyberattacks by Russian groups on vital institutions in Ukraine have been observed since September/October 2021. The cyber war had therefore been in full swing long before the war manifested itself on the battlefield. This realization in turn makes it clear that **cyber is often used proactively as a means of gaining access to important information**. Accordingly, cyber defense must also act with foresight in order to protect itself proactively.

The task is therefore to transfer all this knowledge to the respective levels and sectors that need to be protected, be it the healthcare sector, industry or the financial sector. The focus is not only on the **initial protection of the systems, but also on the ability to detect and react should an attack be underway**. The ability to recognize a compromise of one's own information system in good time is elementary in order to limit the consequences of a potential attack. The information that can be gained from an early detection of a compromise would in turn help to improve early detection. Once again, the aim is to collect information and transfer it to effective protection against cyber attacks. The same applies to attacks that do not affect you directly. Here, of course, you could simply sit back and be happy that you have been spared. However, it would be more effective to take the information from the observed attack and use it again to improve the protection of your own systems.

Proactive, comprehensive risk management

This tactical and strategic information must also be used to constantly review and adapt the company's own risk assessment. Such a risk-based approach has already been practiced for years in many areas outside the cyber world. For example, the currently observable mass of cyber attacks in connection with the wars in Ukraine and Gaza and their secondary theaters must always be included in the company's own risk assessment. Be it because you have specific connections to the actors involved or simply because the attacks are becoming more frequent and more serious. **The risk of becoming a victim of an attack has clearly increased as a result of the wars**. As part of proactive risk management,

the risk assessment must therefore be constantly developed and adapted to the context based on the available tactical and strategic information, as must the company's own cyber security strategy.

In turn, it is essential that action is not only taken when damage has already occurred. Nowadays, automated solutions for early detection and response are already very good. However, if they are not fed with the appropriate input in advance, they will not be able to take full effect and develop further. The better, more reliable and more up-to-date the information is, the more advanced and appropriate the automatic detection and response options will be. Of course, country-specific differences must also be taken into account. Although most information can be used universally as input to a certain extent, the specific context information remains enormously important for a security concept adapted to the respective organization.

Attackers always seek the path of easiest resistance

When designing such a security concept or a cyber security strategy, it is important, as mentioned at the beginning, to **not only consider the technological level, but also to strive for comprehensive protection of its endpoints**, including the human factor and the physical security of systems and facilities. If you neglect one of these areas, you are neglecting a factor that could facilitate an attack tomorrow. Attackers always look for the path of easiest resistance. The more lines of defense are set up to protect a system, the more likely attackers are to focus on other targets. As soon as you credibly signal that you have a certain level of robustness and security measures in place a priori, attackers often look for other, easier targets.

A question of resources

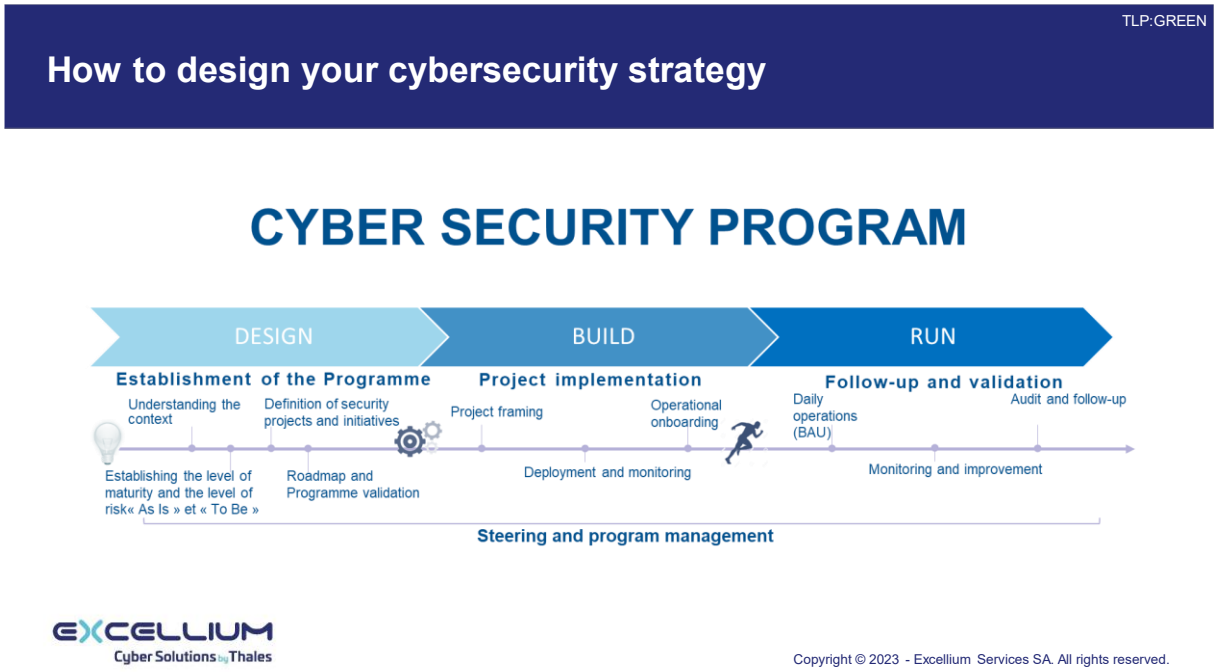
An important question when implementing a cybersecurity strategy is always how many resources should be allocated. The resources available for cyber security vary from organization to organization. Investments in cyber security always mean budget cuts in other areas at the same time. Fortunately, **basic protection in the cyber area is already possible with relatively little effort,** but for this reason it is important to define your goals correctly from the outset. Without defining objectives, it will not be

possible to establish a security strategy that is structured, well thought out and demonstrably effective. It is also important to move away from the idea of a single magical super technology that can offer comprehensive protection. Ultimately, it is always the totality or the overall logic of the measures that constitutes their protection.

Another important aspect that we also need to keep reminding ourselves of is the role of our ecosystem, i.e. our network of relationships**. We are often not in control of our own risk**. The close networks in today's world mean that attacks on partners, people and organizations that we work with could also pose a security risk to us. It is therefore important to take a close look at possible security gaps that could lie in your relationships with partners and incorporate them into your own strategy.

As already mentioned, when talking about cyber security, it is also important to consider how to react if the worst-case scenario occurs. Investments in cyber security are therefore not only used to protect against cyber attacks, but also to detect them and respond accordingly. This is referred to as business continuity management or crisis management. These points must always be prioritized in a security strategy. The companies that suffer the greatest consequences of a cyberattack are always those that have neglected these important points and are therefore unable to ensure their continued operation.

Step by step to effective protection



If we look at the traditional process for developing and implementing a cyber security strategy, the **first step is** usually to **define** the **context**. As already mentioned, no two organizations are the same. It is necessary to understand the benefits of an organization, the risks and the impact on the ecosystem in order to define how cyber protection should be designed. This is followed by an **assessment of the existing level of security** to determine how it is structured and where to start in order to achieve the set goals. The **recommended measures** would then be **modeled**. Again, it is important to emphasize the added value of each measure so that the focus is not only on the respective costs. Milestones and performance indicators should also be defined and the respective progress and activities should be monitored and discussed in regular inventories and safety checks.

Conclusion

As with the development and implementation of any strategy, it is also important to take a structured and pragmatic approach to cyber security. You have to be aware that there **are no magic solutions**. This also means that you have to commit to a **certain logic** and a **certain approach** and set **pragmatic priorities in order to make** optimum use of the available resources. In this context, it is also important to keep reminding oneself of the logic and structure of the chosen strategy and measures and to reflect on why the chosen measures make sense and what goals they achieve. **Looking at the ecosystem** in which you find yourself and **constantly reviewing the context** also helps to achieve a holistic understanding. And finally, you must **always be aware** of the **risks** and align your decisions with them and the potential consequences of an attack. This mindset is fundamental to actively tackling projects to strengthen your own cyber resilience and to be ready if the worst should happen.

The panel discussion

The two presentations were followed by a high-caliber **panel discussion** moderated by **Fredy Müller**, Managing Director of FORUM SECURITY SWITZERLAND. In addition to the four speakers, **Franz Grüter** (Chairman of the Board of Directors of the green.ch Group; National Councilor SVP, LU) also took part in the panel discussion.

At the beginning, the moderator turned to **Franz Grüter** and wanted to know whether he was surprised by the findings from the input presentations.

He replied that he was not speaking as a member of the National Council, but in his role as an entrepreneur in the data center business and that Switzerland's prominent role in Europe should be emphasized first and foremost: **"We are one of the most important data locations in Europe, have a lot of infrastructure and are home to hubs for almost all major cloud providers. From there, we are naturally also exposed and an interesting target for attacks." The fact** that Switzerland is only ranked 42nd in the cyber security ranking was a new statistic for him. He attributes this to the fact that for a **long time, politicians were not sufficiently aware of the risks in cyberspace**. When he was elected to the National Council in 2015, he and a few other parliamentarians submitted the first initiatives on cyber security in parliament, and at the time they were not taken seriously by many. It was only with the major incidents, which then increasingly occurred in Switzerland from 2018 onwards, that the topic gained in importance and a rearmament began.

Espionage as a state instrument

After these introductory words, the moderator turned to **Dr. Myriam Dunn Cavelty** and asked her to go into more detail about the capabilities a state needs to be able to conduct espionage successfully.

She replied that the so-called **PETIO framework, which is** made up of the abbreviations for People, Exploits, Toolset, Infrastructure and Organization, is a widely used tool that describes which resources are required for offensive cyber operations. In the past, people imagined that a group of hackers in a

basement could carry out such operations, but this is not the case. **"It really requires specific, distinct capabilities and in this sense it is not surprising that the states that have already built up their capabilities in cyber space over decades a are also the ones that are most active today,**" she emphasized the high requirements for espionage activities in cyberspace.

Espionage had already been a common tool in the past. However, with the emergence of cyberspace, its occurrence has changed and accumulated. The moderator asked **Major General Setzer what the** emergence of this threat in a new guise means for the Bundeswehr in its everyday life.

It is true that espionage activities were already widespread in the past, but now they are also an essential tool of states in the cyber and information space dimension. The aim of espionage has always been data collection. Today, this data is stored in digital form on servers and in the cloud, making cyber espionage an obvious tool for many.

Conversely, it is of course necessary to set up protective functions to protect one's own systems against external intrusion, but also to set up the systems in such a way that they are protected internally. **"It can never be ruled out that an attacker will infiltrate a system, and in this case you need a functioning system for detection and response,**" said Major General Setzer, underlining the need for comprehensive protection. However, it is also important to her that protection is not simply a centralized approach. If civilians and soldiers are added together, there are around 270,000 employees in the Bundeswehr. They have appointed information security officers (ISBs) down to the lowest organizational element, so that they have a broad sensor network. Finally, it must also be said that although cyber espionage is currently widespread, if someone has already penetrated a network, espionage could at some point turn into sabotage and pose a threat to our critical infrastructures without crossing the threshold of armed conflict. He is happy to quote the military theorist Clausewitz here: war is not about destroying someone in principle, but about imposing your will on them. So if no military means are required for this and the threshold of war does not have to be crossed, then cyberspace is an appropriate means that can be used.

Cyberattacks in various forms

The moderator mentioned that cyberattacks do not always have to take the form of large-scale attacks, but that low-threshold, recurring attacks could also be very effective, and asked **Nicolas Mayencourt** whether he was also observing such activity.

He agreed and replied that low-threshold attacks can be very effective. Especially if there is no information hygiene and there are small leaks in many different places, an attacker can systematically collect valuable information over a period of years. In this way, complete information images could be generated without the need for major technical hacks to gain access. The "persistent" in the term "Advanced Persistent Threat" then also stands for this consistency and this is ultimately what differentiates it from traditional crime. Criminals are normally opportunistic and do not act persistently, but rather look for "easy" victims. Nicolas Mayencourt concluded as follows: **"So to protect yourself from criminals, you don't have to be the best protected, you should simply avoid being the worst protected.**"

The moderator then turned to **Dr. Myriam Dunn Cavelty** with the question of what role high-profile events such as the Snowden affair have played in ensuring that cyber security has become much more prominent in people's minds since 2010.

In her eyes, the interesting thing in this regard is that the Snowden affair brought the intelligence services into the public eye for the first time. It was only through this revelation that it became known that the **intelligence services in particular were active in cyberspace** and had built up corresponding capabilities. In her opinion, such events definitely have the potential to shape public awareness.

Strategic Competition

The moderator turned to **Major General Setzer** and asked him whether he also saw strategic competition, this competition, this concentration of power below the threshold of war, as a reason for the increase in cyberattacks.

Major General Setzer said that in order to ask the question of the reason for state cyber operations, one must always consider the question of the intention. China, for example, has set itself the goal of becoming the world's leading power in all areas by 2049 at the latest. When a country announces such a goal, it also organizes its entire strategy accordingly. In order to achieve this goal, China not only needs military power, but also influence in science, industry, and so on. Therefore, all available means, including cyber, would be used to achieve the goals set. However, it is important to note that **the traditional distinction between state actions in cyberspace and organized crime is often no longer easy to make these days.** Instead, there are sometimes even actors who work for the state during the day and on their own account at night.

Public attribution

The moderator led on to the phenomenon that cyber criminals, when they are convicted, are named very publicly, noting that much has already been said about the motives for cyber espionage and the skills required for it. He wanted to know from **Dr. Myriam Dunn Cavelty** why such a display of the perpetrators occurs.

There are two aspects: An IT security element should make it clear that these perpetrators, their methods and their tools are known and show that it is possible to protect oneself. The second aspect naturally also includes a political component, which is known as **public attribution** and **has** only existed **for around 10 years.** This is part of this strategic competition and has to do with the ability to potentially punish someone later.

The presenter wanted to know from **Major General Setzer** how effective punishment is carried out in cyberspace and how the Bundeswehr strikes back if they are attacked.

Major General Setzer replied that this was a very interesting question. The keyword **public attribution is** very important. In Germany, for example, it had taken over five years for the government to publicly attribute the attack on the Bundestag and name the attacker. Such attributions are considered very carefully from a strategic point of view, but they offer the opportunity to communicate to the attackers that **a certain limit has been reached**. His answer to the question of what would be done if the Bundeswehr was attacked in cyberspace and when the line to an armed conflict had been crossed could be summarized as follows. The NATO Secretary General had clearly stated that an attack in the cyber dimension, which would be equivalent in scale to a conventional attack in an armed conflict, would be responded to with the necessary means.

The moderator then turned to **Dr. Myriam Dunn Cavelty** with the question of whether classifying attacks according to patterns, as the Americans have been doing recently, would help to identify such attacks and their intentions.

Myriam Dunn Cavelty replied that the term "thinking in terms of campaigns" is used to describe this type of cyberattack. In the past, people used to think in terms of individual attacks, but at some point they realized that the perpetrators of such attacks were often similar actors. **It is often the case that the background behind attacks only becomes apparent when attacks are considered together, and that this only provides an overall picture.** For this reason, they have switched to looking at cumulative effects rather than individual effects. As a result, it is often possible to recognize that the effective consequences of attacks are even worse than the monetary consequences of the individual attacks because, for example, the information collected from the various attacks can be significantly more dangerous when accumulated.

Lack of information makes it difficult to assess the situation

The moderator then asked **Franz Grüter** how he assessed the situation for Switzerland in this context.

He began to refer to his time as President of the Foreign Affairs Committee. In this office, which he would continue to hold until the end of the year, they were confronted with two wars, the war in Ukraine and the war in Gaza. In order to carry out their tasks, they would partly obtain information from the intelligence service and even there it was clear that only a certain amount of information was passed on. That is why it is also difficult for him to fully assess the situation. He was therefore also unable to make a conclusive assessment for Switzerland in cyberspace.

Based on this answer, the moderator forwarded the question to **Nicolas Mayencourt** and also wanted to know whether strategic considerations for passing on information and maintaining the sovereignty of opinion within his own ranks were part of this game.

He replied that this was clearly the case and had become much more noticeable in the last 10 years. **Today, it can be observed that perception is systematically shaping the course of the war.** The war in Ukraine was the first time that perfectly orchestrated social media campaigns from both sides could be witnessed. Their influence on perception can therefore be very decisive, as they ultimately even have an impact on budget decisions. It is therefore quite normal that we cannot yet know many things about conventional or cyber warfare, as this knowledge is currently still of strategic relevance.

Johann Alessandroni was then asked whether he was aware that information flows are often filtered or orchestrated and how he perceives this in his work, as his work is aimed precisely at publicizing the dangers of cyberattacks.

He replied that they had also noticed that only certain trendy incidents were being reported in the press and media. However, they have also observed a sharp increase in incidents that are less noticed by the public. However, it would be important for all attacks to be publicly known and received, firstly

to make people aware of the dangers and secondly because a comprehensive understanding of the attack methods underlying these attacks could also be used to protect other systems.

New world - old technologies

The moderator referred to a preliminary discussion and noted that today's cyberspace is actually predestined to be attacked. He then asked **Nicolas Mayencourt** why this fact had not been recognized or addressed earlier.

He replied that the internet and information technology were built to make information accessible. The inventors of these technologies wanted to release and share information. He would almost call the situation he finds himself in today a success-disaster. **The technology was so good that society adapted and absorbed it as quickly as a dry sponge**. But these **technologies**, neither the internet protocol nor the chips, nor the paradigms of how software is developed, **were never built with IT security concepts in mind.** The founders and creators could not have imagined a world like the one we have today and would not have equipped the foundations of today's technologies accordingly. What he sees today is nothing more than the result of immature technologies being installed and attempts being made to close the gaps with a band-aid policy, which can never work completely because the basic technology fundamentally lacks security features. The engineer in him, at least, says that we should actually start with these foundations and revise them. But the man in him also recognizes that this will hardly be possible, because the whole world is already equipped with fundamentally vulnerable technologies.

The moderator passes the topic on to **Major General Setzer** and asks him whether the naming of the weaknesses of the Internet is a topic in their training courses and how they deal with the topic of successive disaster development.

He wanted to put one thing out of the way, namely that the internet and digitalization had brought them a long way forward. You now have to be careful not to throw the baby out with the bathwater. At the moment, they are gradually realizing that there are two sides to everything. However, you shouldn't suddenly scale everything back. In this competition that is being talked about, those who remain at the forefront of technology will at least last as long as the others. He used the common example of AI. AI is new software with new possibilities. These will be used, they are already being used. AI involves risks, but it can also help with information security and system protection. Accordingly, AI can be used to make the system more resilient, as it is able to detect anomalies in the system much faster than any human could. In development, the focus is therefore not just on "fighting the problem", from the point of view that everything they have is bad, but mainly on how existing systems can be improved. He mentions three keywords in this regard. One is "**security by design"** for future systems, so that security code will be included from the outset. Secondly, the people who work with it need to be trained so that they can use it appropriately, particularly with regard to **social engineering**. And thirdly, and this is the biggest challenge, they need to create procedures for the "**legacy systems**" in order to eliminate their vulnerabilities. If possible, these should be replaced by adequate, future systems. But his philosophy is not to bury his head in the sand, but to continue to drive digitalization and security forward at the forefront.

Analogization instead of digitalization?

The presenter followed this up by asking **Nicolas Mayencourt** whether it wouldn't be better if we spent less time in the digital world and more time in the analog world again, making us less reliant on AI to process big data. With a slightly ironic touch, the presenter asked whether it wouldn't be better if we wrote down our passwords on a piece of paper again rather than storing them on the internet.

Nicolas Mayencourt replied that there is a basic rule: **"If you don't move with the times, you move with the times."** Digitalization is here to stay and is bringing many good things with it. He can only agree with that. There are many, many positive aspects. His vote at this point would be to stop being naive. We should take digitalization and cyberspace seriously and treat them with the necessary respect. Considering an operating system for a nuclear power plant where the license agreement states "not fit for any purpose" and any liability is excluded is simply fundamentally wrong. That could not be the point of the matter. This is exactly where you should start and perhaps not only ask yourself what you can do, but also whether it makes sense and how you can do it sensibly. He was saying: yes, don't stop, but proceed in a more controlled and better way.

International regulations

After this answer, the moderator addressed the suggestion that an international set of rules could be created and asked **Dr. Myriam Dunn Cavelty** whether this was a topic that still had a future.

She replies that this is clearly the case and that there are already **standards and rules at** various levels, for example in **NATO** or the **UN**. Of course, regulations are also being discussed; they already exist in the EU and in Switzerland. In the USA, it has also become very clear since this year that there is a desire for increased regulation in the IT sector. She also said that not everything had to be regulated, but that the subsequent implementation had to be approached head on. However, she believes that we will manage this if the will is there.

Nicolas Mayencourt added that we had been there before. As an illustrative example, he pointed out **the development of the car,** to which some parallels can be drawn. Initially, there were no seat belts, but due to the accumulation of serious accidents, a whole set of safety regulations was developed over time, which is why we now have seat belts, airbags and driving licenses. This system has reduced the extent of damage to such an extent that it is now within acceptable limits. In addition, there is the international communications union, without which no telephone network would exist today. Many things are also very well regulated there. For a long time, however, the attitude towards the Internet was that it could not be controlled anyway, which was and still is wrong. The possibilities already existed, we also had the necessary organizations, we simply had to use them.

Towards the end, the moderator turns to **Franz Grüter** again with a question. He wanted to know whether, in his opinion, the development of a cyber council in Geneva, whereby Switzerland could assume a leading role in this regard, seemed realistic.

He said that he saw two possible initiatives. In the first case, Luxembourg had unfortunately beaten them to it by developing an **e-embassy.** This is comparable to an international airport where international law applies. For example, the **ICRC**, the International Committee of the Red Cross, stores **its highly sensitive data** there. Their data is therefore located in a non-governmental, international area. The data is now in Luxembourg. Estonia also set up a complete secondary infrastructure in Luxembourg after the Russian cyberattack in 2007. In his opinion, Switzerland had overslept this. They could probably still build it, because in his opinion a similar digital space would suit Geneva very well.

The moderator asked to what extent the unique topography of Switzerland and associated structures such as the Gotthard tunnel could be an advantage by establishing data centers there.

Franz Grüter replied that there are certainly examples where data centers have been built in bunkers. He is always pleased about these projects because they help **Switzerland's reputation as a data bunker.** In reality, the risks to the stored data are not of a physical nature; they are not classic burglars who would steal a surfer there, but hacker attacks. A data center in a bunker is just as poorly or well protected against such attacks as a conventional data center.

Audience questions

Finally, the presenter opened the question and answer session to the audience.

Adrian Marti, who works for the company Ereneos, then spoke up. He said that they themselves are consultants for information security at large organizations. In his eyes, the most important thing is for security to become a **grassroots movement** and wanted to know from the speakers how this goal could be achieved.

The moderator, visibly pleased with the question, said that this would have been his final question, but that Adrian Marti had beaten him to it. He therefore turned to the panelists with the question of how safety awareness could be raised in general.

Nicolas Mayencourt replied that he believed we needed something like an **update to our social contract,** because it would require something like a "mind-update" from all of us. **Security is fundamentally a team sport** that needs us all, otherwise it won't work. Therefore, the roles, rights and duties of each organization should be discussed. We need to ask ourselves what Mr. and Mrs. Swiss are doing, what the economy is doing, what research is doing, what the state is doing, what the military is doing - and the most important questions that need to be asked are how we know border protection today and whether we need something similar in cyberspace. He then passed the ball to the political representatives.

The moderator made the transition and addressed the question of how we can become more resilient and security-conscious to **Franz Grüter**.

As has already been mentioned, he was recently in the Baltic States and also in Israel before the war broke out. People there often say that there is sometimes a certain "**naivety" in Switzerland** due to the many years of peace. We are sometimes too little aware of what is really going on in the world. Despite everything, a positive conclusion can be drawn here; a rethink has taken place. It is not known whether eight or ten years ago so many people could have gathered here on such a topic as today. Today, however, people have become more aware of this and companies are making great efforts, for example hiring specialists to advise them, and the state has also made progress. Next year, for example, the Federal Office for Cyber Security will be established at the federal level.

For his closing remarks, the moderator turned to **Major General Setzer once again** and asked him how he felt that the population, and young people in particular, had become more security-conscious.

He noted that young people are probably much better at dealing with digitalization than his generation was. However, there is also a need among young people that is currently still being neglected. Awareness must also be raised in educational institutions. In his view, this is something that needs to be increased, as security is a team sport that starts with the individual, as mentioned above. **Cyber attacks usually start with the weakest link in the chain**. Therefore, digitalization and cyber security is not a matter that only a few people need to take care of, but concerns everyone. In this context, the support of the proposed awareness days can only be endorsed.

Last but not least, the moderator put the final question to **Dr. Myriam Dunn Cavelty**.

She indicated that she had actually wanted to communicate what the General had said: **Education and training were definitely required and necessary**. She would also like to see people who are afraid of technology overcome this fear and realize that it is also in their hands, as the system is a man-made system, which means that it can also be changed. To do this, however, people would have to overcome

their fear. In general, this is a very human issue and she would like to see people given more will to act in this area in the future.

This concluded the panel discussion and the moderator thanked the audience for their attention and the panelists for the interesting discussion.

FORUM SECURITY SWITZERLAND

c/o MUELLER Consulting & Partner
Gemeindestrasse 48
CH-8032 Zürich

Phone +41 44 533 04 00
sekretariat@forum-sicherheit-schweiz.ch