Cybersecurity Technologies

An Overview of Trends & Activities in Switzerland and Abroad

January 2022

Impressum

Michael Tsesmelis[1], Dimitri Percia David[2], Thomas Maillart[2], Kilian Cuche[3], Ljiljana Dolamic[1], Giorgio Tresoldi[1], William Lacube[1], Colin Barschel[1], Quentin Ladetto[4], Claudia Schärer[5], Vincent Lenders[1], Alain Mermoud[1].

[1] Cyber-Defence Campus, armasuisse Science and Technology
[2] Information Science Institute, Geneva School of Economics and Management, University of Geneva
[3] Armed Forces Command Support Organisation, Swiss Armed Forces
[4] Research Management and Operations Research, armasuisse Science and Technology
[5] Swiss Academy of Engineering Sciences

Abstract

Several severe cyberincidents are pushing the Swiss federal government to take extensive measures against cyberthreats. The National Strategy for the protection of Switzerland against Cyber risks 2018-2022 (NCS) details the various measures that the government is implementing to adapt Switzerland to the emerging cybersecurity challenges. The NCS delegates to the Cyber-Defence Campus (CYD Campus) of armasuisse S + T the role of monitoring cybersecurity trends. For this purpose, the CYD Campus and its stakeholders from academia and industry have developed qualitative and quantitative technology-intelligence methods for early identification and anticipation of technology development. This report focuses on four technologies of importance for cybersecurity: 5G, Big Data & Machine Learning, Blockchain and Contact-Tracing methods. Interest in these emerging technologies is quickly gathering pace, as is visible thanks to data analytics methods using data on job openings, patents and publications. Relevant startups and companies in Switzerland and abroad have also been identified through data-driven methods and with the help of scouting efforts in startup centers around the world. Overall, this report describes the efforts to identify, analyse and forecast trends related to cybersecurity technologies. Therefore, the insights therein allow for more informed decision-making in technology investment, technology assessment, as well as technology roadmapping.

Corresponding author: alain.mermoud@ar.admin.ch

This work was partially supported by armasuisse Science and Technology and the National Center for Cyber Security. It solely represents the views of the authors.

Table of Contents

Preface

With cybersecurity topics becoming increasingly prevalent nowadays, it has become imperative to inform business and political leaders as well as casual readers about developments in the field. This report aims to provide insights on emerging technologies and startups pushing the state-of-the-art in the industry. The analysis will pay particular attention to Switzerland and its institutions, with dedicated descriptions of the Swiss startup landscape in cybersecurity. Several private and public institutions are surveilling the current technology landscape, and their research will be presented as well.

Chapter 1 will describe the current political motivations and initiatives taking place in Switzerland to make the country more resilient in the cyber world. This political push is driving technology monitoring activities across different institutions, and **Chapter 2** will focus on the Cyber-Defence Campus of armasuisse Science and Technology to illustrate the process of cybersecurity technology identification. Amongst these technologies, **Chapter 3** selects four and describes their potential for the industry in more detail. **Chapter 4** describes the tools and methodologies that different researchers use to monitor technological developments. **Chapter 5** uses the scouting efforts of the Cyber-Defence Campus to illustrate the dense and successful network of cybersecurity startups in Switzerland and abroad. The report will conclude with **Chapter 6**.

Chapter 1

A National Push into Cyberdefence

Recent developments

In the last few years, cybersecurity incidents have hit major public and private institutions. From data breaches at technology companies (Manancourt & Cerulus, 2021), to infamous targeting of news agencies, cyberattacks have become common in today's world. Switzerland, as a pole of innovation and excellence, has naturally not been spared. In 2014, the main Swiss defence firm RUAG suffered a severe breach (swissinfo, 2018), and only three years later the **Swiss federal departments of Defence and Foreign Affairs** were attacked as well (swissinfo, 2017).

To meet these new challenges, the entire cybersecurity ecosystem has greatly expanded in recent years. The public, private and academic sectors are intensifying their efforts to increase the level of security and resilience of society to cyber threats. The government has also actively joined the efforts, and has since 2010 increasingly made cyberdefence a **national security priority**. In order to respond to these new threats, Switzerland has developed the **National strategy for the protection of Switzerland against cyber risks 2018-2022** (NCS), which is already in its second version (NCSC, 2018).

Moreover, the Federal Department of Defence, Civil Protection and Sport (DDPS) has developed in 2017 its own plan called the **Action Plan for Cyber Defence (APCD)**. In April 2021, the **Cyber Strategy DDPS** was adopted (DDPS, 2021). These national strategies present measures to be implemented within the federal administration and beyond, in order to increase Switzerland's cyberdefence and resilience. This report inscribes itself in these efforts by presenting the latest research and technologies in the field.

Some statistics by the National Cyber Security Center (NCSC)

80%	of ransomware incidents target small and medium-sized companies
5'152	cyberincidents registered by the NCSC in the first semester of 2020
57%	of those reports were for fraud
80%	of companies have reported at least one breach of their cloud data in the past 18 months
> $100,000	the average ransomware payment

Source: (NCSC, 2020)

Switzerland, a leader in cybersecurity innovation

Switzerland is undeniably one of the most innovative countries in the world, especially thanks to its leading research centers such as EPFL (Lausanne) and ETHZ (Zurich). A recent report by Bloomberg (Jamrisko et al, 2021) ranks the country third in innovation across the world and at the top in Europe. This statement also translates well in the realm of cybersecurity. **BAK Economics**, an independent Swiss research institute, published a ranking of global innovation according to the number of high-quality patent applications in each country (2021). The combination of patent activity and patent quality results in a value for each individual patent. For each technology, the 10% best valued patents are calculated. These patents are defined as "high quality". In cybersecurity, Switzerland's relatively small size does not hinder it from entering the top ranking countries with the most active high-quality patents (**Figure 1**). Furthermore, proportional to the Swiss population's size, the country's ranking is even higher (**Figure 2**).

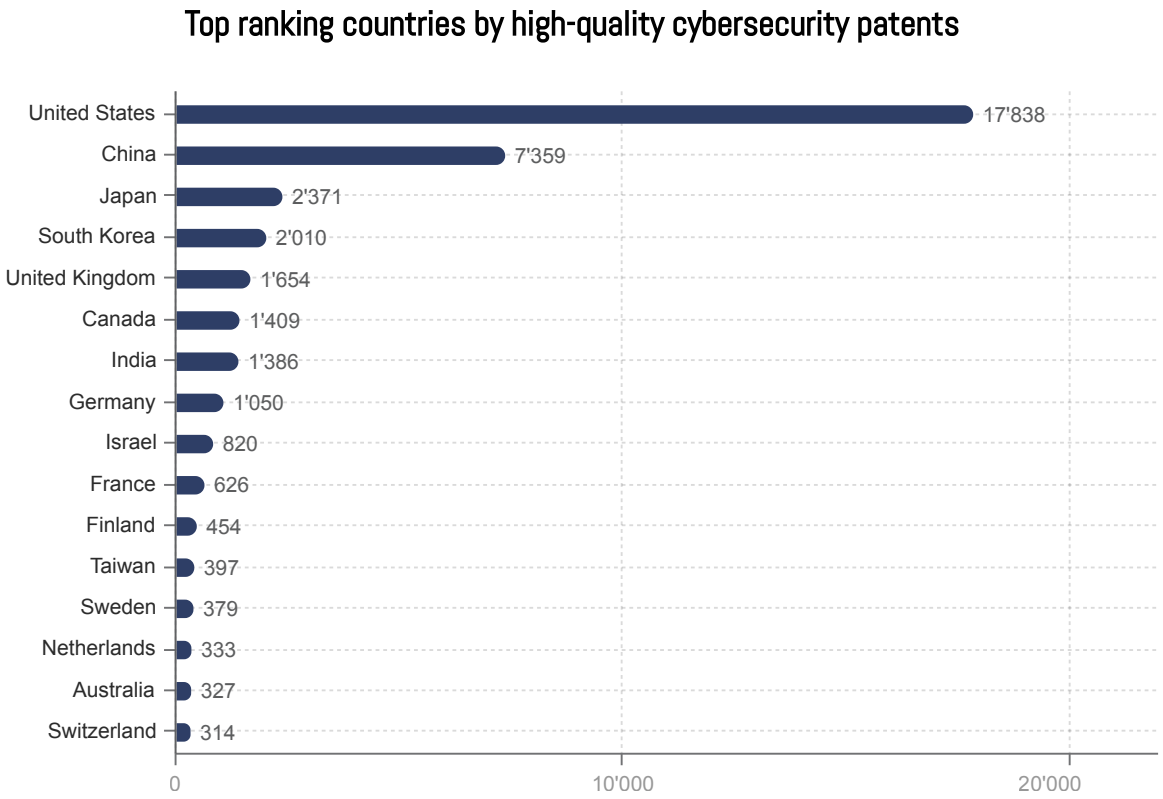


Figure 1: Top ranking countries by high-quality cybersecurity patents in 2020 (BAK, 2021). Finland and Israel are interesting comparison countries, as they are similar in size to Switzerland. Despite its focus on innovation, Switzerland ranks behind these two countries.

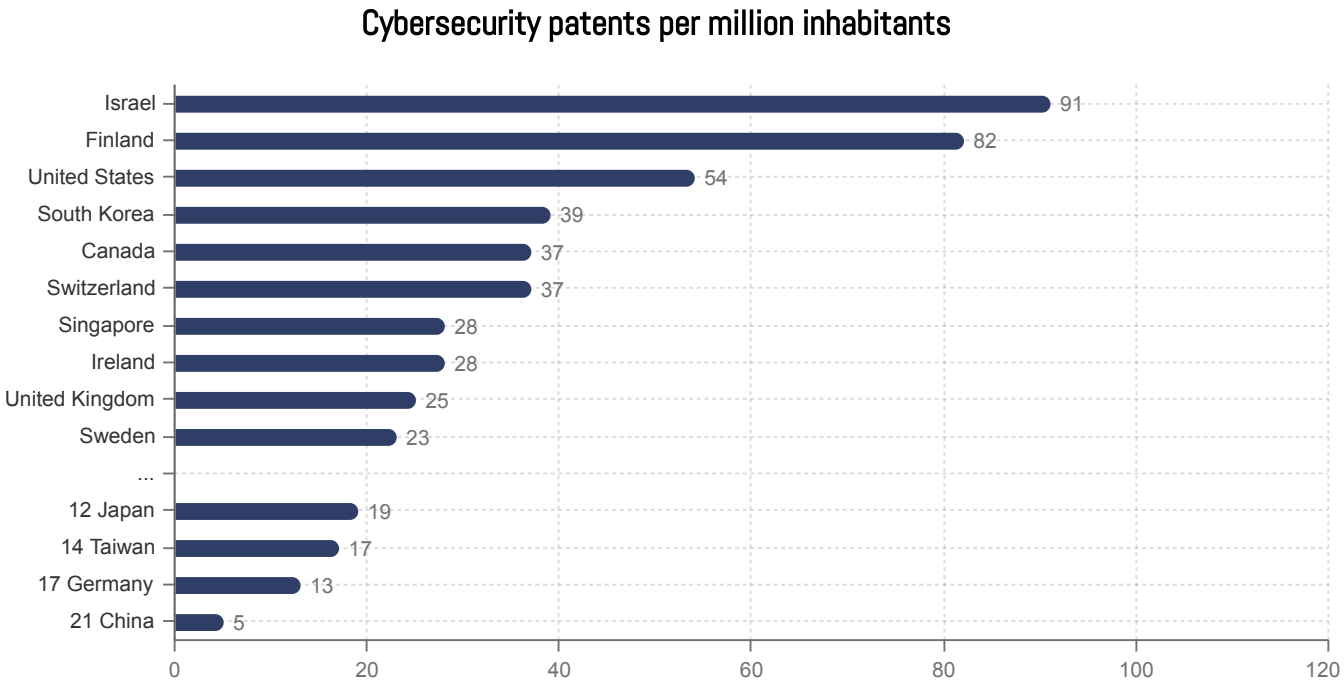


Figure 2: Country ranking by high-quality cybersecurity patents per million inhabitants in 2020 (BAK, 2021).

Major players in the cybersecurity industry are typically located in and around major Swiss metropolitan areas, such as Zurich, Geneva, Lausanne, Bern, Basel and Lugano. The Swiss Cyber Map locates public, academic and private actors in Switzerland (Cuche, 2020b). According to the map, the private sector clearly outnumbers both remaining categories. Swiss public institutions such as universities make scientific discoveries, which private companies then turn into products. Access the Swiss Cyber Map here: To the map

The importance of trend monitoring in the defence sector

Early detection of trends in the domain of cybersecurity is essential for a proper assessment of current and future capabilities. In the 20th century, armies and their research centers were often a source of great technological innovations. The Defense Advanced Research Projects Agency (DARPA), the research and development arm of the United States' Department of Defense, is credited with inventing ground-breaking technologies ranging from the Internet to drones (DARPA, 2021). However, in the 21st century, armies are no longer leading the technological trends of the digital age. The traditional screening and development methods of defence organisations are too slow to keep up with the ever-increasing privatisation of innovation. In this context, a continuously increasing gap (**Figure 3**) has been created between the technological state of the civil sector and that of the defence sector.

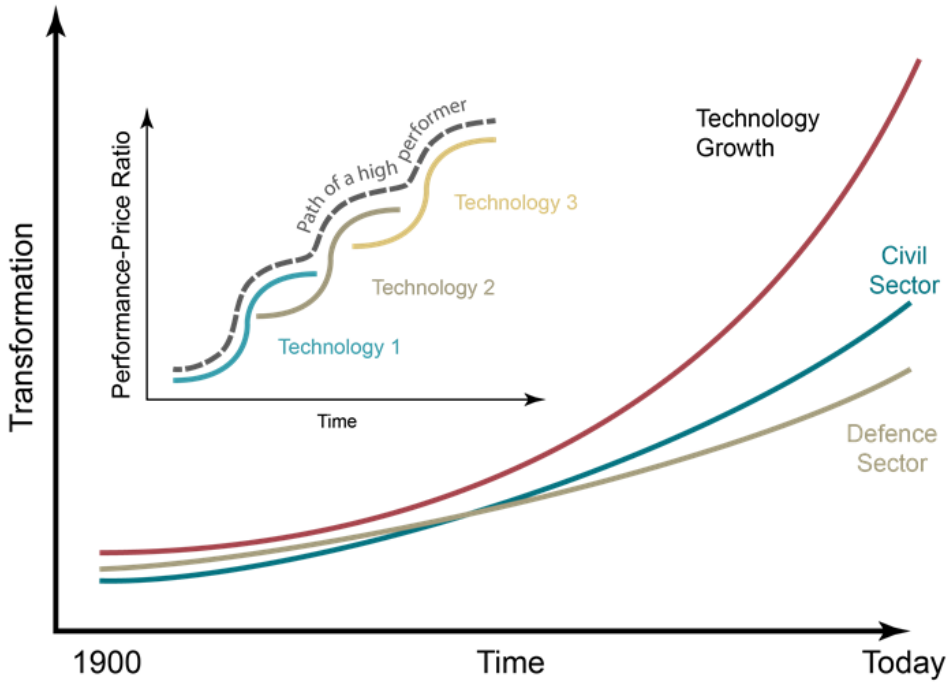


Figure 3: There exists a widening gap between the technology level in the civil sector compared to that in the defence sector. A technology market monitoring activity may reduce this gap by improving the defence sector's knowledge about the technology landscape.

Monitoring activities in Switzerland

The National strategy for the protection of Switzerland against cyber risks 2018-2022 (NCS) coordinates the efforts occuring at the Swiss federal level regarding cybersecurity, cyberdefence and cybercriminality. Its founding purpose is to guard against all types of cyber threats, a list which includes cyber crime, cyber espionage, cyber sabotage and cyber terrorism, disinformation & propaganda, and finally cyber conflicts. The NCS implements a plan of action in order to work on these issues, and this plan distinguishes between ten spheres of action, each of which addresses a different aspect of cybersecurity (Federal Council, 2021). Measures are then delegated among the various responsible agencies in the government and guided by the NCS steering committee with representatives from the private sector, universities, and the government to ensure the strategic coherence and to continuously monitor the strategy's progress.

In this regard, **armasuisse** (the Federal Office for Defence Procurement) has been assigned a leading role. Under its auspices was founded the **Cyber-Defence Campus (CYD Campus)**, which sits at the intersection between academic institutions such as EPFL and ETHZ, the cyber industry and the federal administration (CYD Campus, 2021). In the context of the NCS, the role of the CYD Campus is the "Early identification of trends and technologies and knowledge building (M1)". Chapter 2 will introduce the CYD Campus' methods for technology identification.

Chapter 2

A Search For Relevant Technologies

Security-Relevant Technology and Industry Base

In order to keep pace with developments in the security industry, the Federal Department of Defence, Civil Protection and Sport (DDPS) must maintain current and reliable knowledge about technologies available on the market. The most relevant technologies for Switzerland's security should be listed within the **security-relevant technological and industrial base (STIB)**. STIB is made up of all research institutions and companies that have competencies, capabilities and capacities in the security and defence sector and thus form a vital part of the Swiss armaments policy and strategy (armasuisse, 2021a). The overview of these institutions is to be provided by a digital market- and technology-monitoring tool (TMM).

The main purpose of STIB is to guarantee Swiss sovereignty in its armaments policy (Schüpbach et al., 2021). Switzerland in particular must consider this aspect because, as a neutral state that does not belong to any defence alliance, it is not entitled to military support from other states. The STIB should contribute to reducing Switzerland's dependence on foreign countries in defined areas of armament policy. It should be able to ensure a certain level of technological expertise and industrial capability within Switzerland, including in new fields such as cybersecurity.

armasuisse has formed a Center of Excellence (CoE) STIB that coordinates the various instruments for steering and strengthening the STIB and ensures the strategic significance of these instruments. In addition, the CoE regularly reviews their effectiveness and degree of strategic goal achievement. The assessment is made by experts from different competence areas of armasuisse.

In 2016 however, the manually-maintained STIB database was outdated and with that came the need to create a new monitoring application. Out of this mission was born the **Technology and Market Monitoring (TMM)** platform. TMM 1.0 has superseded the STIB database since 2017 and, using open source data, provides users with a list of relevant companies in Switzerland according to the technology cluster searched for. Information on job openings in the industry, the amount of patents and the number of publications are also available on the platform. Its successor **TMM 2.0** will be extended further by considering more specific needs of different stakeholders and tailoring the application to those requirements. More specifically, the goal of TMM 2.0 is to integrate financial data into the platform, to enable a "follow the money" strategy where evidence of industry trends are extrapolated from market investments. In order to assist in the development of the TMM 2.0 tool, an analysis of the context, stakeholders and user needs was conducted among the relevant actors for the platform. TMM 2.0 shall offer quantitative information to drive acquisition decisions, particularly for government procurement agencies.

The literature around technology market monitoring is quite abundant; books such as Daim & Yalcin (2022), Daim et al. (2016) and Porter et al. (2011) are deep studies into the field of forecasting and technology management. Many practical projects however tend to use patents as the only data source, and fail to integrate the output into a user-friendly format readily available for decision-makers. For instance, Jun et al (2012) construct a technology-forecasting tool using patent clustering techniques. Jin-Ho et al. (2011) complement this simplified analysis by adding a keyword analysis on top of it. TMM on the other hand seeks also to integrate data from job postings and financial investments into a unified platform.

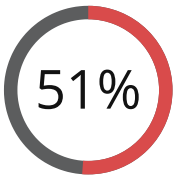
Several third-party applications such as Amplyfi and Gartner can also produce industrial insights. However, their methodologies often rely on qualitative assessments of technologies, and their database contains limited information on Swiss companies. TMM on the other hand is calibrated on the Swiss market.

Figure 4: The Technology and Market Monitoring platform aggregates market data about various technologies.

A use case: offsetting defence contracts

When Switzerland purchases armaments for more than 20 million Swiss Francs from abroad, the foreign manufacturer is generally obliged to compensate the contractual amount by an economic participation in the Swiss industry. Such cases are called **offsetting** initatives (armasuisse, 2021c). Particularly interesting from the point of view of market-monitoring technologies is the fact that **100%** of the compensation benefits must be invested in **STIB-relevant firms**.

CHF 1'354 million in armament purchases in 2020



Percentage that needs to be offset

CHF 685 million in offset amount

Consulting the oracles

Measuring how relevant specific emerging technologies are is no easy feat. However, because these innovations are the product of the work of many scientists and managers, it is a natural solution to consult them for their knowledge. This is traditionally called the **Delphi** method (RAND, 2021); experts answer several questionnaires related to the discussion at hand, and finally the analysis aggregates the opinions and a group decision is derived. This is a robust qualitative method for initial investigation, and is a solid way to gauge the importance of different cybersecurity technologies..

Following this methodology, around twenty armasuisse experts from the CYD Campus came together and, given a list of cybersecurity technologies such as Cryptology and Firewalls, rated each of them on two scales. First, the experts were asked to assess the relative strength of Switzerland's cyberdefence capabilities with regard to a specific technology. This was done on a scale from 1 to 10. Secondly, the experts had to rate the strategic importance of the technology, based on a time horizon of three years. This in effect gauged the general attractiveness of the technology. Overall, the experts handed in opinions on 28 cybersecurity and 20 computer-science technologies. They then discussed their ratings and agreed on a final mark for every technology.

On the right side, the **Strategic Importance (SI)** score is plotted against the **Relative Strength (RS)** score. Each technology can be added to the two dimensional plot, and depending on its location, will fall in one of four categories. Superfluous strengths have a low SI but high RS, and thus highlight very overvalued technologies, perhaps those that might need less attention in the future. On the other hand, key weaknesses need additional effort and encouragement in order to drive them up into the key strengths quadrant. The ideal places are of course the key strengths zone or the zone of irrelevance, for that is where organisational resources are utilised most efficiently.

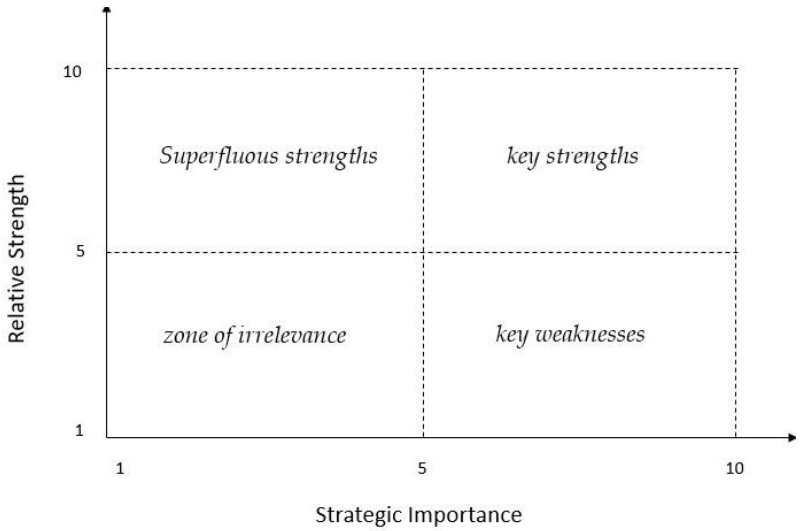


Figure 5: The methodology used by the CYD campus scores technologies based on their Strategic Importance and Relative Strength (Westkämper, 2006, p. 8)

Figure 6 gives a high-level declassified overview of important technologies for Switzerland and in what capability areas they can be applied. The general trend on the RS-SI graph (not shown in this report) is a straight line from the bottom left to the top right, and this in effect represents the ideal portfolio of technologies; irrelevant ones are shown little attention, and critical technologies receive resources and devotion and are therefore relatively developed within the organisation. Chapter 3 will present some of these technologies in more detail.

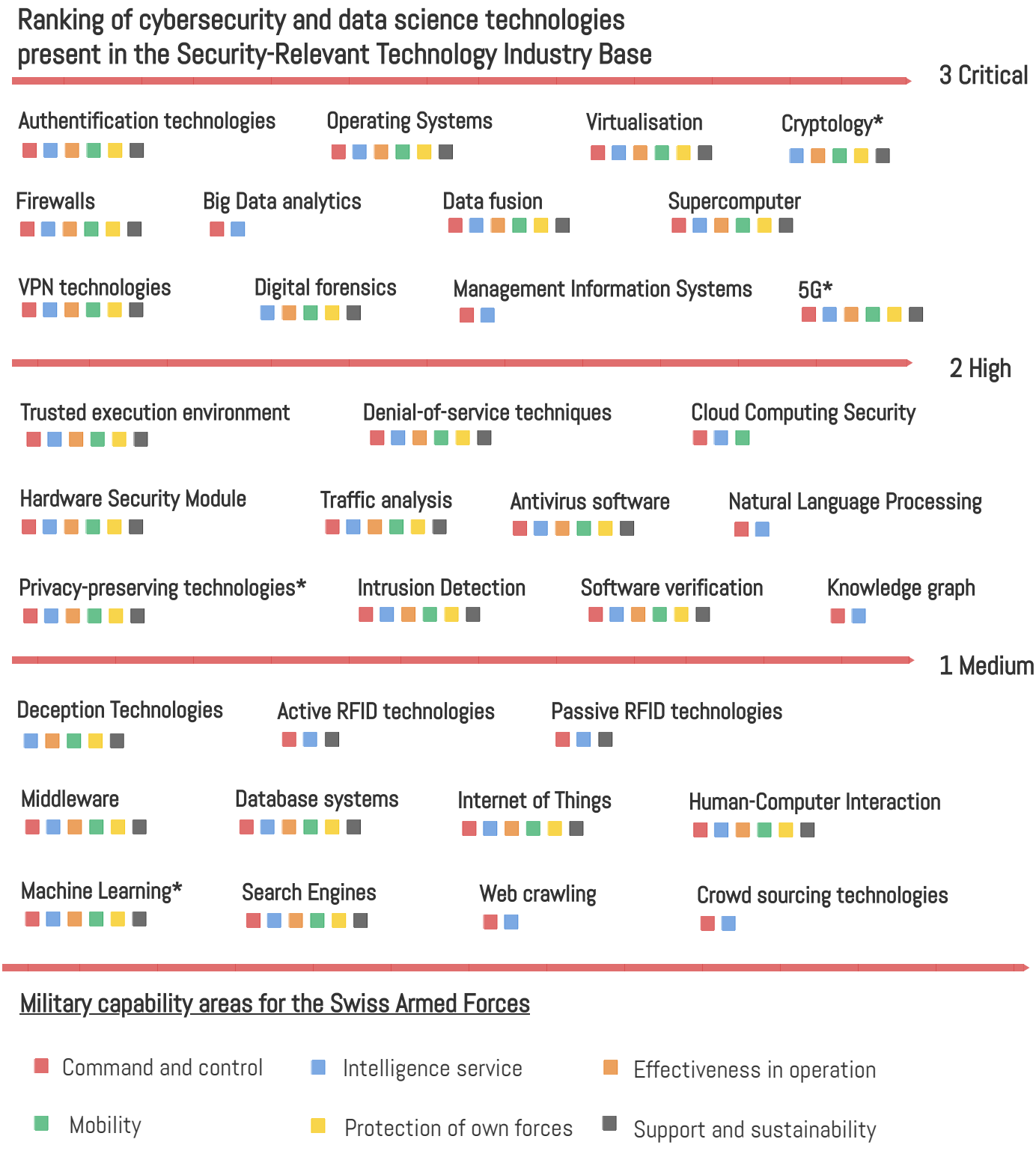


Figure 6: High-level declassified summary of the results of the workshop. Each technology is ranked according to its security relevance, which is based on the production sovereignty of Switzerland in that field, as well as the strategic management capabilities and readiness level of the Swiss Armed Forces. The technologies are also linked to their domains of use. Technologies with a (*) are mentioned again later. A list of security-relevant industrial sectors can be found online:

To the page

.

Chapter 3

Technologies in Focus

A shortlist

This chapter seeks to explain more thoroughly some of the technologies that are currently relevant for Switzerland's cybersecurity strategy. The list in the previous chapter was a compilation of security-relevant focus technologies that were deemed relevant for cybersecurity in Switzerland. From this compilation, we select four technologies for a short portrait. 5G is chosen because of the rapid deployment of its network. Cryptology is looked at through the lens of Blockchain, a record-keeping technology which has witnessed rapid growth these last few years. Big Data and Machine Learning were chosen due to the immense advances in both fields which are triggering innovations in many industries. Finally, the analysis of Privacy-preserving technologies takes place by discussing Contact Tracing, a very pertinent technology in the age of COVID-19. To summarise, the following chapter will present these four technologies:

- 5G
- Blockchain
- Big Data & Machine Learning (ML)
- Contact Tracing

3.1 5G Technologies

A rather new technology building on the success of its predecessors, this fifth-generation of mobile networking allows for **high-bandwidth** (up to several Gigabytes of data per second), **low latency**, and a massive increase in **availability** of connection. 5G's impact will be perhaps most visible in **mobility** (SATW, 2021a). Whether passengers are using bicycles, electric scooters, driverless cars or battery-powered buses, the way we get from point A to B is being remodeled, this time in technology and engineering centers. Intelligent mobility is arising through the interaction of transportation means, and thanks to 5G's extensive network, information can flow almost instantly between road users. Once 5G becomes fully operational, real-time knowledge about a vehicle's surroundings will optimise transportation; cars will know where available parking is located, ambulances will reliably determine the quickest journey to people in need of assistance, and traffic lights connected to a central command will efficiently mitigate traffic jams and remove bottlenecks (SATW, 2021a).

Beyond transportation, the substantial benefits of 5G will be felt in many other fields (SATW, 2021b, p. 31). **Mobile users** can expect significant improvements in connection speeds and quality, and applications can leverage this feature to offer better and more data-hungry services to customers – think real-time high quality streaming services. Moreover, industrial companies are preparing to roll out the technology to get immediate and remote access to their assembly lines, all with the end goal of streamlining the whole production, maybe even automating parts of it. Finally, pilot projects are experimenting with 5G in other industries as well, such as farming and tourism.

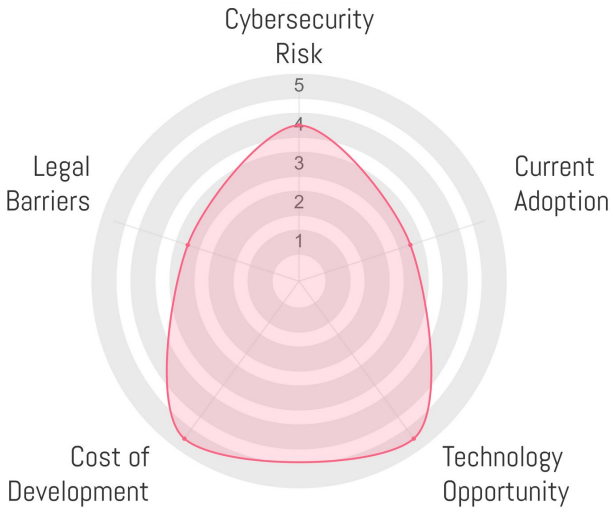


Figure 7: Radar chart showing 5G's strengths and weaknesses

Up to 1 million
connected devices per square km

98 countries

Up to 100x
more bandwidth than current networks

Source: (BAKOM, 2021)

Switzerland is among the world's leading countries in terms of network deployment. However, restrictive radiation protection regulations and refusals by municipalities and cantons are slowing down the nationwide rollout and making the deployment of the technology very expensive by international comparison. At the European-Union level, the target is to expand the network to all urban and transportation zones by 2025, which will surely affect the Swiss market as well (SATW, 2021b, p. 31). Regarding the economic value of the implementation of 5G, by 2030 5G technologies will generate a production value of over CHF 40 billion, of which around 88% should flow to users.

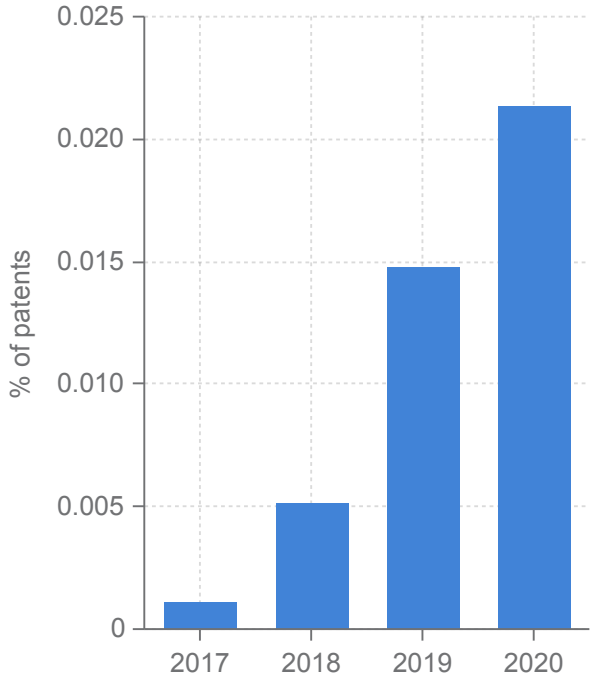


Figure 8: Percentage of total registered patents in Switzerland that relate to 5G (TMM, 2021).

Soaring interest

The TMM platform gathers timely information about 5G technologies, including information on active companies in the sector, granted patents and scientific publications. **Figure 8** shows that an increasing percentage of Swiss patents relate to 5G. Another useful resource in gauging the popularity of the technology is Google Search trends. Below, **Figure 9** shows how over a span of five years, the interest of the general population in 3G and 4G has slowly eroded, and 5G overtook both in 2019. On the next page, **Figure 10** shows the normalised amount of publications related to 5G. Clearly, there has been a steady rise in the amount of those publications, although growth has slowed down since 2017.

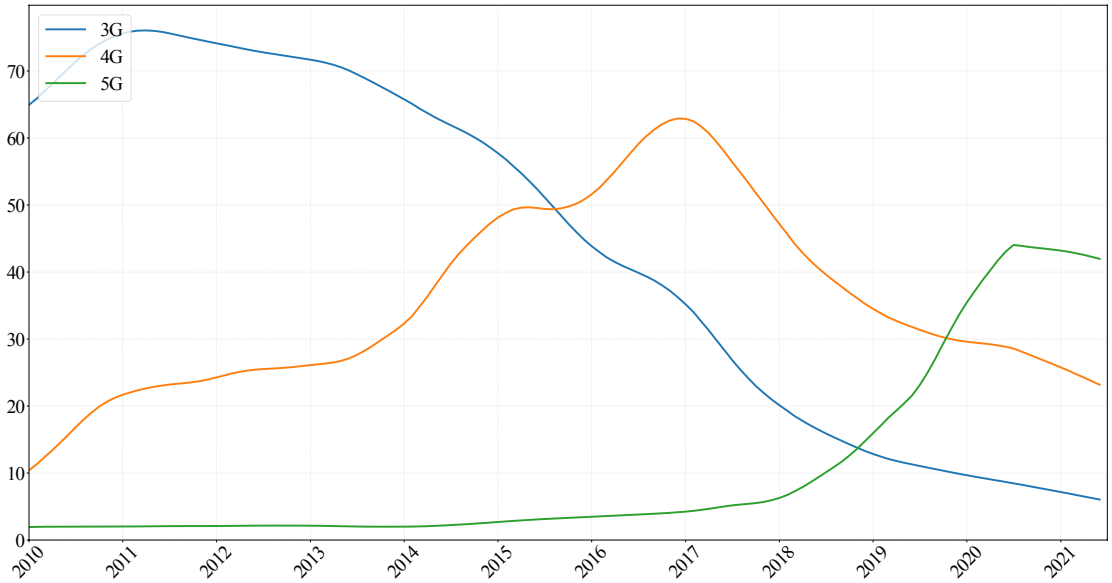


Figure 9: Search trends for 5G (green), 4G (orange) and 3G (blue) (Google Trends, 2021). The vertical axis represents the index of Google Search (a proxy for the interest captured by Google Search across various regions and languages). Such an index is used to compare the search volume of different queries throughout time. The data was cleaned using the LOESS method, which decomposes a time-series into its trend, seasonal and residual components. Only the trend is plotted on the graph above.

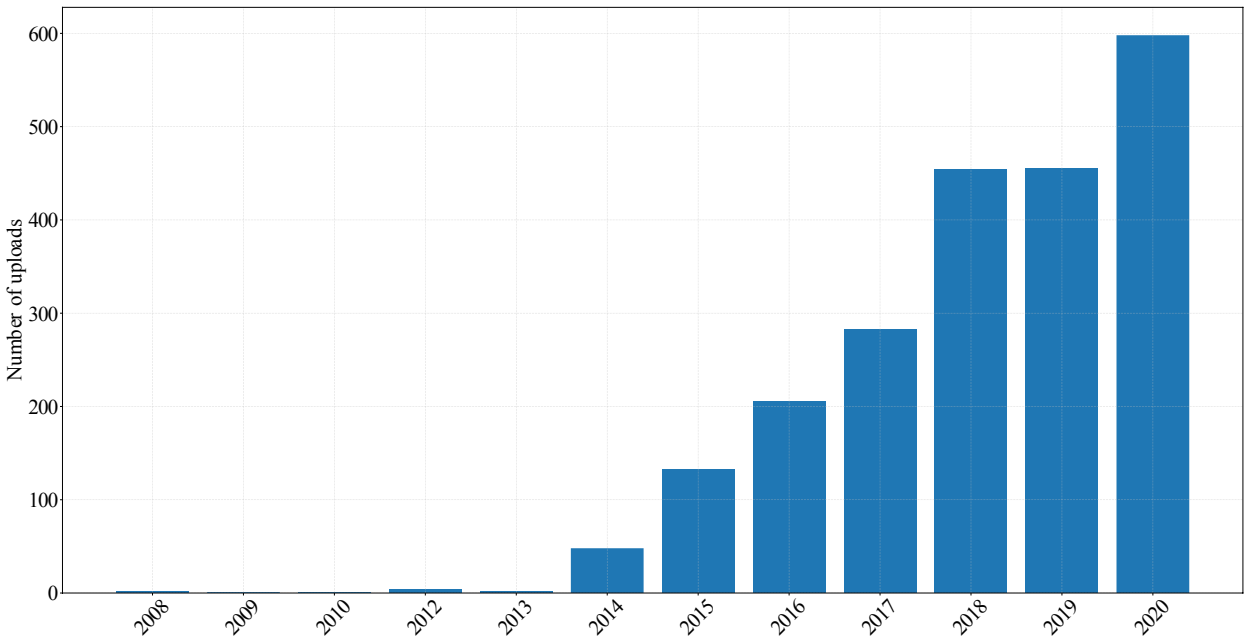


Figure 10: Amount of e-prints related to 5G, from 2014 to 2021 (CYD Campus, 2021). Such a statistic considers uploads of 5G-related papers to the arXiv repository, which is a relevant proxy for academic research worldwide. The rise in 5G-related publications is clear.

Security

Connecting millions of devices and transferring sensitive and real-time information amongst them using 5G quickly becomes a cybersecurity issue. Connected devices must be safe, robust and the data they exchange must remain private. However, experts at Ericsson, a leading 5G technology vendor, believe that 5G holds substantial benefits over its predecessors when it comes to securing online sessions (Ericsson, 2021). All traffic data which is sent over the 5G radio network is protected by end-to-end encryption. The integrity of the data is protected as well; the data sent out cannot be tampered with on the way to its destination. Finally, the device and the network will mutually authenticate in order to create a trusted connection.

On the industry side, Nokia and Ericsson are the two main European manufacturers of 5G equipment. A report published in 2019 by the European Commission and European Agency for Cybersecurity details the security issues surrounding 5G. The report warns against using a single supplier for a carrier's 5G infrastructure, especially those based outside the European Union. Due to fears of potential espionage of users for some vendors and their equipment, several countries (including the United States, Australia and the United Kingdom as of early 2019) have taken actions to restrict or eliminate the use of technologies from companies considered untrustworthy. **Figure 11** on the next page shows that most 5G research money comes from China, followed by the European Union and the USA.

Figure 11: Number of 5G result counts in Web of Science Core Collection Publications, breakdown by funding agencies.

The specific threats for 5G are similar to previous vulnerabilities in 3G and 4G systems. Mainly, devices connected to the network are vulnerable to malware infection. The consequences of an intrusion can vary drastically according to the scenario. Telecommunication data is particularly valuable, as it contains location data and sensitive information like messages and voice conversations between high government officials or decision makers. Conversely, remote industrial spying is also enabled by the onboarding of so many industrial devices onto the network. Overall though, the engineering behind 5G should reduce unlawful access to the network and should thus create a more trustworthy web of connections between devices.

The CYD Campus has carried out its own investigation into 5G. Holtrup et al. (2021) posits that, although 5G holds substantial security and privacy benefits over 4G, these can only be reaped with a proper implementation by the network carriers, otherwise the vulnerabilities persist. Furthermore, 5G's new functionalities will also bring about new attack vectors. Overall though, 5G's security is being carefully monitored and should therefore be a suitable successor to the 4G network.

3.2 Big Data & Machine Learning

"Big data refers to extremely large sets of structured and unstructured data that cannot be handled with traditional methods. Big data analytics can make sense of the data by uncovering trends and patterns. Machine learning can accelerate this process with the help of decision-making algorithms. It can categorize the incoming data, recognize patterns and translate the data into insights helpful for business operations."

Chithrai Mani, Forbes

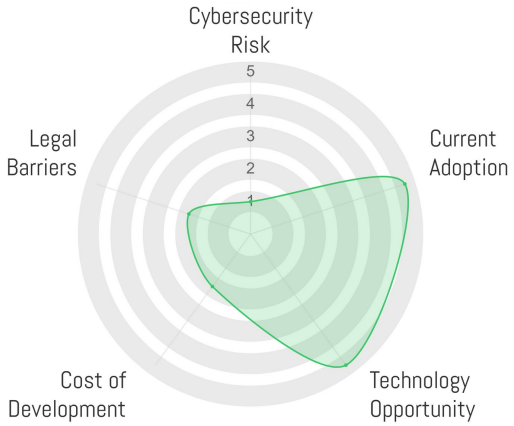


Figure 12: Radar chart showing Big Data's strengths and weaknesses

Big Data's popularity is driven by the rise of two interlinked technologies. On the one hand, Machine Learning (ML) is a technology that makes use of data to derive conclusions about future events. The predicitve power of Machine Learning algorithms improves with experience, meaning the more data they are fed, the better they become. On the other hand, Big Data is also strongly connected to the field of **Artificial Intelligence (AI)**, the umbrella technology sitting above Machine Learning and which seeks to artificially replicate human intelligence. "AI" has become a catchall term to describe any advancements in computing, systems and technology in which computer programs can perform tasks or solve problems that require the kind of reasoning we associate with human intelligence, even learning from past processes (Stahl, 2021). Because many software companies offer access to AI-driven software sitting on remote clouds, small and medium companies can access a range of services delivered by cloud providers that simplify the adoption, customisation and use of AI technologies for Big Data analytics. This removes previous barriers to recruiting or developing skills internally and investing in infrastructure. However, there are also challenges standing in Big Data's rise. In terms of current issues, **data governance and security** continue to be a priority and are becoming important decision criteria for companies looking to adopt commercial solutions for Big Data analytics. Additionally, data is increasingly seen as a private good by individuals, and thus lawmakers are scrambling to legislate on the ownership and rights associated with certain types of personal data.

Quantifying the rise

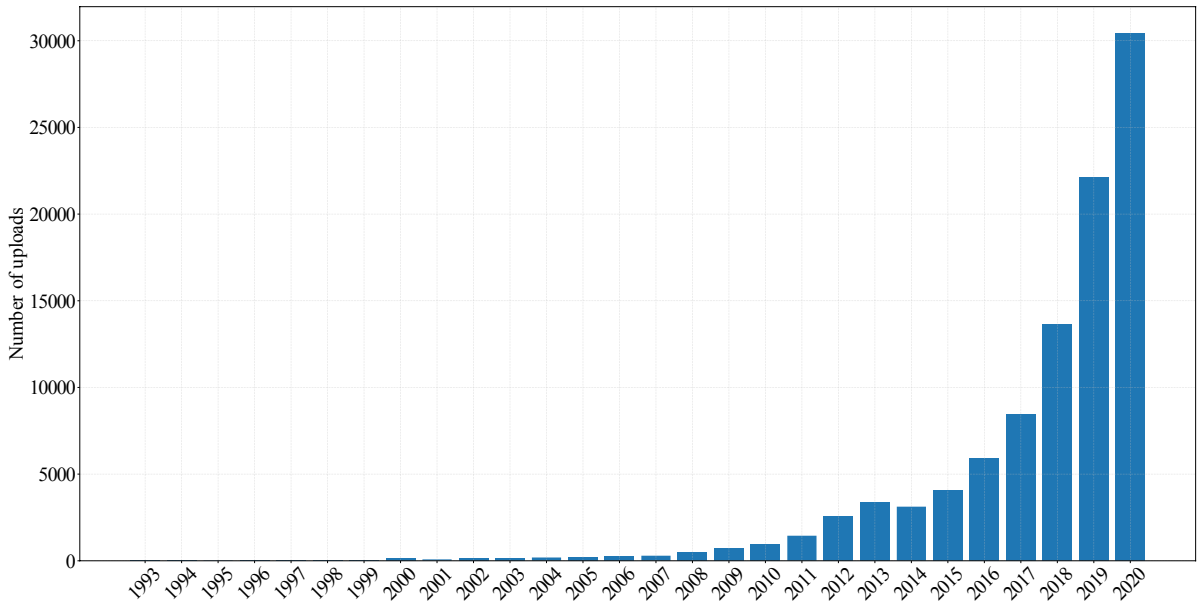


Figure 13: Amount of e-prints related to Artificial Intelligence, from 1993 to 2020 (CYD Campus, 2021). Such a statistic considers uploads of AI-related papers to the arXiv repository, which is a relevant proxy for academic research worldwide.

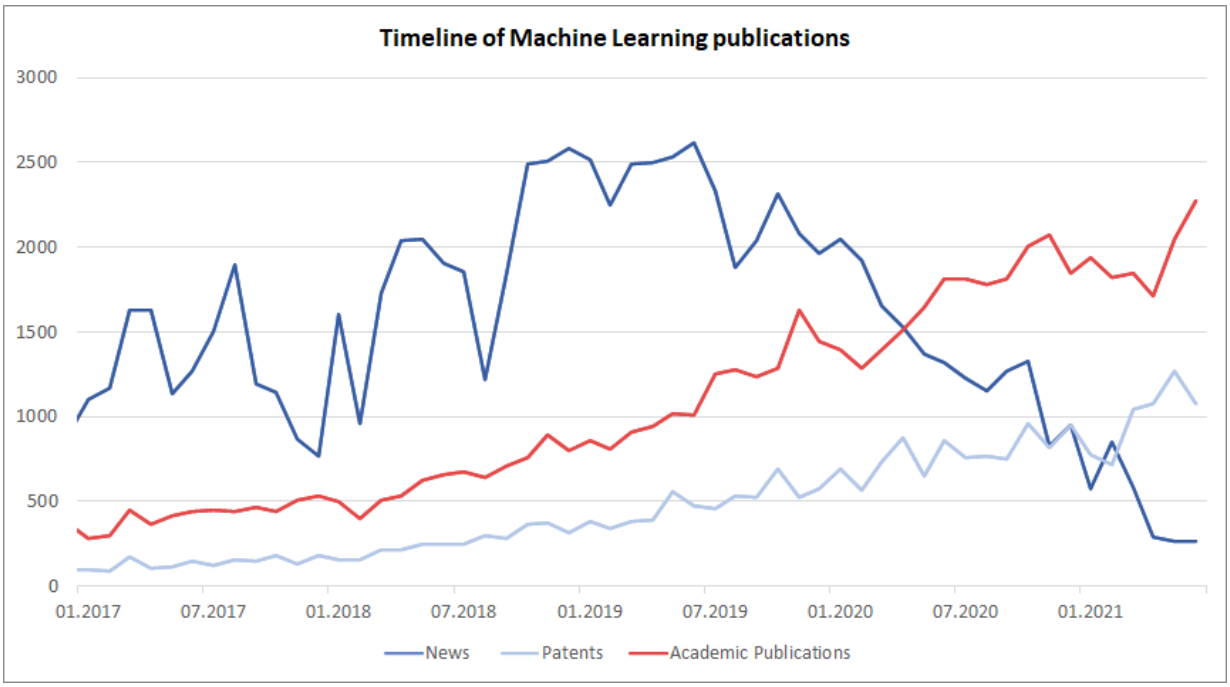


Figure 14: Timeline of publications related to Machine Learning (Amplyfi, 2021). Between the end of 2016 and mid-2019, the technology was mainly talked about in the news. Only later did patents and academic publications take over. Clearly, there is an increasing scientific interest in Machine Learning models.

3.3 Blockchain

In 2008, in his seminal work on Bitcoin, Satoshi Nakamoto introduced a data structure ("a chain of blocks") as well as a consensus mechanism that enables a set of entities to maintain the general ledger of a currency in a **distributed manner** (Gambazzi et al, 2021, p. 2). The construction provides security guarantees as long as more than half of the entities participating in the distributed network are honest. Parts of the difficulty and confusion when talking about "Blockchains" stems from the fact that there is no precise definition of what a "Blockchain" is. Some consider the whole ecosystem, including all its components, such as the consensus mechanism, the execution environment for a scripting language running on the participating nodes, etc. as "the Blockchain", while others restrict the focus on the underlying data structure that consists of blocks containing data and which build a chain. Blocks are tied-up using cryptographic primitives in such a way that it is impossible to modify the blocks' content or to rearrange the blocks, thus resulting in an **immutable chain.**

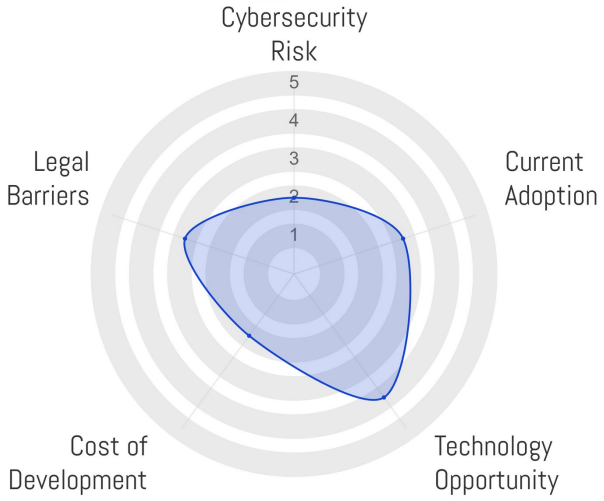


Figure 15: Radar chart showing Blockchain's strengths and weaknesses

Blockchain's emergence

The CYD Campus estimates that the future potential of Blockchain is high to very high. Indeed, according to a report on Blockchain and distributed ledgers (Gambazzi et al, 2021, p. 8), the technology is being introduced in a great variety of fields; **logistics** (Maersk plans to optimize its container logistics), **retail** (IBM and Walmart are developing a solution for food safety), **insurance** (B3i is developing a smart contract solution for insurance contracts), energy (Axpo is developing a solution for peer-to-peer energy markets), **transportation** (Novotrans stores inventory level data for railway repairs) or **public administration** (the Netherlands is developing a border control system for passenger data). **Many Swiss companies** are also implementing Blockchain strategies.

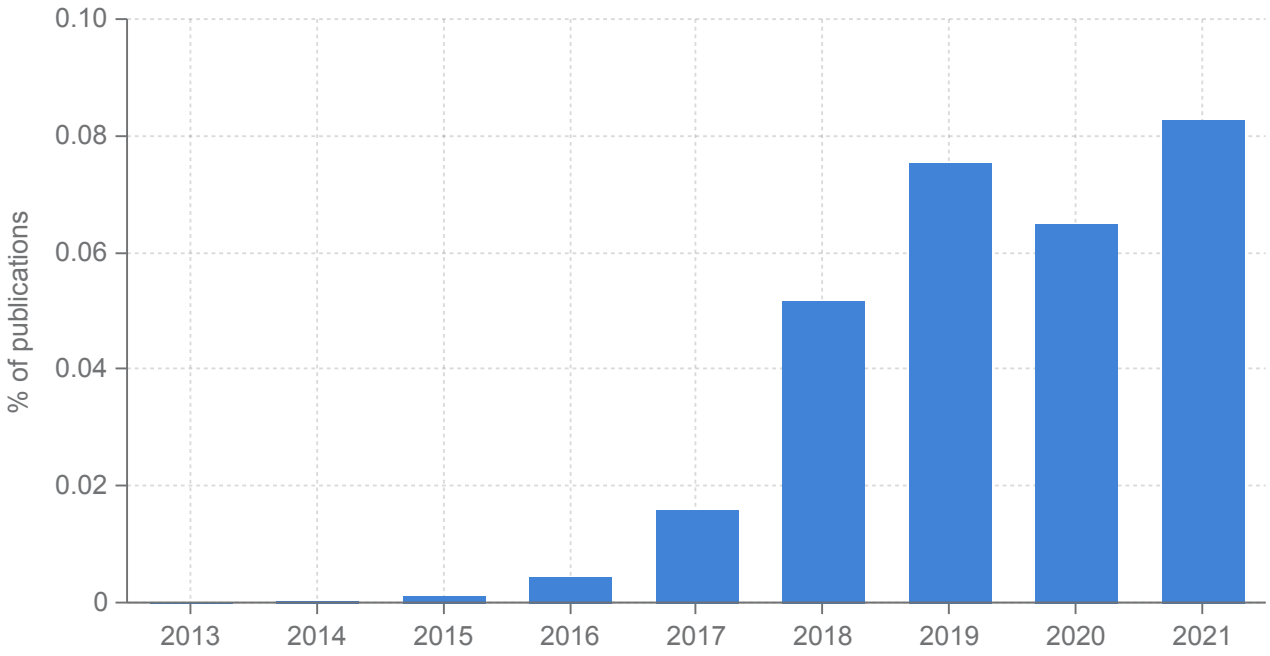


Figure 16: Academic publications referring to Blockchain technology (TMM, 2021). After a clear hype in the research activities related to Blockchain, from 2019 onwards, the same research activities are plateauing. Such a graph indicates that the academic interest in Blockchain is losing speed.

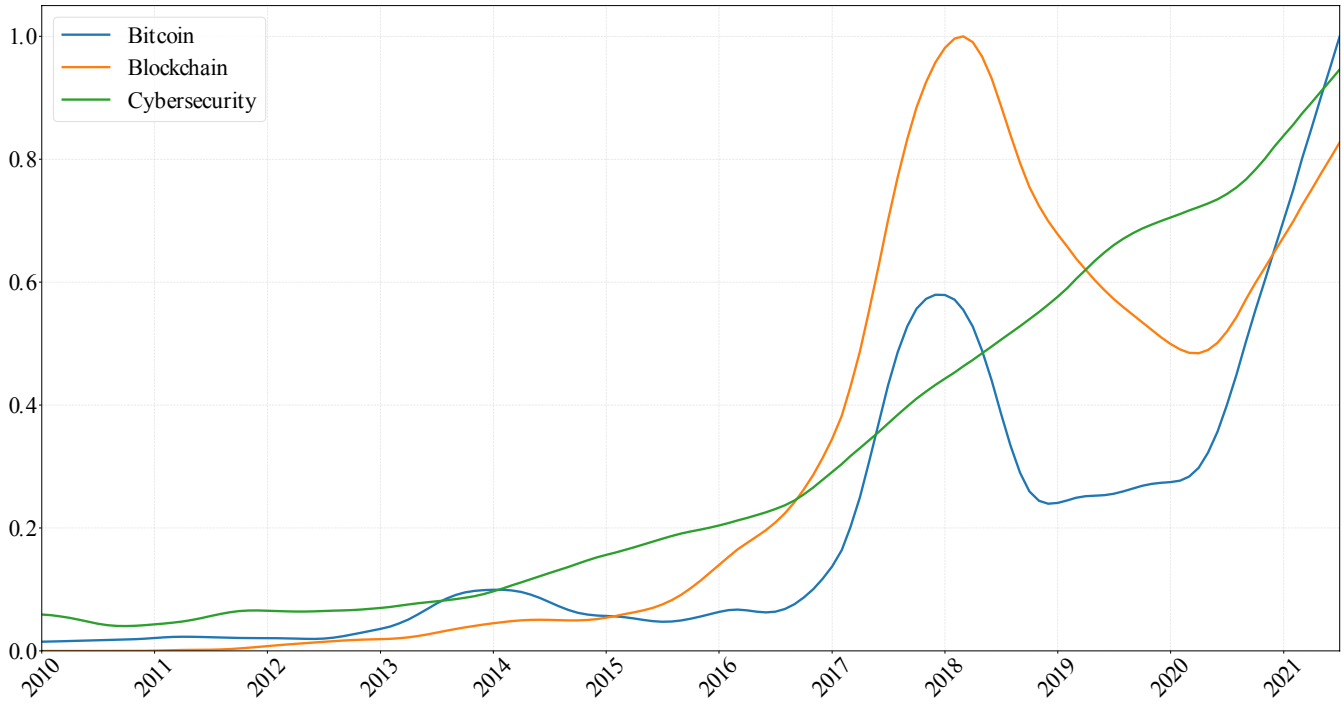
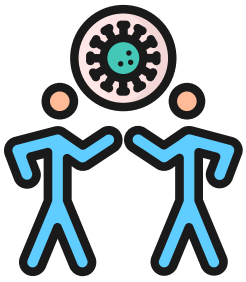


Figure 17: Google search history for Blockchain, Bitcoin (a cryptocurrency built on Blockchain technology) and Cybersecurity (Google Trends, 2021) . The periods of high interest in blockchain at the end of 2017 and beginning of 2021 coincide with large price increases of cryptocurrencies based on Blockchain technology

Blockchain in cybersecurity

The CYD Campus technology review (Gambazzi et al, 2021) concludes that using an open or permissioned Blockchain is justifiable when multiple mutually mistrusting entities want to interact in order to change the state of a system, and are not willing to agree on an online trusted third-party. A Blockchain can then be implemented for instance to enhance supply chain for logistics and procurement in the army. Integrating Blockchain within each step of an operation to secure and share data throughout the manufacturing process, including design, prototyping, testing, and production, may help improve the general knowledge of all entities in the network. Finally, research is also being done on applications of Blockchain for messaging applications, which would use a decentralised structure to send data across devices. These ideas are however only in their infancy, and this fact highlights the need for more advanced research in the field.

3.4 Contact Tracing



The 2020 COVID-19 pandemic has led to a global lockdown with severe health and economic consequences. As a result, authorities around the globe have expressed the need for better tools to monitor the spread of the virus and to notify the general population of any critical developments. Researchers and technology companies such as Google and Apple have offered to develop the tools and interfaces necessary for mobile **Contact Tracing** applications. The goal of these applications is to continuously track people's movements and to notify smartphone users about their past proximity to people who have tested positive to COVID, with the end goal of getting potentially infected people to self-quarantine and test themselves for the virus. A fundamental challenge with these smartphone-based contact tracing technologies is to ensure the security and privacy of their users. Moving from manual to smartphone-based contact tracing creates new **cyber risks** that could suddenly affect the entire population. Major risks include for example the **abuse of people's private data** by companies and/or authorities, or the **spreading of wrong alerts** by malicious users in order to force individuals to go into quarantine (Legendre et al, 2020, p. 3).

The Swiss population is concerned about these new risks and 40% of the population fears that a smartphone-based Contact Tracing system could be turned into mass surveillance and also believes that such an approach will simply not work with too many false notifications (Legendre et al, 2020, p. 3). armasuisse S+T studied Contact Tracing apps in the context of cybersecurity. Their findings show that these apps can broadly be categorised into three subgroups, depending on which signals are used to locate mobile users (Legendre et al, 2020, p. 6). These are:

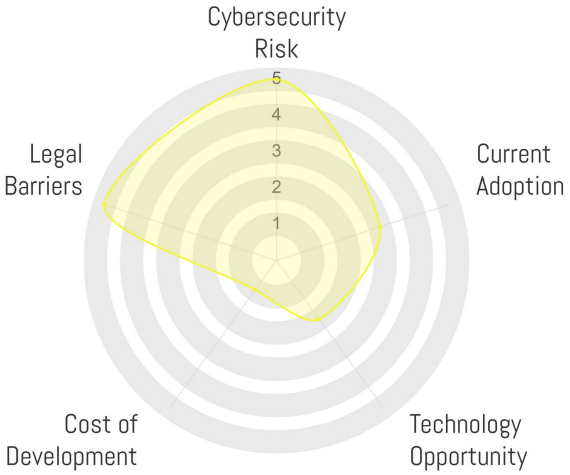


Figure 18: Radar Chart showing Contact Tracing's strengths and weaknesses

- **Mobile Operator Contact Tracing** - The location of a mobile phone can be determined on the mobile operator side using the network infrastructure. Multilateration of radio signals between cell towers can locate a phone with an accuracy of +/-140m in urban areas and up to several kilometers in rural areas. The main advantage of the technology is that it is non-intrusive and can be put in place without any user intervention assuming a legal framework is in place. When applied to Contact Tracing, the main drawback is the poor accuracy and the serious privacy concerns that entail mapping a diagnosed individual's location trail with all the other individuals' trail who have crossed paths.

- **Location-based Contact Tracing** - Smartphones can locate themselves using their on-device capabilities. Those include GPS for precise location, which however mostly works outdoors (+/-2m). For indoors where most encounters happen, device-side cell tower multilateration and crowd-sourced WiFi localisation (+/-10m) can be used. With newer WiFi access-points, indoor WiFi multilateration brings the accuracy down to 1-2 meters. Those capabilities combined have the main advantage of being more accurate than multilateration performed by the mobile operators alone but have the main drawback of requiring users to install a dedicated application on their phone.

- **Proximity-based Contact Tracing** - While location-based contact tracing requires an absolute geographical location, technologies such as Bluetooth and WiFi allow inferring the relative proximity of smartphones by transmitting a small-range signal that others can hear and record (up to 50 metres outdoors and 25 metres indoors for Bluetooth). Those technologies have the main advantage of not having to disclose one's absolute location and offer a finer estimation of distance, especially indoors. It shares the similar drawback of location-based contact tracing requiring users to install an application.

Cybersecurity risks

The study by Legendre et al. (2020, p. 8-23) illustrates the cybersecurity threats that arise with these applications. The most concerning cybersecurity attack is the one that generates **false alarms** (either to targeted people or to large numbers of users) for various malicious purposes. One key threat is to send false alarms to employees of critical infrastructures (power plants, military bases, etc.). A typical scenario is one where the attacker can recruit someone with symptoms and get his phone. The attacker with the borrowed phone can then get in close contact with the targeted employees. When the person with symptoms gets positively tested at the hospital, it will raise an alarm to all exposed employees and recommend for them to stay in quarantine (until they get tested themselves). A more technically sophisticated approach is to relay Bluetooth signals of users that are or might be diagnosed soon (e.g., by staying close to a testing center). **Figure 19** on the next page illustrates such an attack carried out by Dave and Bob.

The description of **Figure 19** is as follows. Bob stays close to Alice who is currently at a test center because of her symptoms. She will soon be diagnosed positive with COVID-19. Bob listens to the messages that Alice is sending (1). He relays those over the Internet to Dave (2 and 3). Dave is close to his target and replays Alice's notifications as if they were sent by her own phone. When Alice is confirmed positive and the target receives Alice's diagnosis key from the health authority, it will receive a notification saying he has been exposed to the virus.

Such attacks can also be carried out remotely, using a satellite to relay signals of infected or soon to be diagnosed individuals living in a rogue state [4G over satellite, SMS from satellite] (4 and 5). The decentralised approach would be particularly prone to this attack as opposed to a centralised approach where the health authority has a complete oversight of notifications and can detect such attacks when done en masse (i.e. "mass notifications").

Overall, Contact Tracing remains a contentious topic. The TMM platform could not highlight any major trends in the area, as it is only in its infancy, a fact that underlines the importance of further research for the time being.

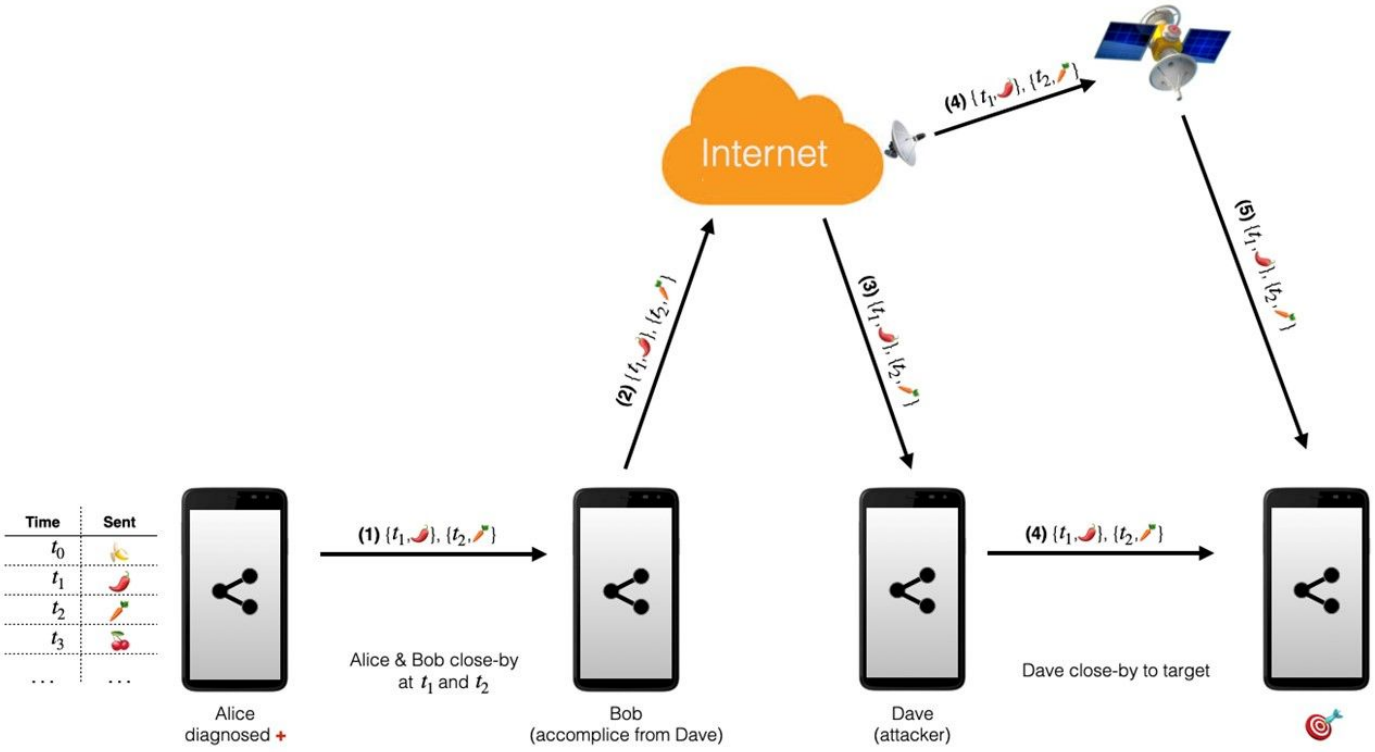


Figure 19: Attack vectors using contact tracing apps (Legendre et al, 2020)

Chapter 4

Modus Operandi

A step-by step walkthrough

One central aspect of technological forecasting is related to detecting and forecasting trends in technological development. To assess such trends, researchers and practitioners have developed different qualitative approaches and models. However, most of them have raised criticisms, especially when it comes to providing empirical evidence. One such model is the Gartner curve, designed by the consultancy firm Gartner. This curves tries to describe the trajectory of innovation clusters throughout time. **Figure 20** depicts this model. According to Gartner, technologies go first through a phase of inflation and hype, until they reach a peak where disillusionment starts to settle in, after which expectations for the technology crash. With time however, the sentiment heals and progressively attracts interest again. This chapter will nuance these statements by presenting the latest research by four experts in technology monitoring.

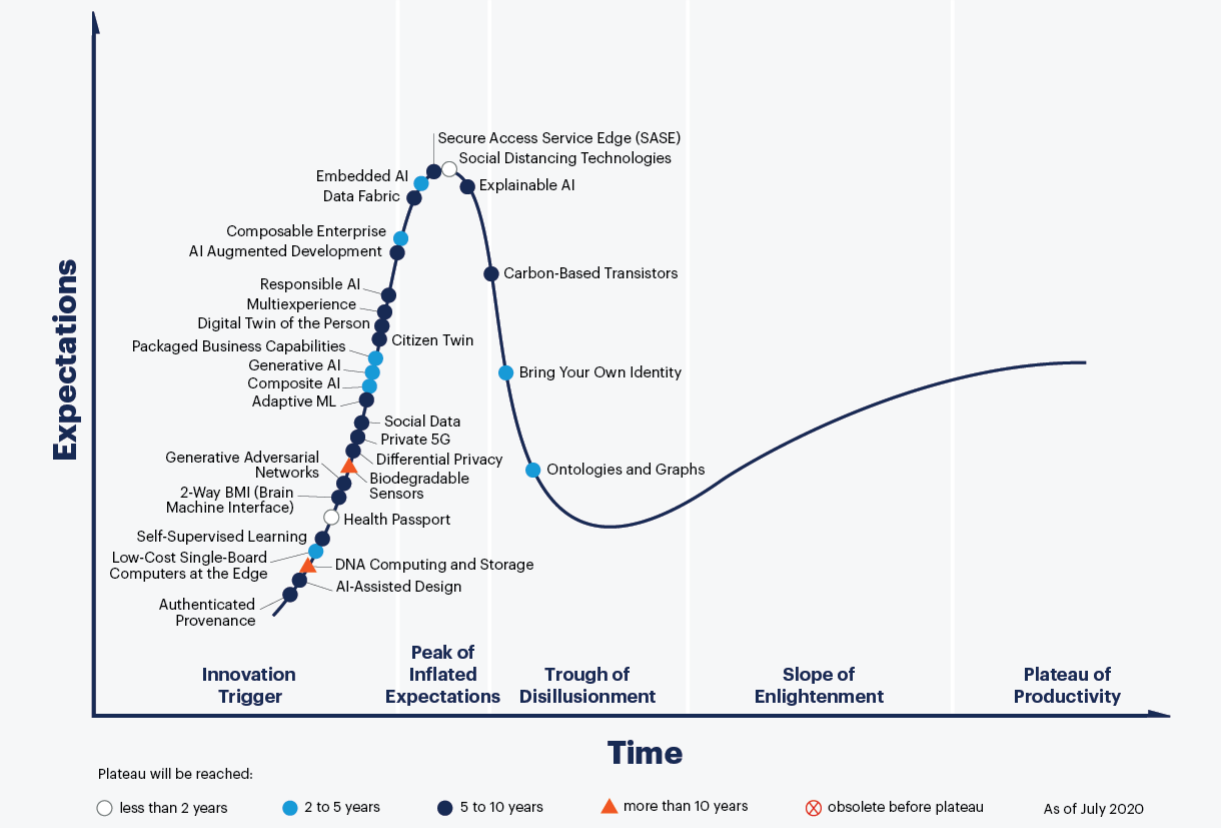


Figure 20: Hype Cycle for Emerging Technologies (Gartner 2021). This cycle is supposed to represent the maturity, the adoption and the social application of many emerging technologies.

4.1 Technology Market Monitoring

Dr. Dimitri Percia David (armasuisse 2020; Ličina, 2020), a Distinguished CYD Postdoctoral Research Fellow from the University of Geneva, is investigating whether the Gartner Curve rings true with reality by using a quantitative approach. Already, several back-testing analyses of the well-known Gartner model of technology adoption and maturity show that, in practice, most of the important technologies adopted since 2000 could not have been identified in their early stage of adoption. This problem is recurrent in other qualitative technology-management indicators such as the Gartner Magic Quadrant, the Rogers' bell curve, or the Technology-Readiness Level (TRL) approach. Theories about diffusion generally cannot account for all variables, and thus might miss critical predictors of universal adoption.

To detect general trends and changes in technological development, Dr. Percia David incorporates various indicators coming from both private- and open-source data. His indicators mainly stem from a bibliometric analysis related to scientific publications, patents, industry-market indicators, or a mix of them. In this aspect, text-mining methods and network analytics are particularly helpful for technology forecasting. Dr. Percia David has explored two approaches to his quantitative method: first, an analysis of e-prints of scientific papers on arXiv using specified clusters, and secondly a network analysis of technologies and companies related to cybersecurity.

He thus collected large datasets from the arXiv website, a repository with almost two million scientific e-prints that represent academic research. All publications on the website are classified by technology category: Machine Learning, Cryptography and Security, Human-Computer Interaction, and so on. From the wide range of categories was chosen a subset of interesting ones for the research at hand, i.e. technology clusters that would easily relate to cybersecurity. The numbers of papers in a cluster could then be compared overtime to the total amount of publications found on arXiv, and would yield results such as Figure 16 on page 22.

Investigating the security facet of these technologies required **Natural Language Processing (NLP).** Scanning the text body of every publication in the shortlisted categories, he looked for specific words related to the concept of cybersecurity: *security, safe, threat, breach*, etc. Finally, using NLP as well, he coded a method to determine whether a technology was seen rather favourably or unfavourably using traditional sentiment analysis methods. Certain words in the English dictionary have positive connotations, others negative, and the association of those terms to the technology presents useful information about how the general feeling about said technology stands. For instance, if researchers praised Machine Learning throughout their papers by using positive words, the overall sentiment towards ML would be positive too.

Secondly, Dr. Percia David used a network analysis approach to understand how companies and technologies influence each other. This sheds light on the dynamics moving the cybersecurity market. Mezzetti et al. (2021) have measured this influence in order to drive more informed technological investment decisions. To recognise the mutual influence of companies and technologies in cybersecurity, a bipartite graph links companies and technologies together with data from Crunchbase. Nodes between entities are weighed by applying a recursive

algorithm based on the method of reflection. This endeavour helps to assign a measure of how an entity impacts the cybersecurity market. Their results first help to measure the magnitude of influence of each entity, and second allow decision-makers to make more informed investment strategies.

Another approach by Santiago Anton (2021) uses the Technology Market Monitoring platform to create a similar bipartite graph structure. Santiago Anton modelled his dataset as a bipartite graph in which nodes are represented by technologies and companies involved in the Swiss cybersecurity market. Then, he used job-openings data to link these two entities, and thus assess the capability needs of companies. By extracting time series of such graphs, and by using link-prediction methods, he forecasts the (dis)appearance of links – and thus companies' capability needs related to specific cybersecurity technologies. His results show good performance and promising forecasting power. Such a framework could be critical in making business decisions involving cybersecurity, because of its assessment of current and future cybersecurity capability needs of companies.

Conclusions and outlook

Dr. Percia David, together with CYD Campus researchers, have found evidence that technology cycles tend to draw **sigmoidal graphs**, often creating a plateau after the peak. For some technologies, there is also evidence that the hype does die down after the peak, however the descent is gradual and slow and never truly reverts to a positive slope as the Gartner curve predicts. In the near future, the team would like to start making predictions about what the future holds for a specific technology. Using statistical tools such as Auto Regressive Integrated Moving Average (ARIMA) or by describing the paths with the help of mathematical functions (such as the sigmoid function), the team hopes to be able to predict how popular a technology will be in the future. The team has also started to consider different approaches to mapping the cybersecurity market.

Check out Dr. Percia David's progression with these three videos: 1 2 3

Anita Mezzetti on her Network-Centrality Approach for Informed Cybersecurity Investment: To the talk

Santiago Anton's talk on Link Prediction for Cybersecurity Companies and Technologies: To the talk

4.2 The Jobs of the Future in Cybersecurity

Dr. Quentin Ladetto is head of the Technology Foresight program at armasuisse S+T. The goal of the program is to identify disruptive technology trends, assess their implications within a military context and inform the Swiss Armed Forces of its possible opportunities and threats. Dr. Ladetto presents here the motivation and the methodology used by his team to present what could be some of the future jobs in cybersecurity.

On the future jobs in cybersecurity

Describing the exact nature of technology foresight is a challenging task. If there are some standard activities involved, like creating scenarios or narratives of possible futures, the processes and resulting products of information might lie at the intersection between science and art. One thing however is clear, foresight is not forecast. **There is no prediction involved, but rather an effort of presenting multiple futures** which, according to the requirement of the stakeholders, can be analyzed with the appropriate focus. Considering a specific domain such as cybersecurity, the anticipation of what can happen in this field over the next twenty to thirty years could be very similar to writing a science-fiction novel. With a growing number of connected microprocessors in all objects not only surrounding us, but also slowly becoming part of us to measure our physiological parameters, the attack surface gradually becomes larger, more challenging to protect, and of course more attractive to attack.

We already face challenges anticipating where single extant technology trends such as quantum computing, blockchain, synthetic biology, cognitive sciences, robotics, internet of things (IoT), and artificial intelligence can lead us to; try now to imagine the complexity when starting to combine them all, adding digital capabilities (and vulnerabilities?) to biological entities and hacking nature itself. Too much? Maybe, so why not anticipate the effects some technologies and combinations can create, rather than focusing on the technologies per se? Such a mindset stimulates actions both in the short as well as in the long term, while taking indirectly care of the uncertainty when these events do occur.

Building on that idea and in the continuity of the book "soldat du futur" (soldier of the future), the technology foresight research program of armasuisse Science and Technologies, called **deftech**, started a project to co-develop a methodology to project people into a possible future, with a reference to present activities. Without too much surprise, it is organized as a sequence of workshops during which participants from all horizons work together to add a layer of imagination on top of what could be only innovation. The first edition considered the topic of cybersecurity.

To set the scene, the first workshop started with a video of experts expressing their own opinions regarding the worst cyberattack they could think of today and what they fear could happen tomorrow. Once the mood was set, the participants were presented a list of different cyberattacks that already took place. They were asked to select the most interesting and describe their consequences in the short, medium and long term. We then added elements to the cybersecurity event, to illustrate that even more severe levels could be

reached. Once the participants understood the effects, it was time to combine two or three of these single cyberattacks to create an entirely new kind. This increasing level of effectiveness can be perceived as a projection into an intermediate future. But this was not enough: it was time to move beyond what would be possible today and use some super-powers. These super-powers, or game-changers, were in fact sourced from current technology trends, but presented as what they would enable when reaching their full potential!

At the end of two sessions, one held in French, the other in German, we collected 11 cyberattacks of a new kind, combining the latest technology trends in development today. The two groups from different languages - and therefore of possible different mindsets - challenging each-other was believed to be a fun factor to stimulate a "battle of the imaginations" and the fighting spirit that goes with it!

The second phase of the methodology resulted in each group fighting the cyberattacks imagined by the other group following the defined sequence: first, understanding how to detect that they were attacked; second, finding a solution to continue operations despite being hacked. Finally, defining new competences associated to new job profiles suggested by the creation or the fighting of the cyberattacks.

The third and last phase of the process is an invitation to all the participants as well as anybody interested to discuss, complete, challenge and hack the initial synthesis of the work.

The deliverable of this collaborative work is a futuristic narrative built around the outputs, lessons learned and discussions around the selected topic. The technologies are present, but explored as enablers and directly put in a possible context. Anonymizing the technology for the profit of what we hope to achieve, could trigger an innovation mechanism to replicate the effect with what we might have available today. We therefore start asking **"how"** and **"why"** in addition to the **"what"** that is generally the only question asked. The document is also voluntarily made accessible to whoever is interested. The aim is to stimulate the exchange of ideas, challenge new and divergent opinions and alert on ever-evolving possible futures that sooner or later might become reality.

Members of the project above are Les propulseurs, IAB GmbH, Longview Sàrl. Find out more about the Technology Anticipation research program at armasuisse Science and Technology on the deftech website:

To the website

deftech
defencefuturetechnologies

Technology trends used to create and fight the future cyberattacks

Below is deftech's own emerging technology list:

- You are an expert in **Artificial Intelligence**. You can make machines autonomous, create intelligent exchanges between machines and humans.
- With **3D printers**, you make objects, houses, boats, food, organs... You are the architect of all shapes with all materials!
- With **Blockchain**, you can certify the history of digital exchanges. You are considered the guardian of all secrets and the virtual safe of the digital world. But, at the same time, you are able to steal those that are best encrypted!
- With **Augmented Reality**, you now have information about everything around you and everything you want. Never before has a wink been so clever!
- **Virtual Reality** allows you to be the master of virtual worlds in a real world. For training, treatment, training, you invent them as you please according to your moods and needs!
- **Quantum Computers** allow you to provide a relevant answer before the question is even finished. Super fast, your processors have no limits and try to calculate, interpret and simulate everything that passes through their optical fibre.
- **Crispr-Cas9** is a molecular scissor that cuts and pastes DNA and performs all kinds of genetic manipulations. With it, you are the magician of the human body, the manipulator of aesthetics and genetic superpowers. Improve, heal, modify permanently or reversibly, the standard human being and everything with a DNA has only to behave well!
- With **Internet-connected objects**, you have access to more sensors than you have neurons. What you once assumed, you now see; what you once modelled, you now measure; you can know everything, about everyone, all the time.
- Your robotic family is growing. No more repetitive tasks, no more dangers to face, wherever possible, you send your little **robots** to do the job, alone, in pairs or in swarms!
- **Nanotechnologies** manipulate structures of nanometric size. Turning water into wine, butter into titanium and electronics into cosmetics has become your daily bread. Conductivity, elasticity, strength, color, odor, properties... you bring materials to life.
- Looking for a needle in a haystack is like hunting for an elephant in a china shop. With **Big Data**, you have the ability to find the right photon somewhere in our solar system, so analyzing data on a global scale has simply become your favorite pastime!

Future cybersecurity jobs

Based on the imagined cyberattacks of the future, here are some possible cybersecurity jobs and their associated definitions (initially created in French):

- **PermIAculator**: a dialogue generator between AIs to promote collective thinking
- **Detacker**: detector of computer system weaknesses
- **Hackarion**: spy for hackers
- **Instraquar**: creator of devices to identify cybercriminals
- **Canarist**: engineer of preventive alert systems
- **Solutikan**: conductor of solutions that can eliminate parasites and viruses from computers
- **Cybernudgian**: specialist in personalised nudges to change computer security behaviour
- **Rangotiator**: negotiator of ransom demands for decryption of data
- **Pirating**: marketing manager specialising in hacking products and services
- **Anticipator**: anticipation experts who turn projections into immediate actions
- **Lowteckist**: specialist who plans non-digital solutions in the event of a malfunction of digital networks
- **Coupenaute**: specialist in the creation of communities that allow people to live during breakdowns
- **Digiatrist**: psychiatrist who specialises in the anguish linked to the hacking of one's digital life
- **Securomist**: guardian of the integrity of human genomes
- **Onirist**: analyst who helps his patients to sort out real and false digital memories
- **Persodist**: specialist in the integrity of personal data
- **IDoctor**: surgeon specializing in identity surgery
- **Climatologist**: senior officer specializing in climate cyberwarfare
- **Machilinguist**: translator in machine languages
- **Emprisoner**: specialist in taking human brains hostage

4.3 State-of-the-art technology classification

Dr. Ljiljana Dolamic discusses the MARTA project (Arous et al, 2021; Duong et al, 2021)

Arous et al. (2021) Duong et al. (2021)

Monitoring the technological landscape is important from different perspectives. It enables deriving the information regarding potential investments as well as directing the research among others. Online encyclopedia such as Wikipedia offers an abundance of information, regularly updated by a large community, and thus imposes itself as valuable source of technology-related entities. Even though Wikipedia contains "Technology" as a top-level domain, one cannot rely on this concept to extract all the technology related entities. On the other hand, new technologies emerge very fast. Manually classifying each new term/entity appearing in a knowledge base/encyclopedia as being a technology or not would be highly inefficient. Being able to perform such a task automatically has become a necessity. The current TMM platform uses Wikipedia as a base for the definition of the technology-related concepts. However, the current mechanism of Wikipedia entities classification to technology/non-technology has shown weaknesses. A definition of what the technology is, and what technologies are available is one of the most important parts of a technology-monitoring platform. Thus, development of a reliable framework, capable of precise and explainable classification of entities as technology or not, is essential.

Using the state-of-the-art neural network classification to perform such a task imposes itself as a solution. However, the main downside of such a process is the incapacity of most of the algorithms to justify their decisions. Explainability is a key requirement for text classification in many application domains ranging from sentiment analysis to medical diagnosis or legal reviews. Existing methods often rely on “attention” mechanisms for explaining classification results by estimating the relative importance of input units, meaning that the attention mechanism assigns weights to each sentence of the text. However, recent studies have shown that such mechanisms tend to mis-identify irrelevant input units in their explanation.

With a goal of creating a framework capable of classifying Wikipedia entities as technology or not, offering simultaneously human-readable description ("a rationale") of the classification result, we have created MARTA. MARTA (MApping human Rationales To Attention) is a unified Bayesian Framework that integrates an attention-based model with labels and rationales contributed by crowd-sourcing workers. The main goal of this project was the development of a classification framework capable of classifying a given entity as a technology or non-technology based on the text describing it, giving in addition human like justification of such a decision. This work proposes a hybrid human-AI approach that incorporates human rationales into attention-based text classification model to improve the explainability of classification result.

Attention-based deep learning models are capable of outputing a justification of their decision in the form of a part of the input having the most influence on the result. However, in a large number of cases this justification is not in line with what we call human rationale, making it hard for users to see the connection.

First, we defined a crowdsourcing task asking the workers to answer the following question: "Does the Wikipedia article describe a technology commonly used by companies?" The workers were also asked to highlight the part of the article in support of their decision. This information was then used to guide the attention of the developed model. In addition, the concept of worker reliability was introduced, in order to weight the importance of each workers answer using, as illustrated in **Figure 21**. Where the ground truth consisted of the set of entities manually annotated by experts. Worker reliability is estimated on the set of Annotation/Rationale Quality for ground truth examples. The more correct answers a user provides, the more reliable he is. We then use the labels, rationales and reliability obtained from the above-described crowdsourcing jobs, to guide the learning attention distribution of our model.

Figure 21: Worker reliability

The developed model was tested on two different data sets in order to prove its robustness. We used the Tech-Wiki dataset (classification of Wikipedia entities as technology of non-technology) and Amazon book review (whether a review talks about a book or not). Our method has proven to outperform various state of art models in classification precision, offering at the same time higher quality rationale as illustrated in **Figure 22**. In this figure the expected rationale is highlighted in italic. Highlighted in bold is the rationale returned by an attention mechanism, while the rational returned by MARTA is highlighted in green with color intensity illustrating the attributed weight.

(a) **Microwave transmission is the transmission of information by microwave radio waves.** Although an experimental 40-mile (64 km) microwave telecommunication link across the English Channel was demonstrated in 1931, the development of radar in World War II provided the technology for practical exploitation of microwave communication. **In the 1950s, large transcontinental microwave relay networks, consisting of chains of repeater stations linked by line-of-sight beams of microwaves were built in Europeand America to relay long distance telephone traffic and television programs between cities.** ***Communication satellites which transferred data between ground stations by microwaves took over much long distance traffic in the 1960s. In recent years, there has been an explosive increase in use of the microwave spectrum by new telecommunication technologies such as wireless networks, and direct-broadcast satellites which broadcast television and radio directly into consumers' homes.***

(b) *The author's have done an outstanding job in writing the book.* I found that even *the mundane details were covered in the right place and with a little humor.* The coverage starts out very simple, so many people won't use the beginning chapters extensively. However, as the book progresses, the coverage becomes more technical and I think that most people will find the authors have covered most of the XML details that any developer will need. The authors also discuss some of the details that other books leave out, such as the default namespaces. Little bits of information like this make the difference between a book that merely teaches and one that really helps. **This book has something for everyone.** Novices will get the most out of the book, but even advanced readers will receive some benefit. The thing I like the best is that the book is arranged as a quick reference–something that makes it especially useful when you're trying to complete a project and need to know some detail you've forgotten

Figure 22: Example of decision justification: a) Tech-Wiki dataset; b) Book review dataset

4.4 An interview with Claudia Schärer

Dr. Claudia Schärer is head of early detection at the Swiss Academy of Engineering Sciences (SATW). Every two years, her team produces the Technology Outlook report, which describes forward-looking technologies and assesses their importance for Switzerland. The 2021 edition considers 43 technologies, ranging from computerized innovations in Big Data and Blockchain to biotech research in Synthetic Biology.

Dr. Claudia Schärer, as head of the early detection team, you surely make important decisions on what technologies make the cut and get published in the report. How do you select worthy innovations? Would you consider your methodology to be rather quantitative or qualitative?

To answer this question, I need to briefly explain SATW's foresight process. It involves our topical platforms, experts and member societies and is governed by the scientific advisory board. The expertise in the 13 platforms and more than 50 member societies is very broad and covers numerous scientific fields ranging from digitalization and manufacturing to energy and life sciences. The boards mentioned above are invited to share their knowledge and to nominate disruptive technology trends in their fields every other year.

The maturity level and relevance for Swiss industry are then determined for the submitted technologies. To make it into the Technology Outlook, the technologies should be expected to reach product maturity within the coming five years. In addition, it is pivotal that Switzerland is home to research and industrial activities in the field. Therefore, technologies appear and disappear in consecutive Technology Outlooks as they exceed the desired maturity level.

Our methodology of technology selection is therefore rather qualitative.

The Technology Outlook 2021 compares Switzerland and seven other European countries with the help of data from social media, especially Twitter. More specifically, you measure differences between these countries by looking at the relative frequency of social media posts from higher education institutions that mention the technologies the report assesses. Why has your team opted for a social media analysis to compare international levels of interest for a technology?

We looked for data sources that are available for all European countries, that are fully searchable without license fees and that reflect trends in an almost real-time manner. Twitter posts fulfill all these criteria. To keep the background noise low, we opted for the messages posted by the official social media channels of European universities.

Even though posts from universities do not necessarily reflect the industrial profile of a country, they do show the topics that universities are working on and that they find of general interest. Since academic research is the foundation for industrial applications, the technologies mentioned by the universities in the posts will

also have industrial relevance in the future. In addition, we observe that country-specific industrial characteristics are to some extent reflected in the posts.

Your team monitors a wide range of technologies spanning many industries. Considering the breadth of content, your reader base is most likely very heterogeneous as well. Who do you consider to be the target audience of your team's work, and who else do you believe could benefit from reading the findings in the Technology Outlook and beyond?

Even though the Technology Outlook is commissioned by the federal authorities, it meets the interest of other target groups as well. CTOs and technology transfer officers in SME, scientific experts at universities as well as location and economic promoters appreciate the broad scope of technologies, the assessment of their relevance for Switzerland and the description of the interactions between the technologies to enable broad technology trends.

We feel that politicians and the general public could also profit from the findings. Obviously, the Technology Outlook in its entirety is too comprehensive and has to be "resized" for these target groups.

The CYD campus of armasuisse S+T is tasked with a similar role of monitoring the market and assessing the importance of certain future-oriented technologies. However, the CYD campus focuses on technologies with a consequential impact on the field of cybersecurity and therefore does not investigate all emerging technologies. What are your thoughts on the differences between the two monitoring strategies? At the end of the day, does monitoring few versus many technology clusters entail the same tasks or are there visible differences in how monitoring is carried out?

I wouldn't think that there are major differences: Both approaches involve horizon scanning, close collaboration with experts and a system for assessing the relevance of the tentatively identified technologies. I see the difference rather in the flight altitude and the mesh size used for technology identification: SATW flies high, covers a broad territory and deploys a net with large mesh size whereas CYD circles above a specific area and works with a closely knit net.

However, the tasks remain the same – to identify technologies of future relevance for Switzerland!

According to your methods, what would currently be the main trends in cybersecurity technologies?

The challenges are numerous as digitalization and cybersecurity go hand in hand. Many security incidents result from the violation of fundamental security principles, which explains why, besides promoting new security solutions, it is increasingly important to provide for the regulation and certification of ICT services, products and processes.

At the technical level, more automation is needed. For example, artificial intelligence should help to identify weaknesses in systems and to close gateways. In future, it will also be important to share information on existing threats.

Talking of a specific technology, we put quantum cryptography in the spotlight. It is pivotal to have highly advanced encryption methods in place once quantum computers are used on a large scale.

Since cybersecurity is also highly dependent on human activity, it is essential that workers but also politicians and private persons understand the mechanisms. Next to technological innovations, there is a need also for education and for unbiased knowledge sharing.

In addition to the Technology Outlook, the SATW developed the Cybersecurity Map to specifically address technological developments in the field of cybersecurity. Therein, the SATW covers technological developments in the field of cybersecurity that will be of relevance for (political) Switzerland in the next five years. The technological developments range from cloud computing, dependency and complexity to internet of things and information warfare.

To the map

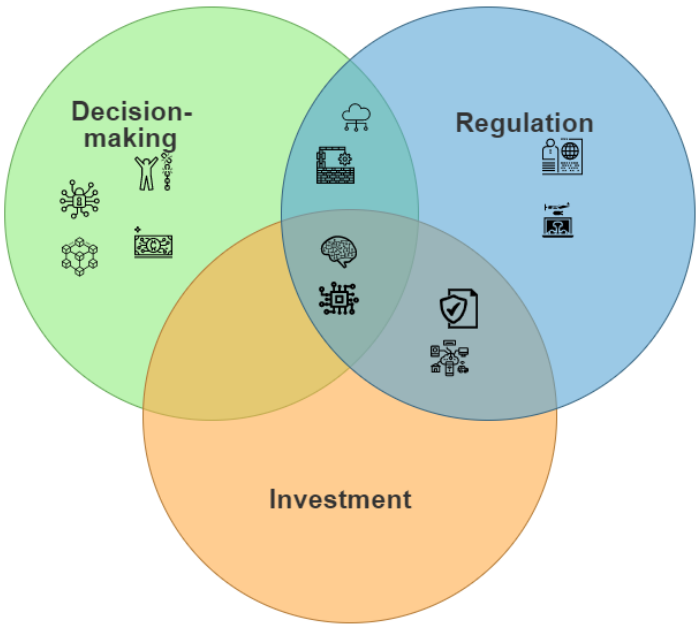


Figure 23: SATW's Cybersecurity Map gives a concise insight into current technological developments relevant from a cybersecurity perspective. Each development is shown as an icon in the Venn diagram above and is backed up with a factsheet, which can be found online:

We thank Dr. Percia David, Dr. Ladetto, Dr. Dolamic and Dr. Schärer for presenting to us their research methods.

Chapter 5

Scouting and Collaborations

Global cybersecurity hubs

Due to the lower cost of hardware and the increasing availability of cheap labour, but also thanks to the latest technologies (such as cloud computing), the barrier to entry for companies in application and software development has never been lower. This evolution requires a change in the way governments seek solutions to their cybersecurity challenges. They need to get to work in the field, where innovation is happening. The CYD Campus addresses these challenges with a combination of quantitative analysis using the Technology Market Monitoring platform and with a qualitative approach through scouting, an international technology watch programme, for which Giorgio Tresoldi of the CYD Campus is responsible. The project mainly targets emerging companies, but sometimes also established companies that can offer innovative products. An international network of partners, including venture capitalists, incubators and local startup promotion structures, helps the scouting efforts identify the right technologies. Geographically speaking, the focus is laid on regions with high-quality startups. In the **United States**, these would be the metropolitan centers around Silicon Valley, Boston, New York, Seattle, Austin and Washington DC. Other places include:

- **Israel**, where the army unit 8200 produces top talents for cybersecurity.
- **United Kingdom**, where renowned universities and a large defence budget contribute to the startup scene.
- **France**; the Cyberpol in Rennes encourages cybersecurity research.
- **Germany**, where organisations such as the Institution for cyberdefence of the University of the Bundeswehr of Munich are excellent promoters of the field.
- **Singapore**, which sits at the center of South-East Asia and has one of the highest per-capita defence spending in the world

Scouting in the United Kingdom

CYD Campus' most recent trip led the team to visit cybersecurity firms in the United Kingdom (Tresoldi, 2020, p. 31). For this scouting effort, the Swiss Business Hub (SBH) in London was instrumental in identifying interesting companies, and with the help of a local expert and the wider embassy team it delivered a longlist of about 100 companies and UK institutions. The SBH approached stakeholders on the list and invited them for a personal meeting, at which every startup had the opportunity to pitch and present their product for around one hour. The startup ecosystem in the United Kingdom is multifaceted. The UK's Cyber Security Strategy (2016) aims at incentivising growth in the cybersecurity sector and at combating cyber-attacks. Cybersecurity clusters have formed in different hubs, such as in Oxford and Cambridge because of the prestigious universities located there, and also in proximity to the **Government Communications Headquarters (GCHQ)** in Worcester. The GCHQ is a British intelligence and security agency that provides signal intelligence and information assurance to the UK government and armed forces. The National Cyber Security Centre (NCSC) is the UK's agency on cybersecurity and is part of the GCHQ.

In the UK, the CYD Campus team talked to a variety of companies, broadly grouped into the following categories: supply chain security, data analytics, network detection response, industrial control systems, infrastructure and threat intelligence. The scouting team analysed each company's resources, the problem the firm was trying to solve and what the proposed solution was. Tying it to the field of monitoring for the benefit of Switzerland, the analysis also tried to ask who in the Swiss government could partner up with these companies; for instance armasuisse, the federal administration or the CYD Campus itself. Overall, the discussions with these companies were an immense success, and further scouting trips are planned to the United States (Summer/Fall 2021), Germany (Fall 2021) and Israel (Spring 2022). Listen to Giorgio Tresoldi's talk on his team's scouting efforts:

To the talk

The benefit of local networks

Evidently, cybersecurity talents are spread all over the world, and in order to keep up with global innovation in cybersecurity, it becomes imperative to meet faces from different horizons. One series of events that gathers security experts from around the world are **RSA conferences**. Over 45,000 people attend them yearly in various locations across the United States, Europe, Asia and the United Arab Emirates. The last edition, held in May 2021 entirely online, focused on relevant topics in this day and age; cybersecurity in times of homeoffice, securing cloud systems and identifying vulnerabilities in devices used for the Internet of Things. The conferences speak mainly to a public of high-level executives, who can no longer ignore the importance of securing their companies from the persistent threats that try to break through their firm's walls.

More in-depth partnerships are a viable alternative to gather information about specific firms and products. Since this year, armasuisse has worked with **Plug and Play Tech Center** to scout the cybersecurity market. The company has over 29 locations across the globe and spans 15 industries (also called verticals). With its workforce of over 100 analysts, Plug and Play is able to gather information on over 17,000 startups, which gives it an unparalled breadth of data. Using this database, for a specific vertical the company creates a list of 100 companies that have above-average potential. This list is sent out to all corporate partners, of which armasuisse is part of, and these partners narrow the list down to 20 interesting startups. The finalists are then invited to pitch in front of the partner and finally the most eligible startups are given the opportunity to join Plug and Play's accelerator, where they can develop with external resources a Proof of Concept with the corporate partners. For the Swiss government, Plug and Play summarises the market in a understandable and efficient way, and the company's platform also allows easy introduction to relevant startups.

Beyond Plug and Play, armasuisse also uses **Swissnex**'s presence in the five global cities to create local contacts. Swissnex is an initiative to "Connect Switzerland and the World in education, research an innovation", and is currently located in San Francisco, Boston, Shanghai, Sao Paolo and Bangalore. Finally, it is important to mention other collaborations that the scouting team at armasuisse has built, including with the venture capital firm **Team 8** in Israel, the seed accelerator **Mach37,** the venture capital firm **Data Tribe** in the United States, and the entrepreneur hub **ICE71** in Singapore.

The Swiss Startup Landscape

A report on cybersecurity startups would not be complete without describing the dense network of innovative firms that have settled down here in Switzerland. Indeed, the country is becoming a leading player in cybersecurity technologies (see Swiss Cyber Map on page 7). The Swiss Cybersecurity Start-Up map has aggregated the main players of the industry into the visual below. Another great resource to get to know the posture of the Swiss startup landscape in the field of cybersecurity is the following video by Clusis Suisse:

To the video

Figure 24: Swiss Cybersecurity Start-Up Map (Swiss Cybersecurity Startup Map, 2021)

Scouting in Switzerland occurs through partnerships between the CYD Campus and public or private stakeholders. A collaborative agreement was set up with the telecoms company **Swisscom**, with the purpose of exchanging information about trends, technologies and products in the areas of cybersecurity, big data and artificial intelligence. Swisscom can tap into the CYD's extensive presence on university campuses such as ETH, EPFL and Oxford, whilst the CYD Campus itself benefits from Swisscom's strong foothold in Silicon Valley, particularly thanks to Swisscom's **Cloud Lab**.

Company	Industries	Headquarters	Total funding amount (USD)
dormakaba Holding AG	Security	Rumlang, ZH	517'153'998
Acronis	Cloud Security, Cybersecurity	Schaffhausen, SH	408'000'000
WISeKey	AI, Blockchain, Cybersecurity	Geneva, GE	256'639'757
Wire	Mobile Apps, Security	Zug, ZG	35'450'000
NetGuardians	Cybersecurity, FinTech	Yverdon-les-bains, VD	33'437'410
GEOSATIS	Cybersecurity, Internet of Things	Le Noirmont, JU	30'168'097
MoonX	Blockchain, Financial Exchanges	Geneva, GE	29'000'000
Flyability	Drones, Robotics	Lausanne, VD	26'612'753
Tresorit	Cloud Security, Cybersecurity	Zurich, ZH	17'776'072
Teralytics	AI, Business Intelligence	Zurich, ZH	17'532'436
Tangem	Cryptocurrency, Security	Zug, ZG	15'000'000
SECUDE International	Consulting, Security	Emmetten, NW	10'700'000
Arviem	Internet of Things, Supply Chains	Baar, ZG	10'152'062
AXSionics	Fraud Detection, Network Security	Biel, BE	9'856'390
Anapaya*	Internet, Network Security	Zurich, ZH	9'382'983
WealthArc	Big Data, Cloud Computing	Zurich, ZH	8'871'145
Nym Technologies	Blockchain, Messaging, Privacy	Neuchatel, NE	8'500'000
Futurae*	Cybersecurity	Zurich, ZH	7'571'221
Scantrust	Consulting, Fraud Detection	Lausanne, VD	5'827'177
ID Quantique	Network Security, Security	Geneva, GE	5'600'000
Bacula Systems	Network Security, Software	Yverdon-les-bains, VD	5'000'000
ProtonMail	Cybersecurity, Messaging	Geneva, GE	4'796'926
High-Tech Bridge	Compliance, Cybersecurity	Geneva, GE	4'300'000
xorlab*	Cybersecurity	Zurich, ZH	3'955'139
Spitch	AI, Analytics, Biometrics	Zurich, ZH	3'375'421
pCloud	Cloud Computing, Cybersecurity	Baar, ZG	3'000'000
ROVENSO	Machinery Manufacturing, Robotics	Villaz-Saint-Pierre, FR	2'844'010
Biowatch	Internet of Things, Smart Home	Lausanne, VD	2'542'006
ComfyLight AG	Internet of Things, Security	Zurich, ZH	2'156'867
CYSEC*	Cybersecurity	Lausanne, VD	2'141'436

Figure 25: Swiss cybersecurity firms with a total funding amount of over $2 million (Crunchbase, 2021). Startups marked with an asterisk were mentioned by startup.ch for their strong contribution to cybersecurity.

Figure 25 draws up an exhaustive list of Swiss cybersecurity startups with funding above US$ 2'000'000. Companies marked with a asterisk (*) also appear on the Startup.ch list "*Cybersecurity: 10 Swiss startups to secure your IT infrastructure in 2021".* Other startups on the list are Decentriq, exeon, PRODAFT, PXL Vision, SHAREKEY and Tune Insight (startup.ch, 2021).

The CYD Campus is also promoting startups with its own initiatives. Indeed, Gartner highlighted the need for security and risk management leaders to evaluate providers through trials rather than simply through requests-for-proposals (RFPs). The **Cyber Startup Challenge** of the Cyber-Defence Campus is thus offering young companies the chance to pitch their ideas for a Proof of Concept executed within the Swiss Armed Forces (armasuisse, 2021b). The challenge offers a great opportunity not only to the young companies that participate, but also to the Swiss army itself, which comes out of the challenge more knowledgeable about the industry. Organised by Dr. Colin Barschel, it is now running into its second edition. This year, the Cyber-Defence Campus launched the call for the Cyber Startup Challenge on the topic of innovative solutions in the area of Information Sharing and Analysis Centers (ISAC). The call was answered by 36 startups, who presented their solutions to the jury, composed of cyber experts and representatives of the Swiss Armed Forces, together with armasuisse Science and Technology. The Zurich-based startup Decentriq was able to impress the jury with its innovative data clean rooms. The company can now implement a Proof of Concept tailored to the Swiss Armed Forces in 2022. Watch the pitch of the three finalists of the 2021 edition (Decentriq, Pandora Intelligence, Constella Intelligence) :

To the video

An extensive collaborative network

In addition, the CYD Campus maintains regular contact with scientists at international conferences and through leading scientific publications in physics, economics and management. Thanks to its international network of partners, the CYD Campus has regular contact with American and Israeli counterparts who often seek answers to the same questions. In France, the CYD campus follows the research in Defence Economics which has recently published a fundamental paper on the role of technology and innovation in the autonomy and defence of a country. At the EU level, collaborations were held with the **European Defence Agency**, which is also pursuing a Tech Watch programme and is working on the research project PYTHIA ("Predictive methodologY for TecHnology Intelligence Analysis"). At the **NATO** level, regular information sharing is taking place, especially with the Cyberspace Technology Horizon Scan (2021 - 2031) of Dr. Alberto Domingo, which focuses on the following key technologies: AI, Quantum Computing, 5G Networks, Cloud & IoT, Blockchain, Software-Defined Radio.

At the Swiss level, the CYD Campus collaborates with the Distributed Information Systems Laboratory of Prof. Karl Aberer at **EPFL**, as well as with the Swiss Academy of Engineering Sciences (**SATW**), which publishes an annual Technology Outlook in which experts assess the potential of 37 promising technologies for Switzerland and its economy. In addition, the CYD Campus maintains a strong link with the **Military Academy (ACAMIL)** of ETH Zurich (Prof. Marcus Mathias Keupp), as well as the University of Geneva (Prof. Thomas Maillart) and the University of Fribourg (Prof. Philippe Cudré-Mauroux).

Chapter 6

Outlook and Conclusion

Dissemination

The continued exchange of knowledge encourages successful efforts in cybersecurity, and to that end the CYD Campus has set up a range of different resources for interested parties. It is important for us to share the work and the conclusions that we arrive to, in order to inform the public of the active policies and market developments in cybersecurity.

- **CRITIS 2021:** the 16th International Conference on Critical Information Infrastructures Security was held in September at the EPFL. Read about the main topics discussed and the papers presented at the conference at critis2021.org

cydcampus.ch

- **CYD website:** read the teams' engaging insights about the campus' mission and goals.

- **CYD Campus Conference on Cyber Threat & Technology Intelligence:** the Cyber Threat Intelligence (CTI) discipline aims to collect and filter all relevant information from the cyberspace, in order to draw up portraits of attackers, threats or technological trends. The CYD Campus Conference on Cyber Threat & Technology Intelligence, held on the 3rd of November 2020 at the SwissTech Center in Lausanne, gathered top experts from EPFL, armasuisse, NATO and the Swiss Armed Forces to discuss these topics. Learn more about threat information sharing and cyber risks with the recorded panels of the event:

To the talks

Community building

- **Cyber Alp retreat:** the CYD team from all three locations (EPFZ, EPFL, Thun) got together and discussed current technologies and developments in the cybersecurity field. Watch the Technology and Market Monitoring seminar by Alain Mermoud here: To the event
- **Swissintell event:** read about Swissintell's conference on technology monitoring, held in December 2021 at the CYD Campus in Lausanne. This report was presented during a joint CYD Campus-Swissintell event in front of an audience from EPFL, the government and the industry. To the website
- **DEVCOM:** The U.S. Army Combat Capabilities Development Command Army Research Laboratory (DEVCOM) is the U.S. Army's corporate research laboratory. DEVCOM and armasuisse have funded joint events to discuss technologies related to technology monitoring. A workshop was held in December 2019 on the topic of *Faceted Taxonomy Construction and Search* (Yan, 2018).
- **Tech4Trust:** located at the EPFL Innovation Park next to the CYD Campus, Trust Valley organises Tech4Trust, the first acceleration programme dedicated to digital trust and cybersecurity. CYD Campus is a recognised partner of the startup programme. To read more about Tech4Trust, go to https://trustvalley.swiss/en/tech4trust/. A short biography of all startups that have joined the programme can be found in the annex at the end of the report. This list is the result of a selection and curation process of the best cybersecurity startups according to criteria set by Trust Valley.

Outlook 2022

As is the case every year, consulting firms have taken out their crystal balls to predict the next trends in the IT market (Chavanne, 2021). Although growth will slow down in 2022, it will remain clearly positive in all segments. Most companies and governments are expected to invest a larger share of their IT budget in system modernization, while the share of spending on maintenance will decrease. According to Gartner, spending on cloud services will increase in 2022, foreshadowing the massive adoption of cloud-native technologies by 2025. After a pivotal 2021, spending on quantum computing will accelerate. In terms of technology development, the AI segment will be driven by responsible AI, platform operationalization, and resource efficiency, among other things. In terms of cybersecurity trends, the next few months will be marked by threats from attacks on the IT supply chain, but also from microservices and deepfake. Companies will also need to keep an eye on ransomware and container hacking.

Cybersecurity experts will have their hands full next year. But they won't be the only ones facing hackers, Check Point predicts (Jaun, 2021). The Israeli specialist vendor has published a list of nine cybersecurity trends for 2022, starting with a surge in IT supply chain attacks. Analysts believe that governments will begin enacting regulations to address these attacks and protect networks. They will also look to collaborate with the private sector and other countries to identify and combat networks operating on a global and regional scale.

Conclusion

This report on cybersecurity has highlighted important aspects of the cybersecurity field. Quantitative and qualitative results show that the rise in patents, publications and startups is growing exponentially, and that expected numbers will be even higher in the years to come. With the growth of the technology landscape follows the need to identify and monitor the entire cybersecurity space, and that is precisely why the National Cyber Security Center (NCSC) and the CYD Campus are building ever more precise tools to gather valuable intelligence. Future projects will seek to include an even greater number of indicators to try and measure the importance of these technologies. Until now, the research has mainly relied on patent, publication and job openings data. The next big step will add a stream of data from the financial sector to map revenue and deal flows onto the relative importance of cybersecurity-related startups. The hope is to identify emerging technologies by surveilling equity firms and their investments.

The rapidly changing environment encourages us to write periodic reports on cybersecurity technology trends. We can already announce that the next trend report is planned. Most likely, we will present a review on encryption technologies with cloud computing and confidential computing in focus.

Acknowledgements

We would like to thank the following people for contributing to this report and/or reviewing its content to insure that only accurate insights were mentioned.

Loïc Maréchal, for his expertise in time series forecasting analysis.

Sebastien Gillard, for the early quantitative forecasting analysis.

Anita Mezzetti, for her insights based on her TechRank project using Crunchbase data.

Santiago Anton, for his insights on bipartite networks analysis using TMM data.

Philipe Cudré-Mauroux, for supervising the MARTA project.

Inès Arous, for her insights based on the MARTA project.

Karl Aberer, for supervising the technology landscape monitoring project.

Chi Thang Duong, for his insight based the technology landscape monitoring project.

Lenning Pedron, for her insights on Trust Valley's Tech4Trust programme.

And the following people for proofreading this document:

- Manuel Suter
- Florian Schütz
- Alain Jacquier
- Tina Werro

Sources

- **Anton, S. (2021)**. Link Prediction for Cybersecurity Companies and Technologies
- **AMPLYFI. (2021, August 13)**. AMPLYFI: Insights Automation Platform. https://amplyfi.com/
- **armasuisse (2020, September 9)**. CYD Campus Distinguished Postdoctoral Fellowship. Ar.Admin.Ch. https://www.ar.admin.ch/en/aktuell/mitteilungen.detail.news.html/ar-internet/news-2020/news-w-t/cyd-fellowship-interview-percia-david.html
- **armasuisse (2021a)**. Sicherheitsrelevante Technologie- und Industriebasis (STIB). ar.admin.ch. https://www.ar.admin.ch/de/beschaffung/ruestungspolitik-des-bundesrates/sicherheitsrelevante-technologie-und-industriebasis-stib.html
- **armasuisse (2021b, June 25)**. Cyber-Defence Campus launches Cyber Startup Challenge 2021. admin.ch. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-84178.html
- **armasuisse (2021c, July)**. Offset Policy. admin.ch. https://www.ar.admin.ch/en/beschaffung/ruestungspolitik-des-bundesrates/offset.html
- **Arous, I., Dolamic, L., Yang, J., Bhardwaj, A., Cuccu, G., & Cudré-Mauroux, P. (2021, May)**. MARTA: Leveraging Human Rationales for Explainable Text Classification. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 35, No. 7, pp. 5868-5876).
- **BAK Economics. (2021, May)**. Zustand und Leistungsfähigkeit der sicherheitsrelevanten Technologie- und Industriebasis (STIB) in der Schweiz.
- **Bundesamt für Kommunikation BAKOM (2021)** Mobile Kommunikation: Auf dem Weg zu 5G. bakom.admin.ch. https://www.bakom.admin.ch/bakom/de/home/telekommunikation/technologie/5g.html
- **Chavanne, Y. (2021, December 17)**. *Tendances 2022: technologies et dépenses IT*. ICTjournal. https://www.ictjournal.ch/articles/2021-12-17/tendances-2022-technologies-et-depenses-it
- **Crunchbase (2021).** crunchbase.com
- **Cuche, K., & Mermoud, A. (2020)**. La veille technologique au service de l'écosystème fédéral de la cyberdéfense. Revue Militaire Suisse, 22–25.
- **Cuche, K. (2020, August)**. Technology Monitoring for the Swiss Public Cyberdefense Ecosystem: A Business Analysis (Master's Thesis). HES-SO. Contact at kilian.cuche@vtg.admin.ch
- **Cuche, K. (2020b, December)**. Swiss Cyber Map. Swiss Cybersecurity Map. https://www.google.com/maps/d/viewer?hl=fr&hl=fr&mid=1jaomc0T_s6-rzoco9UBGK9YiZsi6Fogd&ll=46.77007363511947%2C8.393767348257564&z=9
- **Cyber-Defence Campus (2021)**. ar.admin.ch. https://www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html
- **Daim, T. U., Chiavetta, D., Porter, A. L., & Saritas, O. (2016)**. Anticipating Future Innovation Pathways Through Large Data Analysis. Springer Publishing.
- **Daim, T. U., & Yalçın, H. (2022).** Digital Transformations: New Tools and Methods for Mining Technological Intelligence. Edward Elgar Publishing.
- **DARPA. (2021)**. *Paving the Way to the Modern Internet*. Darpa.Mil. https://www.darpa.mil/about-us/timeline/modern-internet

- **Da Silva Marques, D. (2020, July)**. Etude comparative sur les outils de veille technologique et benchmarking de leurs fonctionnalités.
- **DDPS (2021, April 20)**. VBS legt Cyber-Strategie 2021 bis 2024 fest. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-83160.html
- **Deloitte. (2020, May)**. Projet "Acquisitions DDPS." https://www.newsd.admin.ch/newsd/message/attachments/61731.pdf
- **Duong, C. T., David, D. P., Dolamic, L., Mermoud, A., Lenders, V., & Aberer, K. (2021).** From Scattered Sources to Comprehensive Technology Landscape: A Recommendation-based Retrieval Approach. *arXiv preprint arXiv:2112.04810*.
- **Ericsson (2021).** A guide to 5G network security. https://www.ericsson.com/en/security/a-guide-to-5g-network-security
- **Federal Council (2021, April).** La politique de sécurité de la Suisse: rapport du Conseil Fédéral. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-83266.html
- **FIS. (2021)**. admin.ch. https://www.vbs.admin.ch/en/ddps/organisation/administrative-units/intelligence-service.html
- **Gambazzi, L., Schaller, P., Mermoud, A., & Lenders, V. (2021)**. Blockchain in Cyberdefence: A Technology Review from a Swiss Perspective. arXiv preprint arXiv:2103.02606.
- **Gartner (2021)** Hype Cycle Research Methodology. https://www.gartner.com/en/research/methodologies/gartner-hype-cycle
- **Google Trends (2021)**. trends.google.com. https://trends.google.com/trends/?geo=CH
- **Holtrup, G.; Lacube, W.; Percia David, D.; Mermoud, A.; Bovet, G.; Lenders, V. (2021)** 5G System-Security Overview: Threat and Market Analysis.
- **Jamrisko, M., Lu, W., Tanzi, A. (2021, February 3)**. South Korea Leads World in Innovation as U.S. Exits Top Ten. Bloomberg.com. https://www.bloomberg.com/news/articles/2021-02-03/south-korea-leads-world-in-innovation-u-s-drops-out-of-top-10.
- **Jaun, R. (2021, October 28)**. *Menaces cyber 2022: ransomware et supply chain, mais aussi microservices et deepfake*. ICTjournal. https://www.ictjournal.ch/etudes/2021-10-28/menaces-cyber-2022-ransomware-et-supply-chain-mais-aussi-microservices-et
- **Jin-Ho, C; Hee-Su, K.; Nam-Gyu, Im (2011, December)**. Keyword Network Analysis for Technology Forecasting. https://www.koreascience.or.kr/article/JAKO201113253031257.page
- **Jun, S., Sung Park, S., Sik Jang, D. (2012, May)**. Technology forecasting using matrix map and patent clustering. https://www.emerald.com/insight/content/doi/10.1108/02635571211232352/full/html
- **LaPorte, B., Firstbook, P., MacDonald, N., & Bussa, T. (2020, May)**. Cool Vendors in Security Operations and Threat Intelligence (No. G00720794). Gartner.
- **Legendre, F., Humbert, M., Mermoud, A., & Lenders, V. (2020)**. Contact tracing: An overview of technologies and cyber risks. arXiv preprint arXiv:2007.02806.
- **Ličina, V. F. (2020, December 14)**. CYBER-DEFENCE FELLOWSHIPS: Dimitri Percia David. Epfl.Ch. https://actu.epfl.ch/news/cyber-defence-fellowships-dimitri-percia-david/
- **Manancourt, V., & Cerulus, L. (2021, April 13)**. 'This was not a breach': How Big Tech gaslights the world on data leaks. POLITICO. https://www.politico.eu/article/how-to-leak-data-and-get-away-with-it
- **Mezzetti, A., David, D. P., Maillart, T., Tsesmelis, M., & Mermoud, A. (2021).** TechRank: A Network-Centrality Approach for Informed Cybersecurity-Investment. *arXiv preprint arXiv:2112.05548*.

- **National Cybersecurity Centre (2018, June 7)**. National strategy for the protection of Switzerland against cyber risks (NCS) 2018–2022. https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html
- **National Cyber Security Centre NCSC (2020, October 29)**. Semi-annual report 2020/1. Admin.Ch. https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/semi-annual-report-2020-1.html
- **Porter, A. L., Cunningham, S. W., Banks, J., Roper, T. A., Mason, T. W., & Rossini, F. A. (2011)**. Forecasting and Management of Technology (2nd ed.). Wiley.
- **Rand (2021)**. Delphi Method. https://www.rand.org/topics/delphi-method.html
- **SATW (2021a)** Mobilität der Zukunft. satw.ch. https://www.satw.ch/de/technik-bildung/technoscope/mobilitaet-der-zukunft
- **SATW (2021b)**. Technology Outlook 2021. https://www.satw.ch/de/technology-outlook-2021
- **Schüpbach, S., Grogg, E., Hufschmid, S., & Richter, P. (2021)**. Die sicherheitsrelevante Technologie- und Industriebasis (STIB). *Stratos*, *2*(21), 56–64.
- **Stahl, A. (2021).** How AI Will Impact The Future Of Work And Life. Forbes. https://www.forbes.com/sites/ashleystahl/2021/03/10/how-ai-will-impact-the-future-of-work-and-life/?sh=7a05ae6079a3
- **Startup.ch. (2021)**. Cybersecurity: 10 Swiss startups to secure your IT infrastructure in 2021. https://www.startup.ch/Cybersecurity-10-Swiss-startups-to-secure-your-IT-infrastructure-in-2021
- **Swiss Cybersecurity Start-Up Map. (2021)**. The Swiss Cybersecurity Start-Up Map. Cysecmap.Swiss. https://cysecmap.swiss/map/
- **Swissinfo (2017, September 15)**. Cabinet seeks more data safety as hackers strike. Swissinfo. https://www.swissinfo.ch/eng/cyberattack-and-data-protection_cabinet-seeks-more-data-safety-as-hackers-strike/43522598
- **Swissinfo (2018, August 27)** Swiss close investigation into cyber attack on defence firm. Swissinfo. https://www.swissinfo.ch/eng/ruag_swiss-close-investigation-into-cyber-attack-on-defence-firm/44352550
- **Swissintell (2021, December 17)**. Conférence Swissintell - Cybersecurity Technologies: An overview of trends in Switzerland and Abroad du 2 décembre 2021 au CYD Campus. https://swissintell.ch/conference-swissintell-cybersecurity-technologies-cyd-campus/
- **Tresoldi, G. (2020)**. Exploration internationale des start-ups et de l'innovation pour le DDPS: Contribution du CYD Campus. Revue Militaire Suisse, 31–33.
- **Westkämper, E., & Spath, D. (2006)**. Verfahren für das TechnologieRoadmapping zur Unterstützung des strategischen Technologiemanagements. Fakultät für Maschinenbau der Universität Stuttgart.
- **Yan, X. (2018)**. Faceted Taxonomy Construction and Search. UC Santa Barbaba. http://fts.cs.ucsb.edu/about

Tech4Trust Season I

- **Access Informer:** Access Informer is a simple yet powerful solution for companies to collect, analyze and monitor user authorizations across key systems, including SAP, Active Directory, SharePoint and network shares.
- **CybrQ:** CybrQ is a SaaS platform with self-service solutions ranging from Apps/Devices, Browsing, e-Mail, Authentication to Cyber Awareness.
- **Decentriq:** Decentriq is enabling businesses to identify analytics potential in datasets without having access to the data. We provide a privacy-preserving way of calculating the overlap between the desired characteristics of a dataset and the actual data.
- **ExO-SyS:** ExO-SyS develops Alph@TaV Vault, which protects your data by allowing you to encrypt all types of files and folders, offering you absolute protection against unauthorized access. It is intended for everyone and is, by nature, independent of any external control.
- **Laava:** Laava's Smart Fingerprint™ is a better unique identifier combining authentication, consumer engagement, and supply chain functionality at a much lower cost than other solutions.
- **MedCo:** MedCo is the first operational system that makes sensitive medical data available for research in a simple, privacy-aware and secure way. It enables hundreds of clinical sites to collectively protect their data and to securely share them.
- **Megaverse:** Megaverse is developing adaptive learning in cyber awareness.
- **NextDay.Vision:** NextDay.Vision offers you to replace passwords by authenticating yourself in a simple, efficient and secure way on a multitude of services using a security key, your face or a phone.
- **OneVisage:** OneVisage proposes 3 software development kits that bring one or multiple concurrent factors, including 3D facial biometry (who I am), 3D graphical authentication (what I know) and Premier ID that mixes multiple factors.
- **PRYV:** PRYV is a compliance software for personal health data privacy and consent.
- **Quantum Integrity:** Quantum Integrity develops artificial intelligence for DeepFake detection.
- **ScanTrust:** ScanTrust provides a cloud-based, Internet-of-Packaging platform for product authentication and supply chain visibility.
- **Teserakt:** Teserakt develops software to enable strong encryption between industrial IoT systems.
- **Veintree:** Veintree extends portable QR and barcode readers with a "biometrical IR video reader" add-on, allowing anonymous and GDPR compliant registration of human venous networks (and human-centered actions).

Tech4Trust Season II

- **Bug Bounty Switzerland**: Crowdsourced cybersecurity for a safe digital Switzerland aiming to help large organizations to master their digital transformation.
- **Clearwater Dynamics**: provides horizon smart threat detection for Microsoft SaaS applications. Tackling event fatigue and the cyber skills shortage.
- **Cryptolex**: Cryptolex allows everyone to access and use the Blockchain by recreating the process of certification and traceability.
- **Cyber-Safe Label**: is the Swiss cybersecurity label that tackle SMEs' risks and help them build trust with their partners.
- **CyQuant**: bridges cybersecurity and insurance by providing a platform for insurers to estimate risk exposure for companies and help IT security market close the gap.
- **Cysec**: provides a confidential computing solution applied to the edge that protects data in use by running your critical applications in a trusted execution environment.
- **Decentriq**: enables secure data ecosystem by making data analytics confidential by design. decentriq enables businesses to identify analytics potential in datasets without having access to data.

- **Diadem Technology**: provides an easy, transparent and efficient contracting & billing system for Mobile Network Operators using smart contracts.
- **DuoKey**: helps companies store highly confidential documents and benefit from cloud services while protecting data with privacy and trust.
- **ONLIFE+ powered by Edenair**: provides the platform ONLIFE+ which allows to digitalize one's life and spare time.
- **KETL**: is a Swiss AI-Infused SaaS solution to manage documents, emails and workflows dedicated to professionals who value privacy and productivity.
- **Kimbocare**: provides transparency and trust in the delivery of healthcare in developing regions.
- **Orbitalize**: is a mobile and web application that empowers public authorities and event organizers to oversee drone operations in their local airspace.
- **Origin Food**: enables transparency & collaboration across supply chains, with a focus on product traceability and product compliance.
- **P3KI**: is a decentralized and offline authorization solution that brings human trust to digital devices.
- **Rumya**: Digitalization facilitator helping companies comply with privacy regulations from data subject's rights management to data breach and consents management.
- **Sarus**: empowers enterprises to leverage their most sensitive data assets for analytics and AI applications with the highest standards of data protection: differential privacy.
- **Strong.Network**: defines and automatically reinforces the rules of collaboration around code development by protecting data confidentiality and monitor intellectual property.
- **UBCOM**: is a cybersecurity provider helping organizations to reveal their cyber exposure and digital awareness through a cost effective tool compliant with international standards.
- **X80 Security**: Automated Cyber Defenses by generating threats in a simulation environment.
- **Zimt**: is a digital traceability startup helping food businesses increase transparency & consumer trust.

Tech4Trust Season III

- **Adresta AG**: Adresta connects the manufacturer, retailer and watch owner with one another – creating a new level of interaction for the watch ecosystem.
- **Binare Oy**: Binaré offers a cloud based service with optional professional services that is easy to use and accessible to any organization
- **CollectID**: CollectID protect your brand and connect customers with your products, transform your products into a superior communication and sales channel
- **CondensationDB**: Condensation is an open-source zero trust, distributed database enabling to build modern applications while ensuring data ownership and security.
- **Farmer Connect SA**: Farmer Connect helps farmers connect to the supply chain with the Farmer ID app, get proof of their identity and income so they can get loans, help businesses store & share information about their products.
- **Fully-Verified**: Banking-grade identity verifications for the fintech industry.
- GeneLook: GeneLook is a digital health company empowering rare/chronic disease patients to be actively involved in their healthcare. They are building the future of patient-centric precision medicine based on trust and data sharing.
- **Global Data Excellence SA**: GDE provides an end-to-end AI platform, DEMS-Nixus for corporate governance that allows a dialog between machine and human in natural language for automated Data Cleansing, Business Intelligence, Data Governance and Data Sharing.
- **Hestia.ai**: Hestia.ai builds sustainable personal data pipelines, respectful of the data contributors and responsive to changing circumstances.

- **Jitsuin Inc**: Archivists Inc empowers developers to build applications that provide the provenance, governance and integrity of enterprise assets that businesses and their partners need in a zero trust world
- **kaiosID**: Kaios creates a smart identification solution to tackle counterfeiting, grey market, increase consumer engagement and build trust.
- **Learning Robots**: Learning Robots' mission is to teach Artificial Intelligence in high schools and universities thanks to a robot and a software that propose simple learning scenarios, up to programmation in Python of new algorithms.
- **Logmind**: Logmind aims to empower IT teams in modern organizations with automatic detection and diagnosis of complex problems from their IT infrastructure.
- **MOABI SAS**: Moabi is a software editor which delivers SaaS and on-premise solutions for automted security audits to assess cybersecurity posture of third party software and internal development.
- **MORPHOTONIX**: Morphotonix protects people's health and well-being by providing instant authentication and anti-counterfeiting solutions with the lowest C-footprint to brands.
- **OriginAll S.A.**: OriginAll provids tools and platforms in the fight against counterfeiting and illicit trade.
- **OrphAnalytics SA**: OrphAnalytics is B to B providing for users (Schools, Universities, Police departments, Investigation teams, research group) by IA investigation or judiciary reports, software, or servers.
- **Photocert**: Photocert establishes and certify the authenticity of pictures and videos with the aim to provide processes automation and trustworthy remote digital inspections.
- **Privacy1**: Privacy1 offers Zero Trust data protection that combines security and privacy awareness on the data itself. Enables encryption, entitlement and processing
- **PRODAFT SARL**: Prodaft offers proactive threat intelligence to its customers against the constantly evolving attack techniques in the cyber world.
- **Profiscope / Codescoring**: Codescoring creates automated solutions for source code analysis using modern approaches to data analysis and machine learning.
- **QRCrypto SA**: QRCrypto provides full security from 2G to quantum with patented quantum-resistant SIM card and dedicated secure communication packages beyond quantum.
- **RealTyme**: RealTyme is a Swiss technology start-up that cares about people's privacy and digital well-being.
- **Retreeb**: Retreeb is a payment solution which integrates social responsability into a sustainable business model.
- **Saporo**: Saporo anticipates attacks to allow organisations to be more resilient.
- **Smartcockpit SA**: Smartcockpit supports ISMS, Privacy Management and Digital self-determination. Their solution can scale to a full digital governance for the entire organization.
- **STACKSCIENCES SA**: StackSciences mission is to bring pragmatical solutions to software engineers so that they can deliver secure and reliable Cloud based applications.
- **Tune Insight**: Tune Insight enables organizations to make better decisions by extracting collective insights from confidential data collaborations, while they remain in full control of their own data.
- **Xiphera**: Xiphera designs hardware-based security solutions with standardised cryptographic algorithms. Their cryptographic and system design expertise, and knowledge on digital logic help to protect critical information.
- **ZeNPulsar**: ZeNPulsar helps organizations fight fake news, maintain their reputation and neutralize disinformation. They build the future of cyber forensic through multidimensional DeepTech to advance online trust and integrity.