Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport
armasuisse
Science and technology

Cybersecurity Research Landscape in Switzerland

September 2023

Martin Burkhart, Roland Meier, Bernhard Tellenbach
Cyber-Defence Campus, armasuisse Science and Technology

CYD CYBER DEFENCE CAMPUS

satw technology for society

IMPRESSUM
Authors: Martin Burkhart, Roland Meier, Bernhard Tellenbach, Cyber-Defence Campus, armasuisse Science and Technology
Contributors: Adriana Cantaluppi, Nicole Wettstein, Swiss Academy of Engineering Sciences (SATW)
Reviewers: Vincent Lenders, Alain Mermoud, Cyber-Defence Campus, armasuisse Science and Technology
Contact: cydcampus@armasuisse.ch

This study was supported by armasuisse Science and Technology and the Swiss Academy of Engineering Sciences (SATW) as a contribution to the National Cyberstrategy NCS.

© VBS/DDPS 2023

Contents

Management Summary

The Swiss National Cyberstrategy (NCS) considers cybersecurity research as a crucial pillar to strengthen Switzerland's ability to protect itself against cyberthreats. In addition, cybersecurity research is expected to contribute directly to Switzerland's economic success and leverage Switzerland's position as a neutral country with a high education standard and strong innovation system to drive the development of cybersecurity services and products.

Despite the national importance of cybersecurity research, the actual landscape is not well understood. As Swiss universities and research organisations operate quite autonomously and are mostly free to set their own research priorities, the overall size and the focus areas of the Swiss cybersecurity research ecosystem are hard to assess at the national level.

To this end, we performed a quantitative study assessing the working power invested by universities in different cybersecurity research topics. In total, we surveyed 22 Swiss universities and analysed their research efforts in 14 research domains defined by a taxonomy of the European Joint Research Center.

Our study reveals that the nationwide total working power assigned to cybersecurity research amounts to 297 full-time equivalents (FTEs) across all domains. However, half of the research domains receive only little attention. The five least explored domains receive only 7.2 FTEs in total while the top three domains (software and hardware security engineering, cryptology, and network and distributed systems), consume the majority of the working power (174 FTEs). With nine involved universities, network and distributed systems is the most popular domain.

Our assessment provides the first systematic and quantitative evaluation of the Swiss cybersecurity research landscape and shall serve as basis for policymakers, universities, industry, and funding agencies to address possible research imbalance, incentivise strategic areas, and detect potential blind spots in the Swiss cybersecurity research landscape.

Introduction

Cybersecurity will make or break digital societies and businesses. Is Switzerland ready for the digital age? An answer to this question must consider several perspectives: are challenges addressed properly? Will opportunities be leveraged? What capabilities and resources do Swiss institutions have? Based on this information, politics, businesses, and the society need to assess Switzerland's digital maturity and decide whether possible blind spots require actions to be taken.

Scientific research is a key factor for Switzerland's digital capabilities. Selected research topics and their funding have a major influence on the innovative strength, available talent and hence on current and future capabilities of a country. The correlation between the excellence of universities and innovative power of a country is confirmed by literature [1]. Generally, Switzerland attracts excellent researchers and teaching staff on the international market. However, the current exclusion from the Horizon Europe funding programme threatens Switzerland's attractiveness for researchers and startups [2].

A thorough understanding of the Swiss cybersecurity research landscape in terms of topics studied and investments per topic is essential for any discussion on whether Switzerland is well-prepared for the digital age or whether there are gaps. While different stakeholders might have differing perspectives on relevant gaps, knowing the capabilities and gaps enables the government, the industry, and society to make informed decisions. For example, Swiss companies may refrain from investing in a domain with hardly any research activity. As a consequence, policymakers could introduce funding instruments for strengthening research in a certain domain or topic.

Tasked with anticipating cyber developments, trend monitoring, and the development of skills and technologies for cyber defence, the Cyber-Defence (CYD) Campus of armasuisse Science and Technology has a natural interest in knowing what is being researched in Switzerland. In particular, it has an interest in identifying gaps with potential negative impact on Switzerland's cyber capabilities, such as a lack of appropriate personnel or limited access to technology. As a suitable overview of the Swiss cybersecurity research landscape was missing, the Cyber-Defence Campus joined forces with the Swiss Academy of Engineering Sciences (SATW) to perform a quantitative and empirical assessment. On behalf of the federal government, SATW identifies industrially relevant technological developments and informs politics and society about their significance and consequences. This study focusing on cybersecurity represents a particularly significant contribution in this regard.

We believe the study provides value to different stakeholders. For example, research institutions will be able to deliberately tune their focus based on knowledge of the greater research environment. For companies, identification of competent research partners will be easier and media representatives will be able to identify institutions with specific domain expertise. And, most importantly, this study informs the discussion about the focus of cybersecurity research in Switzerland. It is up to policymakers and funding agencies to decide whether resources are prioritized in accordance with future challenges - or whether Swiss cybersecurity research has blind spots that need to be eliminated.

Scope and Contributions

The present study focuses on strategic cybersecurity topics researched at Swiss universities. We consider a topic strategic if it has been assigned at least one FTE over a period of at least two years. If a project is opportunistic with one-off publications on a topic, the entity will hardly be able to cover the topic sustainably and in sufficient depth.

The main contribution of the study is the collection, consolidation, presentation, and interpretation of data on strategic cybersecurity topics from Swiss universities. In particular, the study provides detailed insights and findings related to the following questions:

- What cybersecurity research topics are (not) covered by Swiss universities?
- What are the resources invested per topic per university?

Furthermore, the collected data, the proposed methodology, and especially the lessons learned, are contributions for future iterations of this study and for others carrying out similar studies.

Related Work

To our knowledge, there is neither a study nor publicly accessible and consolidated data on cybersecurity topics researched at Swiss universities and the related investments per topic. Some organisations provide an overview of research areas on their web pages. One example is the Swiss Support Center for Cybersecurity at ETH Zurich [3], listing the research groups at ETH Zurich with a focus related to cybersecurity. Another example is published by the Center for Digital Trust [4] from EPFL, listing affiliated laboratories. However, these pages focus on single organisations and do not follow a common taxonomy. Outside Swiss universities, the situation looks similar: there is no central directory covering research in cybersecurity.

A study performed by SATW in 2016 [5] has a somewhat similar focus as our study. The authors first created a matrix with research domains and topics. This matrix was then used to collect the domains and topics in which the participating entities conduct research. Of the 20 participants, 10 were universities and another 10 were sub-entities of ETH (2) and EPFL (8). The matrix was complemented with information on the entities, obtained through surveys of the research institutes. The main differences between this study and ours are threefold: First, we focus on strategic research topics – topics with significant investments and active for a minimum amount of time. Second, we use a standard taxonomy created by the European Joint Research Center [6]. And third, we perform a quantitative analysis of the research landscape; we measure the number of full-time equivalents (FTE) assigned to each topic, allowing a direct comparison of topics with regard to available working power.

A number of studies focus on topics related to cybersecurity research. Regarding innovative startups, the Swiss Cybersecurity Start-Up Map [7] is a good starting point. Focusing more on politics, culture, and legal conditions surrounding cybersecurity, the Federal Departments of Foreign Affairs (FDFA) and Finance (FDF) published a "Cybersecurity Capacity Review" for Switzerland [8], conducted by the University of Oxford. An overview of cybersecurity training offerings in Switzerland was published by the NCSC in 2021 [9]. The Swiss Technology Observatory [10], a collaboration of the CYD Campus and Swissintell, performs technology and market monitoring for cybersecurity using automated quantitative analysis based on publicly available resources. In contrast to our study, it does not estimate the FTEs in a certain domain.

Methodology

For this study, we followed an approach with four steps:

1. Definition of the scope and the data to be collected
2. Identification of points of contact
3. Data collection (i.e., performing the survey)
4. Data review and consolidation

Steps two to four sometimes required several iterations, e.g., because a contact person had left an institution or information was unclear or incomplete. The individual steps are explained in more detail below.

Definition of the Scope and Data Analysed

Many entities conduct research in cybersecurity, often in collaboration with international partners. These entities include, in particular, universities, private research institutes, companies with their research departments, private individuals and, to a limited degree, the government. In this study, we restrict ourselves to research conducted at Swiss universities due to the fundamental role they play in education, research, knowhow development, and innovation for the Swiss economy. We believe that research performed at universities is representative of the strategic and foundational cybersecurity research in Switzerland and, hence, indicative for future Swiss cybersecurity capabilities.

While corporations may also perform cybersecurity research, their focus tends to be more on technologies with relatively high maturity, focussing on product and service innovation. Notable exceptions are large international corporations with research divisions in Switzerland, for example, IBM Research.

From the selected universities, the following data was collected: [1]

- Active research domains
- Research topics within the domains
- Full-time equivalents (FTE) per topic

The reported FTEs cover projects and positions funded by the universities directly or by third-party agencies, such as the Swiss National Science Foundation or Innosuisse. The FTEs include fixed positions such as doctoral students, but exclude semester or master thesis projects carried out by students. For an overview of the research domains of interest and their descriptions, please refer to Appendix A.

Identification of Universities and Contact Points

We used the list of all accredited Swiss universities to identify 22 relevant universities, listed in Appendix C. Of these universities, all labs and research groups related to cybersecurity research were identified using publicly available information on websites. In the next step, the heads of these groups were contacted by e-mail to verify whether they were the right point of contact. In total, 111 points of contact were identified.

Obtaining Data from the Points of Contact

The identified points of contact were requested to give input directly in an Excel sheet. In a few cases, the sheet was pre-filled with our best guess regarding research domains and topics, derived from publicly available information. The motivation behind using a pre-filled survey was to reduce effort for participants and to speed up the process.

To be included in this study, topics had to fit in the pre-defined taxonomy of research domains. Moreover, they required assignment of at least one FTE over a period of at least two years. The point of contact could either submit the requested information directly or ask the project management for support. In some cases, the assessment was done in a phone interview.

Data collection was performed between June and December 2022. Various reasons contributed to the relatively long collection timeframe: sometimes, several iterations were necessary, contacts were not available for extended periods of time, or multiple follow-ups were necessary.

Data Review and Consolidation

From the total of 111 initial contacts across 22 universities, we received 55 valid answer sheets documenting strategic research projects. Even though the number of returned sheets may seem rather low, the provided answers cover the landscape of reviewed universities. In some cases, a single contact provided answers for multiple contacts on our list. In other cases, contacts replied that their research is not strategic or relevant or that they were no longer working at the respective institution.

Only three universities (UNIFR, UNIGE, ZHdK) provided no or only partial feedback. These universities were excluded, as it remained unclear whether they perform strategic research or not. Four universities appear not to have a dedicated cybersecurity group (FHGR, HES-SO, KALAIDOS and UNILU). Hence, 15 of the 22 assessed universities were finally considered in the study.

Lessons Learned

Besides the core findings of the study, we learned some lessons while creating it. In the beginning, identifying the right contacts was difficult, mainly due to complex organizational struc-

1 The survey collected information regarding technologies, use cases and sectors, as well. However, these data are not discussed in the study.

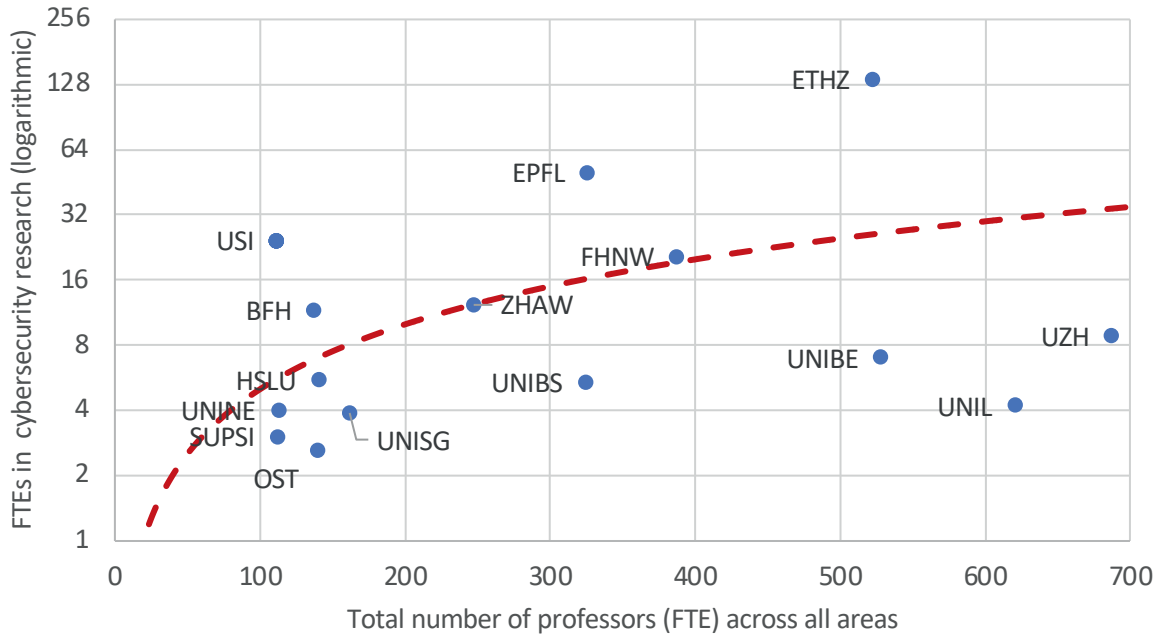

Figure 1: FTEs in strategic cybersecurity research versus the total number of professors (FTE) across all areas, for each university. The dotted line represents the average of 5% security research FTEs per professor.

tures of some universities and a lack of information on public websites. Then, getting replies was hard as well. Even though we sent a reminder and tried to reach some of the contacts on the phone, we were not successful in all cases. Some contacts replied that it was difficult to do the assessment because their topic did not fit into the pre-defined taxonomy. For future iterations, identification and interaction with points of contacts should become easier, due to the existing contacts database and the recognition of the study. The difficulty in matching active research areas with pre-defined topics requires some attention, either by revising the taxonomy or by providing guidelines for mapping topics.

Findings

Summary of the Main Insights

Below, we summarize the main insights of our survey.

- **Most Swiss universities conduct strategic cybersecurity research.**

Out of the 22 Swiss universities considered, 15 perform strategic cybersecurity research with a total of 297 FTEs. To put this in perspective: in Switzerland, companies with less than 250 FTEs are considered to be small and medium-sized enterprises (SMEs).

- **Most research domains are covered.**

13 out of the 14 considered research domains are covered by at least one research group. The only domain not covered at all is "Steganography, Steganalysis and Watermarking". Of the 145 comprised research topics 57 are covered.

- **Resources are not distributed evenly.**

While most domains are covered, they are not funded equally well in terms of working power. The majority of resources (174 FTEs) is assigned to the top three domains, while half of the domains receive only little attention. The most popular research domains are "Network and Distributed Systems" (covered by the highest number of universities) and "Software and Hardware Security Engineering" (covered by most resources). Yet, even well-funded domains have topics with little attention.

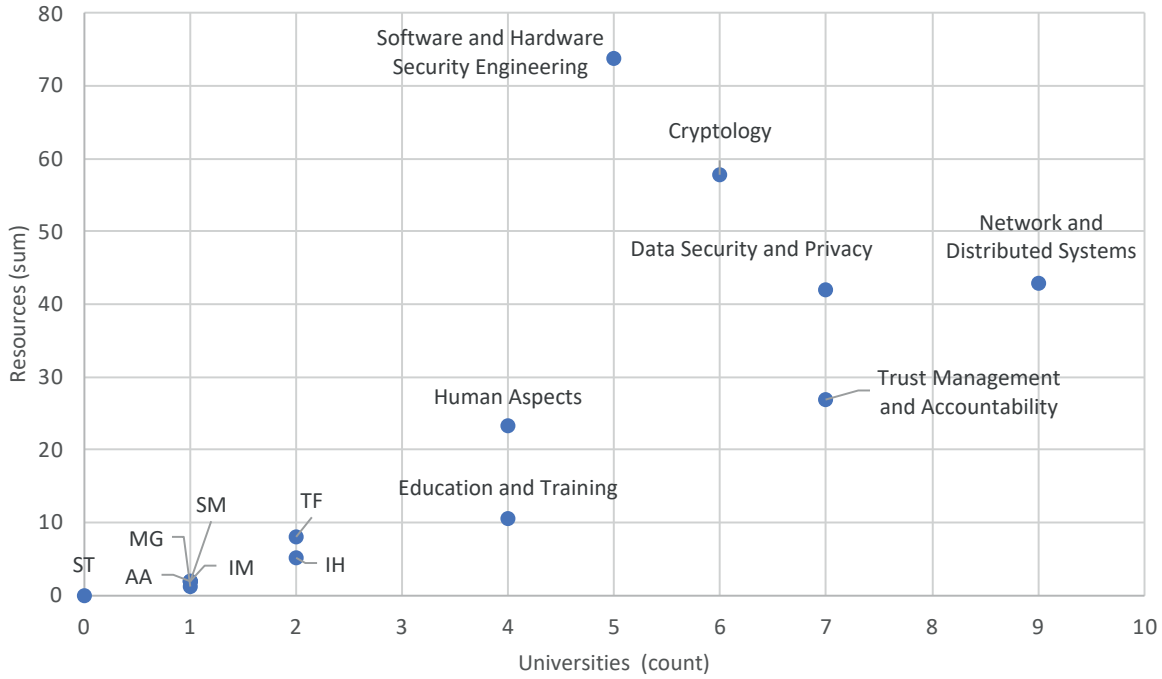

Figure 2: Number of universities and total resources allocated for each research domain.
Legend: TF: Theoretical Foundations; IH: Incident Handling and Digital Forensics; AA: Assurance, Audit, and Certification; IM: Identity Management; SM: Security Measurements; MG: Security Management and Governance; ST: Steganography, Steganalysis and Watermarking.

- **Technology-focused universities invest most in cybersecurity research.**

In absolute numbers, the two Swiss Federal Institutes of Technology (ETHZ and EPFL) assign the highest number of resources (measured in FTEs) to cybersecurity research.

Security Resources per University

In this section, we discuss the number of resources each university assigns to strategic cybersecurity research. Since university sizes vary, we use the total number of professors[2] across all areas to estimate the size of a university [11]. The cybersecurity resources are viewed both in terms of absolute numbers and relative numbers compared to the size of a university, showing which institutes have a dedicated security focus.

Figure 1 depicts the total number of professors and the number of resources in cybersecurity research for each university. The dotted line represents the average of 5% cybersecurity research (FTEs) per professor position. Note that the line is curved, because the vertical axis uses logarithmic scaling (with base 2). Universities above the dotted line have an above-average cybersecurity focus. Please refer to Appendix D for details on the absolute and relative numbers.

In absolute numbers, the Swiss Federal Institutes of Technology (ETHZ and EPFL) assign the highest number of resources to cybersecurity research.

This is not surprising given the technology focus of these institutions and their relatively large size. ETHZ invests by far the most in cybersecurity research (134.5 FTEs), contributing more than twice the amount of EPFL (50 FTEs), which is second.

In relative numbers, ETHZ, EPFL and USI assign the highest number of resources to cybersecurity research.

ETHZ and EPFL rank high also in relative numbers, which underlines their strategic commitment to cybersecurity research. USI ranking among the top three is noteworthy, since it is not specifically focused on technology or security topics. Compared to ETHZ and EPFL, USI is more focused, covering only 3 domains compared to 8 at ETHZ and 6 at EPFL.

2 For universities of applied sciences, lecturers with management responsibility are counted as professors.

Activity per Research Domain

Swiss universities cover all research domains except one.
The only domain not addressed by strategic research is "Steganography, Steganalysis and Watermarking". This does not necessarily imply there is no research in this domain. There could be non-strategic activity or certain topics could be covered by resources in the cryptology domain, which also contains aspects of steganography (see Appendix A).

While most domains are covered, only 57 of the 145 comprised research topics are covered by strategic research (see Appendix B).

Half of the domains seem unattractive.
Research domains can be clustered in two clusters of approximately equal size: half of the domains receive relatively little attention (less than 10 FTEs and at most 2 universities work on it) and the other half receives high attention. The top three domains ("Software and Hardware Security Engineering", "Cryptology", and "Network and Distributed Systems") together receive more than half of all resources.

Four of the domains with less attention are investigated by a single university each ("Assurance, Audit, and Certification", "Identity Management", "Security Management and Governance", and "Security Measurements"). The total number of resources assigned to these domains is only 7.2 FTEs.

Most universities address multiple research domains.
All universities performing strategic cybersecurity research, except UNIL, are active in multiple research domains (see Appendix E). However, often one research domain appears to be the main focus because it owns most resources (e.g., "Cryptology" at HSLU and "Human Aspects" at UZH).

The domain "Network and distributed systems" has the highest number of universities working on it.
Nine universities perform strategic research in the domain "Network and distributed systems". The biggest contribution comes from ETHZ (25 FTEs), while most other universities assign around 2 FTEs to this domain.

The domain "Software and Hardware security engineering" has most resources.
In terms of resources, "Software and Hardware security engineering" is the most popular research domain. Five universities assign a total of 73.8 FTEs to this domain. The biggest share comes from ETHZ (33.5 FTEs), followed by EPFL (18 FTEs) and USI (9.6 FTEs).

Even though the domain has substantial resources assigned, these resources are split among topics unevenly (see Appendix B). For example, "security testing and validation" gets 22.2 FTEs, while "privacy by design" has only 1.2 FTEs assigned. Ten topics within the domain are not covered at all. Hence, while a domain may seem well covered, a look at specific topics may give additional clues when looking for potential gaps.

Limitations

It is difficult to present a complete picture of the cybersecurity research in Switzerland, and we are aware that this study does not cover all aspects. Below, we discuss the main limitations.

We only considered strategic research. There are often more resources in a research domain we did not consider because they are rather opportunistic.

We only considered 14 out of the 15 research domains proposed in the European cybersecurity taxonomy [6]. We excluded the domain "Legal Aspects", because the selection of universities followed a technological perspective. Hence, universities with a non-technical

focus potentially doing research on legal aspects of cybersecurity were not included. Without claiming completeness, we are aware of UNIGE, UNIL, ETHZ, FHNW and UZH being active in this domain.

Sometimes, research activities involve more than one research domain. In these cases, respondents were asked to select the domain to which the largest part of the work belongs. However, this might have distorted our results. For example, strategic research in cryptography could also include theoretical foundations or steganography.

Conclusions

This study shows that most universities in Switzerland perform strategic research in cybersecurity. Together, they cover almost the entire spectrum of research domains. However, half of the research domains and many research topics receive only little attention. On the other hand, the top three of the 14 domains attract the majority of the 297 FTEs invested in total. A match of future digital challenges against the current distribution of resources may provide insights into possible knowledge gaps of the Swiss society and actions to be taken by policymakers and funding agencies. The detailed breakdown of nationwide working power spent per research domain and topic provides a valuable foundation for discussion – for policymakers, universities, companies, and society as a whole.

References

[1] O. H. Yüregir, Ç. Sicakyüz and S. Güler, "Comparison of relationship between global innovation index achievements and university achievements in terms of Countries," International Research Journal of Social Sciences, April 2022.

[2] C. Roth, "Switzerland faces startup talent brain drain," May 2023. [Online]. Available: https://sifted.eu/articles/switzerland-startup-talent-brain-drain.

[3] "Swiss Support Center for Cybersecurity," [Online]. Available: https://sscc.ethz.ch/resources.html.

[4] "Center for Digital Trust," [Online]. Available: https://c4dt.epfl.ch/laboratory/.

[5] B. Hämmerli and S. Ghernaouti, "Cyber Security Research Capabilities in Switzerland," SATW, 2016.

[6] "A proposal for a European cybersecurity taxonomy," Joint Research Centre (European Commission), 2019. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/a1fcc114-01eb-11ea-8c1f-01aa75ed71a1/language-en.

[7] "The Swiss Cybersecurity Start-Up Map," [Online]. Available: https://cysecmap.swiss/.

[8] "Cybersecurity Capacity Review Switzerland," 2020. [Online]. Available: https://www.eda.admin.ch/content/dam/eda/en/documents/aktuell/news/2020_06_CMM_Switzerland.pdf.

[9] "Swiss tertiary-level training programmes in cyber field," 11 2021. [Online]. Available: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/bildungsangebote.html.

[10] "The Swiss Technology Observatory," [Online]. Available: https://technology-observatory.ch.

[11] "Staff in educational institutions," Federal Statistical Office (FSO/BFS), 2021. [Online]. Available: https://www.bfs.admin.ch/bfs/en/home/statistics/education-science/educational-staff/tertiary-higher-institutions.html.

Appendices

Appendix A: Research Domains of Interest

This section describes the 14 research domains of interest for the overview and their corresponding descriptions included in the survey. Domain definitions are taken from "A proposal for a European cybersecurity taxonomy" [6] published by the Publications Office of the European Union. The Domain "Legal Aspects" was excluded in our survey.

Research Domain	Research Domain Description
Assurance, Audit, and Certification	This domain refers to the methodologies, frameworks and tools that provide ground for having confidence that a system, software, service, process or network is working or has been designed to operate at the desired security target or according to a defined security policy.
Cryptology (Cryptography and Cryptanalysis)	Cryptology groups together by definition of Cryptography and Cryptanalysis. For the scope of this taxonomy, under this sub-domain fall the mathematical aspects of cryptology, the algorithmic aspects, their technical implementation and infrastructural architectures as well as the implementation of cryptanalytic methodologies, techniques and tools. Furthermore, this domain also considers digital steganography, which is a technique for concealing information in a particular digital format.
Data Security and Privacy	This domain includes security and privacy issues related to data in order to (a) reduce or avoid by design privacy, confidentiality, and integrity risks without inappropriately impairing data processing purposes or (b) by preventing misuse of data after it is accessed by authorized entities.
Education and Training	The learning process of acquiring knowledge, know-how, skills and/or competences necessary to protect network and information systems, their users, and affected persons from cyber threats.
Human Aspects	The interplay between ethics, relevant laws, regulations, policies, standards, psychology and the human being within the cybersecurity realm.
Identity Management	This domain covers processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain. Furthermore, it also considers access management aspects including authentication, authorization and access control of individuals and smart objects when accessing resources. These concerns may include physical and digital elements of authentication systems and legal aspects related to compliance and law enforcement.
Incident Handling and Digital Forensics	This domain refers to the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidences.
Network and Distributed Systems	Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network [SOURCE ISO/IEC TR 29181-5]. Information Security in the network context deals with data integrity, confidentiality, availability, and non-repudiation while is sent across the network. A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context cybersecurity deals with all the aspects of computation, coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.
Security Management and Governance	Governance and management activities, methodologies, processes and tools aimed at the preservation of confidentiality, integrity and availability of information as well as other properties such as authenticity, accountability and non-repudiation [SOURCE ISO/IEC 27000].

Research Domain	Research Domain Description
Security Measurements	Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements [SOURCE NIST SP800-55].
Software and Hardware Security Engineering	Security aspects in the software and hardware development lifecycle such as risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment and runtime monitoring of operation.
Steganography, Steganalysis and Watermarking	This domain consists of techniques for steganography, steganalysis, and watermarking. Steganography is a technique for hiding secret data within files or message while steganalysis deals with the detection of data hidden using steganography. Digital watermarking is similar to steganography where the embedded data typically is not secret and the goal is also to ensure data integrity.
Theoretical Foundations	This domain refers to the use analysis and verification techniques based on formal methods to provide theoretical proof of security properties either in software, hardware and algorithm design.
Trust Management and Accountability	This domain comprises trust issues related to digital and physical entities such as applications, services, components, or systems. Trust management approaches can be employed in order to assess assurance and accountability guarantees.

Appendix B: Research Topics and Assigned Resources

This section lists the 145 research topics covered along with their associated resources. For the 57 research topics covered by Swiss universities, the corresponding FTEs and the number of involved universities is shown. The sum of FTEs for all topics in a domain is shown in bold. 88 Topics are not covered by any university.

Research topics grouped by domain	Universities	Resources (FTEs)
Assurance, Audit, and Certification		**2.0**
Certification	1	2.0
Assurance	–	–
Audit	–	–
Assessment	–	–
Cryptology (Cryptography and Cryptanalysis)		**57.7**
Asymmetric cryptography	2	7.0
Cryptanalysis methodologies, techniques and tools	2	4.2
Mathematical foundations of cryptography	3	14.0
Post-quantum cryptography	2	3.5
Quantum cryptography	2	17.5
Secure multi-party computation	2	3.5
Symmetric cryptography	2	8.0
Functional encryption	-	-
Crypto material management (e.g. key management, PKI)	-	-
Random number generation	-	-
Digital signatures	-	-

Research topics grouped by domain	Universities	Resources (FTEs)
Hash functions	-	-
Message authentication	-	-
Homomorphic encryption	-	-
Data Security and Privacy		**42.0**
Anonymity, pseudonymity, unlinkability, undetectability, or unobservability	1	3.0
Data integrity	2	6.0
Data usage control	1	1.2
Design, implementation, and operation of data management systems that include security and privacy functions	5	16.2
Privacy Enhancing Technologies (PET)	4	8.2
Privacy requirements for data management systems	1	3.2
Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack)	2	4.2
Digital Rights Management (DRM)	-	-
Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise)	-	-
Education and Training		**10.5**
Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness	2	3.5
Education methodology	1	2.0
Higher Education	2	3.0
Vocational training	1	2.0
Professional training	-	-
Cybersecurity-aware culture (e.g. including children education)	-	-
Human Aspects		**23.2**
Computer ethics and security	1	2.0
Human aspects of trust	1	2.0
Human perception of cybersecurity	2	3.2
Human-related risks/threats (social engineering, insider misuse, etc.)	2	3.2
Privacy concerns, behaviours, and practices	2	3.2
Psychological models and cognitive processes	2	3.2
Usability	2	3.2
User acceptance of security policies and technologies	2	3.2
Accessibility	-	-
Socio-technical security	-	-
Enhancing risk perception	-	-
Forensic cyberpsychology	-	-
Automating security functionality	-	-
Non-intrusive security	-	-
Transparent security	-	-
Cybersecurity profiling	-	-
Cyberpsychology	-	-

Research topics grouped by domain	Universities	Resources (FTEs)
Security visualization	-	-
Gamification	-	-
History of cybersecurity	-	-
Identity Management		**2.0**
Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.)	1	2.0
Protocols and frameworks for authentication, authorization, and rights management	-	-
Privacy and identity management (e.g. privacy-preserving authentication)	-	-
Identity management quality assurance	-	-
Optical and electronic document security	-	-
Legal aspects of identity management	-	-
Biometric methods, technologies and tools	-	-
Incident Handling and Digital Forensics		**5.2**
Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting	1	1.2
Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence	2	4.0
Vulnerability analysis and response	-	-
Digital forensic processes and workflow models	-	-
Digital forensic case studies	-	-
Policy issues related to digital forensics	-	-
Resilience aspects	-	-
Anti-forensics and malware analytics	-	-
Citizen cooperation and reporting	-	-
Coordination and information sharing in the context of cross-border/organizational incidents.	-	-
Network and Distributed Systems		**42.8**
Distributed consensus techniques	2	2.6
Distributed systems security	3	8.0
Distributed systems security analysis and simulation	1	2.0
Network layer attacks and mitigation techniques	4	10.2
Network security (principles, methods, protocols, algorithms and technologies)	3	15.0
Secure distributed computations	1	5.0
Managerial, procedural and technical aspects of network security	-	-
Requirements for network security	-	-
Protocols and frameworks for secure distributed computing	-	-
Network attack propagation analysis	-	-
Fault tolerant models	-	-
Network interoperability	-	-
Secure system interconnection	-	-
Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication)	-	-
Network steganography		

Research topics grouped by domain	Universities	Resources (FTEs)
Security Management and Governance		**1.2**
Attack modelling, techniques, and countermeasures (e.g. adversary machine learning)	1	1.2
Risk management, including modelling, assessment, analysis and mitigations	-	-
Modelling of cross-sectoral interdependencies and cascading effects	-	-
Threats and vulnerabilities modelling	-	-
Managerial aspects concerning information security	-	-
Assessment of information security effectiveness and degrees of control	-	-
Identification of the impact of hardware and software changes on the management of Information Security	-	-
Standards for Information Security	-	-
Governance aspects of incident management, disaster recovery, business continuity	-	-
Techniques to ensure business continuity/disaster recovery	-	-
Compliance with information security and privacy policies, procedures, and regulations	-	-
Economic aspects of the cybersecurity ecosystem	-	-
Privacy impact assessment and risk management	-	-
Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)	-	-
Capability maturity models (e.g. assessment of capacities and capabilities)	-	-
Security Measurements		**2.0**
Security metrics, key performance indicators, and benchmarks	1	2.0
Security analytics and visualization	-	-
Validation and comparison frameworks for security metrics	-	-
Measurement and assessment of security levels	-	-
Software and Hardware Security Engineering		**73.8**
Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)	4	8.0
Privacy by design	1	1.2
Runtime security verification and enforcement	3	9.2
Secure programming principles and best practices	1	2.0
Secure software architectures and design (security by design)	6	14.0
Security support in programming environments	1	2.0
Security testing and validation	6	22.2
Self-* including self-healing, self-protecting, self-configuration systems	1	2.2
Vulnerability discovery and penetration testing	3	9.0
Security design patterns	1	4.0
Security requirements engineering with emphasis on identity, privacy, accountability, and trust	-	-
Security and risk analysis of components compositions	-	-
Security documentation	-	-
Refinement and verification of security management policy models	-	-
Quantitative security for assurance	-	-
Intrusion detection and honeypots	-	-

Research topics grouped by domain	Universities	Resources (FTEs)
Malware analysis including adversarial learning of malware	-	-
Model-driven security and domain-specific modelling languages	-	-
Fault injection testing and analysis	-	-
Cybersecurity and cyber-safety co-engineering	-	-
Steganography, Steganalysis and Watermarking		**0.0**
Steganography	-	-
Steganalysis	-	-
Digital watermarking	-	-
Theoretical Foundations		**8.0**
Formal specification of various aspects of security (e.g properties, threat models, etc.)	1	3.0
Formal specification, analysis, and verification of software and hardware	1	2.0
New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications	1	3.0
Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis	-	-
Formal verification of security assurance	-	-
Cybersecurity uncertainty models	-	-
Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects	-	-
Trust Management and Accountability		**26.9**
Identity and trust management	1	1.1
Semantics and models for security, accountability, privacy, and trust	2	10.0
Social aspects of trust	1	2.0
Trust and privacy	1	10.0
Trust management architectures, mechanisms and policies	2	1.8
Trusted computing	1	2.0
Trust in securing digital as well as physical assets	-	-
Trust in decision making algorithms	-	-
Trust and reputation of social and mainstream media	-	-
Reputation models	-	-
Algorithmic auditability and accountability (e.g. explainable AI)	-	-
Total		**297.3**

Appendix C: List of Universities

We used the list of accredited Swiss universities[3] to identify 22 relevant universities. Universities with a special focus, e.g., education ("Pädagogische Hochschulen"), were excluded from the beginning. These universities were considered:

- Berner Fachhochschule (BFH)
- Ecole Polytechnique Fédérale de Lausanne (EPFL)
- Eidgenössische Technische Hochschule Zürich (ETHZ)
- Fachhochschule Graubünden (FHGR)
- Fachhochschule Nordwestschweiz (FHNW)
- Ostschweizer Fachhochschule (OST)
- Haute Ecole Spécialisée de Suisse occidentale (HES-SO)
- Hochschule Luzern (HSLU)
- Kalaidos Fachhochschule Schweiz (KALAIDOS)
- Scuola universitaria professionale della Svizzera italiana (SUPSI)
- Universität Basel (UNIBS)
- Universität Bern (UNIBE)
- Universität Fribourg (UNIFR)
- Universität Genf (UNIGE)
- Universität Lausanne (UNIL)
- Universität Luzern (UNILU)
- Universität Neuenburg (UNINE)
- Universität St. Gallen (UNISG)
- Università della Svizzera italiana (USI)
- Universität Zürich (UZH)
- Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)
- Zürcher Hochschule der Künste (ZHdK)

Appendix D: Security Resources Versus Number of Professors

Table 2: Resources allocated to strategic cybersecurity research for each university.

Shortcode	Institution	Security Resources (FTEs)	Professors in all areas	Security Resources per Prof. (FTEs)
ETHZ	Eidgenössische Technische Hochschule Zürich	134.5	522	0.258
USI	Università della Svizzera italiana	24.2	112	0.216
EPFL	Eidgenössische Technische Hochschule Lausanne	50.0	326	0.153
BFH	Berner Fachhochschule	11.6	137	0.084
FHNW	Fachhochschule Nordwestschweiz	20.4	387	0.053
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften ZHAW	12.2	247	0.049
HSLU	Hochschule Luzern	5.5	140	0.039
UNINE	Universität Neuenburg	4.0	113	0.036
SUPSI	Scuola universitaria professionale della Svizzera italiana	3.0	112	0.027
UNISG	Universität St. Gallen	3.9	162	0.024
OST	OST - Ostschweizer Fachhochschule	2.6	140	0.019
UZH	Universität Zürich	8.8	687	0.013
UNIBS	Universität Basel	5.4	324	0.017
UNIBE	Universität Bern	7.0	528	0.013
UNIL	Universität Lausanne	4.2	620	0.007

3 https://www.swissuniversities.ch/organisation/mitglieder

Appendix E: Resources per Domain and University

Table 3: Resources invested for each university and research domain (empty cells correspond to a value of zero).

	BFH	EPFL	ETHZ	FHNW	OST	HSLU	SUPSI	UNIBS	UNIBE	UNIL	UNINE	UNISG	USI	UZH	ZHAW	**Total Resources**	**#Universities**
Assurance, Audit, and Cert.				2.0												2.0	1
Cryptology	5.2	12.0	28.0			4.0						1.5	7.0			57.7	6
Data Security and Privacy	1.2	6.0	18.0					3.0		4.2			7.6		2.0	42.0	7
Education and Training				6.0	1.5		1.8							1.2		10.5	4
Human Aspects			12.0									2.4		7.6	1.2	23.2	4
Identity Management			2.0													2.0	1
Incident Handling/Forensics	4.0							1.2								5.2	2
Network and Distr. Systems	1.2	5.0	25.0	2.0		1.5		0.6	2.0		2.0				3.5	42.8	9
Security Mgmt and Govern.							1.2									1.2	1
Security Measurements				2.0												2.0	1
Software and Hardware Sec.		18.0	33.5	7.2									9.6		5.5	73.8	5
Steganography etc.																	0
Theoretical Foundations		2.0	6.0													8.0	2
Trust Mgmt. and Account.		7.0	10.0	1.2	1.1			0.6	5.0		2.0					26.9	7
Total Resources	11.6	50.0	134.5	20.4	2.6	5.5	3.0	5.4	7.0	4.2	4.0	3.9	24.2	8.8	12.2	**297.3**	
# Domains	4	6	8	6	2	2	2	4	2	1	2	2	3	2	4		