SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Cyber Security

Research Capabilities in Switzerland

Bernhard Hämmerli & Solange Ghernaoutie

March 2016

Schweizerische Akademie der Technischen Wissenschaften
Gerbergasse 5, CH-8001 Zürich
Tel. +41 44 226 50 11, Fax +41 44 226 50 19
info@satw.ch, www.satw.ch

Mitglied der
Akademien der Wissenschaften Schweiz

Introduction

Security and the cyber domain embrace many walks of life and research subjects. A number of disciplines address themes associated with cyber security. For a long time already, questions associated with cyber security have been studied in computer science and engineering, information systems, information processing, ICT technology and automation science and engineering.

Traditionally, universities have dedicated separate departments to information technology, information processing and automation science and engineering. In addition to these, research has been intensified in big data, cloud services, usability and embedded systems, among others, which also include perspectives on cyber security. However, economics, politics, social sciences and law start to address relevant security topics as well.

Switzerland has several approaches to Cyber Security Strategy, and the major ones are as follows:

- National strategy for Switzerland's protection against cyber risks (June 19-27, 2012). Measures 1-8 are related to research, either directly or indirectly. Most prominent in this respect are Measure 1, "New cyber risks connected with related problems must be researched," and Measure 7, "Establish an overview of competence building offers and identification of deficiencies."
- Cyber Defence Strategy for Swiss Armed Forces
- The Federal Council's Basic Strategy for Critical Infrastructure Protection, Federal Office for Civil Protection

MELANI (Reporting and Analysis Centre for Information Assurance) is an active and integral part in fighting against cyber threats.

The Cybercrime Coordination Unit Switzerland (CYCO) is Switzerland's central office for reporting illegal subject matter on the Internet. After conducting an initial analysis of the incoming report and securing the relevant data, CYCO forwards the case to the appropriate law enforcement agencies in Switzerland and/or abroad. The Cybercrime Unit also actively searches the Internet for illegal subject matter and carries out in-depth analyses of Internet crime. The Cybercrime Unit is available to the public, the authorities and Internet service providers to answer questions on legal, criminal and technical aspects of Internet crime. It is also contact point for its foreign counterparts[1].

All of those stakeholders need access to research and education in cyber defence. With this report we have an initial answer on Switzerland's status on cyber security research.

What is the scope of this report?

In Switzerland the freedom of each university is kept high. This means that little coordination between institutions has taken place. The funding instruments at the university, foundation, national and European level have certain coordination - each in itself - but even the various projects have no in-depth knowledge of each other.

[1] Quelle: https://www.cybercrime.admin.ch/kobik/en/home/ueberuns/kobik.html

This report is an initial step towards more transparency in the cyber security research landscape. It aims to stimulate further activities for Switzerland's better cyber defence readiness. This goal may be achieved, thanks to ready-to-use research and knowledge capabilities mentioned in this report.

In addition to this report the contributing institutions participated in the elaboration of a fine-grained matrix of research fields in cyber security. An initial set of topics were given to the first contributing institutions. Those institutions have broadened the topics with their expertise. In a second round it was asked again for new additional topics, but there were only four new topics added. This is a hint that quite a complete list was present at this time.
The matrix demonstrates an impressive capacity of Switzerland's research power in ICT security. From about 321 ICT professors (according to the Swiss Informatics Research Association for the Swiss Informatics Society) around 10% work in the field of cyber security. Additionally, some professors of law and security policy were included. The matrix is available as a separate file.

Because both the matrix and the report are based on self-declaration, not all institutions dealing with cyber security aspects are represented in the corresponding documents.

Caption

ETH Zurich	Swiss Federal Institute of Technology Zurich
EPFL	Swiss Federal Institute of Technology Lausanne
BFH	Bern University of Applied Sciences
FHNW	University of Applied Sciences and Arts Northwestern Switzerland
HES-SO	University of Applied Sciences Western Switzerland
HSLU	University of Applied Sciences Lucerne
ZHAW	University of Applied Sciences Zurich

Part I: Universities

ETH Zurich, Department of Computer Science (D-INFK)

ETH has a long-running and successful history of designing computer systems and developing software tools. Out of this success, the Department of Computer Science was formed in 1981.

Since then, the department has quickly grown and developed into the renowned institution it is today.

Currently, more than 30 professors from over 10 countries are active at the Department of Computer Science. More than 200 PhD students and research assistants and over 50 postdocs and senior scientists contribute to maintaining the high standards in research and teaching for which the department is known worldwide. More than 800 students benefit from this directly, leading many to go on to innovative careers in research, education and industry.

In research and education, the department covers a broad spectrum of thematic areas with focuses on:

- Software Engineering and Programming Languages
- Computational Intelligence
- Information and Computer Systems
- Networks and Distributed Systems
- Algorithms and Theory
- Information Security
- Computer Graphics and Vision
- Scientific Computing and Computational Sciences

www.inf.ethz.ch

ETH Zurich, Institute of Information Security IIS

Information Security is both a problem of fundamental importance for modern society and a scientific discipline with its own foundations and methods. The IIS carries out research across this spectrum, ranging from mathematical foundations of cryptography to building solutions to pressing problems in securing networks, cyber-physical systems, and applications. As security is highly interdisciplinary, work is collaborative, with strong links to industrial partners and other faculty areas. The IIS has a track record of impact through publications at top venues, open source software releases, products, and spin-off companies.

The IIS consists of the following research groups:

- The Information Security Group performs research and education on methods and tools for the analysis and construction of safe and secure systems.
- The System Security Group performs research in the design and the analysis of security protocols for wired and wireless networks and systems.
- The Network Security Group, performs research in building secure and robust network systems—with a particular focus on the design of future Internet architectures.

http://www.informationsecurity.ethz.ch/

ETH Zurich, Affiliated faculty: Information Security and Cryptography Research Group

The Information Security and Cryptography research group at ETH Zurich is and has been active in a wide range of topics in cryptography, primarily centred on the theme of defining and proving security of cryptographic schemes and protocols, where the mathematical techniques used range from algebra and number theory to probability and information theory. A current focus topic is the development of a new theory of cryptography, called constructive cryptography, allowing for a modular design of provably secure cryptographic protocols. Future work includes the design of efficient provably-secure protocols for secure channel establishment over the Internet, with the goal of providing an alternative for TLS/SSL and other protocols, eliminating the existing weaknesses and short-comings.

https://www.crypto.ethz.ch/

ETH Zurich, Zurich Information Security and Privacy Center ZISC

The goal of the ZISC is bringing together academia and industry to carry out research and education in information security. The plan is to develop both basic and applied research, which will revolve around issues stimulated by industry partners. Projects will be partially carried out in cooperation with partners. Open innovation for all to see will remain the overarching principle throughout.

Since it was founded in 2003, ZISC has worked closely with the business world to jointly develop solutions for practical problems. Current and past partners include Armasuisse, Credit Suisse, Google, IBM, Kaba, NEC, Sun Microsystems. Zürcher Kantonalbank will become a founding partner of the ETH-ZISC OpenLab, an open platform enabling researchers and IT experts from ZISC’s participating partners and companies to exchange views and opinions.

In future ZISC's existing subject areas will be broadened. Researchers will focus on issues relating to the security of networks, systems, software and applications, the cloud and mobile computing. Researchers at ETH-ZISC will also continue to work on next-generation networks, cyber-physical systems and cryptography.

http://www.zisc.ethz.ch

ETH Zurich, Center for Security Studies CSS

The CSS is a center of competence for Swiss and international security policy in the Department D-GESS. It offers security policy expertise in research, teaching, and consultancy. The CSS trains highly qualified junior researchers and serves as a point of contact and information for the interested public.

The CSS has maintained a strategic partnership with the Federal Department of Defence, Civil Protection, and Sports (DDPS) since 2004 and a similar partnership with the Federal Department of Foreign Affairs (FDFA) since 2012.

For 20 years, CSS has conducted research on cyber-governance issues and has consulted various national and international bodies on cyber-security matters. The CSS analyses how cyber-incidents shape, sometimes even transform the cyber-security discourse by stabilizing or challenging different kinds of (political) interventions and even the material infrastructure of cyberspace. In particular, the CSS is interested in how knowledge about these incidents is formed, transformed and utilized by different actors and in how this knowledge shapes policies and politics.

http://www.css.ethz.ch/en/center.html

EPFL, School of Computer and Communication Sciences (IC)

The IC is one of the main European centres for education and research in the field of Information Technology. Divided into two teaching sections, a computer science and communication system, the IC has three main missions: education, research and tech transfer.

The research activities span the following areas:

- algorithms and theoretical computer science
- artificial intelligence and machine learning
- computational biology
- computer architecture and integrated systems
- data management and information retrieval
- graphics and vision
- human-computer interaction
- information and communication theory
- networking
- programming languages and formals methods
- security and cryptography
- signal and image processing
- systems

The IC highly values the transfer of knowledge and idea to industry, both through its graduates as well as research conducted in its laboratories. This process is furthered through partnerships with industry, the creation of start-ups and R&D projects sponsored by the CTI.

http://ic.epfl.ch/our-mission

http://ic.epfl.ch/files/content/sites/ic/files/ic-at-a-glance-2014-01-light.pdf

EPFL, Artificial Intelligence & Machine Learning

The modern world is full of artificial, abstract environments that challenge our natural intelligence. The goal of the research is to develop **Artificial Intelligence** that gives people the capability to master these challenges, ranging from formal methods for automated reasoning to interaction techniques that stimulate truthful elicitation of preferences and opinions. Another aspect is characterizing human intelligence and cognitive science, with applications in human-computer interaction and computer animation.

Machine Learning aims to automate the statistical analysis of large complex datasets by adaptive computing. A core strategy to meet growing demands of science and applications, it provides a data-driven basis for automated decision making and probabilistic reasoning. At EPFL machine learning applications range from natural language and image processing to scientific imaging as well as to computational neuroscience.

The group Artificial Intelligence and Machine Learning includes amongst others the Artificial Intelligence Laboratory – LIA. The LIA develops knowledge-based technologies that allow humans and computers to deal better with the artificial world that surrounds them.

http://lia.epfl.ch/

EPFL, Data Management & Information Retrieval

We live in a world where data is at the core of everything we do on a daily basis as enterprises, governments, research and service organizations, and individuals alike. Today, we generate and measure data at a much higher rate than conventional technologies can sustain.

This tipping point in information technology is often referred to as the era of "big data" or "data deluge." At EPFL, we are investigating theoretical frameworks and experimental systems to enable data analytics, data management and information retrieval with the goal of enabling accurate, efficient, fast and robust handling of large scale data.

http://ic.epfl.ch/data-management-and-information-retrieval

The group Data Management and Information Retrieval includes amongst others the Distributed Information Systems Laboratory – LSIR. People working for LSIR believe that the future of IT belongs to systems that are truly distributed, self-organizing, and capable to quickly respond to changes of their environment. Research focuses on efficient peer-2-peer systems, trust management, large-scale semantic interoperability, and self-organization in decentralized information systems.

http://lsir.epfl.ch/research/themes/

EPFL, Security and Cryptography

Information security is a very broad term that refers to all aspects of safeguarding or protecting information or data, in all its forms. Information security related expertise at EPFL concentrates on the more technical side of the subject, with a particular focus on the security of digital communication and information systems, and the underlying mathematical principals and applications of cryptography.

http://ic.epfl.ch/security-and-cryptography

The group Security and Cryptography consists amongst others of following laboratories

- Laboratory for cryptologic algorithms – LACAL: Computational aspects and security assessments of cryptographic methods.
  http://lacal.epfl.ch/home
- Laboratory for Communications and Applications – LCA:
  basic and applied research in networking and related fields
  http://lca.epfl.ch/
- Security and Cryptography Laboratory – LASEC:
  research and education on the security of communication and information systems, cryptography, and applications.
  http://lasec.epfl.ch/

EPFL, Systems

Computer Systems at EPFL targets a broad spectrum of fundamental and emerging challenges in efficiency, dependability, scalability and security in data processing, communication and storage. The group works on the design and evaluation of systems, with a strong emphasis on prototyping experimental systems, from embedded and mobile platforms, all the way to servers in emerging cloud computing systems and data centers.

http://ic.epfl.ch/systems

The systems group consists amongst others of following laboratories

- Dependable Systems Lab – DSLAB
  The DSLAB develops techniques and abstractions for building trustworthy computer systems, i.e., systems that are safe and secure. The DSLAB operates at the intersection of operating systems, programming languages, and computer architecture.
  http://dslab.epfl.ch/
- Network Architecture Lab – NAL
  The NAL works on fundamental questions regarding the design and construction of practical and dependable network systems. The core interest is the functionality deployed inside the network infrastructure, e.g., inside Internet routers, data-center switches, or intermediate nodes in a sensor network.
  http://nal.epfl.ch/

EPFL Innovation Park

A venue for exchanges and meetings between the scientific research sector and companies; a vast laboratory that can support even the most audacious projects: this is EPFL Innovation Park, at the heart of EPFL. It currently houses 13 buildings that provide major companies and promising start-ups with the conditions they need to flourish.

EPFL Innovation Park includes start-ups in the security area such as NexThink, and leading research centers of prestigious companies such as Debiopharm, Nestle, Logitech, Credit Suisse, Constellium and Cisco and Siemens. The Innovation Square could create over 2'000 jobs.

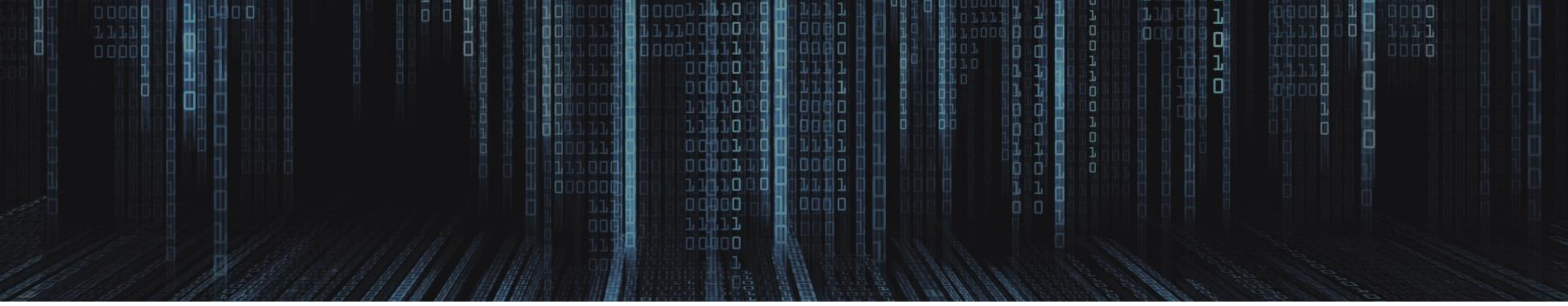
http://vpiv.epfl.ch/innovationpark

EPFL, Center of Risk Analysis and Governance – CRAG

Recognizing that risk governance is an important component for the successful deployment of engineering and technologies, in particular in the context of public policy, EPFL created a Center on Risk Analysis and Risk Governance (CRAG). The mission of CRAG is to develop and communicate knowledge and expertise related to risk analysis (risk assessment, risk management, risk perception and risk communication) and risk governance.

Amongst others, CRAG addresses questions of Cyber Security.

http://crag.epfl.ch/



University of Basel

At the University of Basel, questions related to cyber security are addressed by the following departments' und faculties:

- Department of Philosophy and Media Sciences: Seminar for Media Sciences
- Department of Law (machine learning for corruption analysis, intelligent agent regulations)
- Department of Mathematics and Computer Science (privacy preservation, secure information centric networking, computational intelligence)
- Department of Physics
- Other orthogonal activities such as "Data Life Cycle Management" and "National Infrastructures in Information Supply and IT".

The Seminar for Media Sciences deals with the subject of cybercrime, particularly from the perspective of media sociology and media pedagogy; for example, risks and courses of action regarding online images, and observations concerning the need for self-disclosure when establishing an (online) identity. The seminar furthermore looks at questions of media competency, particularly in terms of cybercrime prevention (keywords: peer education, cyberbullying, sexting, selfies, parental guide 'Family Photos on the Internet').

www.netzbilder.net

www.medienkompetenz.unibas.ch

University of Bern

The institute of information systems at the University of Bern is mainly concerned with innovating and enhancing business processes in organizations by developing and managing computer-based information systems. The focus of the research and teaching endeavours is twofold: firstly, the institute studies principles, methods, and tools for the development and use of information and communication systems, taking into account technical, economic, and socio-economic aspects. Secondly, the institute deals with the management of the information systems function within and across organizations, including its leadership, governance, organization, planning, and control.

http://www.iwi.unibe.ch/index_eng.html

Partly located at the institute of information systems is the competency network digital information, a cooperation project with the Swiss Post, the Faculty of Humanities and the Faculty of Business, Economics and Social Sciences. In this context, in collaboration with Swiss Post (incl. SwissSign, etc), different topics related to cyber security were researched.

University of Fribourg

The **international institute of management in technology (iimt)** conducts research and education in the fields of information security culture, social media security culture, information security management, as well as cyber risk management for energy networks. Besides its internationally recognized research in information security culture, the iimt is involved in projects concerning the "National strategy for Switzerland's protection against cyber risks" since several years.

www.iimt.ch

The Dependable Systems Research Group of the **Department of Informatics** is conducting research on what makes systems more reliable and secure. The research is partly application oriented, but covers also more fundamental problems that arise in the context of dependability: Automata Theory, Temporal Logics, Verification, Formal Methods, Cryptographic Protocols, and Security Models.

https://diuf.unifr.ch/drupal/tns/home

Within the **Faculty of Law** of the University of Fribourg the legal aspects of the application of information and communication technology and the related security problems and challenges are looked at in an interdisciplinary manner.

http://www.unifr.ch/ius/de/home

University of Lausanne

The main cybersecurity related activities are realised within the Swiss Cyber Security Advisory and Research Group – SCARG of the Faculty of Business and Economics. The group offers strategic and practical advice, targeted research, and detailed education in a variety of fields related to Cybersecurity, Cybercrime, Cyber-Defence, Cyber-Conflicts, Cyber-Power, Cyber-Resilience and risk management. The group's specific areas of research include fields related to political, economic, managerial, technical, human, and cultural dimensions of digital risks and security. It contributes to developing an interdisciplinary and integrative cybersecurity approach for citizens, organisations and states as response to real needs of society.

Within the Faculty of Law, Criminal Justice and Public Administration complementary competencies and expertise can be found in legal dimension of information technology and related to justice and police matters.

The Faculty of Business and Economics and the Faculty of Law, Criminal Justice and Public Administration deliver joint interdisciplinary master degree called «Maîtrise universitaire en droit, criminalité et sécurité des technologies de l'information».

www.scarg.org

www.unil.ch/dcs/home.html

University of St. Gallen (HSG)

The research in areas related to cyber security takes mainly place at the Institute of Information Management – IWI-HSG, part of the School of Management.

The IWI-HSG is dedicated to applied and design oriented research at the interface between business and IT. Cyber Security is an integral part of the research topics. The main focus lies on strategic, organizational and design oriented topics such as management of change etc.

The IWI-HSG has recently been involved in the following research projects and subjects:

- Very large IT-Projects and Architecture Management – both with a distinct relation to cyber security.
- Analysis of the trustworthiness of information systems as well as the design and evaluation of trust-supporting design elements for information systems
- Research and expertise related to 1) white and black hat research where security and privacy aspects of the cybercrime are studied to better understand motivation, incentive and reasons for cybercrime behaviours in order to identify counter-measures to mitigate the risks; 2) human factors, being the weakest link, with various aspects which deal with awareness, education, training, persuasive technologies, compliance, etc.

  http://www.iwi.unisg.ch/

Part II: Universities of Applied Sciences

BFH, Institute for ICT-Based Management (ICTM)

The research group “Identity and Access Management” of ICTM is involved in various international and Swiss research projects with a strong focus on Electronic Identities (notably SuisseID), Identity and Access management (IAM) and Security Configuration Management. In most cases prototypes are produced that serve to validate the theoretical results.

Core competences of the IAM group of ICTM are:

- Electronic Identities
- IAM Solutions
- IAM in E-Government
- Security Policy and Configuration Management
- Cloud Security

http://bit.ly/1HzWBg7

BFH, Research Institute for Security in the Information Society (RISIS)

The mission of RISIS is to conceive, design, and implement novel techniques and tools to further advance IT security in the information society. The expertise of RISIS covers a wide range of IT security topics. Activities range from fundamental research over applied R&D to selected consulting services. Projects are supported by various funding agencies including CTI, EU, SNSF, Hasler Foundation, etc.

Core competences of RISIS are:

- Design, implementation and security review of cryptographic systems
- Malware analysis and reverse engineering
- Security engineering in the domains of IP, cellular networks and web intelligence
- Forensic analyses of devices and network/internet activities
- Privacy-by-design such as secure electronic voting, e-ticketing, and road pricing systems
- Working with large sensitive datasets, e.g., in medical applications
- R&D activities of RISIS are regularly published on some of the best known IT security conferences.

http://bit.ly/14dIOx1

BFH, E-Government Institute (EGI)

The research group “Virtual Identity” of EGI is involved in various international and Swiss research and consulting projects on IAM in federated environments. In most cases specifications / standards for governmental institutions or economic models are produced to validate the theoretical results.

Core competences of the Virtual Identity research group of the EGI are:

- IAM in distributed information systems, embedded in heterogeneous social and business contexts, including attribute-based access control and identities of legal persons, servers, and things. A special focus lies on quality models for services.
- Representation, measurement, and controlled evolution of electronic identity (eID) ecosystems – including aspects of legal regulation, policy simulation implementation, PPP collaboration.
- User-centric focus: Reclaiming control of your digital identity through the application of privacy enhancing technologies including trustworthy anonymity.
- Further areas of investigation: Pro-active and reactive measures against identity theft, development of psychological trust models etc.

http://e-government.bfh.ch

FHNW

The FHNW has the biggest computer science department among the Swiss Universities of applied sciences. It has strong research activities supported by various funding agencies including CTI, EU, ESO (European Space Agency) & NASA, SNF, Hasler Foundation, etc. Currently, the CS department is establishing a cyber-security lab for teaching, research and services offered to private companies and government.

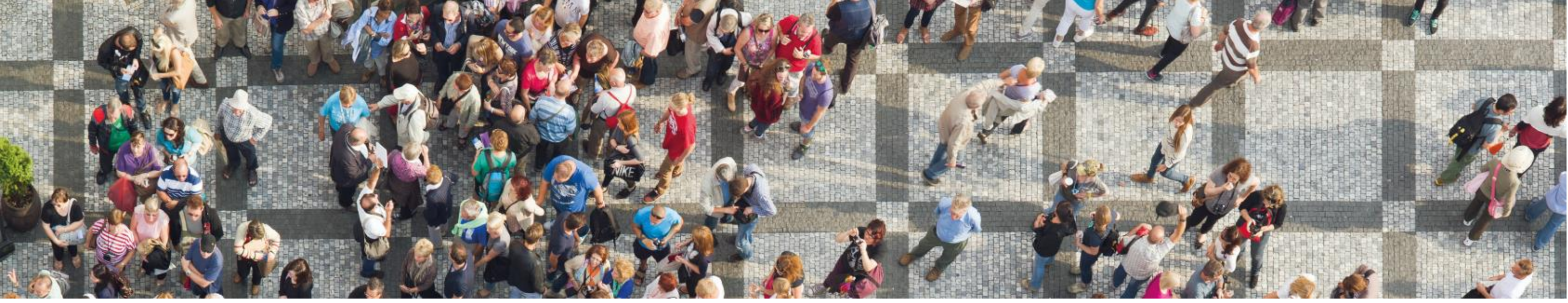
Research in the area of cyber security at FHNW is primarily done at the Institute of Mobile and Distributed Systems (IMVS), focusing on the following topics:

- Network security
- Security for mobile phones
- Security for smart grids and infrastructures
- Security for embedded systems

Current or recently completed research projects in this particular field include:

- Secure data exchange and payment with smart phones via NFC
- Mobile on- and offline NFC based access control systems
- Optimized CPU architecture for cryptologic functions
- Network security: Intrusion detection, defense against DDoS attacks
- End-to-end security for communication applications
- Security in smart grids and infrastructures
- Security concepts for the operation of embedded devices

http://www.fhnw.ch/engineering/imvs



HES-SO, Institut de lutte Contre la Criminalité Economique – ILCE

The ILCE is a multidisciplinary higher teaching and research institution. It offers a Master of Advanced Studies in Economic Crime Investigation (ILCE's flagship course), as well as several Certificates of Advanced Studies, e.g. in financial investigation, computer forensics, and criminal prosecution. ILCE's research activities cover all areas of economic crime, including its law, economic, forensic, IT, and social aspects. Its main fields of expertise in Cybersecurity are computer auditing, digital evidence, human factors and cybercrime.

Through a separate institute, the CINC (Centre d'investigation numérique et de cryptologie), ILCE carries out research in computer forensics and cryptology, and offers highly specialized services to cantonal police agencies and other entities of the Swiss Confederation.

ILCE is also part of HEG Arc's Institute du Management et des Systèmes d'information (imsi.he-arc.ch), which conducts research in the fields of cybersecurity.

Within the HE-Arc, complementary competencies and expertise can be found in business informatics, economics, IT, law, and anthropology.

http://ilce.he-arc.ch

Réf. MAS criminalité économique
http://www.hes-so.ch/data/documents/Brochure-MAS-Lutte-criminalite-economique-1015.pdf

HES-SO, Institute for Information and Communication Technologies – IICT (HEIG-VD)

The University of Applied Sciences and Arts in Yverdon-les-Bains (HEIG-VD) notably delivers a bachelor curriculum involving more than 50 credits fully dedicated to information security, as well as several specialized master-level lectures part of a Master of Science in Engineering. These teaching activities in the domain of information security are possible thanks to a group of three professors that are specialized in information security; they additionally supervise a research group fully dedicated to cyber-security.

The HEIG-VD security group's expertise fields include academic and industrial cryptography, software security, software protection, development of automatic obfuscation and de-obfuscation tools, software reverse engineering, software exploitation, ethical hacking, penetration testing, security processes, network security, design and security assessment of complex IT solutions, design and development of govwares, operating systems security, mobile security, etc.

Additionally, other professors at the HEIG-VD are recognized experts in domains closely connected to information security, such as big-data, cloud computing, and machine learning.

http://www.heig-vd.ch/actualites/2014/12/04/a-bon-entendeur-decrypte-le-fleau-de-la-cybercriminalite

http://iict.heig-vd.ch/

HES-SO, Competence Center for Complex Digital Forensics (HEG-GE, Geneva)

Within the HEG, several people are actively enrolled in cyber-security-related activities. The HEG relies extensively on a network of cooperating partners in academy, industries, public institutions (mainly justice) and police forces. The activities are segregated in several domains:

- Bachelor, master and continuous education courses on security governance, secure software development, eDiscovery and digital forensics methods;
- Academic research in eDiscovery and Small Scale Devices Digital Forensics, with many projects and publications and the recent creation of the Swiss Competence Center for Complex Digital Forensics in collaboration with HSLU;
- Consultancy to companies, from SMEs to large corporates;
- Training for law enforcement bodies;
- Expertise for courts of justice in civil litigation or criminal investigation.

In the academic field, our main partners are in Switzerland (other HES-SO departments, University of Lausanne, HSLU Lucerne) and worldwide (University of Stockholm, University of Montpellier, University of Nice…).

http://www.grstiftung.ch/de/portfolio/projekte/alle/y_2011/GRS-060-11.html

http://3cdifo.hesge.ch/

HSLU

HSLU has in general no specific cyber research know-how. However, specific employees have in-depth know-how e.g. in security, artificial intelligence, big data and crypto.

Distributed Secure Software Systems Institute

The Distributed Secure Software Systems Institute (D3S) specializes in process support, mobile systems, artificial intelligence, image processing, security, data management and software engineering.

https://www.hslu.ch/de-ch/technik-architektur/forschung/kompetenzzentren/distributed-secure-software-systems/

Institute for business informatics – IWI

At the Institute for Business Informatics (IWI), applied research and development consists of researching topics, developing solutions and putting these into practice. IWI is committed to a business-oriented use of computer science.

https://www.hslu.ch/de-ch/wirtschaft/ueber-uns/institute/iwi/

ZHAW, Institute for Applied Information Technology – InIT

In the InIT the cyber security research themes are Secure Applications and Systems and Information Infrastructure Protection.

In the Secure Applications and Systems area the InIT has a strong expertise in secure web- and mobile applications design. Its applied research focuses on studying and refining methods and tools to design secure software and services and to develop new security mechanisms where required.

In the information infrastructure protection area the InIT has a strong expertise in securing traditional and cloud computing infrastructures. Its applied research focuses on studying and refining methods and tools to protect data in the cloud, to detect and mitigate cyber-attacks, to do privacy preserving authentication and data sharing and on malware techniques for testing and training purposes. Furthermore, research related to methods and tools in risk assessment and risk engineering of IT infrastructures complement the profile of the InIT as well as expertise from other focus areas of the InIT like cloud computing (ICCLab), data science (DataLab), information engineering, distributes software systems and human-information interaction.

https://www.zhaw.ch/de/engineering/institute-zentren/init/

Images: © Fotolia