CyberSchool: Development of the first *Ecole Universitaire de Recherche* in cybersecurity in France

Frédéric Renouard, Université de Rennes and Pierre-Alain Fouque, Université de Rennes

***Abstract* — CyberSchool is a winning project of the French "Investments for the Future" program and is the only *Ecole Universitaire de Recherche* (EUR) in cybersecurity in France.**

Launched in 2020, CyberSchool is coordinated by the Université de Rennes 1 and relies on the cooperation of Rennes universities, four major engineering schools (Université Rennes 2, CentraleSupélec, IMT Atlantique, INSA Rennes and ENSAI), ENS Rennes, Sciences-Po Rennes, in close collaboration with the CNRS and the Inria Rennes Bretagne Atlantique Center, with the support of the DGA, the Brittany Region and Rennes Métropole.

CyberSchool aims at offering innovative and international training, backed by research, at Master's and Doctoral level. The school trains future experts, engineers and scientists, involving them from their first year in research, in all key areas related to cybersecurity.

CyberSchool offers a complete and interdisciplinary program on the challenges of digital security, combining mathematics, digital sciences and technologies and human and social sciences around six research axes.

The article describes some of the issues and solutions implemented to develop an interdisciplinary training offer in cybersecurity – creating a coherent offer of courses at master's level – bringing together the strengths of a network of ten academic partners.

***Index terms* — cybersecurity, Ecole Universitaire de Recherche, EUR, graduate school, master program, pedagogical cooperation**

I. Introduction

Cybersecurity is a worldwide key strategic concern with the explosion of digital technologies raising major sovereignty issues and privacy challenges. In this context, cybersecurity is facing a major training and recruitment problem. Rennes has many distinctive assets to tackle this challenge. It features research teams covering the cybersecurity chain, from Physics to Law, through Electronics, Maths and Computer Science, either in CNRS joint labs, in Inria or in companies such as Orange Labs. Together they represent over 140 researchers and lecturers. A dense socio-economic ecosystem in cybersecurity has been furthermore steadily developed in Rennes over the past 30 years, with a major acceleration since 2014 when the national Center of Excellence in Cybersecurity (PEC) was created by the Ministry of Defence and the Brittany Region to foster training, research and innovative start-ups development. Based in Rennes, the PEC has multiple dimensions: civil-military, private-public, research-education-innovation. It federates Ministry's entities, the IRT B<>com and numerous companies ranging from large groups (Orange, Airbus CyberSecurity, Thales, …) to SMEs and startups, as well as public research labs, universities and schools.

CyberSchool has been designed as a research-oriented Graduate School in cybersecurity aiming at training future engineers and scientists through early exposure to contemporary research in all security related issues. It draws on the expertise of Rennes 1 and Rennes 2 universities, the ENS, 4 prestigious schools of engineering (CentraleSupélec, IMT Atlantique, INSA Rennes and ENSAI) and Science-Po Rennes. CyberSchool also benefits from the strong involvement of CNRS and Inria.

II. CyberSchool objectives, challenges

Thanks to CyberSchool, the aim is to double the number of students in cybersecurity in Rennes (from 100 to 200 Master's graduates each year).

CyberSchool aims at offering an innovative and attractive scientific training at Master's and PhD levels focusing on both fundamental and advanced areas of cybersecurity. It applies an interdisciplinary (see figure 1) approach to tackle security challenges by combining mathematics (cryptography), digital science and technologies (electronics, computer science, system security, privacy, formal methods) and social sciences (law, use, acceptability). The school deals with theories, methods and algorithms ensuring a secure digital society as well as with the contents to be protected in a wide variety of settings and conditions of use (mobility, cloud, industrial systems).

CyberSchool priority is to produce experts by training scientists (PhD students) and engineers (master or engineering school students). However, introductory courses will be opened to other master programs. More generally the Cyberschool wants to better foster the relationship between the academic and industrial worlds and to help mitigating the skills gap crisis.

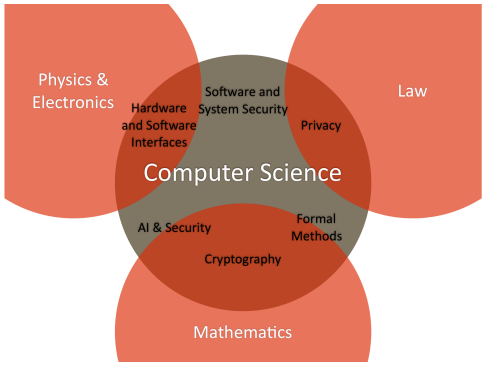

Figure 1: CyberSchool cross-disciplinarity

CyberSchool will offer students the ability to pursue their education to the highest level, according to each student's ability. CyberSchool's innovative approach w.r.t. the French system consists in bridging the gap between the Master studies and the PhD studies, breaking barriers, and making the master students working shoulder to shoulder with faculties. PhD students should not be the only ones deserving to carry on research activities, because research is a way of thinking. Courses will thus be opened to both Master and PhD students, leading to blended and dynamic studentship audiences.

Goal is also that it becomes self-evident for students who graduate that they can advance their knowledge and skills with PhD studies. Currently, companies instead enroll students before they figure out that PhD studies might be a long-term investment for their career. CyberSchool aims at better involving companies in the definition of the curriculum and in the teaching and research activities. In particular, PhD students will soon be encouraged to perform a 2-month internship in a company during their studies.

While research activities are already well structured thanks to CNRS' UMRs (joint labs), the education programs in cybersecurity are fragmented, and spread over many institutes. This is due to the existence of numerous higher education institutions that have separately started different curriculums in cybersecurity almost fifteen years ago. CyberSchool will deeply mutate Rennes' education landscape in cybersecurity.

This transformation is possible because universities and schools in Rennes are not competitors. Instead, they provide complementary programs to different types of students:

- On the one hand, cybersecurity requires both an extremely solid background in computer science, together with additional skills relative to the threat landscape, security concepts and tools, and a good understanding of law, human factors and social sciences, economics, and risk management. This interdisciplinary nature of cybersecurity fits the competence of the EUR partners, and Rennes is a good place to cover all the aspects of cybersecurity in an integrated way.
- On the other hand, due to their natures, the EUR partners are able to provide an education program that fully complies with the Knowledge, Skills, and Abilities requirements. Very broadly, on the technical aspects of cybersecurity, the engineering schools train very strong students with theoretical backgrounds (skills, since engineers must be operational on day one), while ENS Rennes and universities better perform on the fundamental education (knowledge).

This transformation is possible also because EUR partners are already close collaborators, both in research (with common research teams at IRISA and other labs) and education (e.g., through a joint research master). Most of them also are located on the same campus.

III. CyberSchool Master programs architecture

CyberSchool offers two formats of master programs of 120 ECTS: a 'traditional' and a 'work-study' format. Both are divided into 4 semesters, comprising lectures, tutorials and practical work (see figure 2). The teaching is provided in French and English.

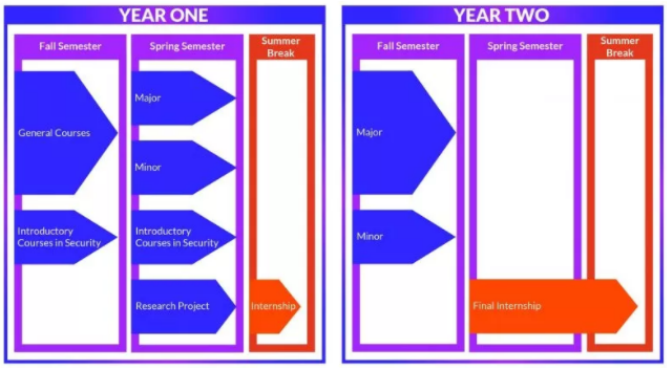

Figure 2: CyberSchool master programs architecture

In the 'traditional format', students select a security Major and a Minor, conduct a research project in cybersecurity in an academic lab (half-day a week during year one), and complete an internship during the last semester. This format targets students who demonstrate a strong aptitude for research.

In the 'work-study' format, students share the same programme architecture in year one as the 'traditional format' and complete a work-study during their second year of studies. They spend 60% of their academic year working within a company and 40% in class. This format, which combines theory and practical in-company training, provides students with concrete professional experience. It is mainly geared towards students who wish to begin a career in industry after their studies.

On top of that, all CyberSchool students are encouraged to do an internship during the summer break between year one and year two.

Students are trained by doing research as soon as possible

during the master. Since research labs are collocated on the university campus, students realize a research project during year one and will work half-day a week in the labs. It introduces all students to research thinking and also allows us to detect the best highly skilled students, who fulfill the requirements for realizing an excellent PhD.

Table 1 presents the general courses in Computer Science and Mathematics for all cybersecurity Majors. The introductory courses in Security are taken by all CyberSchool students, and possibly by students outside CyberSchool, and provide the basics in Cybersecurity for Computer Science master students.

General Courses	Introductory Courses in Security	Minors
Computer Science Analysis of Algorithms Assembly and C Language Operating System Database Network **Mathematics** Discrete Maths and Graph Algebra for Cryptography Machine Learning	**Introduction to Cryptography** **Software Security** **System Security** **Network Security** **Information Security** **Privacy**	**Cryptography** **Formal Methods** **Software & System Security** **Hardware & Embedded** **AI & Security** **Privacy and Law** **Innovation & Entrepreneurship (EIT Digital)** **Digital Law (UR1 Law dpt)** **Security, Defense and strategic intelligence (IEP)**

Table 1. CyberSchool General, Introductory and Minor Courses

CyberSchool aims at offering 6 different Majors with advanced courses that are taught by experts or researchers from all partners (cf. Table 2). Majors are aligned with the research topics in cybersecurity in Rennes: Cryptography, Software and System Security, Hardware and Embedded Systems, Formal Methods and Security, AI and Security and Privacy. These majors allow students to best suit their interests and career goals.

Major Cryptography	Major Formal Methods	Major Software & System	Major Hardware & Embedded	Major AI & Security	Major Privacy & Law
Lattice-based Cryptography Lattice Problems: SVP/CVP Lattice alg. & cryptanalysis **Security Proofs** Security of Lattice Schemes Other Crypto Primitives **Elliptic Curve Cryptography** Elliptic Curve Theory Isogenies **Symmetric Cryptanalysis & Error-Correcting Code** Statistical Attacks for Block and Stream Ciphers Boolean Functions Coding Theory	**Security Policies** Non-interference Declassification **Cryptographic Protocols** Symbolic Technique Computational Technique **Obfuscation & Binary Analysis** Obfuscation Reverse Engineering Compilation **Language Based Security** Formal semantics Static Analysis Proof Assistants	**Intrusion Detection System** Anomaly detection Behaviour /Signature **Malware Analysis** Static / Dynamic Analysis Concolic Method **Pentest** Network Security Exploit **Software Security** Buffer Overflow Fuzzing	**Side-Channel Attack** SPA / DPA analysis Masking Countermeasure **Fault Attack** Electromagnetism Rowhammer **Timing Attack** Cache Prefetch **Secure Hardware Element** SGX / TEE Security	**AI for Security** ML for Side-channel ML for Intrusion Detection Watermarking **Security for AI** Robustness of ML algorithms **Economic & Security** Recommandation System Cryptocurrencies	**Applied Cryptography** Key Exchange Security of OB Homomorphic Encryption **Law** Privacy (GDPR) Intellectual Property Reverse-Engineer Licences

Table 2. CyberSchool Majors

To encourage multidisciplinarity, students also have to choose a Minor either in the basic level courses of a Major, or in "Innovation & Entrepreneurship", already offered at EIT Digital Rennes, which aims at developing students' entrepreneurial and innovation skills.

Currently, CyberSchool organizes and runs two cybersecurity Master's programme, offered within Université de Rennes 1.

1) **Mathematics and Applications – Mathematics and Cryptography track, which includes the cryptography major.** The programme trains students to become digital information protection experts. Students are able to master the complex mathematics involved from both theoretical and algorithmic points of view and implement them in very diverse infrastructures.

With the cryptography major, students will gain in-depth understanding of cryptography by learning the necessary theory behind modern cryptography and information theory, as well as practical knowledge for effective application in real life. Students approach fundamental mathematics for modelisation and digital information in order to master mathematics and algorithms, such as algebra, geometry, combinatorics and probability.
Graduates are able to apply for the following positions:

- R&D Engineer and IT Security Developer,
- Research Engineer specialized in IT security,
- Security Software Developer.

2) **Computer Science, Cybersecurity track which includes the Software & System Security major and the Hardware Security major.** The programme trains specialists skilled in assessing and ensuring security of information infrastructures. Students will be able to design, code, validate and manage new secure architectures or assess and correct existing architectures to protect them from cyberthreats.

With the Software & System Security major students focus on software, system, and network security. They study subjects such as security, reverse engineering, network and protocol security, cryptography, and security management. The first year of the Masters concentrates on reviewing IT system design: object-oriented analysis and design, compilation, project management, and a software development project. In the second year, students specialize in system infrastructure security.
Graduates enter the workforce as information system infrastructure security specialists and are recruited in positions where they design, create, and ensure the robustness and the security of complex IT architectures.

With the Hardware Security major students focus on IoT's ecosystem security. They discover the methods, tools, technical means necessary for the audit of embedded electronic systems: key concepts of electronic architectures, interfaces with their external environments, embedded software. Vulnerabilities at all these levels and as the theory necessary for the understanding of security challenges in these environments (Cryptography and associated mathematics, signal processing basis) will be presented to students.
Graduates are able to apply for the following positions:

- Pentester or embedded systems auditor,
- Cybersecurity consultant in the field of IoT.

IV. Institutional and Pedagogical Cooperation

Cooperation within the CyberSchool results both from a commitment of the partner establishments themselves but also from the direct involvement of the teachers of these establishments. CyberSchool then aims at fostering both institutional and teachers' cooperation.

CyberSchool institutional cooperation – The CyberSchool Master will soon be co-chaired by several of the CyberSchool partner institutions. Students will continue to be enlisted in their own institution. Students having successfully followed a CyberSchool track will receive the diploma of their own institution and initial curriculum and another one from CyberSchool.

CyberSchool teachers' pedagogical cooperation – The development of teachers' pedagogical cooperation within the CyberSchool is key to support the expansion of our training offer and the increase in the number of students, for the benefit of our students and teachers. This is indeed the way:

- To allow the improvement of the quality of education, in particular through the exchange of practices and feedback,
- To allow the joint development and/or sharing of courses and educational resources, by pooling efforts and investments,
- To better meet our growing needs for teachers, by enabling the upskilling of young teachers, particularly in electronics, AI and security, SHS,
- To allow the development of new teaching methods,
- To respond to concrete problems of teachers, to save time, find speakers and educational resources.

CyberSchool instruments allowing the development of pedagogical cooperation between teachers in cybersecurity will therefore occupy a central place in the CyberSchool.
Such instruments, coordinated and led by the CyberSchool in conjunction with the partner establishments, are or will be:

- The teachers' community of practices in cybersecurity,
- An inter-establishment catalog of cybersecurity courses,
- A program of extra-curricular activities and inter-establishment conferences,
- A catalog of shared educational equipment and resources,
- Support for teachers involved in cooperation projects.
- The community of practice occupies a central place. The other instruments are at the disposal of this community and enriched by it.

The community of practice occupies a central place. The other instruments are at the disposal of this community and enriched by it.

V. Next steps, perspectives

The development of the CyberSchool is a 'work in progress'. It is original in several respects, among them the large portfolio of cybersecurity Majors and Minors we are aiming at, the close link with research and the importance of both institutional and teachers' pedagogical cooperation.

Other important objectives of the project have not been presented here and are currently being developed. Notably:

- A CyberSchool doctoral track, which will be offered from mid 2022 to all doctoral students in cybersecurity,
- National and international cooperation. Such cooperation will build on bilateral cooperation as well as on existing networks where notably the Université de Rennes 1 is involved, such as EIT Digital (with its European Master School and its cybersecurity program) and the EDUC European University (with its focus on virtual/hybrid/short mobilities and the internationalization of programs).

Other areas of extension are considered to extend the reach of the CyberSchool, such as bachelor tracks and lifelong learning. Finally, introductory courses in good behaviors in computer and cybersecurity for non-specialized students are currently studied.

References

CyberSchool Master study programme:
https://cyberschool.univ-rennes.fr/en/study-programme/

CyberSchool Master career opportunities:
https://cyberschool.univ-rennes.fr/en/education/masters/career-opportunities/