CyberMACS

Handbook for Candidates

Erasmus Mundus Master's Programme in Applied Cybersecurity

2025-2026

Consortium

Beneficiaries

Kadir Has University (KHAS)
SRH University of Applied Sciences Heidelberg, Berlin campus (SRH Berlin)
Ss. Cyril and Methodius University (UKIM)

Associated Partners

Lostar
Rijksuniversiteit Groningen
Cyber Struggle
Masit Skop Chamber of Commerce for Information and Communication Technologies - Masit Skopje
Tacas Tac Bilişim Hizmetleri İç Ve Dis Tic. A.Ş.

Foreword

Dear CyberMACS Students and Prospective Candidates,

This Handbook aims to provide essential information (programme rules, guidelines, and procedures) for current students and candidates interested in the CyberMACS, the full-time 2-year joint European MSc programme focusing on "Applied Cybersecurity". The Handbook summarises the programme's partner universities, application, selection and scholarship management, programme structure, joint events and internships, CyberMACS curriculum and course descriptions, academic assessments, master thesis and graduation, and the Erasmus Mundus Student and Alumni Association.

Please acknowledge that this document should be read in conjunction with the other official documents such as the Welcoming Guide, Student Agreement and academic regulations of the Partner Universities and Programme webpage, www.cybermacs.eu.

While the Welcoming Guide is prepared to provide practical tips about visas, accommodation, etc., the Handbook contains additional information to help you make your academic journey more successful and smoother. Please acknowledge that the Handbook can be revised and modified concerning the updates and developments in CyberMACS.

With any feedback, comments, and suggestions, please feel free to contact us at info@cybermacs.eu

We are looking forward to welcoming you soon!

CyberMACS Team

CONTENTS

ABBREVIATIONS

NC : Non-Credit

C : Compulsory

CEFR : Common European Framework of Reference for Languages

E : Elective

EACEA : The European Education and Culture Executive Agency

ECTS : European Credit Transfer System

KHAS : Kadir Has University

CCIP : Centre for Cybersecurity and Critical Infrastructure Protection

SRH : SRH University of Applied Sciences Heidelberg (Berlin campus)

UKIM : Ss. Cyril and Methodius University

1. Partner Universities of CyberMACS

The dramatic rise in cyber-attacks has made cybersecurity a significant global concern. It is estimated that cybercrime cost the world economy about $1 trillion in 2020. In February 2021, a cyber-attack targeted a water treatment facility in Florida to change chemical levels in the water supply. In May 2021, a ransomware attack targeted the largest fuel pipeline in the USA. Cyber-attacks come in all shapes, including worldwide data breaches affecting companies and people. For instance, a social media app cyber-attack resulted in 1.3 million users' information leakage.

The changing landscape of cybersecurity threats requires the urgent need for comprehensive, dynamic, and applied cybersecurity education to qualify cybersecurity professionals to prevent, mitigate, and manage threats. **CyberMACS** proposes a full-time 2-year joint European MSc programme (120 ECTS) focusing on "Applied Cybersecurity" to provide a solid background within cybersecurity with a focus on educating future cybersecurity experts to detect, prevent, mitigate, and manage cyber-attacks.

During this programme, you will be trained in the basics of cybersecurity in the first year. Opportunities will be provided for specialisation in the second year with compulsory following the winter/summer schools and compulsory internship. Besides specialisation tracks, you will receive training in soft skills such as entrepreneurship and complete your degrees with master theses.

To guarantee CyberMACS's vision of high-quality education, three European higher educational institutions combine their complementary competencies: Kadir Has University (KHAS) (the Coordinator University), SRH University of Applied Sciences Heidelberg, Berlin campus (SRH) (full partner University), and Ss. Cyril and Methodius University (UKIM) (full-partner University).

In addition to the leading partner Universities, the programme is supported by an academic associated partner (Groningen University) and four non-academic associated partners (***Cybersecurity Companies***: Lostar, Cyber Struggle and TAC AS; ***Industrial Associations***: Chamber of Commerce for Information and Communication Technologies - MASIT Skopje). CyberMACS' associated partners will contribute to the programme by delivering special lectures on cybersecurity (such as legal aspects of cybersecurity), facilitating your internship processes, enhancing your career prospects in cybersecurity, and keeping the CyberMACS curriculum dynamic.

CyberMACS is a solid institutional cooperation for European excellence in higher education with a high-level integrated & transnational study programme on applied cybersecurity targeting the best students worldwide.

1.1. Kadir Has University (KHAS)

Kadir Has University (KHAS) was founded in 1997 in Istanbul. The university, with its five faculties (Art and Design, Communication, Economics and Administrative Sciences, Engineering and Natural Sciences, and Law), is dedicated to becoming a leader in educational and cultural fields in Türkiye and establishing itself as an international centre for research and scientific development. KHAS aims to become a research university at world standards that can produce sustainable solutions to local, national, regional, and global problems faced by humanity with an approach based on universal and humanitarian values; to train students equipped with individual

and professional competencies in their fields of expertise; can produce high-impact research outputs as well as human-oriented and innovative solutions for social problems and is capable of transferring the knowledge it makes to the society in all dimensions. KHAS's master's program on cybersecurity has been accepting students since 2018. The department works in collaboration with KHAS CCIP (Cybersecurity and Critical Infrastructure Protection), a research centre dedicated to developing innovative solutions for the cybersecurity of critical infrastructures. You can check the other information regarding KHAS in your Welcoming Guide or on the University's webpage.

1.2. SRH University of Applied Sciences Heidelberg, Berlin campus(SRH Berlin)

SRH Berlin, part of SRH Holding, is a private school founded in 2006. It is divided into 17 schools located all over Germany , with 385 teaching and research staff. SRH is a very international university with 383 staff members and almost 20.000 students from all over the globe. SRH offers more than 200 study programmes. The cybersecurity department in SRH enjoys excellent relations with the industry including big players in cybersecurity, such as Deutsche Telekom AG, Siemens AG, Bosch AG, and Deutsche Bahn AG. SRH's cybersecurity master's degree is listed as one of the best Cyber Security schools for 2019. You can check the other information regarding SRH in your Welcoming Guide or the University's webpage.

1.3. Ss. Cyril and Methodius University (UKIM)

UKIM is the largest state University in the Republic of North Macedonia. The University was founded in 1949 and comprises 22 faculties, 5 research institutes and 11 accompanying members. Currently, UKIM has around 50000 enrolled national students and over 700 international students. UKIM has more than 2300 teaching and scientific staff and over 300 associates engaged in the faculties' teaching, educational, and scientific processes. UKIM has long-term cooperation with more than 75 foreign universities participating in many international projects. The University provides the most significant part of ICT experts for the Macedonian labour market. You can check the other information regarding UKIM in your Welcoming Guide or on the University's and Faculty webpage.

2. Application, Selection and Scholarship Management

2.1. Application

To ensure full transparency, the applications and admission process of CyberMACS are clearly defined on Programme's website. Even though the general layout regarding the applications is identified below, it is always recommended that students check the Programme website with respect to recent updates and changes. Please check the general eligibility requirements from our webpage.

Student application, eligibility, selection, admission, and scholarship attribution are based on joint criteria and procedures identified by the three Full Partners. **The application process is entirely online.** No application is accepted in any other form.

Non-submitted applications, incomplete applications, and applications received after the application deadline are not taken into consideration. All completed applications are recorded and archived to ensure full transparency of the selection process.

For a student application for the Programme to be considered, the candidate must comply with the minimum requirements regarding administrative, academic, and *language prerequisites*.

Administrative prerequisites are:

(a) Compliance with the application calendar and deadlines.
(b) Submission of a complete set of required application documents in English (certified English translation if needed).

Academic prerequisites are:

(a) Completed Bachelor of Science in computer science, computer engineering, electrical/electrical-electronics engineering or another degree in science (physics, math, information technologies, management information system, information system engineering etc.) recognized by the EU as a 1st or 2nd cycle degree equivalent to at least 180 ECTS. The required background consists of sufficient studies in:
- *mathematics (linear algebra, calculus, probability theory, statistics, and discrete mathematics)*
- *programming skills*
- *algorithms and data structures*
- *databases*
- *theory of computation*

This prerequisite must be fulfilled at the time of administrative enrolment. Applications from students in the last year of Bachelor or equivalent study programmes will be accepted conditionally. Students with a different background from those mentioned above have the right to apply. The application will be reviewed thoroughly to determine whether completing the degree requirements successfully is possible.

Language prerequisites are:

(a) Proficiency in written and spoken English at a B2 level of the Common European Framework of Reference for Languages (CEFR) duly confirmed by language certificates **specified in the Call for Applications.**

Applicants who are not awarded an EMJM scholarship grant may be admitted if they meet the academic prerequisites.

Call for Applications

(a) The Call for Applications is launched and disseminated prior to every edition (intake) at least three months before the application deadline specified by this Call.
(b) The call clearly states the application deadline.
(c) All the relevant and updated information on the Programme, particularly the tuition fees, application procedures, required documentation and Programme curriculum description, are published on the Programme website.

Application process

(a) The application process **is entirely online.**
(b) **No application is accepted in any other form.**
(c) Non-submitted applications, incomplete applications, and applications received after the application deadline are not taken into consideration.
(d) All completed applications are recorded and archived to ensure full transparency of

the selection process.

Required Documentation

Required documentation must be uploaded as digital copies and in the English language. The required documents are:

(a) A completed application form.
(b) Curriculum Vitae (preferred format: Europass).
(c) A cover letter (max. 1000 words) demonstrating the consistency between the Programme's objectives and the applicant's motivation, academic/professional background, and professional project.
(d) A scan of the passport (a scan of the national ID will be accepted conditionally if the applicant does not have a passport at the time of application).
(e) Proof of residence (residence certificate or a certificate from the applicant's workplace, study institution or training institution; certified translation to English).
(f) A scan of an official 1st cycle degree diploma or another eligible diploma in bachelor, along with an official supplement listing courses taken and the respective grades (certified translation to English). **If the applicant has not completed the 1st cycle degree at the time of application, she/he must send available transcripts, proof of current enrolment, and a declaration of the end date.** The bachelor's diploma must bear the university's and the relevant Higher Education Institution's stamp.
(g) **At least two recommendation letters** specifying the contact details of the referees. The referees can upload their reference letters online.
(h) Certificates of English language proficiency, at least B2 level of the CEFR. The list of accepted certificates will be published along with the Call for applications.
(i) If applicable, any academic publications of which the applicant is the first author or a co-author. In case of publications in languages other than English, an English translation of the abstract should be provided.

Privacy policy

Applicants' personal information will be collected and used in accordance with Regulation (EC) N° 45/2001 of the European Parliament and of the Council from December 18, 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L8 of 12.1.2001, p. 1).

Application support

Dedicated contact forms for technical support (ensured by the Full Partner responsible for the application process), administrative matters and content-related questions (ensured by the Coordinating Institution). Every request is tried to be answered within 3 business days.

2.2. Scholarship Management Rules of EACEA and CyberMACS

CyberMACS Joint Selection Committee selects scholarship students with respect to their **academic merit** (to be assessed in the three-stage process defined in Section 2.3) **and geographical balance.**

The Scholarship holders shall comply with the following conditions:

(i) have — at the date of enrolment — a first higher education degree (or demonstrate a recognised equivalent level of learning according to national legislation and practices in the degree-awarding countries)

(ii) not have already benefitted from a previous Erasmus Mundus Joint Masters (EMJM) scholarship

The scholarship is awarded for full-time enrolment and will cover the entire duration of the master's programme.

Max 10% of (regular) total scholarships that CyberMACS plan to grant can be provided to students of the same nationality.

2.3. Selection and Scholarships

Ensuring equality and transparency are the key principles of CyberMACS. To this end, we publish our selection process on our Programme website in addition to the results of each student edition period.

The 3-stage processing and selection include the following criteria and procedures:

Screening phase: Applications are first checked for completeness of the required documents. The applicants with missing one or more documents are not considered further.

Administrative, language, and academic validity check: Applications passing the screening phase are subjected to further detailed administrative and academic checks. At the end of this process, invalid applications are put aside with no further processing, while valid applicants are elevated to the detailed academic merit-based processing and ranking level. The verified applicants' documents are evaluated by two selection committee members separately and assigned a grade. The average of both grades is used for ranking.

Interviews: Depending on the applicant's ranking, the 10% cap on scholarship holders from a particular country, and the number of students foreseen for admission, the following rules were applied for developing an interview list and conducting the face-to-face (online) interview. Every applicant called for an interview by joint selection committee members is first given a 30-minute 25-multiple choice computer and math basics test. The formation of the interview has the following rules:

> If there are less than or equal to six applications from a country, every applicant passing the administrative, language and academic validity is called for an interview.
>
> If there are seven to ten (inclusive) applications from a country, then the top-ranked 50% of all applicants passing the administrative, language and academic validity are called for an interview.

If there are more than ten applications from a country, then the top-ranked 30% – 35% of all applicants passing the administrative, language, and academic are called for an interview.

At the interview stage, students are evaluated based on their motivation, experience, and ability to integrate into this international program.

Applicants are then ranked depending on their overall mark, including the mark for merit (75%) and motivation (25%). The mark is not changed after application of the other criteria. Two main ranked lists and one ranked reserve list are then drawn up.

The consortium determines the numbers in each list (full scholarship or self-financed) every year.

Applicants offered a full scholarship are not allowed to change their mobility path; however, applicants offered a self-financed option are given a chance to petition a change of mobility path. The Executive Board evaluates the petition, and a final decision is then made.

In the case of equality with male students, female students are promoted right before male students with the same overall mark.

Geographical limitations apply then.

If a student on the full scholarship list should decline the offer or should not reply in due time, the next student on the reserved list is offered a place with a scholarship**, except if his/her nationality quota has been reached.** If so, the next student on the main list is considered for a scholarship.

The Program Manager communicates the absolute ranking to The European Education and Culture Executive Agency (EACEA). All candidates admitted to the interview phase are informed by email of the final score of their application and their place in the ranking. These notifications are sent no later than one week after the end of the interview period.

Additionally, admitted candidates are informed of their allocation to a mobility path and of the enrolment procedure and provided with all relevant documents, including the Student Agreement.

Candidates who have been awarded the EMJM grant shall receive the Notice of Letter, a document notifying the grantee that an award has been made, containing or referencing all terms and conditions of the award, as well as the Scholarship Contract.

Appeal Procedure

If the applicant believes there has been a failure in the admissions procedure or that they have been discriminated against unlawfully, the appeal procedure is open. **All appeals should be made in writing within ten days after the decision has been communicated.** All appeals should be directed to the European Programme Coordinator (Prof. Dr Hasan Dağ) unless the appeal is regarding the Coordinator, in which case the written appeal should be directed to the Executive Board.

Any appeal is accorded thorough consideration and is normally addressed within 28 calendar days of receipt. Where an appeal does not produce the outcome sought by the applicant, reasons are given for any decision.

The Executive Board is encouraged to acknowledge when an error has been made and to take steps to ensure that similar problems do not arise in future.

Due to data protection requirements, the Executive Board will only correspond on any issue regarding an application with the applicants themselves unless the applicant has provided written permission to discuss it with another person.

2.4. Enrolment and Registration

All students should be enrolled at their starting university and subsequently at the universities at which they are hosted as part of their compulsory mobility paths.

The Local Administrative Coordinators will communicate the information about all students enrolled at their university to the students with respect to the Academic Calendar and Institutional procedures.

3. Programme Structure, Mobility, Curriculum and Course Descriptions

The main idea or the philosophy of the Joint European Master Programme is to have students be exposed to different cultures, be trained by as many other institutions and professors as possible, and exchange ideas/experiences with students worldwide. Thus, each student in the program must have at least two compulsory mobilities.

Kadir Has University offers the first year of the CyberMACS curriculum. The second year will be completed at one of the other consortium universities: UKIM and SRH Berlin.

CyberMACS academic structure follows a joint program which is an outcome of solid cooperation of partner universities by combining different disciplines and sub-branches of cybersecurity that can be studied at various universities.

The Master's thesis is written under the joint supervision of both the first- and second-year universities. The language of instruction in all universities is English.

You will start all together at KHAS with the active support of the University of Groningen, SRH and UKIM and acquire core competencies in both basics of computer science and cybersecurity, but also soft skills such as communication skills, research methods, and project development skills will be provided.

During the second year, with respect to your mobility, you will specialise in cybersecurity management/ cybersecurity technologies/ cryptography or web and security. In this vein, the consortium represents all relevant branches necessary for theoretical research and practical applications in cybersecurity.

The CyberMACS programme is designed based on the employability need of the students. The programme encourages a proactive mindset through innovative teaching and training methods such as joint courses, interactive labs, hands-on training, competition etc.

3.1. Courses at KHAS

The first year of CyberMACS is dedicated to the **fundamental courses of the field of cybersecurity** at KHAS, including the research methods and language courses to enhance your intercultural awareness and support you to integrate into the academic life, social and cultural community in Türkiye.

Year/Partner	*Term*	*Course Name*	*ECTS*
2024/ KHAS	*Fall*	Introduction to Data Science Tools / Artificial Intelligence (C)*	NC***
		Seminar** (C)	1
		Research Methods and Scientific Ethics (C)	6,5
		Cybersecurity Basics (C)	7,5
		Computer Networks and Security (C)	7,5
		Operating Systems & System Programming (C)	7,5
		Language Courses: Turkish I,	NC

* C : Compulsory
** Seminar : Seminars will be collectively held in Winter School.
*** NC : Non-Credit
Ei : i^{th} Elective Course

Year/Partner	*Term*	*Course Name*	*ECTS*
2025/ KHAS	*Spring*	Cryptography (C)	7,5
		System Exploitation and Penetration Testing (C)	7,5
		Elective Course (E1)	7,5
		Elective Course (E2)	7,5
		Language Courses: German I, or Macedonian I	7,5

List of Elective Courses (E):

Course Name	*ECTS*
Information Security Management Systems	7,5
Scripting Languages for Cybersecurity	7,5
Cyber Resilience	7,5
Legal Aspects of Cybersecurity	7,5
Cyberwarfare	7,5

Course Descriptions at KHAS

Introduction to Data Science Tools: This course aims to familiarise students with Data Science and Big Data fundamentals. Students will be trained in the skills needed to become a data scientist, including Introduction to R (Python) Programming and Advance Features in R (Python). The course introduces students to Visualization (Basic principles, ideas, and tools) and Advanced Visualization in R (Python). Exploratory Data Analysis and the Data Science Process will be presented. Basic tools (Visualization: plots and graphs and summary statistics) of EDA Using R (or Python) will be provided. Statistical Inference and Extracting Meaning from Data (Feature Generation, Feature Selection algorithms – Filters; Wrappers; Decision Trees; Random Forests, Example: Churn Analysis will be taught. Three Basic Machine Learning Algorithms - Linear Regression will be presented. Ethical Issues in Data Science (Privacy, Security, and Ethics) will be introduced.

Research Methods and Scientific Ethics: This course introduces graduate students to essential topics in social science research, such as epistemology, research design and methodological choices. Students will learn basic concepts such as method, theory, paradigm and research ethics, and approaches such as positivism and post-positivism. Students will be given a comprehensive education on qualitative and quantitative research methods. Students will learn about the stages of research in social sciences. Philosophy and sociology of information, theory, positivist social science, quantitative research methods, post-positivist and critical social science, feminist and

post-modern research, qualitative research methods, theory research design and method, literature review, writing strategies, research ethics, and the politics of social research.

The competence objectives of this course are as follows:

1. To understand, define and explain the basic concepts and approaches in social research,
2. To gain the ability to use qualitative and quantitative research methods,
3. To acquire knowledge of social research processes,
4. To gain experience in designing social research.

Cyber Security Basics: This course will equip students with fundamental knowledge in the cybersecurity field. The course introduces key concepts and definitions, assets, cyber threats & vulnerabilities, and inherent risks. The course will familiarise students with a comprehensive cybersecurity strategy and teach them how to provide cybersecurity awareness (Training and Education) in their organisations. Other topics to be covered: Risk Management, Security Architecture, Security Implementation (Network security, routers, switches, firewalls, intrusion detection and prevention, application security, software development lifecycle, web application firewall, data security), Incident Response (Detection, prevention, response, security events and incidents, legal aspects), Mobile Security, Social Engineering, and Legal and Ethical issues in cybersecurity.

Computer Networks and Security: The course covers principles of building secure systems. It explores the principles of up-to-date network systems and focuses on key operational and technical aspects. The course content is as follows: An Overview of Computer Security, Linux/Unix Security Basics, Software Security: Vulnerabilities, Attacks, and Countermeasures, Privileged programs (Set-UID programs) and vulnerabilities, Buffer Overflow Vulnerability and Attack, Race Condition Vulnerability and Attack, Format String vulnerability and Attack, Input Validation, Shellshock Attack, Web Security, Vulnerabilities, Attacks, and Countermeasures, Same Origin Policy, Cross-Site Scripting Attack, Cross-Site Request Forgery Attack, SQL-Injection Attack, Click-Jacking Attack, Web Tracking, Web Proxy and Firewall, Smartphone Security, Access control in Android Operating System, Rooting Android devices, Repackaging attacks, Attacks on Applications, Whole-disk Encryption, Hardware protection and TrustZone.

Operating Systems and System Programming: Operation System (OS) purposes are resource management and the extended virtual computer, historical development. Processes are critical sections and mutual exclusion, semaphores, monitors, classical problems, deadlock, process scheduling. Input and Output: hardware and software control. Memory management: multi-programming; swapping; virtual memory, paging and symbolic segmentation; File System: operations, implementation, performance. Operating System Security and Protection Mechanisms: protection domains, access lists, capability systems, the principle of minimum privilege, security threats and attacks, encryption, and authentication.

Turkish: The course aims at helping students improve their skills in written and oral narration by teaching them the features and rules of the language. Course Content: General information about language in general, world languages, the historical evolution of Turkish and its relationship with other languages, phonetical and morphological characteristics of Modern Turkish, applying/practising rules of orthography and punctuation.

German/Macedonian: Based on the Common Framework Program for European Languages, it aims to improve students' ability to communicate at the initial level, as well as their reading

comprehension, listening comprehension, writing and speaking skills. Course Content: Greeting, introducing yourself and someone else, ordering in a cafe and paying an account, objects, cities and attractions, countries and languages, geographical directions, items, home recipe, daily flow, giving information about life and workplaces, ordinal numbers, prepositions.

Cryptography: This course explores cryptography concepts for enhancing the security properties of systems being designed, implemented, and maintained. Common cryptanalysis techniques and tools are covered.

System Exploitation and Penetration Testing: This course explores common vulnerabilities and how an adversary can exploit vulnerabilities to disrupt a system's integrity. The course covers the common attack techniques that can be used for penetration testing but also can help understand how to avoid common exploits that creep into systems during the design and implementation phases.

Information Security Management Systems (ISMS): After completing the module, students are able to apply the standards of BSI Basic Protection and ISO 27001 / ISO 27002. They can analyse and evaluate the security level within an organisation concerning these standards and develop measures for optimisation. They can convincingly defend these optimisations against objections. The course content consists of these main topics.

1. Introduction and Fundamentals – ISMS and ISO,
2. Overview of the standards of the ISO/IEC 27000 family,
3. Fundamentals of Information Security Management Systems (ISMS),
4. ISO/IEC 27001 – Requirements,
5. ISO/IEC 27002 – Recommendations and Guidance,
6. Related Standards and Frameworks,
7. Processes of an ISMS,
8. Certification Opportunities with ISO/IEC 27001.

Cyber Warfare: This course addresses unique and emerging policies, doctrines, strategies, and operational requirements for conducting cyber warfare at the nation-state level. It provides students with a unified battlespace perspective. It enhances their ability to manage and develop operational systems and concepts, resulting in the integrated, controlled, and effective use of cyber assets in warfare.

Cyber Resilience: The skills that the course will equip the students with the following skills:

- Identify the key business assets needed to be protected within an organisation,
- Compare attacker profiles, motivations, and tactics to know enemies better,
- Analyse the risk and prepare your response,
- Analyse current strategies, methodologies, and frameworks to protect business assets and promote organisational resilience,
- Demonstrate the common cyber security tools and techniques used by organisations to protect their critical assets,
- Articulate the basic regulatory, legal, and ethical requirements that frame the work of cybersecurity professionals.

Scripting Languages: Perl, PHP, JavaScript, and Visual Basic are often-requested skills for employment, but most of us need more time to find out what they are all about. This course teaches you how to use scripting languages for rapid prototyping, web programming, data processing, and application extension. Besides covering traditional programming language concepts as they apply to scripting (e.g., dynamic typing and scoping), this course looks at new concepts rarely found in conventional languages (e.g., string interpolation, hashes, and polylingual code). Through a series of small projects, you use different languages to achieve programming tasks that highlight the strengths and weaknesses of scripting. As a side effect, you practice teaching yourself new languages.

Legal Aspects of Cybersecurity: This course examines legal and policy challenges stemming from rapidly evolving cybersecurity threats. Cyber insecurities affect many types of actors—individuals who suffer data breaches, local governments disabled by ransomware, businesses whose intellectual property is plundered, and states that both undertake and attempt to defend against espionage, election interference, and destructive cyber operations. This course will explore the national and international legal frameworks governing malicious and defensive actions in cyberspace, including cybercrime, cyberespionage, and cyberwar laws. The course will consider legal questions within the context of broader debates about issues such as the roles of governmental and non-governmental actors and the role of law in governing a constantly changing domain where many actors operate in secret. The objective of the course is to contextualise cybersecurity threats and responses to them in a national and international law framework while also recognising the limits of current law, the need for further policy evolution, and the real-world impacts of different legal and policy options. No technical knowledge is required.

3.2. Courses at UKIM

Students at UKIM for the 2nd year have two specialisation paths: Web and Cybersecurity and Cryptology. The courses for these two mobility paths are presented below.

Web and Cybersecurity/Fall 2025:

Year/Partner	*Term*	*Course Name*	*ECTS*
2025/ UKIM	*Fall*	Applied Cryptography (C)	6
		Digital Trust and Identity (C)	6
		Multimedia and Scalable Web (C)	6
		Elective Course (E1)	6
		Elective Course (E2)	6

Cryptology/Fall 2025:

Year/Partner	*Term*	*Course Name*	*ECTS*
2025/ UKIM	*Fall*	Applied Cryptography (C)	6
		Digital Trust and Identity (C)	6
		Coding Theory and Applications (C)	6
		Elective Course (E1)	6
		Elective Course (E2)	6

Both Specializations/Spring 2026:

Year/Partner	*Term*	*Course Name*	*ECTS*
2026/ UKIM	*Spring*	Thesis jointly supervised with KHAS (C)	18
		Advanced Information Security (C)	6
		Research Project (C)	6

List of Elective Courses in UKIM

Course Name	*ECTS*

Mobile and Web Application Security	6
Biometric Systems	6
Application of Machine Learning in Information Security	6
Cryptanalysis	6
Cryptographic Engineering	6
Cryptographic protocols	6
Mathematical Logic for Computer Science	6
Advanced algebraic structures	6
Advanced coding algorithms	6
Applied Information Theory	6
Random processes	6
Change and risk management	6
Practical application of digital forensics	6

* Students can choose one of the elective courses from an expanded list of elective courses

Course Descriptions at UKIM

Applied Cryptography: Course program content: Real cryptographic problems and their application, Internet and communication protocols, Anonymous communication, Privacy saving techniques (in data mining, publishing and processing data), Identity-based cryptography and attributes, Zero Knowledge evidence, Secret sharing and multiparty computation, Electronic voting, Cryptographic aspects of E-Cash and block-chain technology.

Course program goals (competencies): Students' ability to apply more advanced cryptographic techniques in real problems. Studying more advanced cryptographic algorithms and techniques will enable understanding and solving. The security problems in the industry and the daily systems used.

Digital Trust and Identity: Course program content: Digital Identity, Digital Identity Authentication and Authentication Levels, Digital Identity Exchange Protocols, Digital Identity Federations, Trust in Digital Identity Federations, Trusted Services, EIDAS.

Course program goals (competencies): After completing the course, the student is expected to know the mechanisms for identifying users in the digital world and the protocols for exchanging this information between systems. In addition, the student will be familiar with the legal framework related to trusted services.

Multimedia and Scalable Web: Course program content: The use of multimedia content in web products, including standards and technologies. Use of various multimedia technologies and combinations of multimedia technologies. Designing multimedia web, streaming media, advanced multimedia content scripting, multimedia web applications, web availability, mobile multimedia applications, HTML 5 Canvas, JavaScript. SEO Search Engines – SEO, Multimedia web applications for mobile devices such as mobile phones and downs, but also large screens, and TVs. Development of games, design, mobile viewers, and categories of multimedia content. Scalable web design. Safe Web Development (Principles, Error Management, Authentication, Authorization, Record, IO Validation, Sessions Management), (XSS, SQL Injection, CSRF, ClickJacking, DOS, DT, FI, CI).

Course program goals (competencies): After completing the course, candidates are expected to know how to develop contemporary design websites, including structure, architecture, compatibility with different devices, cascading styles, usability, scalability with different number of users, search engine optimisation, etc. Candidates are expected to: Demonstrate an advanced understanding of the importance of good design, interaction and usability of web pages on

different platforms and devices. Demonstrate practical knowledge of design and usability and be able to apply knowledge when designing effective multimedia websites. Communicate with the terminology specific to this area. Critically evaluate examples of design and interactivity on websites, including an assessment of their own products. Demonstrate awareness of strategies related to understanding the needs of web multimedia products users.

Coding Theory and Applications: Course program content: Introduction to codes that correct errors and their application. Linear codes. Coding and decoding in linear codes. Hamming codes. Cyclic codes. Codes of Reed Miller and Codes of Reed-Solomon. Codes that detect errors and CRC codes.

Course program goals (competencies): The main purpose of coding theory is to find codes that provide fast and correct transmission through the channel with noise. Different codes are optimal in different applications. The course aims to know the basic codes that reveal and fix errors and their practical application.

Advanced Information Security: Course program content: Information security concepts: integrity, confidentiality, secrecy, privacy, anonymity, Advanced methods for authentication and authorisation, Types of access controls, Advanced security models, Advanced Methods for Detection of Attacks, Realistic authentication protocols, Analysis of protocol security, Software security, Malicious software, Advanced Operating System Safety Methods, Types of tape techniques, Information security management.

Course program goals (competencies): Learning Advanced Methods for Authentication and Authorization, Safety Models for Access Control, Protocols and software for computer configurations.

Mobile and Web Application Security: Course program content: Modeling web security, modelling the security of mobile applications, the configuration of HTTP security, Detection of unauthorised content modification, Protecting the interaction between application and databases, Session Authentication Management, performing an entrance validation, protecting web services, Scan the weakness of applications, Model of Safety in Mobile Operating Systems.

Course program goals (competencies): The subject will introduce students to possible threats and attacks on web and mobile applications and detecting them. It will give a detailed review of approaches to achieving greater security in mobile and web applications, using: web server security, using the security of mobile operating systems, implementation of application protection mechanisms, promoting AJAX security, Web service protection. Upon completion of the course, the student is expected to be able to: configure web server protection, designing a security solution for mobile applications, and implement appropriate techniques for protecting mobile and web applications. Students will be able to analyze and determine the weaknesses of existing mobile and web applications, as well as to propose solutions to overcome them.

Biometric Systems: Course program content: Introduction and basic concepts in biometric systems. History of biometric systems. Requirements and properties of biometric systems. Processing images and extracting visual features. Classification techniques. Recognizing fingerprints. Venous recognition. Recognition of persons. Recognition of 3D persons. Iris recognition. Multi-modal biometric systems. Evaluation schemes for biometric systems, performance testing and safety aspects. E-Pass. Privacy of data in biometric systems.

Course program goals (competencies): The course aims to get acquainted with the basic principles used in biometric algorithms and systems. After completing the course, candidates will have deepened knowledge of advanced technologies and methods in biometric systems; You will be able to choose an appropriate algorithm and system for a given application context; will understand the complex relationships between biometric systems and environmental conditions (brightness, variations in the placement of objects of interest, etc.); You will have an understanding of the principles of privacy and their impact on the design and configuration of biometric systems.

Application of Machine Learning in Information Security: Course program content: Analysis of methods from machine learning and application of a suitable method for solving problems related to information security. Analysis of the results obtained with machine learning methods and finding solutions to improve them by using various features of the methods and algorithms.

Course program goals (competencies): The aim of the course is to apply machine learning through examples from the field of information security and to illustrate the use of different learning techniques in clear scenarios.

Cryptanalysis: Course program content: Types of brute force attacks, statistical attacks, differential and linear cryptanalysis, representations of cryptosystems as Boolean functions and tests of linearity properties, special types of attacks for special crypto primitives (hash functions, block ciphers, public key, protocols). Application of ML, DL, NLP in cryptanalysis.

Course program goals (competencies): Study of cryptanalysis tools and their application.

Cryptographic Engineering: Course program content: Introduction to secure implementation of cryptographic software. Implementation of modular arithmetic and arithmetic of finite fields. Implementation aspects for symmetric crypto primitives (AES, SHA). Implementation aspects for public key cryptographic primitives (RSA, ECC). Implementation aspects for lightweight cryptography. Secure implementation of cryptographic primitives. Side-channel attacks and countermeasures. Cryptographic software packages

Course program goals (competencies): After completing the course, the student is expected to know how to program a secure crypto-primitive. Will have knowledge of implementing crypto-primitives on different platforms. Through examples, the student will understand how side-channel cryptanalysis works on different cryptographic implementations and what countermeasures should be taken.

Cryptographic protocols: Course program content: Safety assumptions. Proving protocols' security. Key exchange protocols. Binding schemes. Challenge-Answer Protocols for Identification. Zero-Knowledge Identification Protocols. Tools for formal verification of protocols. Real-World protocols

Course program goals (competencies): Acquiring the basic knowledge of cryptographic protocols, their design and analysis.

Mathematical Logic for Computer Science: Course program content: Propositional logic: Boolean operations and interpretations, formulas, logical equivalence and substitutes, semantic charts, deductive evidence, resolutions, Gencenov and Hilbertov system. Predicate logic: relationships, predicate formulas, interpretations, logical equivalents and substitutes, semantic

charts, deductive forms, functions, and terms. Resolution and logical programming: basic resolution, replacement, unification, general resolution, logical programming. Temporal logic.

Course program goals (competencies): Understanding the notions and properties of propositional and predicate logic and their application in computer science.

Advanced algebraic structures: Course program content: Study of the structures and properties of Grupoids: half -groups, groups and quasigroup. Multi-operations algebra: rings, fields, Boolean algebra. Relational algebra. Special reference to the finite algebraic structures of the previous species, which are important for the application.

Course program goals (competencies): Introduction of algebraic structures that will be used in other subjects from studies.

Advanced coding algorithms: Course program content: Iterative decoding methods: Turbo codes. Decoding with probabilities (Posteriori Probability (App) Decoding). Statistical Analysis Methods (Monte-Caro Simulations and Exit-Chart Analysis). LDPC Codes (Low-Density Single Parity Check). Representing LDPC codes with matrix and graphs. Construction of the code. Iterative decoding with Message Passing. Statistical and Graph-based Analysis Methods (Density Evolution, Stopping Sets). Algebraic decoding methods: Syndrome decoding. Reed-solomone codes. Decoding with Peterson-Gorenstein-Zierler and Forne algortes. IRS codes (Interleaved Reed-Solomon). Interpolation-based techniques. Interpretation of the decoding problem as a problem of polynomial interpolation. Sudan's algorithm. Decoding with a list. Quasigroup-based detection and correction codes.

Course program goals (competencies): The aim of the course is to deepen the knowledge in coding theory and to study advanced and new aspects in codes for correcting and detecting errors. Iterative and algebraic decoding methods will be considered. The course foresees the development of papers with new results from coding theory.

Applied Information Theory: Course program content: Communication system. Entropy. Information. Data compression: loss coding. Asymptotic Equipartition Property (AEP) for independent random variables. Shannon's theorem for source signal coding. Loss-free coding. Symbolic codes. The problem of only decoding. Instant codes. Kraftovo inequality. The theorem of silent coding. Construction of optimal codes. Communication through a noise channel (communication channel. Communication channel models. Discrete channel without memory. Discrete channel capacity without memory). Sources of information: Markov's chains. Source of information. Regular Markov source. The entropy of the source. Source order. Approximation of a general source of information with a final order source. Earnest source. Shannon theorem - McMillan (Asymptotic Equipartition Property (AEP)). Discrete channel with memory: Model models with memory. Channel with a finally set of states. The capacity of the general discreet channel. The coding theorem for a regular channel with a finally set of conditions. Continuous channels: entropy of continuous random variables. The entropy of Gaussian random variable. Types of non-jet channels. Gaussian channel (time discreet). AEP for continuous random variables. Coding theorem for Gaussian Channel.

Course program goals (competencies): Studying the advanced aspects of a mathematical model of a communication system.

Random processes: Course program content: Random processes: definition, features, classification, transformations. Razing processing processes. Processes with independent stationary growths; Marks processes with a discreet and continuous set of conditions: birth and die processes; Markov's chains, Markov's nested chains. Special random processes: accidental wandering, POSONOV, Vinerov process. Branching processes. Recovery processes. Advanced queues waiting.

Course program goals (competencies): Random processes are a mathematical model that models many processes in computer science. The purpose of this course is to introduce in the theory of random processes, studying the characteristics of special accidental processes, so they can be used to model real processes.

Change and risk management: Course program content: Basic risk management concepts; the importance of risk management for business success; risk types; risk analysis; Systems, models and frameworks when managing information security risks; Objectives of risk management; risk identification; risk management strategies; Management of changes in software projects, risk assessment, organisational changes in IT environment, IT process improvement, open software change and consumer software, project research by: IT security, cloud calculation, agile methods, projects with exceeding budget and high delays, Euladin projects and new technologies.

Course program goals (competencies): The course highlights the need for good risk management and changes. By successfully completing the course, the student will be able to independently identify problems related to risk management and their application in information security and changes in software projects and to apply different ways and techniques to solve these problems.

Practical application of digital forensics: Course program content: Analysis of methods, techniques and tools for digital forensics and their practical application to solve problems related to digital forensics.

Course program goals (competencies): The course highlights the need to study elements of digital forensics and its practical application. The aim is to study the stages of digital forensics and apply them practically using appropriate tools and methods.

Research project: The students, together with the supervisor, define a project that will be related to the Master's thesis research. The project allows students to get acquainted with current research in preparation for the Master's topic. Specific problem statements are derived from recent research activities. All rules for ensuring fair scientific work in their current version are applicable. The competence goals of this course are:

Professional Competence: Students can apply their previously acquired knowledge and skills in projects in the focus subject.

Methodological Competence: Students can apply scientific methods learned during their studies in the focus subject.

Personal Competence: Through project work, students will develop the habit of responsibility and motivation to solve a problem. They can create different perspectives on a problem and find optimised solutions.

Social competence: Students will improve their intercultural experience by working in international teams and projects, and they can develop solution strategies in groups.

Thesis jointly supervised with KHAS: Students will be able to conduct research on their Master topic independently. The ability to do research and to formulate it scientifically is tested in the Master thesis. The contents of this competence field are defined with respect to the selected topic of the Master thesis. The competence goals of this course are:

Professional competence: Students can follow the state of the art in knowledge and technology in their respective research fields.

Methodological competence: Students can apply appropriate scientific methods to tackle research questions.

Personal competence: Students can manage their Research project, including the outline of the Research project and staying within the timeline.

Social competence: The students can defend their Master's thesis and discuss it with scientific language.

3.3. Courses at SRH

For CyberMACS students, SRH offers two specialisation tracks: Cybersecurity Management and Cybersecurity Technologies. For students who prefer long-term practical training instead of regular courses, a third specialisation focusing on practical skills in cybersecurity is possible. The following infrastructures are offered for advanced research of CyberMACS students: Lab. for Cybersecurity, Lab. for Big Data and Artificial Intelligence, Lab. for Industrial Automation and Lab. for Renewable Energy and Industry 4.0.

Advanced Technologies in Cybersecurity /Fall 2026:

Year/Partner	*Term*	*Course Name*	*ECTS*
2026/ SRH	*Fall*	Cybersecurity Management Project (C)	6
		Open-Source Intelligence OSINT (C)	6
		IT Forensics (C)	6
		Cloud Solutions (C)	6
		Elective Course (E1)	6

Cybersecurity Management /Fall 2026:

Year/Partner	*Term*	*Course Name*	*ECTS*
2026/ SRH	*Fall*	Cybersecurity Management Project (C)	6
		IT Security Management & DevOps (C)	6
		IT Revision and Audit (C)	6
		Elective Course (E1)	6
		Elective Course (E2)	6

Long-Term Practical Training/Fall 2026

Year/Partner	*Term*	*Course Name*	*ECTS*
2026/ SRH	*Fall*	SRH will connect students with industrial partners for long-term practical work. In this case, a representative from the industry might be involved in students' thesis defence examination. This might be confidential should the industrial partner requests so. Professors in SRH have part-time Professor positions in SRH University and hold management and research positions in big companies (Price Waterhouse Coopers, Ernst & Young, Siemens, etc.). This ensures good cooperation with different companies for long-term practical training and technology transfer, internship and master thesis work, and job opportunities for students.	30

Both Specializations/Spring 2027:

Year/Partner	*Term*	*Course Name*	*ECTS*
2026/ SRH	*Spring*	Thesis jointly supervised with KHAS (C)	24
		Master Project (C)	6
		Thesis Project (C)	6

List of Elective Courses in SRH

Course Name	*ECTS*
Advanced Data Technologies	6
Machine Learning	6
Artificial Intelligence	6
Big Data and Business Intelligence	6
Advanced Penetration Testing	6

Course Descriptions at SRH

IT Forensics: This course equips students with the theoretical knowledge and practical skills needed to investigate and analyze cyber incidents systematically. Students will learn to identify, collect, and preserve digital evidence, ensuring adherence to legal and ethical guidelines.

The course content consists of these main topics:

1. Introduction to Computer Forensics
2. TDigital Evidence Basics
3. L Computer Forensics Investigation Process
4. File Systems and Storage Devices
5. Forensic Tools and Techniques
6. Network Forensics
7. Mobile Device Forensics
8. Email and Web Forensics
9. Malware and Antivirus Forensics
10. Legal and Ethical Issues in Computer Forensics
11. Reporting and Presenting Forensic Findings
12. Case Studies and Practical Applications
13. Emerging Trends in Computer Forensics

The competence goals of this course are:

Professional competence: Students will develop the ability to conduct comprehensive forensic investigations, including data acquisition, analysis, and reporting.

Personal competence: Students will reflect on their own investigative approaches, identifying strengths and areas for improvement.

Social competence: Students will collaborate in teams to conduct forensic investigations, fostering skills in communication, coordination, and shared problem-solving.

Cloud Solutions: Technology refers to the ability to use distributed hardware and software resources provided by a provider on the Internet on demand and to pay for them based on usage. This course introduces concepts (e.g., "Everything-as-a-Service", virtualisation) of cloud computing and some cloud architectures, cloud offerings, programming models, software tools and applications developed in recent years. Economic considerations, as well as opportunities and

risks of cloud computing, will be explained. One focus of the course is on practical testing of the concepts taught in the form of programming exercises in an IoT background.

The course content consists of these main topics:

1. Cloud Computing Basics,
2. Framework and Terminology,
3. Case Studies,
4. Cloud Solution Architect,
5. Amazon AWS, Google
6. Essential Cloud Infrastructure: Google, Amazon, Microsoft,
7. Docker Technologies
8. Compartmentalising web applications,
9. Cloud Monitoring and SysOps,
10. Monitoring EBS, RDS, ELB, EC2, Elasticcache,
11. High-availability, Deployment & provisioning Opsworks,
12. Data management Security, networking with Route53, VPC,
13. Serverless.

The competence goals of this course are:

Professional competence: Students will be able to independently solve technical programming tasks and problems in a cloud as well as meet the changing technical demands of the profession.

Methodological competence: Students are able to handle the processing of professional requirements, tasks and activities and proceed in work in a targeted, structured and effective manner.

Personal competence: The students are well trained in oral communication skills in the exercises by practising free speech in front of an audience and during discussion. They are able to assess their strengths and weaknesses by means of exercises and to organise and optimise their time and learning management.

Social competence: Students will be able to communicate and justify their own approaches to solutions within the group structure but also be enthusiastic about the solution in the group and work on it profitably.

Open-Source Intelligence: This module looks at how we can store, manipulate, and analyse big data. We define big data essentially as data that is nonatomic and is not well suited to tabular storage and manipulation.

It is important to ensure that the students can understand why these two broad classes of data really are different and why they warrant such different treatment. The course content consists of these main topics:

1. This Advanced OSINT Lab consists of several exercises that start with setting up a working environment and teach how to work efficiently in it., Afterwards, freely available tools are presented, and the use of these tools is trained. This is followed by the presentation of the most common commercial tools, which are worked out step by step in the individual exercises. Finally, it is shown how all these tools can be used to aggregate search results from many individual data.

2. Linux Fundamentals for OSINT: Linux Shell Fundamentals, – Linux File System Hierarchy Fundamentals, – Linux Pipe Fundamentals. OSINT Basics; – Advanced Google Search, – Linux Networking Tools, – Linux Forensics Tools. OSINT Commercial Tools; – Hacking-Lab Environment Preparation, – PassiveTotal, – Censys, – Shodan, – Maltego.

The competence goals of this course are:

Professional competence: The students have a comprehensive overview of the topic of Open-Source Intelligence. It allows them to work independently with the newly taught tools, collect data from freely available sources, and aggregate it into investigation results. They are well prepared for the requirements of the profession and can use acquired knowledge profitably.

Methodological competence: Students are able to recognise and name possible solutions based on given tasks. They are able to work out suitable solutions and apply the professional knowledge they have acquired. Students are able to solve complex problems and transfer them to other situations. Students apply networked and abstract thinking and analyse their solution approach before and after solving the problem.

Personal competence: Students are able to coordinate their working methods and time management in a concrete and complex project environment and act in a self-reliant and independent way.

Social competence: Students are able to work on complex tasks in a self-reflective way and discuss solutions constructively in the group, and defend them in a diplomatic manner.

Cybersecurity Management Project: Students will be able to independently manage a cybersecurity project and gain expertise in the terminology. Information Security terminology: Security targets, threats, vulnerabilities, risks, security controls, management systems, Introduction in the Information Security Management Systems (ISMS) based on the standards family ISO 27000, Identification, assessment and treatment of typical risks in information systems, Typical security measures in distributed information systems, in particular in web-based systems Special fields of interest, e.g., malware control, firewalls systems hardening, encryption technologies, cyberwar, cybersecurity, auditing and reviewing information security, business continuity management, Darknet, network security etc., Passwords & biometrics, Introduction to cryptography, Sessions, SSL/TLS, Certificates, electronic signatures, public key infrastructures, Side-channel analysis, Access control, Privacy.

IT Security Management & DevOps: The aim of the module is to equip the students with the analytical skills and knowledge to assess security in large systems and organisations and to incorporate appropriate levels of security in the various steps of a system's lifecycle.

The course content consists of these main topics:

1. Introduction to the Management of Information Security,
2. Compliance: Law and Ethics,
3. Governance and Strategic Planning for Security,
4. Information Security Policy,
5. Developing the Security Program,
6. Risk Management: Assessing Risk
7. Risk Management: Treating Risk,
8. Security Management Models,

9. Security Management Practices,
10. Planning for Contingencies,
11. Security Maintenance,
12. Protection Mechanisms,
13. Devsope.

The competence goals of this course are:

Professional competence: Identify and discuss the benefits of embedding security throughout an organisation; Understand how to relate and adapt information systems in general and security solutions in particular to specific business processes and requirements to meet overall goals.

Methodological competence: Methods of IT Operations and Software Development (holistic).

Personal competence: Be able to communicate clearly and unambiguously about security problems to other people in an organisation; Be able to identify assets and threats and assess risks; Assess own competence.

Social competence: Students are able to discuss several fundamental IT Security Management problems in the group to bring about an agreement process and to share responsibility for this.

IT-Revision und Audit: In an interactive seminar, the students learn the principles of IT revision and audit and have to show their level of mastery in a portfolio exam consisting of different tasks. The course content consists of these main topics:

1. Auditing and Internal Control,
2. Auditing IT Governance Controls,
3. Security Part I: Auditing Operating Systems and Networks,
4. Security Part II: Auditing Database Systems,
5. Systems Development and Program Change Activities,
6. Transaction Processing and Financial Reporting Systems Overview,
7. Computer-Assisted Audit Tools and Techniques,
8. Data Structures and CAATTs for Data Extraction,
9. Auditing the Revenue Cycle,
10. Auditing the Expenditure Cycle,
11. Enterprise Resource Planning Systems,
12. Business Ethics, Fraud, and Fraud Detection

The competence goals of this course are:

Professional competence: Students will be able to describe all steps of an information security auditing process for IT systems / IACS / processes. The students know all the essential steps/phases of the auditing process and can apply auditing processes to IT systems and processes. The students know the essential requirements for an auditing process of the relevant standards. Students will be able to perform audits for an object of investigation (IT system, part of an IT system, process).

Methodological competence: Students can select the correct type and appropriate procedure of an audit for an object of investigation (IT system, part of an IT system, process) and evaluate the criticality of identified deficiencies. Students will be able to assess whether certain measures are suitable to remedy or alleviate identified deficiencies / weaknesses / findings.

Personal competence: Through the exercises that take place, students are encouraged to work out issues independently and present them in a comprehensible manner.

Social competence: Students perform audits on case studies as a team in changing roles. Through this collaboration, the knowledge and skills of other students are experienced as helpful and beneficial.

Long-Term Practical Training: This course is one of the areas of specialisation that can be selected in the first semester of the 2nd year. SRH will connect students with industrial partners for long-term practical work. In this case, a representative from the industry might be involved in students' thesis defence examination. This might be confidential should the industrial partner request so. Professors in SRH have part-time Professor positions in SRH University and hold management and research positions in big companies (Price Waterhouse Coopers, Ernst & Young, Siemens, etc.). This ensures good cooperation with different companies for long-term practical training and technology transfer, internship and master thesis work, and job opportunities for students.

Advanced Data Technologies: With the interplay of lectures and exercises, the students develop the knowledge of state-of-the-art methods of Artificial Intelligence for problem-solving. The level of mastery is tested with a written exam.

The course content consists of these main topics:

1. Exploring Data, Regression,
2. Linear Regression Multiple Regression,
3. Non-linear Regression Assessing Model Accuracy,
4. Classification, Logistic Regression,
5. K-Nearest Neighbors Naive Bayes,
6. Decision Trees,
7. Random Forests,
8. Unsupervised Learning K-Means Clustering Hierarchical Clustering, Using R.

The competence goals of this course are:

Professional competence: Students know methods for data exploration like regression, classification and unsupervised learning as the methodological basis for Artificial Intelligence.

Methodological competence: Students are able to explore data by applying common methods like regression, classification, or unsupervised learning. They develop problem-oriented as well as abstract and joined-up thinking. They are able to apply the methods in practice. Personal competence: plan, organise and prioritise their work efficiently and effectively; critically reflect on their work and results; communicate their ideas in class; held group meetings and demonstrate their results.

Social competence: effectively work in teams; take on team responsibilities; receive and discuss constructive feedback; analyze and transform requirements into feasible tasks.

Machine Learning: Machine learning is a field of scientific study concerned with algorithmic techniques that enable machines to learn performance on a given task via the discovery of patterns or regularities in exemplary data. Consequently, its methods commonly draw upon a statistical basis in conjunction with the computational capabilities of modern computing hardware. This

course aims to acquaint the student with the main branches of machine learning and provide a thorough introduction to the most widely used approaches and methods in this field.

The course content consists of these main topics:

1. Introduction to Machine Learning,
2. Supervised and Unsupervised learning,
3. Clustering,
4. Linear Regression with One Variable,
5. Linear Algebra Review,
6. Linear Regression with Multiple Variables,
7. Logistic Regression,
8. Regularisation,
9. Predictive and Classification Algorithms,
10. SVM, k-NN, Decision trees, Random Forests,
11. Convolution,
12. Neural Networks, CNNs,
13. Applying Machine Learning: Natural Language Processing.

The competence goals of this course are:

Professional competence: On successful completion, students will be able to learn different machine learning model classes; comprehend the difference between supervised, unsupervised, and reinforcement learning methods; understand common machine learning models; analyse trade-offs in the application of different models; appropriately choose machine learning models according to a given task.

Methodological competence: The students understand the statistical foundations of generalisation, i.e., the induction of models from data, as well as practical tools for model validation. They are able to apply basic methods of supervised learning to problems of classification and regression. The students have an overview of methods for multi-class classification, the learning of nonlinear models, and extensions of the simple setting of supervised learning. They understand algorithmic concepts of corresponding methods and are able to apply them to real problems.

Personal competence: Students will be able to communicate and justify their approaches to solutions within the group structure but also be enthusiastic about the solution in the group and work on it profitably.

Social competence: Students work in teams, present their results and reflect their results in the group.

Artificial Intelligence: With the interplay of lectures and exercises, students develop the ability to apply methods of Artificial Intelligence to different use cases. The level of mastery is tested with the written exam.

The course content consists of these main topics:

1. Support Vector Machines, ROC Curves,
2. Neural Networks, Deep Learning Projects Using R or similar language,

The competence goals of this course are:

Professional competence: Students know typical methods of Artificial Intelligence like Neural Networks, Deep Learning, ROC curves and how to implement these methods in a programming language like R or Python.

Methodological competence: Students are able to analyse problems of industrial automation and digital systems by using methods of Artificial Intelligence. They develop problem-oriented as well as abstract and joined-up thinking. They are able to apply the methods in practice.

Personal competence: Students are able to plan, organise and prioritise their work efficiently and effectively; critically reflect on their work and results; communicate their ideas in class; held group meetings; and present their results.

Social competence: Students are able to effectively work in teams; take on responsibilities in teams; receive and discuss constructive feedback; analyse and transform requirements into feasible tasks.

Big Data and Business Intelligence: This module looks at how we can store, manipulate, and analyse big data. We define big data essentially as data that is non-atomic and is not well suited to tabular storage and manipulation. It is important to ensure that the students can understand why these two broad classes of data really are different and why they warrant such different treatment. The course content consists of these main topics:

1. Introduction to Big Data,
2. Big Data Modelling and Management Systems,
3. Big Data Integration and Processing, -Machine Learning with Big Data,
4. Graph Analytics with Big Data,
5. Big Data Project.

The competence goals of this course are:

Professional competence: Describe the purpose and uses of Business Intelligence & Big Data in the business world today; identify the terminology used in Big Data and quantitative analysis programs in general.

Methodological competence: Build a dataset based on gathering data from multiple sources and merging those databases into a single unified set; clean a database through automated methods like winsorizing and evaluation of univariate metrics to determine the accuracy of inputs; identify key risk issues involved in Big Data and the role that information governance plays.

Personal competence: Be able to communicate clearly and unambiguously about Big Data and Business Intelligence problems to other people in an organisation; be able to identify assets and threats and assess risks; assess own competence.

Advanced Penetration Testing :

This module equips students with theoretical and practical knowledge of penetration testing, focusing on identifying, verifying, and exploiting security vulnerabilities in enterprise environments. Students will learn to assess the real-world feasibility of attack vectors, simulate adversarial behavior, and evaluate an organization's ability to detect and respond to threats. Through a combination of lectures, hands-on labs, case studies, and cloud-based network simulation, students will master the terminology, tools, and techniques used by professional

penetration testers, culminating in the application of their skills in simulated network environments.

The course content consists of these main topics:

1. Ethical Hacking Overview
2. TCP/IP Concepts Review
3. Network and Computer Attacks
4. Footprinting and Social Engineering
5. Port Scanning
6. Enumeration
7. Programming for Security Professionals
8. Desktop and Server OIS Vulnerabilities
9. Embedded Operating Systems
10. Hacking Web Servers
11. Hacking Wireless Networks
12. Cryptography
13. Network Protection Systems
14. PenTesting Practice
15. Sample Pentesting Reports, Part I
16. Sample Pentesting Reports, Part II
17. Practical Exercises in Hacking Lab

The competence goals of this course are:

Professional competence: Upon completion, students will: Learn and understand the importance of "Security by Design" in future system applications.Plan, scope, and conduct reconnaissance as part of a structured network penetration test.Methodological competence: Students will evaluate advanced exploitation techniques, frameworks, and tools to identify and exploit vulnerabilities effectively. They will design, implement, and document a comprehensive security test for network infrastructures within defined constraints.

Personal competence: Students will critically reflect on their own skills and progress, identifying strengths and areas for improvement in penetration testing methodologies.

Social competence: Students will collaborate in teams to conduct penetration testing simulations, practicing effective communication, task delegation, and knowledge sharing. They will explore social engineering techniques, such as phishing and pretexting, and develop strategies to educate organizations on mitigating these human-centric attacks.

Thesis jointly supervised with KHAS/Master Thesis and Defence: Students will be able to conduct research on their Master topic independently. The ability to do research and to formulate it in a scientific way is tested in the Master thesis. The contents of this competence field are defined with respect to the selected topic of the Master thesis. The competence goals of this course are:

Professional competence: Students are able to follow the state of the art in knowledge and technology in their respective research fields.

Methodological competence: Students are able to apply appropriate scientific methods to tackle research questions.

Personal competence: Students are able to manage their Master project including following the outline of the Master project and staying within the timeline.

Social competence: The students are able to defend their Master thesis and to discuss it with scientific language.

Master Project: This course serves to deepen students' ability to practically implement previously acquired knowledge and skills in the field of security management as well as offers an opportunity for networking within a company or research institution. Students can add to their personal profiles via acquired in-depth knowledge of key corporate functions. The project phase allows students to get acquainted with current research and industry topics in preparation for the Master's topic. Specific problem statements are derived from current research activities in the industry partners' subject area or practical requirements. All rules for ensuring fair scientific work in their current version are applicable. The competence goals of this course are:

Professional competence: Students are able to apply their previously acquired knowledge and skills in projects in the focus subject.

Methodological competence: Students are able to apply scientific methods learned during the studies in the focus subject.

Time and Project Management

Personal competence: Through project work, students will develop the habit of responsibility and motivation to solve a problem. They have the ability to create different perspectives on a problem and to find optimised solutions.

Social competence: Students enhance their communication abilities by working in companies or projects. They also improve their intercultural experience by working in international teams and projects, and they can develop solution strategies in groups.

Research Project: This course serves to deepen students' ability to practically implement previously acquired knowledge and skills as well as offers an opportunity for networking within a company or research institution. Students can add to their personal profiles via acquired in-depth knowledge of key corporate functions. The student defines a project with the internship company or research institution and agrees with the supervising faculty member. The approach to this project is discussed with the university supervisor and agreed to by the company or research institution. At the end of the practice phase, the student reflects on their experiences in practice and how they relate to the theories and models that were covered during their studies.

The competence goals of this course are:

Professional competence: Students are able to apply their previously acquired knowledge and skills in projects in the focus subject.

Methodological competence: Students are able to apply scientific methods learned during the studies in the focus subject.

Personal competence: Through project work, students will develop the habit of responsibility and motivation to solve a problem. They have the ability to create different perspectives on a problem and to find optimised solutions.

Social competence: Students enhance their communication abilities by working in companies or projects. They also improve their intercultural experience by working in international teams and projects.

4. Joint Events, Internships, and Academic Calendar

4.1. Cultural Orientation Week

Date : 01-04 September 2025*
Venue : Kadir Has University, Istanbul

The CyberMACS Cultural Orientation Week Program, taking place in Istanbul from 1st to 4th September 2025, is designed to introduce participants to the CyberMACS program and provide them with essential information and experiences related to living in Türkiye.

The program begins with a welcome speech and introduction to the CyberMACS program, followed by a meeting with buddies from KHAS (Kadir Has University) to foster connections. Participants then embark on a campus tour and engage in ice-breaking activities such as the Name Game and Speed Networking. The first day concludes with an orientation session by the KHAS International Office.

The subsequent days of the program include sessions on personal safety, intercultural training focused on Türkiye, cultural workshops, and a documentary on Turkish culture. Participants also could engage in Cyber BINGO, receive tips for living in Türkiye, attend library information seminars, and enhance their academic skills as graduate students. A cultural event featuring an Istanbul Old City Tour and visits to the Rezan Has Museum and Cibali Tobacco Factory are scheduled. The program concludes with presentations from student associations, a farewell lunch, and a welcome and wrap-up party in the Research Centre Building.

4.2. Joint Integration Week

Date : 08-11 September 2025*
Venue : Kadir Has University

The Joint Integration Week takes place in Istanbul before the start of every first year of the CyberMACS. This event is the main welcome and introduces you to the CyberMACS programme.

Since Joint Integration Week provides a comprehensive introduction to the programme's academic structure, you will be introduced to the possible research fields in cybersecurity that you can pursue in your thesis research.

At the beginning of Joint Integration Week, you will be asked to form working groups and choose a “Pilot Case” (as a cybersecurity challenge) in cybersecurity according to the area where you want to specialise (cryptography, web and security, cybersecurity technology, cybersecurity management, cybersecurity technologies etc.).

During the week, each group will be guided by the local academic coordinators of CyberMACS. They will have separate sessions to sit down and reflect on their creative ideas to solve the given challenge. On the last day, we will ask you to present your work in 20-25-minute-long sessions with all participating academics listening to your ideas. Your group advisor may also suggest writing a review paper on the topic.

In addition to the working group sessions, we will have separate sessions dedicated to different topics in cybersecurity, where you will find a chance to meet with some of the CyberMACS Industrial Advisory Board (IAB) members and guest lecturers.

Reiner Creutzburg from SRH will give a 15-hour course on the basics of cybersecurity during the Joint Integration Week as he must return to Berlin shortly after that week.

We will inform you about the latest programme and agenda of the Joint Integration Week before the event.

4.3. Winter School

Date : 08-11 January 2026*
Venue : Istanbul

Winter School takes place between the first and second semesters every academic year with the attendance of guest lecturers, representatives of associative partners, faculty of both SRH and UKIM and industry experts.

The Winter School programme allows you to get 2-3 days of tutorial/seminar/lecture on a newly developed technology and/or research breakthrough in cybersecurity as a part of the CyberMACS Syllabus/fall semester seminar series.

The Joint Winter School is an in-residence activity where you will be physically present in the event for one week to develop your academic and multicultural skills and competencies related to the most recent and up-to-date topics in the cybersecurity field.

Each year the Winter School should focus on a specific cybersecurity topic, such as the energy sector, health infrastructures, etc. You will be working closely with mentors, experts from industry and academics on solving problems in cybersecurity.

In the Winter School, you will be able to assess the first academic semester's performance with the CyberMACS Team based on your first semester results and experiences.

The Winter School will include talks/seminars and workshops. Scholars from UKIM and SRH will participate and teach in the Winter School. The University of Groningen will organise a 1–2-day workshop in Winter School on ethical and legal aspects of cybersecurity.

In addition to the traditional seminars, we plan lunch talks as part of social skills to share good practices, insights, and approaches that would support your academic progress, such as "how to write an excellent academic thesis" and "get your manuscript accepted".

To familiarise you with cybersecurity career prospects, industry experts will also deliver practical modules such as "career prospects" in cybersecurity. We will integrate courses such as entrepreneurship in cybersecurity seminars to focus on your soft-skill development.

Finally, you are invited to participate in the Winter School's organisational and administrative tasks to develop your organisational skills. **If you want to join the Winter School organisation team, please drop us an e-mail at info@cybermacs.eu address.**

As we have informed you, your participation in the CyberMACS Winter School is compulsory.

There is no cost for participation in the CyberMACS Winter School; however, you will need to pay for transportation and accommodation during the event.

We will inform you about the latest programme, dates, and agenda of the Winter School before the event.

4.4. Summer School and CyberMACS International Conference

Date : 08-11 June 2026
Venue : TBC

Summer School is hosted by the CyberMACS consortium for the first intake, with the attendance of guest lecturers and industry experts. For the first year of the programme (2024), the event will be in the form of a workshop; however, starting from the second year, it will evolve into an International Applied Cybersecurity Conference where you can participate and present your papers resulting from your thesis work. During the Summer School, there will be 2-3 days of tutorials given by internationally renowned experts on a new topic of cybersecurity or a research break.

One of the overall benefits of the Summer School/International Conference is to be expected that you can present and discuss your master thesis plans with your supervisors and broader audience, which provides an excellent networking and feedback platform.

Finally, you are invited to participate in the Summer School's organisational and administrative tasks to develop your organisational skills**. If you want to join the Summer School organisation team, please drop us an e-mail at info@cybermacs.eu address.**

As we have informed you, your participation in the CyberMACS Summer School is compulsory.

There is no cost for participation in the CyberMACS Summer School/International Conference**; however, you will need to pay for transportation to and accommodation during the event, should it be organised in a different venue other than the main campus.**

We will inform you about the latest programme and agenda of the Summer School before the event.

4.5. Internships

CyberMACS internships foresee a minimum duration of approximately 320 hours, with a typical duration of 8 weeks full-time at an organisation linked to the field of studies. All CyberMACS students are expected to complete this program; however, those with a couple of years of experience in the cybersecurity industry may petition to be waived from this compulsory training, which aims to familiarise students with practical applications of theoretical studies in the courses.

An internship report (20 pages) needs to be provided at the end of the internship. Internships can be carried out either at a company or a research organisation linked to cybersecurity in the host country or abroad (for instance, this could be an option if a collaborative project between the host university and the company/research organisation/university exists).

You may suggest an alternative company/industry/country where you would like to conduct your internships if the CyberMACS management and your co-supervisors approve.

For the organisation of your internships, we have created an internship database so that you and the CyberMACS Industrial Advisory Board (IAB) members can keep feeding in new internship possibilities for a genuinely international internship database.

Please acknowledge that in-person internships are only possible in any of the three programme countries, online internships are accepted only if the student is physically in any of the programme countries.

You will receive further instructions about internships at the proper time.

4.6. Academic Calendar

The recent and most updated Academic Calendar for KHAS can be found in the link. The one for SRH Berlin can be found here, for UKIM can be found here.

5. Academic Assessments

Performance Assessment: Your performance in CyberMACS is assessed on every course separately by its instructor. To pass the courses, you need to pass the exams and other exercises, such as submitting laboratory/internship reports as well as performing oral presentations and computer-based tests. The lecturer, who is in charge of grading a particular course, and/or the local academic coordinator will guide you about the assessment methods.

Your performance will be graded according to the national grading scale (depending on your mobility) and the ECTS grading scale and will contribute to the final grade for the course.

You must participate in compulsory parts of the courses such as Winter and Summer Schools.

Your performances are also monitored by the coordinator (KHAS) (after each semester) and locally at each university (depending on your mobility) during the semester by regular assessments, which could be group presentations on projects, individual homework, and group reports. This is important to identify as soon as possible that you need help with specific lectures to provide specific assistance.

If some students choose to have long-term training in SRH rather than **regular courses, SRH and the host institution will ensure the quality.**

Other than the student's master thesis, the student with long-term practical training in SRH is expected to come up with a final training report with scientific value. The ultimate aim of this report is to have a publication.

Diploma obligations and ECTS credits: The ECTS credits associated with each course are available in your Student Agreement ***Article 5/ Degree Award.***

Examinations for each course are conducted according to the regulations of the host institution. Attendance of every CyberMACS course and activity as set out in the student agreement is mandatory.

In order to successfully complete CyberMACS and obtain a double diploma, you need to participate in all courses of their mobility track, validate a minimum of 30 ECTS/semester, perform your internships (unless you are granted with an exception by the Executive Board) and participate in the joint activities.

As stated in your Student Agreement, you should recognise that the pre-condition of starting the mobility is attending and successfully completing all the courses, attending the winter school for the first intakes, attending the summer school for the later intakes attending CyberMACS/Applied Cybersecurity International Conference, completing the compulsory practical training (unless you are granted with an exception by the Executive Board), KHAS, according to the University's academic regulations. The final decision on progression to Year 2 of the programme is at the discretion of the CyberMACS Executive Board.

It is the student's responsibility to check the academic calendar and the local academic regulations regularly.

Should the student not obtain 30 ECTS per semester at the end of the first year, s/he will be excluded from the CyberMACS and must reimburse the EMJM grant, if applicable. Students are only admitted to the second year if they have validated 30 ECTS/semester during the first year.

6. Master Thesis and Graduation

For your thesis examination, a report of a minimum of 20 pages (preferably with a submitted scientific publication) is mandatory, which should include at least the following sections: introduction, objectives, materials and methods, results, discussion, and bibliography. You will receive further instructions at the right time.

While your thesis will be jointly supervised (KHAS- SRH or UKIM scholars with respect to your mobility), an additional industrial supervisor can also be appointed for industry-related research if your topic is relevant.

If your advisor approves, your master thesis defences can be organised during Summer School to reach a wider audience.

If your thesis evaluation is positive, the 30 ECTS devoted to the master thesis are granted to you. In such a case, the 2nd year is validated, and you will be graduated by both involved universities (conferring the double degree).

The lecturers from other universities can also be invited to participate remotely in the defence.

As indicated in the Welcoming Guide, the graduation ceremony is currently set at the end of summer 2026 in Istanbul/KHAS. But the date and venue could be changed with respect to practical and administrative needs.

Please kindly acknowledge that the programme's participation rules, including your rights and obligations concerning academic, administrative, and financial aspects, are also defined in your Student Agreement. So read your Student Agreement carefully.

7. The Erasmus Mundus Students and Alumni Association

Erasmus Mundus Students and Alumni Association (EMA) EMA is an association for students and alumni of Erasmus Mundus Master and Doctoral programmes. EMA's vision is to become a global network of distinguished, connected, and active members of the greater Erasmus Mundus community. **As stated in your Student Agreement, you need to join EMA as a part of your student obligations.**