JÖNKÖPING UNIVERSITY
School of Engineering

PROGRAMME SYLLABUS
Preliminary, not confirmed

Cybersecurity (master), 120 credits

Cybersäkerhet (master), 120 högskolepoäng

Programme Code:	TACVJ	Programmestart:	Autumn 2027
Confirmed:		Education Cycle:	Second-cycle level

Title of qualification

Degree of Master of Science (120 credits) with a major in Computer Science, specialisation in Cybersecurity

Filosofie Masterexamen med huvudområdet datavetenskap, inriktning Cybersäkerhet

Programme overview

Main field of study

"Computer science (CS) is the study of computers and algorithmic processes, including their principles, their hardware and software designs, their applications, and their impact on society." (Tucker, Allen, ACM, 2006.)

The Computing Sciences Accreditation Board—which is made up of representatives of the Association for Computing Machinery (ACM), and the IEEE Computer Society (IEEE CS)—identifies four areas that it considers crucial to the discipline of computer science: theory of computation, algorithms and data structures, programming methodology and languages, and computer elements and architecture.

In addition to these four areas, CSAB also identifies a large number of fields as being important areas of computer science, e.g., software engineering, artificial intelligence, database systems, parallel and distributed computation, computer networking and communication, operating systems, human–computer interaction, and computer graphics.

The scientific basis for computer science is logic and discrete mathematics. Consequently, mathematical deduction is an important tool. Scientific studies in computer science are usually conducted using quantitative methods from science or engineering. The most typical research approach is controlled experiments, with subsequent statistical analysis and inference; but traditional social science methods like case studies and interviews can be used where appropriate. Another approach is design science, where an IT-artifact is developed to demonstrate how concepts, theories, models and methods work in practice.

Computer science is related to computer engineering, which in turn has a strong connection to electrical engineering. Internationally, computer science is broadly defined, specifically, hardware and computer architectures are usually included, as can also be seen from CSAB's description above. In Sweden, the distinction is often made that computer engineering mainly studies the design and construction of computers and other hardware, while computer science focuses on software systems. Areas such as hardware programming, internet-of-things, embedded systems and robotics are thus shared between the two subjects.

Computer science is also related to information systems, and the border between the two subjects is not sharp. In computer science, the information technology is usually studied from a scientific or an engineering perspective, typically with a focus on the computer system itself. Information systems, on the other hand, mainly uses methods from social science while emphasizing the business context and processes around the IT systems.

Studies in computer science grants knowledge about, e.g., the theoretical underpinnings of computer science, their implementations in computer systems, methods for software development, and methods for evaluating systems and other deliverables. The student develops skills in analyzing problems, systems, and data, in designing and programming tools and systems, in evaluating technology and its uses, and in doing all of this both independently and in collaboration with others.

At JU, computer science is organized under the discipline Industrial Product Realization. Product realization is defined as including all tasks and activities needed to develop solutions to customer needs, and to realize these solutions through physical products and associated services. Research and education in this discipline can focus on specific parts of the product realization process or apply a holistic perspective. Industrial product realization is characterized by customer adaptation, standardization, flexible production, and automation. The process often includes market- and customer analyses, structured requirements elicitation and management, analyses of production processes and materials, optimization of components, systems, and logistics flows, and development of product lifecycle support services (including usage analyses supporting maintenance, product development, and product recycling). Research and education in computer science support these tasks by way of methods and techniques for scalable data analysis, systems development, and intelligent embedded digital solutions.

Background

Cybersecurity breaches are having a profound impact on society, and the protection of digital and physical assets has become a critical and lucrative area of focus. Cybersecurity-related incidents—such as ransomware attacks, identity theft, and data breaches—frequently make headlines, highlighting the growing threat landscape. In recent years, the rise of financially motivated adversaries and state-sponsored attacks has further intensified the situation, creating an uneven playing field, particularly for smaller organisations with limited resources.

Cybersecurity is considered a horizontal market, meaning it spans across a wide range of vertical sectors, including manufacturing, automotive, banking, education, healthcare, and retail, and more. Consequently, this means there is a need to protect assets virtually anywhere in society. A notable example is the manufacturing sector, which is progressing towards Industry 5.0—a paradigm characterised by digitalisation, connectivity, and automation. This transformation increases reliance on hardware and software systems that manage and monitor industrial operations, particularly operational technology (OT). OT systems are integral to production processes, and their proper functioning is vital for operational continuity. As these systems become networked and involve human operators, new cybersecurity challenges inevitably arise.

The growing importance of cybersecurity has led to a strong demand for skilled professionals in the field. This master’s programme in cybersecurity is designed to equip students with the knowledge and expertise necessary to address these complex and evolving threats, ultimately contributing to the protection and resilience of modern society.

Objectives

The programme is intended for students with a bachelor's degree in computer science, computer engineering, informatics, information systems or similar. By introducing students to core technologies and concepts in the field, the programme will help them understand, use and implement solutions that address cybersecurity-related issues. The programme aims to provide knowledge that enhances the skills and abilities of students with different IT-related backgrounds by providing broad cybersecurity skills and the possibility to select a focus on several courses that align with personal interests or backgrounds.

Post-graduation employment areas

This master's programme in cybersecurity prepares students for third-cycle courses and research projects or work in the industry. With the knowledge provided by the programme, students will be able to undertake a variety of roles, such as cybersecurity specialist, security analyst, cybersecurity engineer, cybersecurity manager, security operations centre analyst or cybersecurity consultant.

Objectives

Common learning outcomes

After the completion of the programme, students must meet the intended learning outcomes, as described in The Higher Education Ordinance by Degree of Master (1-9), and also the intended learning outcome, as described by JTH:

Knowledge and Understanding

1. demonstrate knowledge and understanding in the main field of study, including both broad knowledge of the field and a considerable degree of specialised knowledge in certain areas of the field as well as insight into current research and development work
2. demonstrate specialised methodological knowledge in the main field of study

Competence and Skills

3. demonstrate the ability to critically and systematically integrate knowledge and analyse, assess and deal with complex phenomena, issues and situations even with limited information
4. demonstrate the ability to identify and formulate issues critically, autonomously and creatively as well as to plan and, using appropriate methods, undertake advanced tasks within predetermined time frames and so contribute to the formation of knowledge as well as the ability to evaluate this work

5. demonstrate the ability in speech and writing both nationally and internationally to clearly report and discuss his or her conclusions and the knowledge and arguments on which they are based in dialogue with different audiences
6. demonstrate the skills required for participation in research and development work or autonomous employment in some other qualified capacity

Judgement and Approach

7. demonstrate the ability to make assessments in the main field of study informed by relevant disciplinary, social and ethical issues and also to demonstrate awareness of ethical aspects of research and development work
8. demonstrate insight into the possibilities and limitations of research, its role in society and the responsibility of the individual for how it is used
9. demonstrate the ability to identify the personal need for further knowledge and take responsibility for his or her ongoing learning
JTH. prove ability to embrace interdisciplinary approaches

Programme-specific learning outcomes

Upon completion of the program, the intended learning outcomes provided for programme must also be met.

Knowledge and Understanding

10. display knowledge of the area of cybersecurity and its related subject areas, and
11. display knowledge of the definitions, terminology, and concepts of cybersecurity.

Competence and Skills

12. demonstrate skills in using tools for penetration testing and cybersecurity operations, and
13. demonstrate the ability to create risk and privacy impact assessments.

Judgement and Approach

14. demonstrate an insight into the societal, legal and ethical aspects of cybersecurity operations, and
15. demonstrate the ability to suggest risk-based security controls to counter threats and vulnerabilities.

Contents

Programme principles

Instruction is delivered through a combination of lectures, seminars, exercises, laboratory sessions, and project work. All courses are conducted in English, and all final examinations are held in English. The teaching approach within the programme places strong emphasis on real-life scenarios and collaborative learning. Lectures and lab sessions frequently include examples drawn from real-world projects, helping to contextualise theoretical concepts through practical application.

In course assignments, students work in groups to plan and implement solutions to problems based on real-life cases. These solutions are presented in both written and oral form, fostering skills in communication and leadership within a team setting.

The programme culminates in an independent degree project worth 30 higher education credits. Students, either individually or in pairs, undertake and present a project in cybersecurity that demonstrates their ability to apply the knowledge and skills gained throughout the programme. The degree project is completed during the final term and may be conducted in close collaboration with a company or organisation.

Research basis

Within the Department of Computer Science and Informatics, there is a strong emphasis on research related to cybersecurity - a field that impacts all sectors of society. At the department, the research focus is particularly centred on cybersecurity and privacy in industrial and public sector contexts, where the majority of the department's cybersecurity research is conducted. Furthermore, there is a particular focus on human aspects among the staff, where contributions to, for example, awareness, management, usable security, and social engineering have been made.

Cybersecurity is inherently a multi- and interdisciplinary field, drawing on principles from a wide range of disciplines. These include computing (e.g., artificial intelligence, privacy, software development) and the social sciences (e.g., psychology, ethics, economics), among others.

The programme is also closely aligned with Jönköping University's Areas of Strength’s within its research environment, particularly with sub-environments Integrated Product and Production Development for Sustainability and Resilience and Human-Centred Industrial AI. These areas address the digitalisation and digital transformation of products and services - domains that are fundamentally dependent on cybersecurity. As such, cybersecurity serves as a crucial foundation for fostering interdisciplinary research across schools and departments, as well as for facilitating collaboration between academia, industry, and the public sector.

Equal terms, gender equality and diversity

The School of Engineering (JTH) strives in all its activities to ensure that all individuals are given equal opportunities and treated equally. At both the JU and JTH levels, this is reflected in governing documents concerning organizational and personnel matters, the establishment and delivery of programmes and courses, as well as the monitoring of educational quality. At JTH, student influence is also ensured through student representation in various educational and industry councils.

Courses in the programme that address aspects of gender equality include *Digital Ethics and Privacy* (7.5 credits), *Penetration Testing* (7.5 credits), *Human Aspects of Cybersecurity* (7.5 credits), *Cybersecurity and AI* (7.5 credits), and *Forensics, Cybercrime and Incident Response* (7.5 credits). Gender-related issues are explored by identifying and analysing the diverse perspectives, conditions, and needs of individuals across different contexts. One concrete example is the course *Cybersecurity and AI*, which includes a discussion on the risks of biased outcomes stemming from AI models trained on unbalanced or biased datasets, highlighting how such biases can reinforce structural inequalities, including those related to gender.

Study abroad

JTH has internationalization as a focus area where the educational programmes include opportunities for both international experiences at home as well as various opportunities to do internships and study abroad, giving students valuable experiences and skills to prepare them for a global labour market.

Semester three of the programme is intended as an exchange semester. Therefore, the third semester is designed with flexibility in mind and comprises 30 credits intended for exchange studies. Students may choose from the following four options:

(1) Exchange studies: Students can pursue courses within the field of cybersecurity or a closely related area at a partner university. The selection of courses is made in consultation with the programme manager to ensure relevance and academic coherence.

(2) Combination of exchange studies and internship: Students may combine 15 credits of coursework (chosen within the cybersecurity field or a related area, in consultation with the programme manager) with a 15-credit internship. The internship is carried out at a private company or public organisation with a focus on cybersecurity practice or research.

(3) On-campus course package with internship: Students who do not opt for an exchange semester follow a predefined course package at the School of Engineering. The semester begins with two courses - *Applied Cryptology* and *State-of-the-Art in Cybersecurity* - followed by the *Industrial Placement Course in Cybersecurity*.

(4) On-campus course package with elective studies: Students who choose not to undertake either an exchange semester or an internship follows the same initial courses - *Applied Cryptology* and *State-of-the-Art in Cybersecurity* - and subsequently take 15 credits of elective courses offered at Jönköping University.

Programme progression

The course *Cybersecurity Overview* provides a holistic perspective on cybersecurity and its relationship to adjacent fields, such as information security and privacy. It also introduces general and industry-specific standards and frameworks, offering a reference point for understanding the field. Furthermore, the course presents key concepts in risk management and cybersecurity operations.

Running in parallel is the course *Human Aspects of Cybersecurity*, which addresses the socio-technical nature of cybersecurity as shaped by the interaction between technology, individuals, and the surrounding social context. The course explores user expectations and the various factors that influence individuals' ability to comply with cybersecurity requirements - such as social environments, personality traits, and cognitive abilities - and introduces theoretical models that explain the formation of cybersecurity-related behaviours.

These courses are followed by *Research Methods in Cybersecurity* and *Penetration Testing*, which also run in parallel. The concept of red team/blue team is central in cybersecurity practice, and *Penetration Testing* focuses on the red team perspective, i.e., offensive security. Topics include hacking, penetration testing, and associated tools and methodologies. In parallel, *Research Methods in Cybersecurity* introduces both quantitative and qualitative research approaches. Topics covered include descriptive statistics, sampling, survey design, regression analysis, qualitative data collection and analysis, and experimental design.

The second semester begins with *Critical Infrastructure and Industrial Cybersecurity* and *Digital Ethics and Privacy*. The former addresses cybersecurity challenges specific to critical infrastructure and associated systems. It introduces threats, vulnerabilities, and security controls relevant to industrial control systems (e.g., SCADA and operational technology) and networks (e.g., Industrial Internet of Things). The latter course,

Digital Ethics and Privacy, explores the legal and societal dimensions of cybersecurity. It addresses human values, vulnerability, and intersectionality, fostering critical thinking and ethical reflection. The course also covers privacy-related legal and professional frameworks, including privacy by design and privacy impact assessments.

The final two courses in the first year are *Forensics, Cybercrime and Incident Response* and *Cybersecurity and AI*. The *Forensics, Cybercrime and Incident Response* course focuses on blue team activities, i.e., defensive security. It covers network security mechanisms (such as intrusion detection/prevention systems, firewalls, network admission control, and virtual private networks), incident response standards and frameworks, digital forensics, digital evidence, and monitoring techniques. *Cybersecurity and AI* examines the intersection of cybersecurity and artificial intelligence, introducing foundational AI concepts and their application in both offensive and defensive contexts. Topics include adversarial uses of AI (e.g., deepfakes and personalised phishing) as well as AI-driven defences such as anomaly detection and automated threat analysis.

The second year begins with a flexible semester (30 credits), which may include an exchange opportunity, internship, or campus-based coursework. If the on-campus option is selected, students take *Applied Cryptology* and *State-of-the-Art in Cybersecurity*. *Applied Cryptology* introduces cryptographic techniques fundamental to ensuring confidentiality and integrity. It covers cryptographic primitives, formal security models, elliptic curve cryptography, blockchain technologies, and their practical applications. *State-of-the-Art in Cybersecurity* explores current and emerging developments in the field, equipping students with advanced knowledge and skills.

Students then have the option to enroll in the *Industrial Placement Course in Cybersecurity* or undertake 15 elective credits at Jönköping University. The placement can take place in either the public or private sector and may focus on applied cybersecurity practice or research.

The final semester is dedicated to the *Final Project Work in Computer Science* (30 credits), where students are expected to deepen their knowledge of contemporary cybersecurity challenges and contribute original work to the field. The project requires students to identify and analyse a problem, evaluate alternative solutions, and implement an appropriate approach.

Courses

Course changes can occur, as long as they do not substantially affect the programme's content and learning goals.

Mandatory courses

Semester	Course Name	Credits	Main field of study	Specialised in	Course Code
1	Research Methods in Cybersecurity	7.5	Computer Science	A1F	T2FICP
1	Human Aspects of Cybersecurity	7.5	Computer Science	A1N	T2MAAC
1	Penetration Testing	7.5	Computer Science	A1F	T2PMBS
1	Cybersecurity Overview	7.5	Computer Science	A1N	TCSR24
2	Cybersecurity and AI	7.5	Computer Science	A1F	T2COAE
2	Forensics, Cybercrime, and Incident Response	7.5	Computer Science	A1F	T2FCOI
2	Critical Infrastructure and Industrial Cybersecurity	7.5	Computer Science	A1F	T2KIOI
2	Digital Ethics and Privacy	7.5	Informatics	A1N	TEKR23
3	Possibility to study abroad	30			
3	Elective courses	15			
3	State-of-the-art in Cybersecurity	7.5	Computer Science	A1F	T2SICI
3	Applied Cryptology	7.5	Computer Science	A1N	T2TKEK
4	Final Project Work in Computer Science	30	Computer Science	A2E	TEXV23

Elective courses

Semester	Course Name	Credits	Main field of study	Specialised in	Course Code
3	Industrial Placement Course in Cybersecurity	15	Computer Science	A1F	T2NKIC

Teaching and examination

The academic year is divided into two semesters, and the semesters into two study periods. In each study period two courses are generally taken in parallel. Assessment is part of each course or module. Modes of assessment and grades are shown in each course syllabus.

Entry requirements

The applicant must hold a minimum of a bachelor's degree (i.e., the equivalent of 180 ECTS credits at an accredited university) with at least 90 credits in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent. Proof of English proficiency is required.

Continuation Requirements

In order to begin the second year, at least 37,5 credits from the programme's first year must be completed.

Qualification Requirements

To obtain a Degree of Master of Science (120 credits) with a major in Computer Science, specialisation in Cybersecurity, students must complete a minimum of 120 higher education credits in accordance with the current programme syllabus, at least 60 of which must be in the main field of study Computer Science.
In addition a Degree of Bachelor of Science in Engineering/Degree of Bachelor of Science or an equivalent Swedish or foreign qualification is required.

Quality Development

At JTH, systematic quality assurance is carried out within JU's established quality system. This system, based on the requirements of the Higher Education Act, the Higher Education Ordinance, and the Standards and Guidelines for Quality Assurance in the European Higher Education Area, has been reviewed and approved by the Swedish Higher Education Authority.

Active and continuous course evaluation, including student feedback through course surveys, forms one of the cornerstones of this system. Annual programme evaluations and student representation in JTH's various educational and industry councils are two additional examples.

Other Information

Admission is under ‘Admission regulations for first- and second cycle courses and study programmes at Jönköping University (Admission regulations)’.

This syllabus is based on ‘Regulations and guidelines for first-, second- and third-cycle education at Jönköping University’.