

# Academic Guide Exchange

## Safety & Security Management Studies

Inbound Exchange Students

2024-2025



**let's change**  
YOU. US. THE WORLD.

**THE HAGUE**  
UNIVERSITY OF  
APPLIED SCIENCES

# Academic Guide Exchange

Safety & Security Management Studies

Faculty Public Management, Law and Safety

**Author**

Irene van der Wal

**Date**

21 March 2024

**Version**

March 2024 – Laura Díaz

**NOTE: this academic guide is still subject to change.**

## Disclaimer

The information contained in this guide is, to the best of our knowledge, true and accurate at the time of publication and is solely for information purposes. Changing circumstances may cause alterations in its outline at any time. The programme of The Hague University of Applied Sciences accepts no liability for any loss or damage howsoever arising as a result of use or reliance on this guide or on the information thereon or in respect of information accessed via any links from the Web pages.

# Foreword

The Faculty of Public Management, Law & Safety is one of the largest faculties at The Hague University of Applied Sciences. The faculty contains six programs, three of which are full-time English streams, namely International Public Policy & Leadership (IPPL), International and European Law (Law) and Safety and Security Management Studies (SSMS). Please note that it is only possible to choose courses within one programme. Combining courses from different programmes is not possible.

In making the decision to study here, you will choose to be part of a dynamic and multicultural community where personal growth and intellectual stimulation are prioritised. In this programme, we teach our students to be analytical, to question, to engage in 'out of the box' thinking, to ask challenging questions and to use their imagination in solving real world problems. So that you return to your home country a changed individual, equipped to make a difference in society.

If this sounds exciting to you, then you will definitely thrive in The Hague, world's capital of Peace, Justice and Safety, and you will enjoy your time with us.



# Content

<b>Your Exchange Programme at SSMS.....</b>	<b>5</b>
<b>Course Overview .....</b>	<b>6</b>
<b>Semester 1 – Course descriptions .....</b>	<b>7</b>
MINOR Safety Risk & Safety Compliance.....	7
MINOR Terrorism and Counter-Terrorism.....	8
MINOR Intelligence Collection & Analysis .....	9
MINOR Crime, Safety & Security .....	11
MINOR Human Security .....	12
MINOR Cybercrime .....	14
<b>Semester 2 – Course descriptions .....</b>	<b>16</b>
Research Consultancy Project .....	16
Cyber Security Lab .....	17
Managing Corporate Challenges (MCC) .....	19
<b>Practical Information .....</b>	<b>21</b>

# Your Exchange Programme at SSMS

Safety and security are high on the agenda in our contemporary global community. In various fields, ranging from politics to private businesses, there is an increasing need for professionals with the ability to understand the challenges and interests at stake. Beyond the "insecurity frame" resulting from environmental, criminal, and industrial threats, the safety of the citizens, employees, buildings and facilities pose critical challenges. Working in this field requires you to keep a cool head and bring parties together for successful cooperation. You need to assess and analyse risks and defuse critical situations where necessary. The SSMS programme focuses on these various angles and issues by exploring academic source material, practising skills in workshops, and working in teams during projects.

In the academic year 2024-2025, SSMS offers the possibility to choose between a semester or a full-year exchange programme. A semester programme should add up to 30 ECTS and a full-year programme up to 60 ECTS. For clarification, at THUAS 1 ECTS represents a workload of 28 hours (contact hours + self-study).

SSMS is a fulltime English stream programme. All minors and courses are taught in English and require physical attendance.

## Course Overview

Course title	ECTS	Semester 1 Term 1	Semester 1 Term 2	Semester 2 Term 3 + 4
<a href="#">Minor Safety Risk &amp; Safety Compliance</a>	15	x		
<a href="#">Minor Terrorism and Counter-Terrorism</a>	15		x	
<a href="#">Minor Intelligence Collection &amp; Analysis</a>	15	x		
<a href="#">Minor Crime, Safety &amp; Security</a>	15	x		
<a href="#">Minor Human Security</a>	15		x	
<a href="#">Minor Cybercrime</a>	15		x	
<a href="#">Research Consultancy Project</a>	15			x
<a href="#">Cyber Security Lab</a>	9			x
<a href="#">Managing Corporate Challenges (MCC)</a>	6			x

## Semester 1 – Course descriptions

Below you will find a list of the courses within the bachelor programme. These courses are offered in English, unless stated otherwise.

MINOR Safety Risk & Safety Compliance	
Credits	15 ECTS
Code	SSMS-SRC-23
Entry requirements	This is a work-intensive course. Very good command of the English language and the willingness to read legal texts are basic requirements.
Semester	1, Term 1
Method	Lectures, research and exercises
Lecturer(s)	D. Christian, M.I. Bohm, R.M.J. Wong
Learning outcomes	
Recommended or required reading/tools	T.B.A
Assessment methods	SRC-Attendance, SRC-Training, SRC-Workshops, SRC-Written exam
Level	Third year
Course content	<p>In today's world safety is everywhere, and it is often highly regulated: laws govern almost every aspect of industrial and corporate safety. This minor responds to a growing demand for safety compliance professionals in both the public and private sector.</p> <p><b>What will you do?</b></p> <p>In this SSMS minor, students will familiarize themselves with a range of safety risks, the legal rules applicable to their management and approaches to control these risks within the applicable legal framework. A special focus is placed on risks found in high-risk sectors. The minor builds upon existing knowledge of risk management and industrial safety gained in the first two years of the SSMS programme. The application of the newly gained knowledge is done during practical exercises, guest lectures and through field trips.</p> <p>Topics discussed include Occupational Health, Fire Safety, Dangerous Goods Safety, Process Safety, Personal Safety and Emergency preparedness and response and Business Continuity.</p> <p>To pass the minor, students will need to complete group projects, write a safety and compliance plan, and deliver a training on a safety topic. Sessions will be taught on up to three days per week, including lectures, exercises and excursions. Attendance is mandatory.</p>

<b>MINOR Terrorism and Counter-Terrorism</b>	
Credits	15 ECTS
Code	SSMS-TCT-22
Entry requirements	Good command of English (oral and written)
Semester	1, Term 2
Method	Lectures, research and exercises
Lecturer(s)	Dr. Klaas Voss
Learning outcomes	<ol style="list-style-type: none"> <li>1. Students can distinguish between different types of terrorist activities and terrorist groups on the national, international, and transnational level.</li> <li>2. Students can apply different theoretical approaches to the underlying socio-economic, ideological, and political root causes of both home-grown (domestic) and foreign terrorism.</li> <li>3. Students can explain different tactics and “best practices” of both terrorist and counterterrorist actors in a variety of geographical and cultural settings.</li> <li>4. Students can apply different models and paradigms of (counter-) terrorism studies to address concrete (fictitious or historical) problems and challenges they are confronted with.</li> </ol>
Recommended or required reading/tools	Nacos, B. L. (2019). <i>Terrorism and counterterrorism</i> (6th ed.). New York: Routledge.
Assessment methods	<ol style="list-style-type: none"> <li>1. Individual research proposal (P/F)</li> <li>2. Individual research report (45%)</li> <li>3. Group simulation (15%)</li> <li>4. Written exam (40%)</li> <li>5. Reading quizzes (P/F)</li> <li>6. Attendance (P/F)</li> </ol>
Level	First, second, third or fourth year (for regular bachelor student)
Course content	<p>Interdisciplinary approach on terrorism and counter-terrorism. The SSMS minor Terrorism and Counterterrorism aspires to bridge the gap between practitioners and academia by integrating theoretical approaches to the topic with practical elements. Such practice-oriented components of the course include exercises in counterterrorist decision-making, introductions to weapons and tactics, and exposure to experienced practitioners in fields like military force protection, police counterterrorism, or CBRN counterproliferation.</p> <p>On a more abstract level, students will learn how to categorize terrorist groups and their organizational structures, learn about models of radicalization and de-radicalization, and examine military doctrines like counterinsurgency. They will also study specific phenomena, such as lone wolf attacks, the terror-crime nexus, or ISIS and their recruitment of so-called foreign fighters.</p>



On a more general level, the minor will also help students to chart counterterrorism as a field of employment and gain greater awareness of career opportunities in this area.

**What will you do?**

These are the main elements addressed in this course:

1. We will focus on the essence of terrorism as an instrument to achieve certain goals, in addition to an exploration of this phenomenon and the difficulties in defining it. It critically assesses conventional wisdom, theories, and assumptions that have emerged in recent years. It will also provide an overview of the state of the art in (counter-)terrorism studies.
2. We look more in-depth at the different types of terrorists. Moreover, it will examine the possibilities and implications for policymaking including its practical applications at an international level.
3. Different historical and regional cases will also be addressed in the minor. Although media primarily focus on Jihadi terrorism, the phenomenon of terrorism exists beyond the Islamic world in great variety and severity.
4. There will also be a focus on how to conduct research within the field of terrorism studies. Researchers, as well as other actors linked with this field, encounter various problems at different fronts. It is therefore crucial to explore different channels and methods in order to gain further insight into how terrorism may possibly develop in the near future and how it should be dealt with.

**MINOR Intelligence Collection & Analysis**

Credits	15 ECTS
Code	SSMS-ICA-22
Entry requirements	Familiarity with the basics of security studies, Good command of English (oral and written)
Semester	1, Term 1
Method	Lectures, research and exercises
Lecturer(s)	Dr. Klaas Voss
Learning outcomes	<ol style="list-style-type: none"> <li>1. Students can use international key terminology from the field of intelligence studies.</li> <li>2. Students can explain the universal tools and basic models of intelligence tradecraft, such as the intelligence cycle, the collection plan, and the gathering disciplines.</li> <li>3. Students can employ specific key methodologies from the fields of criminal intelligence, military intelligence, financial intelligence and counterintelligence.</li> <li>4. Students can apply selected structured analytic techniques (SATs) for intelligence analysis.</li> </ol>

	<ol style="list-style-type: none"> <li>5. Students can compare and contrast different national approaches to intelligence and counterintelligence work.</li> <li>6. Students can develop their own case studies and scenarios for intelligence analysis on the basis of international academic literature.</li> <li>7. Students can professionally operate at least one OSINT cyberintelligence tool.</li> </ol>
Recommended or required reading/tools	Dover, R., Goodman, M.S, & Hillebrand, C. (Eds.). (2015). Routledge companion to intelligence studies. London: Routledge
Assessment methods	<ol style="list-style-type: none"> <li>1. Report (35%)</li> <li>2. Group presentation (25%)</li> <li>3. Written exam (45%)</li> <li>4. Reading quizzes (P/F)</li> <li>5. Attendance (P/F)</li> </ol>
Level	Third year
Course content	<p>No matter whether they work for investment firms, international organisations, NGOs, private security companies, government intelligence agencies, the military or the police – intelligence analysts are the true experts when it comes to making the best use of limited available information. This minor covers various aspects of intelligence work in both domestic and international contexts, including the major fields of political, military and criminal intelligence.</p> <p><b>What will you do?</b></p> <p>Students will be familiarised with basic techniques of espionage and surveillance, counterintelligence, and technologies used for the collection of information. They will understand how foreign intelligence services operate, how the military analyses aerial photography, and how intelligence-led policing is used in the battle against organized crime. Practical exercises in information analysis are based on the same structured analytic techniques that are employed within the international intelligence community.</p> <p>The Minor Intelligence Collection &amp; Analysis encourages students to apply skills and methods of intelligence collection and analysis in a multitude of professional contexts. The curriculum covers many topics and problems of paramount contemporary relevance from an intelligence perspective. These issues include terrorism, maritime piracy, money laundering, human trafficking, privacy issues, civil wars, and peace operations. In the end, students will have achieved a profound understanding of the benefits of intelligence tradecraft in a variety of security-related working environments.</p> <p>The course content comprises of the necessary theoretical background to intelligence, including the connected academic disciplines of intelligence studies and intelligence history. However, the emphasis is upon intelligence methodology and the practical application of intelligence analysis to international security, foreign policy, and law enforcement. In this context operational case studies are presented and sessions are devoted to intelligence lessons learned.</p>

<b>MINOR Crime, Safety &amp; Security</b>	
Credits	15 ECTS
Code	SSMS-CSS-21
Entry requirements	Good command of English (oral and written)
Semester	1, Term 1
Method	Lectures, research and exercises
Lecturer(s)	Dr. Anna Matczak
Learning outcomes	<ol style="list-style-type: none"> <li>1. Students can explain the relationship between crime, safety &amp; security.</li> <li>2. Students can compare, analyse and discuss the criminological issues raised in the course and situate them in various international contexts.</li> <li>3. Students can explain and apply crime prevention techniques [practiced in the course].</li> <li>4. Students can discuss and apply criminological topics as policy issues.</li> <li>5. Students can express criminological issues through creative outlets and media.</li> </ol>
Recommended or required reading/tools	T.B.A
Assessment methods	<ol style="list-style-type: none"> <li>1. Written exam (45%), minimum pass rate 5.5</li> <li>2. Policy brief (25%), minimum pass rate 5.5</li> <li>3. Creative assignment (25%), minimum pass rate 5.5</li> </ol>
Level	First, second, third or fourth year (for regular bachelor student)
Course content	<p>Crime is a very dynamic and context-dependant concept. There is more to our understanding of crime than just that it should be seen as a violation of formally implemented laws. Crime is socially constructed which means that the criminalisation and decriminalisation of a certain act/behaviour is determined by social processes, and these vary among countries. Crimes routinely dealt with in the criminal justice system are only the tip of the iceberg to all the harms and wrongdoings committed in societies and its nature is changing rapidly also due to technological advances.</p> <p>The purpose of the minor is to help students acquire a more sophisticated understanding of major contemporary debates in comparative criminology with reference to sexual violence, transnational organised crime, drug and human trafficking, crimmigration, corporate crime, safety crimes, environmental crime, plural policing, restorative and criminal justice and learn how to apply relevant criminological issues to policy questions. Each week of the minor completes with one of the following practical exercises: crime script analysis, social network analysis, situational crime prevention, multi-agency policing exercise in relation to domestic violence, mock trial and restorative justice conference.</p>

<b>What will you do?</b>
Week 1 – Topics: Introduction to the minor, An uneasy relationship between crime, safety and security, crime script analysis (exercise).
Week 2 – Topics: Sexual violence, domestic violence, online grooming, multi-agency response to domestic violence (simulation).
Week 3 – Topics: Transnational organized crime, Netherlands as a narco-state, drug and human trafficking, crimmigration, social network analysis (exercise).
Week 4 – Topics: Crimes of the powerful, the corporate criminal, situational crime prevention (film analysis + exercise).
Week 5 – Topics: Environmental crimes, wildlife and waste crimes, the implications of climate change and green criminology.
Week 6 – Topics: Policing, state police, the role of private sector in policing, policing humanitarian emergencies (case studies: Hurricane Katrina, Ebola outbreak, Fukushima disaster).
Week 7 – Topics: Seeking justice, sentencing, criminal and restorative justice, the role of probation in criminal justice, mock trial and restorative justice conference (simulation).

MINOR Human Security	
Credits	15 ECTS
Code	SSMS-HS-23
Entry requirements	Good command of English (oral and written)
Semester	1, Term 2
Method	Lectures, research and exercises
Lecturer(s)	Dr. Tessa de Rijck van der Gracht
Learning outcomes	<ol style="list-style-type: none"> <li>1. The student can contrast the human security approach with conventional state-centric approaches in tackling past and current problems, including health, food, economic, political and conflict related issues presented in the minor.</li> <li>2. The student can apply formats and strategies, related to citizen engagement, to address current global and local security issues.</li> <li>3. The student can demonstrate critical and conceptual thinking on local and global cases and phenomena, based on theories and frameworks, including from the United Nations, taught in the minor.</li> <li>4. The student can formulate security management strategies for human rights, development, and humanitarian aid workers, using risk assessment and other relevant security tools, presented in the minor.</li> </ol>

	<ol style="list-style-type: none"> <li>5. The student can distinguish the different and interconnected roles of various stakeholders, including civil society, government and policy makers, security sector agents, and private actors, in security related issues.</li> <li>6. The student can cooperate effectively and constructively in a team.</li> </ol>
Recommended or required reading/tools	<p>Gaspar D. &amp; Gomez O.A. (2022). The Position of Crisis in Human Development Processes and Thinking: Using the Human Security Perspective in an Era of Transitions. UNDP Special Report on Human Security Background Paper No.3-2022.</p> <p>Glasius, M (2008). Human Security from Paradigm Shift to Operationalization: Job Description for a Human Security Worker. Security Dialogue 39: 31, 31- 54.</p> <p>Schirch, L. (ed.) (2016). Handbook on Human Security: A Civil-Military-Police Curriculum. The Alliance for Peacebuilding, GPPAC, Kroc Institute.</p> <p>United Nations Development Programme (1994). Human Development Report. Oxford University Press.</p> <p>United Nations Development Programme (2022). New threats to human security in the Anthropocene – Demanding greater solidarity. Retrieved from UNDP website: <a href="https://hs.hdr.undp.org/pdf/srhs2022.pdf">https://hs.hdr.undp.org/pdf/srhs2022.pdf</a></p> <p>Other literature to be determined.</p>
Assessment methods	<ol style="list-style-type: none"> <li>1. Exam (30%), minimum pass rate: 5,5</li> <li>2. Portfolio (50%), minimum pass rate: 5,5</li> <li>3. Creative Assignment (20%), minimum pass rate: 5,5</li> <li>4. Attendance: Pass/Fail</li> </ol>
Level	First, second, third or fourth year (for regular bachelor student)
Course content	<p><b>What will you do?</b></p> <p>Human security, a people-centred approach to security, was first introduced by the United Nations Development Programme in 1994. Ever since, it has been embraced as a useful framework that addresses local and global security issues in a preventative and comprehensive manner, engaging a multitude of stakeholders to formulate solutions that are sustainable and leave no one behind.</p> <p>The main goal of this minor is to enrich and broaden student perspectives on complex security issues and how to analyse and tackle these. Human security offers an alternative approach to security, with practical tools and methodologies, that can complement or replace existing practices. The minor covers a wide range of issues such as the climate crisis and migration, technology and threats to democracy, militarization and the war on drugs. We question current responses and power relations to aim for alternative solutions that address the root causes of insecurity.</p> <p>Once students have explored the main approaches that underlie human security, they will learn how to apply these to existing case studies and scenarios. Students</p>

will learn directly from practitioners in the field, from refugee case workers and international human rights activists to government representatives and humanitarian aid workers. Through field visits, public events and guest lectures, they will experience what it means to be a human security practitioner.

## MINOR Cybercrime

Credits	15 ECTS
Code	SSMS-CC-23
Entry requirements	Good command of English (oral and written)
Semester	1, Term 2
Method	Lectures, research and exercises
Lecturer(s)	Dr. Anna Matczak
Learning outcomes	<ol style="list-style-type: none"> <li>1. Students can identify and discuss the features of different types of cybercrime. (Bloom's taxonomy - Comprehension)</li> <li>2. Students can describe different profiles of cyber offenders and victims. (Bloom's taxonomy - Comprehension)</li> <li>3. Students can illustrate the current interventions to curtail cybercrime. (Bloom's taxonomy - Comprehension)</li> <li>4. Students can construct a digital portfolio on cybercrime. (Bloom's taxonomy – Application)</li> <li>5. Students can construct a research report on cybercrime. (Bloom's taxonomy - Application)</li> <li>6. Students can develop a creative method to raise awareness about cybercrime and propose solutions to curtail it. (Bloom's taxonomy - Application)</li> </ol>
Recommended or required reading/tools	Van der Wagen, W., Oerlemans, J.J. and Kranenbarg, W.M. (2022). Essentials in cybercrime. A criminological overview for education and practice. The Hague: Eleven.
Assessment methods	<ol style="list-style-type: none"> <li>1. Written exam (40%), minimum pass rate 5.5</li> <li>2. Research report (30%), minimum pass rate 5.5</li> <li>3. Creative assignment (30%), minimum pass rate 5.5</li> <li>4. Class participation/attendance (P/F)</li> </ol>
Level	First, second, third or fourth year (for regular bachelor student)
Course content	Cybercrime includes all criminal conduct in which Information Communication Technology (ICT) systems are essential in the execution of the offence (Wagen et al. 2022). The opportunities provided through digital and communications technologies, in particular social media, have not only influenced the way we live in a 'digital society', but also the way we violate norms, commit crimes, fall victims to crimes and participate in justice processes. Cybercrime as a criminal domain, but also as an academic field of study, is rapidly developing. Although cybercrime can be very technical in nature, this minor is primarily criminological

in content and approach, and offers a comprehensive educational package to take a modern perspective on crime and its human factor. The main objective of the minor is to demonstrate how criminal activity has been changing over the recent decades, how these new ways of violating norms change the traditionally-perceived profiles of offenders and victims, and explore the range of interventions applied in cybercrime prevention. Hence, the course is structured as follows: (1) introduction and digital investigations, (2) cyber offending and victimisation, (3) cybercrime prevention, (4) 3-day long workshop aimed at enhancing students' digital skills.

### **What will you do?**

Week 1 – Topics: Introduction to the minor, Cybercrime in a digital society, Types of cybercrime and their criminalization, The application of crime theories in cybercrime (exercise).

Week 2 – Topics: Digital investigations (part I), Digital investigations (part II), Digital investigations (part III), (Cyber) Crime script analysis (exercise).

Week 3 – Topics: Prevalence and trends in cybercrime offending, Typologies and background characteristics of cyber offenders, The role and structure of online markets in cybercrime, Online escape room (exercise).

Week 4 - Risk and protective factors of cybercrime victimization, The extent and developments of cybercrime victimisation in the Netherlands, Victimhood of cybercrime in small and medium-sized enterprises, Sexual abuse in a digital society.

Week 5 – Topics: Policing cybercrime – an international perspective (part I), Policing cybercrime – an international perspective (EUROPOL), Policing cybercrime in the Netherlands, Study visit to the Dutch High-Tech Crime Police Unit.

Week 6 – Topics: A walk-through of cybercrime interventions, The application of situational crime prevention in cybercrime, Hacktivism: motivations, engagement processes and organizational aspects, The role of campaigns in cybercrime prevention.

Week 7 – Topics: Enhancing digital skills training (incl. social media protection toolkit, Darknet, data analytics and visualization). The final outcome of the training will be to produce (in groups of 5) a digital evidence portfolio/report for the police/court/probation.

## Semester 2 – Course descriptions

Research Consultancy Project	
Credits	15 ECTS
Code	SSMS-3P1-23
Entry requirements	Good command of English (oral and written)
Semester	2
Method	Lectures, research and exercises
Lecturer(s)	Enrique Gomez-Llata Maria Ines Trigo de Sousa Menandro S. Abanes
Learning outcomes	1) The student executes applied research for a local and international client. 2) The student coordinates with a client in a professional and structured manner. 3) The student presents sound conclusions and applicable recommendations. 4) The student develops an implementation plan from the recommendations.
Recommended or required reading/tools	NA
Assessment methods	1. Research proposal 30% 2. Research report 50% 3. Presentation 20% 4. Attendance P/F
Level	First, second, third or fourth year (for regular bachelor student)
Course content	<p>In this project, students practise and experience the conceptualisation, design, practice and valorisation of applied safety and security research. Students focus on a specific problem in the field of safety and security management. They stay directly in touch with their assigned clients to work on problems that may have affected their respective organisations and that pose potential security and safety risks to their operations. After contextualising the problem students then develop their own research strategy to address the problem. Through a combination of lectures, interactive workshops, desk research, external appointments, interviews, and group discussions students will learn how to design, conduct (field) research and write a research report.</p> <p>Moreover, students take up the role of proactive consultants, rather than mere researchers, that are ultimately tasked with providing viable approaches to the problem taking into account various angles as well as the short- / long-term consequences for the 'client'. They use knowledge and skills that they have acquired during previous modules, e.g. professional and presentation skills, research skills and others. These knowledge and skills will be of added value for this project, which constitutes a crucial exercise in preparation for the Year 4 thesis as well as internship experience.</p>



	<p><b>What will you do?</b></p> <p>The Research Consultancy Project will touch on various elements from previous SSMS projects, courses including risk assessment, problem analysis in combination with clear and effective communication skills, and research methods. Additionally, this project will present students with real-life conditions that safety and security professionals must handle effectively, particularly regarding dealing with potential clients.</p> <p>Ultimately, based on research findings, the students must develop effective but realistic and practical recommendations that best fit the character and expectations of the 'client'. Students will produce research proposals, conduct data collection and analysis, and deliver the final report and presentation at the end of the semester.</p>
--	--

Cyber Security Lab	
Credits	9 ECTS
Code	SSMS-3P2-23
Entry requirements	Good command of English (oral and written)
Semester	2
Method	Lectures, research and exercises
Lecturer(s)	Raoul Notté, Jan Treur
Learning outcomes	<ol style="list-style-type: none"> <li>1) The student can understand the human element in cyber security, and its profound impact on digital security.</li> <li>2) The student can explore diverse examples to grasp the significance of human behavior in cyber security processes.</li> <li>3) The student can analyse how different circumstances and measures influence potential outcomes. Dive into what-if analysis to foresee and address cybersecurity challenges.</li> <li>4) The student can apply network-oriented modeling techniques to investigate variations of scenarios within the cybersecurity field, tackling real-world substantial challenges.</li> <li>5) The student can collaborate with fellow participants, exchanging ideas, perspectives, and insights in order to solve cybersecurity problems.</li> <li>6) The student can comprehend the intricacies of human dynamics in cybersecurity but also possess the skills to apply computational analysis in research.</li> </ol>
Recommended or required reading/tools	NA
Assessment methods	Research report for publication
Level	First, second, third or fourth year (for regular bachelor student)

Course content	<p>This course offers an introduction into analysis of cases of processes related to cyber security. As the human factor plays a crucial role in cyber security, human mental and social processes will be analysed for a wider variety of example cases in some depth and applied to analyse scenarios specifically related to cyber security. As such processes usually involve dynamics and adaptivity, the analysis approach will be computational analysis by computer simulation of adaptive dynamical systems, represented by mental and social network structures. By simulation experiments it can be analysed how certain circumstances and measures may affect the possible outcomes (e.g. ‘what-if’ analysis). During the second half of the course, the focus is on analysis of a more substantial case study concerning variations of scenarios within the field of cyber security. This will be finished by a presentation and a report with the aim of getting student products published via a conference.</p> <p><b>What will you do?</b></p> <p>Week 1 – Cybersecurity and computational analysis (Prof.dr. Peter Roelofsma), Lecture on Introduction of computational analysis by network models for dynamical systems, Getting familiar with network modelling.</p> <p>Week 2 – Designing mental and social network models, Computational analysis of a soap scenario, The role of emotions in mental processes, Computational analysis of emotions and their regulation.</p> <p>Week 3 – From mental processes to social processes, Computational analysis of opinion contagion in social networks, Using self-models to model adaptive mental and social processes, Computational analysis of plasticity in mental processes.</p> <p>Week 4 – Modeling higher orders of adaptivity in mental processes: metaplasticity, Computational analysis of metaplasticity in mental processes, Bonding by homophily in social networks, Computational analysis of bonding in a soap scenario.</p> <p>Week 5 – Modeling the use of internal mental models and organisational learning, Computational analysis of organisational learning by first-order adaptive networks, Examples of higher-order adaptivity in evolutionary processes, Computational analysis of organisational learning by second-order adaptive networks.</p> <p>Week 6,7 – Setup of the final project workshop assignment, Choosing a topic, Literature search Lecture, Formulating a scenario use case.</p> <p>Week 8,9 – Formulating a scenario use case, Designing a conceptual network picture, Working on presentation, Presenting the scenario use case and the conceptual network picture.</p>
----------------	--

<b>Managing Corporate Challenges (MCC)</b>	
Credits	6 ECTS
Code	SSMS-3T1-23
Entry requirements	Good command of English (oral and written)
Semester	2
Method	Lectures, research and exercises
Lecturer(s)	Dr Heinrich Matthee
Learning outcomes	<ol style="list-style-type: none"> <li>1) The student can identify key risks and opportunities for international business in a complex and hostile environment.</li> <li>2) The student can assess the likelihood and impact of the risks and opportunities in order to prioritize those needing attention.</li> <li>3) The student can generate different options to address the challenges.</li> <li>4) The student can evaluate options to address the challenges and their possible consequences.</li> <li>5) The student can evaluate organisational behaviour in a change situation especially when it comes to international safety and security matters in a corporate setting.</li> <li>6) The student can explain how to communicate in a change situation and thereby influence the organisation he/she is working in.</li> <li>7) The student can compare different change management models.</li> </ol>
Recommended or required reading/tools	Rice C. & Zegart A. (2018). Political risk: Facing the threat of global insecurity in the twenty-first century. (London: Weidenfeld and Nicolson)
Assessment methods	Memorandum (individual & group component) 50% group component 50% individual component
Level	First, second, third or fourth year (for regular bachelor student)
Course content	<p>International business encounters political and security factors that create risks as well as opportunities for them. This course teaches students to assess the challenges and to generate options for the company executives in managing these challenges. Such challenges also bring about organisational change, which causes stress, resulting in internal resistance. In order to achieve positive change in the behaviour of people, it is more important to make people feel differently rather than to make them think differently. This, in turn, requires innovative solutions that aid companies in overcoming obstacles.</p> <p>Hence, this course will also study different approaches as to how (corporate) environments tackle change and ensure business continuity.</p> <p><b>What will you do?</b>  Week 1 – Geopolitical shifts, business models and corporate strategies.  Week 2 – Political succession, policy changes and armed politics.</p>

Week 3 – Organized crime and insider threats.  
Week 4, 5 – Political unrest, reputation management, and NGOs.  
Week 6 – Dilemmas of political and security risk analysis.  
Week 7 – Alternative futures and anti-fragility.  
Week 8 – Political and security risk management.  
Week 9 – Change management.  
Week 10 – Organizational strategy & dynamic capabilities.

# Practical Information

## Location Main Campus

The Hague University of Applied Sciences (THUAS)  
Faculty of Public Management, Law & Safety  
Johanna Westerdijkplein 75  
2521 EN The Hague  
The Netherlands

## How to Apply & accommodation

For practical information on how to apply and also on accommodation, please see THUAS' website: <https://www.thehagueuniversity.com/programmes/other-courses/exchange-programmes/practical-information>

## Contact

If you would like more information about the exchange application procedure, deadlines, accommodation, visa/permits, bank account, health care insurance the like, please contact our International Office at: [exchange@hhs.nl](mailto:exchange@hhs.nl) / +31 (0)70 – 4458505

Enquiries about the academic information of the Safety & Security Management Studies Programme, please contact the Exchange Coordinator, Ms. Laura Díaz at [exchangeBRV@hhs.nl](mailto:exchangeBRV@hhs.nl)

## Exchange Information page

All relevant information needed to start at our SSMS programme will be posted on our Student Portal on the [Exchange Information portal page](#). The content will be posted nearer the date and exchange students will get access as soon as they have activated their THUAS student account.

Note: the exchange information page will be updated in May/June 2024.