Module number 24 - 26	**Module title** Specialised Elective Module: Security Studies (Security Studies)		
Code SES	**Semester** 4/5, 6, 7	**Number of WSH** 4	**Module offered** Changing Catalogue. Details can be found online (faculty web page).
Module coordinator Prof. Dr. Bresinsky	**Tuition type** Seminar-style tuition		**Module duration** 1 Semester
Lecturer Prof. Dr. Bresinsky	**Compulsory/Elective** Elective		**Module language** English

Access requirements

Course segment 2

Learning outcomes

On completing the module the students will have achieved the following learning outcomes on the basis of scientific methods:

Competencies:

- Understand the issues of non-traditional security challenges
- Know how to identify a non-traditional security challenge in specific domain of politics or business.
- Know how to analyze the actor, structures and processes of international security challenges
- Know how to support an analysis and intelligence cycle by creating intelligence products
- Know how to apply specific analysis procedures (e.g. Business Process Models, Scenario Technique)
- Know how to apply specific software tools (e.g. Visual Understanding Environment, Scenario Wizard, ARIS Express etc.)
- Know how to document and log results on e-learning platform
- Know how to present results to plenum and work groups
- Improve English conversation, reading and writing

The modul is concerned both with traditional and non-traditional security threats, which are no longer, stop at borders of nation states and are therefore subject of a more comprehensive approach in analysis and research.

The SES course will address these challenges by focusing on three international topics, which are highly relevant for international security. For each topic a group of students build a analysis team

Topic 1: Cyber security and their relevance for critical infrastructure. This topic is in cooperation with KPMG Cologne ‘Cyber Security’.

Topic 2: Subsahara Africa. Potential outcomes of security threats in this region. This topic is in cooperation with German Foreign Office.

Topic 3: Hybrid threat.

By using a topic as a case study, the course will address two aspects. Firstly students will learn to create a situational picture, assess the information and develop possible future scenarios of the ongoing events. Secondly students will apply methods, tools, and best practice for the analysis and the development of decision support products. The last aspect will address the processes of analysis as known in policy and business intelligence.

Students are invited to develop their own problem statements and topics for research. As the course is designed as research based learning, students are expected to prepare information and reading outside the course sessions.

Content

- Administration & Organization; Introduction
- Develop definition of security and security challenges
- Introduction into planning and analysis tools
- Definition of subject matter of interest
- Developing work plan and research design
- Work groups and plenum discussion
- Symposium

Required reading

-

Recommended reading

On Cybersecurity:

Ayala, Luis (2016): Cybersecurity Lexicon. Berkeley, CA: Apress. Available online at http://gbv.eblib.com/patron/FullRecord.aspx?p=4605485.

Beyond Cybersecurity. Protecting Your Digital Business (2015). With assistance of James M. Kaplan, Tucker Bailey, Derek O'Halloran, Alan Marcus, Chris Rezek. 1., Auflage. New York, NY: John Wiley & Sons.

Christou, George (2015): Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy. Basingstoke: Palgrave Macmillan (New Security Challenges Series). Available online at http://gbv.eblib.com/patron/FullRecord.aspx?p=4096827.

Donaldson, Scott E.; Siegel, Stanley G.; Williams, Chris K.; Aslam, Abdul (2015): Enterprise Cybersecurity. How to build a successful cyberdefense program against advanced threats. New York, NY: Apress (The expert's voice in cybersecurity). Available online at http://dx.doi.org/10.1007/978-1-4302-6083-7.

Dykstra, Josiah (2015): Essential cybersecurity science. Build, test, and evaluate secure systems. First edition. Sebastopol, CA: O'Reilly Media Inc. Available online at http://lib.myilibrary.com/detail.asp?id=878982.

Grobman, Steve; Cerra, Allison (2016): The second economy. The Race for Trust, Treasure and Time in the Cybersecurity War. Berkeley, CA: Apress. Available online at http://dx.doi.org/10.1007/978-1-4842-2229-4.

Holt, Thomas J.; Smirnova, Olga; Chua, Yi-Ting (2016): Data Thieves in Action. Examining the International Market for Stolen Personal Information. New York, s.l.: Palgrave Macmillan US (Palgrave Studies in Cybercrime and Cybersecurity). Available online at http://dx.doi.org/10.1057/978-1-137-58904-0.

Hubbard, Douglas W.; Seiersen, Richard (2016): How to Measure Anything in Cybersecurity Risk. 1. Auflage. New York, NY: John Wiley & Sons.

Kremer, Jan-Frederik; Müller, Benedikt (Eds.) (2014): Cyberspace and international relations. Theory, prospects and challenges. Heidelberg, New York, NY, Dordrecht, London, Berlin: Springer.

Lehto, Martti; Neittaanmäki, Pekka (Hg.) (2015): Cyber security: analytics, technology and automation. Cham: Springer (Intelligent Systems, Control and Automation, 78). Online available on http://dx.doi.org/10.1007/978-3-319-18302-2.

Mehan, Julie (2014): Cyberwar, Cyberterror, Cybercrime & Cyberactivism (2nd Edition). An in-depth guide to the role of standards in the cybersecurity environment. Ely: IT Governance Ltd. Available online at http://gbv.eblib.com/patron/FullRecord.aspx?p=1778762.

Nicholson, Denise (Ed.) (2016): Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA. Cham, s.l.: Springer International Publishing (Advances in Intelligent Systems and Computing, 501). Available online at http://dx.doi.org/10.1007/978-3-319-41932-9.

Shackelford, Scott J. (2014): Managing cyber attacks in international law, business, and relations. In search of cyber peace. New York, NY: Cambridge Univ. Press. Available online at http://www.loc.gov/catdir/enhancements/fy1215/2012035324-d.html.

Teaching and learning methods

Seminar-style tuition

Symposium

Group works

Digital learning and teaching techniques are applied: e-learning platform, collaboration and conference software.

Type of examination/Requirements for the award of credit points	Written essay (English) 1500 words
Other information	Max. 25 students (circa 10 IRM, circa 15 BW) Registration necessary. Details can be found online (faculty web page). Lecture Times: Will be released in the schedule and online via WebUntis. Reading of literature, scientific working style, and self-commitment to work groups is mandatory! Please download free software ‘Scenario Wizard’, ‘Aris Express’ and ‘Visual Understanding Environment’ (keyword search will lead to download page) The course will be held together with students of the study program “International Relations and Management”.

ECTS-Credits	**Workload**	**Weighting of the grade in the overall grade**
5	150 hours Contact/attendance time: 60 h Additional work: 90 h	5