<table>
<tr><td>Module number
24 - 26</td><td colspan="3">Module title
Specialised Elective Module:
Scenario Thinking Technique – Method & Development
(Scenario Thinking Technique – Method & Development)</td></tr>
<tr><td>Code
STT</td><td>Semester
4/5, 6, 7</td><td>Number of WSH
4</td><td>Module offered
Changing Catalogue.
Details can be found online (faculty web page).</td></tr>
<tr><td>Module coordinator
Prof. Dr. Bresinsky</td><td colspan="2">Tuition type
Seminar-style tuition</td><td>Module duration
1 Semester</td></tr>
<tr><td>Lecturer
Prof. Dr. Bresinsky</td><td colspan="2">Compulsory/Elective
Elective</td><td>Module language
English</td></tr>
<tr><td colspan="4">Access requirements
Course segment 2</td></tr>
<tr><td colspan="4">Learning outcomes
On completing the module the students will have achieved the following learning outcomes on the basis of scientific methods:
<u>Subject skills</u>
• Understand the requirements of scenario thinking for decision-making
• Know how to identify drivers and trends for scenario development.
<u>Method skills</u>
• Know how to use software tool to develop, create and analyze scenarios.
• Know how to document and log results on e-learning platform
<u>Social skills</u>
• Know how to present results to plenum and work groups
• Know how to collaborate with virtual teams in an international work environment.
<u>Personal skills</u>
• Improve English conversation, reading and writing</td></tr>
<tr><td colspan="4">Content
In strategic decision-making scenario thinking plays a crucial role. Good management and leadership both are based on assumptions about possible future developments. Preparing scenarios for the decision support needs a method based approach. This course aims to give students an introduction into scenario thinking and provides the opportunity to create scenarios about a real world subject matter. Student will be instructed to use a software tool and to apply critical thinking methods. Due to the fact that management in a globalized world is multinational in scope and objective, the course will be in cooperation with students of international cooperation partners of OTH Regensburg.</td></tr>
</table>

For this term it is planned to develop scenarios about Critical Infrastructures and Cybersecurity and to tackle the problem of preparedness.

- Administration & Organization; Introduction
- Introduction and understanding of subject matter
- Introduction into scenario development tool
- Developing work plan and research design
- Work groups and plenum discussion
- Symposium

Required reading

-

Recommended reading

Scenario Wizard Introduction and free download: http://www.cross-impact.de/english/CIB_e_ScW.htm

Free availiable via OTH access:

Emodi, Nnaemeka Vincent (2016): Methodology, Data, and Scenario Development. In: Nnaemeka Vincent Emodi (Hg.): Energy Policies for Sustainable Development Strategies: The Case of Nigeria. Singapore: Springer Singapore, S. 85–122. Online verfügbar unter https://doi.org/10.1007/978-981-10-0974-7_4.

Grienitz, Volker; Hausicke, Michael; Schmidt, André-Marcel (2013): Scenario development without probabilities — focusing on the most important scenario. In: European Journal of Futures Research 2 (1), S. 27. DOI: 10.1007/s40309-013-0027-0.

Gurjar, Nikhil (2017): A Forward Looking Approach to Project Management : Tools, Trends, and the Impact of Disruptive Technologies.

Pesonen, Hanna-Leena; Ekvall, Tomas; Fleischer, Günter; Huppes, Gjalt; Jahn, Christina; Klos, Zbigniew S. et al. (2000): Framework for scenario development in LCA. In: The International Journal of Life Cycle Assessment 5 (1), S. 21. DOI: 10.1007/BF02978555.

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.

Critical Infrastructure:

European Council (2008): Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available online at https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

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)

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