Friedrich Schiller Universität
Institut für Politikwissenschaft
Lehrstuhl für Internationale Beziehungen

Analyzing Cyberspace in International Relations: Cyber-War
(Pol 340), WS 2013/14
Wednesday 4-6 p.m., c.t.
Room 120

Teacher: Matthias Schulze, M.A.
Office hours (R. 446): Mittwoch 14-15 p.m. Or per request
Contact: matthias.schulze@uni-jena.de
Tel:+49 3641 945414
www.metacoon.uni-jena.de

1. Requirements

- By participating in this seminar I expect you to read all the mandatory literature and actively engage in the seminar discussion. There are 5 types of assignments in this course. To be admitted to the final exam (Hausarbeit) and thus to gain 5 ECTS points you must do **two** of the following:
    - 1) *Input-presentation* (max 10 minutes)
    - 2) *Abstract/Comment* of one of the course readings (3 pages)
    - 3) *Fact-sheet* on an individually chosen topic (including own research), (2-3 Pages)
    - 4) *Discussion Moderator*
    - 5) Do not miss more than 2 seminar sessions
- Now and then I will give you a little task or question about the Literature you should answer on Metacoon. Please do so.
- If all assignments are handed in, you are permitted to write a research paper (Hausarbeit, 15-20 pages) on a topic of your choice.

2. Assignments

2.1 Input-Presentation

- The task is to shortly introduce a topic fitting to the seminars theme and thereby to lay the foundation for further discussion. The aim is not to simply reproduce the course reading in an oral presentation. Rather you should present an argument (hypothesis) or a critique about which you elaborate in your presentation.
- Make bold and interesting claims and give arguments for your reasoning (roter Faden).
- There should not be more than two people giving one presentation.
- 10 minutes max!
- Conduct own research. Add interesting sources, images and movie-clips!
- Use visual material (ppt) only where it is necessary! If you do so, work with it, don't just let it "explain itself".
- Prepare a short summary (Thesenpapier) of your argumentation for the audience on which you outline your argument and literature!
- If you sign in for a presentation and get sick before, I expect a short info per mail one day in advance!

2.2 Abstract

- The task is to discuss one of the course readings in detail. There should be two parts included: 1) a short summary of the main line of argumentation and 2) a critical discussion/reflection of it. In other words: What is the author saying? What is wrong with it?
- Please write min. 3 pages (Times New Roman 12pt, 1 1/2 spacing).
- If you point to other arguments/literature, please add a short literature list as well.

2.3 Fact-Sheet

- A Fact-sheet should some up relevant data (statistics, maps, bullet-points) on a topic and thereby presenting key elements of a topic on a short space. It has often two columns and is divided into short chapters.
- The aim is to provide a quick and easy accessible introduction to a topic. Fact-sheets are often used in politics to prepare politicians for meetings.
- A fact sheet is not a reproduction of the course reading. You are required to make a small research effort (mostly Google Search) and add additional Information and Data.
- An example could be a short overview of the recent cyber-crime incidents in the US. There is an example of a fact sheet on Metacoon.

2.4 Discussion-Moderator

- Become teacher for one session! The aim is that you start and moderate the group discussion in a session.
- You should be well prepared for this (mandatory and optional reading). While reading the literature you should extract discussion questions or bold claims out of the text. Your aim is to activate your fellow students to engage in the discussion.
- This is sometimes called "expert-groups" as well.
- If there is a oral presentation in this session, you should coordinate yourself with the speaker.

2.5 Do not miss more than 2 sessions

- General attendance is not mandatory in this seminar! However, being present and engage in the discussion all the time is an easy way to do one of the two tasks in this course.
- If you choose this assignment-option, please notify the teacher because I must make sure, that you are indeed present during all the sessions (therefore registering your attendance).
- If you have chosen this option and miss the seminar more than 2 times (without a certificate of a public health officer), you will not be allowed to write the final exam. However, you can hand in another assignment (fact sheet, abstract) as compensation.

2.6 Final Paper (Hausarbeit)

- 15-20 pages of text, 12 pt Times New Roman, 1 1/2 spacing
- You should prepare a "research proposal" (Exposé) beforehand. We are going to discuss this proposal during one of our sessions. It should contain a formulated research questions, a theoretical perspective, a hypothesis or assumption about the case and a very first index (Gliederung).
- Language: English or German.
- The deadline for the final paper will be **10.03.2014.**
- The deadline for the second attempt will be announced later during the seminar. Note, if you choose to hand in your paper for the 2nd attempt, you will have to choose a completely new topic.

3. General Information

- You should choose which of the two assignment options you want to do during the first three weeks of the seminar. It will not be possible to change it later on.
- All the assignments are tied to a session and must be handed in 1 day in advance.
- We will use the e-learning platform Metacoon. There you can find the reading materials, topics and tasks and general information about the course. It is mandatory for all (including Erasmus & foreign students), that you register there! As a foreign student you can register as "externer Nutzer", using the form on the right hand side of the screen @ https://metacoon1.rz.uni-jena.de/
    - On metacoon I will give you additional information (interesting links), please check them out.
    - Feel free to share your ideas or interesting links on that platform. Feel free to use the forum for discussions and your own research projects (finding sources, asking for ideas, sharing insights etc.).
    - If you have any questions about procedures and administrating stuff (like deadlines or exam formalities), please use the forum for questions of general interest instead of writing me an email.
    - I will use Metacoon for feedback and evaluation as well. Now and than I will create some polls which you should answer to. Feel free to do the same if you are unsatisfied with the course.
    - Upload your work (abstracts, fact sheets, research proposals to the "Abgabe Aufgaben" Section. You can create a new entry in the upper right hand corner. Please attach PDF files.
- The seminar is held in English and so should be the discussions and assignments. Don't be afraid about speaking English for the first time in a Seminar. I will not evaluate your English skills and for me it is also the first time ;)
- However, some of the literature will be in German.
- Academic honesty: final papers will be checked for plagiarism. A plagiarism incident will be added to your student documents.
- Deadlines: please hand your stuff in on time! Otherwise I simply might not accept it.

4. Course Goals

The primary goal of this course is to increase your understanding what cyberwar actually is, and more importantly, what it is not. The media is full of talk about cyber attacks and cyber war but those to concepts are not the same and must be carefully distinguished. Not every incident is an attack and not every attack represents an act of war. Furthermore, it is has serious implications to view a cyber attack as an act oft war. Therefore the aim is to equip you with a proper toolkit of questions to analyze occurring incidents in the future.

Date	Topic	Mandatory and *optional reading*
16.10.13	**1. Introduction**	
23.10.13	**2. New Technology and Society**	- Gaycken, S. (2010). Cyberwar: Das Internet als Kriegsschauplatz (1 ed.). Open Source Press. Kap 1 - Fritsch, S. (2006). Technology as a Source of Global Turbulence? In E. F. Halpin, P. Trevorrow, D. Webb, & S. Wright (Eds.), Cyberwar, Netwar and the Revolution in Military Affairs. Palgrave Macmillan. - *Herrera, G. L. (2003). Technology and International Systems. Millennium - Journal of International Studies, 32(3), 559-593.*
30.10.13	**3. Problem Area Cyber Security**	- Hansel, M. (2013). Internationale Beziehungen im Cyberspace: Macht, Institutionen und Wahrnehmung (Globale Gesellschaft und internationale Beziehungen) (German Edition) (2013 ed.). Springer VS. Chapter 2. - Latham, R. (2003). Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security (First Edition ed.). New Press,Chapter 1 - *Latham, R. (2003). Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security (First Edition ed.). New Press,Chapter 2*
06.11.13	**4. Core Concepts and Definitions** - suitable for fact sheets and research paper	- Dunn, C., Myriam. (2010). Cyberwar. In G. Kassimeris & J. Buckley (Eds.), The Ashgate Research Companion to Modern Warfare. Ashgate. - Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation, Chapter 2. - *Cornish, Paul u.a., 2010, On Cyber Warfare, Chapter 1 & 2.*
13.11.13	**5. Concepts 2**	- Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation, Chapter 3. - Liff, A. P. (2012). Cyberwar: A New Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, 35(3), 401-428. - *Schreier, Fred ,2012, On Cyberwarfare, Geneva Centre for the Democratic Control of Armed Forces* - *Baker, Stewart,Waterman, Shaun,Ivanov, George 2010. In the crossfire, Critical infrastructure in the age of cyberwar. McAffee Report*

Date	Topic	Mandatory and *optional reading*
20.11.13	**6. Law of Cyberwar?** Debate: Does Cyberwar fit with International law?	- Kelsey, J. T. (2008). Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. Michigan Law Review, 106(7), 1427-1451. - Darnton, G. (2006). Information Warfare and Laws of War. In E. F. Halpin, P. Trevorrow, D. Webb, & S. Wright (Eds.), Cyberwar, Netwar and the Revolution in Military Affairs (part 1). Palgrave Macmillan. - *Schumacher, S. (2012). Vom Cyber-Kriege. Gibt es einen Krieg im Internet? Magdeburger Journal zur Sicherheitsforschung, 2, 285-307.* - *Melzer, N. Cyberwarfare and International Law. UNDIR Resources, 2011.*
27.11.13	**7. Theorizing Cyberspace** - Presentations possible in this complex	- Eriksson, Giacomello, 2007,Introduction; Closing the gap between international relations theory and studies of digital-age security - Hansel, M. (2013). Internationale Beziehungen im Cyberspace: Macht, Institutionen und Wahrnehmung (Globale Gesellschaft und internationale Beziehungen) (German Edition) (2013 ed.). Springer VS., Chapter 4 & 5.
04.12.13	**8. A a theory of cyberspace?**	- Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562. - Fung, A., Russon, G., Hollie, & Shkabatur, J. (2013). Six Models for the Internet + Politics. Int Stud Rev, 15(1), 30-47. - Nye, Joseph S. (2010). Cyber Power, Cambridge, Harvard Kennedy School, Belfer Center for Science
11.12.13	**9. Constructitivsm and Securitization**	- Hansen, L., & Helen, N. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, 1155-1175. - Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (Css Studies in Security and International Relations) (1 ed.). Routledge., Chapter 2 - *Lawson, S. (2011). Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History. Mecatus Center George Mason University, Working Paper 11-01.* - *Cavelty, M. D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (Css Studies in Security and International Relations) (1 ed.). Routledge., Chapter 1*
18.12.13	**10. Risk & Security Studies**	- Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. Space and Culture, 15(2), 110-123. - Bendrath, R. (2001). The Cyberwar Debate. Perception and Politics in U.S. Critical Infrastructure Protection. Information and Security: An International Journal, 7, 80-103. - *Aradau, C., Lobo-Guerrero, L., & Van, M., R. (2008). Security, Technologies of Risk, and the Political: Guest Editors' Introduction. Security Dialogue, 39(2-3), 147-154.*

Date	Topic	Mandatory and *optional reading*
08.01.14	**11. Control of Cyberspace?: Militarisation and Surveillance** - Debate: Who should Control the Internet?	- Deibert, R. J., & Rohozinski, R. (2010). Liberation vs. Control: The Future of Cyberspace. Journal of Democracy, 21(4), 43-47. - Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. Strategic Studies Quarterly, Spring 2011, 32-61. - Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly, 54, 381-401. - A declaration if Independence of Cyberspace: https://projects.eff.org/~barlow/Declaration-Final.html
15.01.14	**12. Cases: National Motivations to Cyberwar** - Poll: Which country should we focus on? - Fact sheets & presentations useful	- Billo 2004, Cyber Warfare. An Analysis of the means and motivations of selected nation states - Giacomello, G. (2005). National Governments and Control of the Internet. - Kap 3 (What democracies do), - Kap 4 (US), - Kap 5(DE) - Gaycken, S. (2010). Cyberwar: Das Internet als Kriegsschauplatz (1 ed.). Open Source Press. Kap 4 - Wu, C. (2006). An Overview of the Research and Development of Information Warfare in China. In E. F. Halpin, P. Trevorrow, D. Webb, & S. Wright (Eds.), Information Warfare and Laws of War (Vol. Cyberwar, Netwar and the Revolution in Military Affairs (part 1)). Palgrave Macmillan. - Carr, J. (2009). Inside Cyber Warfare: Mapping the Cyber Underworld (1 ed.). O'Reilly Media. Kap 11_ Cyber Military Doctrine China and Russia - Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23-40. - https://opennet.net/research/profiles
22.01.14	13. Cases 2 & Exposés	
29.01.14	**14. Hacktivism and the Individual**	- Hansel, M. (2013). Internationale Beziehungen im Cyberspace: Macht, Institutionen und Wahrnehmung (Globale Gesellschaft und internationale Beziehungen) (German Edition) (2013 ed.). Springer VS. Chapter 3. - *Carr, J. (2009). Inside Cyber Warfare: Mapping the Cyber Underworld (1 ed.). O'Reilly Media., Kap 6: Non-State Hackers and the Social Web* - Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. Journal of Strategic Studies, 35(5), 689-711.
05.02.14	**15. Final Session**	- summing up & evaluation