Online Surveillance, Privacy, and Cybersecurity

Fall 2017
Copenhagen
3 Credits

Major Disciplines: Human Rights, International Relations, Political Science

Faculty: Ulrik Graff Rasmussen, ulrikgraff@hotmail.com
Program Director: Iben de Neergaard, Vestergade 10 A23 idn@dis.dk
Assistant Program Director: Nya Oxfeldt Jensen, Vestergade 10 A23, nj@dis.dk
Program Assistant: Jenny Han, Vestergade 10 A23, yh@dis.dk

Course Description
The world is connected like never before. Government satellites, nuclear submarines and power plants, your bank details, medical records, and holiday pictures are all online and vulnerable. What does this connectivity entail for the future of warfare and for the future of privacy? This course is a study of the applicability of and challenges to international law in relation to harmful cyber activities perpetrated by states and non-state groups alike. The course furthermore explores issues in relation to personal privacy as they pertain to online surveillance by government agencies, but also to the immense amount of big data and personal information we voluntarily "give away" through Facebook, cell phone logs, etc. Who are the stakeholders in these new security scenarios and how does international law apply?

Course Objectives:
This course aims to provide you with a thorough understanding of the legal aspects of conflict and espionage in cyber space. It is also the aim to provide you with an introduction to the technical aspects of cyber conflict. Finally, we will explore privacy issues in relation to surveillance and the increasing amount of information we voluntarily make available in cyber space.

The objectives of this course are to enable you to:

• Gain an understanding of how international law applies in cyber space through selected readings and class discussions.
• Identify and explain main principles of human rights law and international humanitarian law applicable to cyberspace.
• Gain an idea of the possibilities in cyber space and separate facts from myths about cyber conflict through selected readings and class discussions,
• Identify and discuss the main issues related to personal privacy and security, and whether those two are contrarian concepts.
• Examine and conduct basic analyses of contemporary cases while applying the main principles of international law. It is the aim that students by the end of the course will be able to analyze a cyber event through a prism of international law and separate legal aspects from political considerations.
• Increase your ability to write analytical papers using legal argumentation supported by a political perspective.

Prerequisites:
Knowledge of political science or international law. No knowledge of computer science is necessary.

This syllabus is subject to change.
Course Instructor:

Ulrik Graff Rasmussen

E-mail:

Evaluation and Assessment:
- Two research papers.
- Participation (preparation for class, active participation during discussions in class with quality inputs rather than quantity – based an analysis and reflection).
- Presentation of an analysis of a cyber event.

Course Evaluation:
- Research papers 70% (1x20% and 1x50%)
- Participation and attendance 15%
- Presentation 15%

Main Themes:
This course will have three main themes.
- **Technical.** The first part of the course will establish the framework for the work during the semester. We will discuss how international law applies to cyber space and which are the primary actors in cyber space.
- **Major issues.** The second part of the course will be a case study of some of the major issues in cyber space. We will discuss privacy issues and human rights in cyberspace, we will discuss cyber war and concepts of sovereignty in a seemingly borderless space.
- **Contemporary issues.** The course will include with a series of smaller case studies and selected topics in order to further examine the practical issues relating to the development of international law norms and their applicability to cyberspace. We will look at different cyber incidents and how states have reacted to them.

Literature:
Katharina Ziolkowski (ed.) Peacetime Regime for State Activities in Cyberspace, CCDCOE 2013


Michael N. Smith (ed,) Tallin Manual on the International Law applicable to Cyber Warfare, Prepared by the international group of experts at the invitation of the CCDCOE 2013

Selected readings from open source media, academic journals, Human Rights Instruments, Security Council resolutions, court cases, legal opinions and textbooks relevant to the individual topics.

Note: Some of the readings might be subject to change during the course, but you will receive any new readings in due time to prepare for class.

**Academic Honesty:** DIS expects that students abide by the highest standards of intellectual honesty in all academic work. DIS assumes that all students do their own work and credit all work or thought This syllabus is subject to change.
taken from others. Academic dishonesty will result in a final course grade of “F” and can result in
dismissal. The students’ home universities will be notified. DIS reserves the right to request that
written student assignments be turned in electronic form for submission to plagiarism detection
software. See the Academic Handbook for more information, or ask your instructor if you have
questions.

**Late Paper Policy:** Late papers will not be accepted. It is possible to obtain a deadline extension if it
is agreed upon well in advance.

**Attendance:** You are expected to attend all DIS classes when scheduled. If you miss multiple classes,
the Director of Teaching and Learning, and the Director of Student Affairs will be notified and they will
follow-up with you to make sure that all is well. Absences will jeopardize your grade and your standing
at DIS. Allowances will be made in cases of illness, but in the case of multiple absences, you will need
to provide a doctor’s note.

**Disability and Resource Statement:** Any student who has a need for accommodation based on the
impact of a disability should contact Sean Green (sgr@dis.dk) to coordinate this. In order to receive
accommodations, students should inform the instructor of approved DIS accommodations within the
first two weeks of classes.

This syllabus is subject to change.
Course Schedule (subject to change)

<table>
<thead>
<tr>
<th>Class No</th>
<th>Date</th>
<th>Subject &amp; Objectives</th>
<th>Readings</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td><strong>Introduction</strong>&lt;br&gt;Objectives:&lt;br&gt;• Students are introduced to instructors including their teaching methodology.&lt;br&gt;• The semester program is explained to the students.&lt;br&gt;• Grading and academic requirements for papers are explained to the students.</td>
<td>• Class objectives&lt;br&gt;• Semester program&lt;br&gt;• <a href="http://gizmodo.com/5912383/how-to-destroy-the-internet">http://gizmodo.com/5912383/how-to-destroy-the-internet</a></td>
<td>UG</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td><strong>What is cyber space and who are the main actors in it?</strong>&lt;br&gt;Objectives:&lt;br&gt;• Students are introduced to the concept of cyber space and the actors</td>
<td>Peacetime Regime for State activities in Cyberspace, Christian Czosseck&lt;br&gt;State Actors and their Proxies in Cyberspace, page 1-30</td>
<td>UG</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Students get an understanding of the special position of states in international law</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Students get a understanding of the interplay of different actors and their status under international law</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 3 | **Main actors continued non-state actors**  
**Objectives:**  
- Students are introduced to the main non-state actors in cyberspace and how to define non-state actors like APT's, havtivist, black hat hackers etc.  
- Students are introduced to the essential aspect of attribution for cyber-activities | NSA, UNIT 8200, PLA UNIT 61398, Bureau 121, Anonymous, Syrian electronic army, Cyber kalifat  
Attribution and direct participation | UG |

*This syllabus is subject to change.*
| 4 | Does international law apply in cyberspace? **Objectives:** Students are introduced to the concept of international legal regimes in cyberspace  
- Students are able to identify the legal regimes relevant for cyberspace. | UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174, 22 July 2015, page 1-14  
NATO Wales Summit declaration on legal rules applicable to cyberspace | UG |
|---|---|---|---|
| 5 | How does international law apply in cyberspace? **Objectives:** Students are introduced legal regimes applicable in cyberspace mainly IHL and HR  
- Get an understanding of how cyber differ from application in real world and how it does not  
- Its new – it is not unique | Peacetime Regime for State activities in Cyberspace, Katharina Ziolkowski General Principles of International Law as Applicable in Cyberspace, 135-188 | UG |
| 6 | **Human Rights in cyberspace**  
**Objectives:**  
- Students gain an understanding of the scope of human rights.  
- Students are able to identify non-derogable rights. | **Objectives:**  
- European Convention of Human Rights article 8  
- Declaration on the protection of all persons from being subjected to torture and other cruel, inhuman or degrading treatment or punishment, 1975.  
- Peacetime Regime for State activities in Cyberspace, Dinah PoKempner, Cyberspace and State Obligations in the Area of Human Rights, page 239-260 | UG |
- See synopsis on “blackboard”  
- What is the status of the indicted Chinese citizens  
- Are their actions attributable to the Chinese government? | UG |
| 7 | **1st research paper**  
1000 words – 20%  
**Read** [https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf](https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf)  
- See synopsis on “blackboard”  
- What is the status of the indicted Chinese citizens  
- Are their actions attributable to the Chinese government? | UG |
| 8 | **Human Rights case – mass surveillance and security.**  
**Edward Snowden – Hero or villain.**  
**Objectives:**  
Students can differ between myth and facts on the topic of mass surveillance and how HR obligations impact states ability to conduct mass surveillance | **Objectives:**  
- Do an open source search on yourself  
- Think about how you communicate and what data you give away.  
- Look up PRISM  
- Look up metadata  
- We will discuss whether you are – or should be – worried about the alleged mass surveillance. | UG |
<table>
<thead>
<tr>
<th></th>
<th>Draft Syllabus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>We discuss the role of whistleblowers in state service</td>
</tr>
</tbody>
</table>
| 9 | **State Sovereignty in Cyberspace**  
**Objectives:**  
- Students understand how the concept of Sovereignty applies in cyberspace  
- Peacetime Regime for State activities in Cyberspace, Benedikt Pirker: Territorial Sovereignty and Integrity and the Challenges of Cyberspace, page 189 - 216  
- Tallinn Manual page 15-41 (rule 1-9) | UG |
| 10 | **Espionage legal in cyberspace**  
| 11 | **Use of force and self-defence in cyberspace**  
- UN Charter art. 2(4) and 51  
- Nicaragua judgment art.  
- Tallinn Manual page 42-68 (rule 10-17) | UG |
| 12 | **Cyber-war?**  
**Objectives:**  
- Students are introduced to the basic concepts of *jus ad bellum* and *jus in bello*.  
- Students know when IHL applies to a situation/conflict in cyberspace.  
- International Law studies 89th, 2013, Yoram Dinstein Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference  
- Tallinn manual, page 75-91 (rule 20-23)  
- [https://www.youtube.com/watch?v=5Ujlqwf9f yk](https://www.youtube.com/watch?v=5Ujlqwf9f yk) | UG |

*This syllabus is subject to change.*
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Targeting in cyberspace</td>
<td>Tallin manual 95-170 Distinction, necessity, precautions, proportionality AP art. 47-57..</td>
</tr>
<tr>
<td></td>
<td>Objectives:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Students get an understanding of how targeting works in military operation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• And how targeting works in cyberspace is different from classic kinetic targeting</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Topic TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>15</td>
<td>Topic TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>16</td>
<td>Group presentation</td>
<td>Estonia 2007&lt;br&gt;Georgia 2008&lt;br&gt;Israel attack on Syria&lt;br&gt;Stuxnet&lt;br&gt;Sony hack&lt;br&gt;Ukranian powerout</td>
</tr>
<tr>
<td>17</td>
<td>US vs PLA3 and Objectives: Students are able to apply the legal principles in analyzing the US DOJ vs 3 chinese APT members</td>
<td>Case material</td>
</tr>
<tr>
<td>18</td>
<td>The internet of things and emerging threats Objectives: Students are able to apply the legal principles in analyzing the future of the internet and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Hacking of cars, etc.</td>
<td></td>
</tr>
</tbody>
</table>

This syllabus is subject to change.
<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Topic TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>
| 20   | Cyberarmageddon and how the world ended | Taking some of the doomsday predictions into account the class looks at legal and practical implications of cyberarmageddon.  
- NSA director cyber Pearl Harbor  
| 21   | Topic TBD | TBD |
| 22   | Contemporary Case  
Objective: Students will get a chance to unpack a current case both in preparation for the last paper but also to get a chance to see their academic method at work. | TBD |
| 23   | Conclusion  
Objectives: Instructors will follow up on remaining questions and issues. | TBD |

This syllabus is subject to change.
<table>
<thead>
<tr>
<th>Free assignment</th>
<th>Instructors will give individual guidance (within reason)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 2000 words.</td>
<td>Hand in paper.</td>
</tr>
<tr>
<td>• Relation to</td>
<td></td>
</tr>
<tr>
<td>course curriculum.</td>
<td></td>
</tr>
<tr>
<td>Must contain</td>
<td></td>
</tr>
<tr>
<td>legal analysis.</td>
<td></td>
</tr>
</tbody>
</table>

This syllabus is subject to change.

Online Surveillance, Privacy, and Cybersecurity | DIS