2.1 Course Outline

<table>
<thead>
<tr>
<th>Course Outline</th>
<th>Lectures</th>
<th>Seminars</th>
<th>Homework</th>
<th>Academic hours per topic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topic 1. Introduction to the course. Political implications of Internet technologies, Internet Governance and regulation of Cyberspace</strong></td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Nov. 8 16.00-17.20 Lecture 1.1. Internet as a subject of study in political studies: technological, legal and organizational aspects. Overview of the history of Internet technologies and their political implications. – Mr. Mikhail V. Yakushev</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Nov. 8 17.30-18.50 Lecture 1.2. Internet Governance: global, regional, national layers. Principle of multi-stakeholderism. Global and regional organizations of the Internet Governance. – Mr. Mikhail V. Yakushev</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Nov. 15 16.00-17.20 Seminar 1.1. National control over Cyberspace: may it be efficient? If yes – how? If not – why? – Mr. Mikhail V. Yakushev</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Nov. 15 17.30-18.50 Lecture 1.3. Actual and perspective problems of the Internet Governance and regulation of Cyberspace. Identification in Cyberspace. Trust and Internet technologies. – Mr. Mikhail V. Yakushev</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td><strong>Topic 2. Cyberspace and ICTs in the international security agenda: international cooperation and regulation of cyberspace</strong></td>
<td>4</td>
<td>4</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Nov. 22 16.00-17.20 Lecture 2.1. Cyber space as a new strategic domain and factor in international politics and diplomacy. Turning points and major incidents. Key concepts and terms. Russia-US cooperation and conflicts in the cyber domain. – Dr. Elena V. Chernenko</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
Nov. 22
17.30-18.50
Lecture 2.2. Cyber security vs non-proliferation and arms control: similarities and differences. Cyber diplomacy at the UN GGE, UN GA, OSCE, SCO and other multilateral platforms. Private, non-governmental initiatives and governmental initiatives aimed at establishing norms of responsible behavior of states in cyber space. The Tallinn manuals and the applicability of existing humanitarian law to cyber conflicts. – Dr. Elena V. Chernenko

Nov. 29
16.00-17.20
Seminar 3.1. US and Russian strategic documents and approaches in the cyber security field. Similarities and division lines. Deterrence as a new military concept for cyber space. – Dr. Elena V. Chernenko

Nov. 29
17.30-18.50
Seminar 3.2. Surveillance and espionage in the cyber space. Practical and legal aspects. The Dark Web as a risk factor for non-proliferation efforts. – Dr. Elena V. Chernenko

Dec. 13
16.00-17.20
Final Test

Total:

TOPIC 1. INTRODUCTION TO THE COURSE. POLITICAL IMPLICATIONS OF INTERNET TECHNOLOGIES, INTERNET GOVERNANCE AND REGULATION OF CYBERSPACE

November 8, Friday. 16.00-17.20

Lecture 1.1. Internet as a subject of study in political studies: technological, legal and organizational aspects. Overview of the history of Internet technologies and their political implications. Mr. Mikhail V. Yakushev

November 8, Friday. 17.30-18.50

Lecture 1.2. Internet Governance: global, regional, national layers. Principle of multi-stakeholderism. Global and regional organizations of the
Internet Governance.

Summary: The lectures will cover technological, legal and organizational aspects of the Internet in political studies. The lecturer will give an overview of different levels of the Internet Governance and tell about its main players.

Essential Readings
- J.Kurbalja. An Introduction to Internet Governance
- Report of the Working Group on the Internet Governance (Chateau de Bossey)

General Readings
- History of Internet Governance by Wolfgang Kleinwaechter
- Oskar H.Gandy Jr. Exploring Identity and Identification in Cyberspace
- Max Seddon and Henry Foy. Russian technology: can the Kremlin control the Internet?

November 15, Friday. 16.00-17.20

Seminar 1.1. National control over Cyberspace: may it be efficient? If yes – how? If not – why?

Summary:
Presentation 1: National regulation of cyberspace (Russia, U.S., UK, France, China etc.): current status, pro’s and contra’s

Presentation 2: Who should ‘regulate’ the global Internet? Best candidates are welcome.

Presentation 3: De-fragmentation of the global Cyberspace (‘Balkanization’ of the Internet): inevitable trend or wrong way (dead end)?

Presentation 4: Is there anything else important in Cyberspace, besides Cybersecurity? Your version(s).

November 15, Friday. 17.30-18.50

Lecture 1.3. Actual and perspective problems of the Internet Governance and regulation of Cyberspace. Identification in Cyberspace. Trust and Internet technologies.

Summary:

Essential Readings
- J.Kurbalja. An Introduction to Internet Governance
- Report of the Working Group on the Internet Governance (Chateau de Bossey)

General Readings
### History of Internet Governance

- By Wolfgang Kleinwaechter

### Exploring Identity and Identification in Cyberspace

- By Oskar H. Gandy Jr.

### Russian technology: can the Kremlin control the Internet?

- By Max Seddon and Henry Foy.

### TOPIC 2. CYBERSPACE AND ICTS IN THE INTERNATIONAL SECURITY AGENDA: INTERNATIONAL COOPERATION AND REGULATION OF CYBERSPACE.

#### November 22, Friday. 16.00-17.20

**Lecture 2.1.** Cyber space as a new strategic domain and factor in international politics and diplomacy. Turning points and major incidents. Key concepts and terms. Russia-US cooperation and conflicts in the cyber domain.

<table>
<thead>
<tr>
<th>Dr. Elena V. Chernenko</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary: The lecture will cover aspects of cyber security as a new topic in international relations studies. The lecturer will give an overview of key approaches to cyber security among the most important international players, outline terminology differences and main points of conflict.</td>
</tr>
</tbody>
</table>

#### Essential Readings

- **Suggestions on Russia-U.S. Cooperation in Cybersecurity** by the Russian International Affairs Council (RIAC) and the EastWest Institute (EWI)

- Thomas Remington, Chris Spirito, Elena Chernenko, Oleg Demidov, and Vitaly Kabernik «Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity»

#### General Readings


- Smeets, M. "There Are Too Many Red Lines in Cyberspace", Lawfare

- **A cyber revolt in the making**, Valdai paper, Julien Nocetti, Elena Chernenko

#### November 22, Friday. 17.30-18.50

**Lecture 2.1.** Cyber security vs non-proliferation and arms control: similarities and differences. Cyber diplomacy at the UN GGE, UN GA, OSCE, SCO and other multilateral platforms. Private, non-governmental initiatives and governmental initiatives aimed at establishing norms of responsible behavior of states in cyber space. The Tallinn manuals and the applicability of existing humanitarian law to cyber conflicts.

<table>
<thead>
<tr>
<th>Dr. Elena V. Chernenko</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary: The lecturer will give an overview of the current proposals of the creation of norms of responsible behavior of states in cyber space and outline the main differences between global players that prevent them from adopting such regulation as it was the case with...</td>
</tr>
</tbody>
</table>
nonproliferation.

Essential Readings

- Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
- The Paris Call for Trust and Security in Cyber Space

General Readings

- Global Cyber Security Norms: A Proliferation Problem?
- Discussing state behaviour in cyberspace: What should we expect?
- International Cyber Norms. Legal, Policy & Industry Perspectives
- UN GGE on Cybersecurity: The End of an Era?, The Diplomat
- The need for a Digital Geneva Convention. Brad Smith, President and Chief Legal Officer Microsoft
- The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?
- Tallinn Paper: The Role of Offensive Cyber Operations in NATO’s Collective Defence, CCD COE

TOPIC 3. MILITARY AND STRATEGIC USE OF CYBER SPACE AND ITS IMPACT ON GLOBAL SECURITY AND STRATEGIC STABILITY.

November 29, Friday. 16.00-17.20

Seminar 3.1. US and Russian strategic documents and approaches in the cyber security field. Similarities and division lines. Deterrence as a new military concept for cyber space

Dr. Elena V. Chernenko

Summary:

Presentation 1: US strategic documents in the cyber field (US national cyber strategy and the DoD cyber strategy).
Presentation 2: Russian strategic documents in the cyber field (Ministry of defense, MFA, Kremlin).
Presentation 3: Deterrence as a new military concept for cyber space.
Presentation 4: Case studies of cyber-attacks on state-to-state level.

Essential Readings
• US National Cyber Strategy

• Dod Cyber Strategy

• Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве/CONCEPTUAL VIEWS ON THE ACTIVITIES OF THE ARMED FORCES OF THE RUSSIAN FEDERATION IN INFORMATION SPACE

• Doctrine of Information Security of the Russian Federation

General Readings

• Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Fundamentals of the State Policy in the field of international information security for the period to 2020

• Taddeo, M. "Deterrence and Norms to Foster Stability in Cyberspace", Philosophy & Technology, 31: 323-329

• Henry Farrell, «The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine»

• Deterrence and Dissuasion in Cyberspace, Joseph S. Nye Jr., 2017

• The Role of the U.S. Military in Cyberspace, Center for Strategic and International Studies, Friday, October 9, 2015

• Offense-defense theory analysis of Russian cyber capability. Medvedev, Sergei A., 2015-03


• Moscow's cyber-defense. How the Russian government plans to protect the country from the coming cyberwar, Meduza, 19 July 2017

November 29, Friday. 17.30-18.50

Seminar 3.2. Surveillance and espionage in the cyber space. Practical and legal aspects. The Dark Web as a risk factor for nonproliferation efforts. Dr. Elena V. Chernenko

Summary:
Presentation 1: The Snowden Files and what we know about US cyber surveillance and espionage.
Presentation 2: Russian surveillance and espionage capabilities.
Presentation 3: Chinese surveillance and espionage capabilities.
Presentation 4: The Dark Net (from the angle of global security issues).

**General readings**
- Permanent Record. Edward Snowden, 2019

**Movies**
- Snowden (2016)
- Zero Days (2016)
- Who am I (2014)

**December 13, Friday. 16.00-17.20**

<table>
<thead>
<tr>
<th>Final Test</th>
<th>Dr. Elena V. Chernenko</th>
</tr>
</thead>
</table>

**Examples of questions**

1. **The Stuxnet computer virus was used against which Iranian Atomic program site?**
   a. Not-yet-completed heavy-water research reactor at Arak
   b. Uranium enrichment plant at Natanz
   c. Uranium enrichment plant at Fordow
   d. Bushehr Nuclear Power Plant

2. **Name at least two things Edward Snowden revealed**