MGIMO University
School of Government and International Affairs

Syllabus approved
Dean, The MGIMO School of Government and International Affairs
Mikhail Troitskiy
« » 2019

ICT and Cybersecurity

Undergraduate Course Syllabus

Instructor
Oleg I. Shakirov

This syllabus is designed in accordance with the MGIMO Educational Standard for the Bachelor Program in International Affairs.

Author_____ O.I. Shakirov

Director MGIMO Library_____M.V. Reshetnikova

PART 1:
INSTRUCTOR INFORMATION, COURSE DESCRIPTION AND TEACHING METHODS

1.1 General information

- Full course title: Information and Communications Technology (ICT) and Cybersecurity
- Type of course: Mandatory
- Level of course B.A.
- Year of study: 4th
- Number of ECTS credits allocated: 4
- Name of lecturer(s) and contact details:
  Oleg Shakirov, Consultant, PIR Center
  E-mail: shakirov@pircenter.org

1.2 Course aims and learning outcomes

Aims

This course aims to introduce students to information / cyber security and develop the understanding of the transformative effect of Information and Communications Technologies (ICT) on international relations.

It is designed for students seeking to learn about international politics in the prism of new technologies, the role ICT play in state' domestic and foreign policies with a particular emphasis made on diplomacy and security domains. The course will should serve as a solid foundation for students wishing to further study or engage in research in this field.

Learning outcomes

After completing this course students should be able:

- To understand basic concepts of information security needed to build awareness of the field and to navigate professional literature;
- To place technical issues related to cyberspace into a global context, to assess their political implications and to get a grasp of problems that are currently discussed;
- To analyze national and international policy documents, agreements and reports related to the field using reliable sources;
- To articulate and explain positions and issues at stake regarding key debates in the international information / cyber security field;
- To assess strengths and weaknesses of efforts to develop international rules for cyberspace;
- To do oral presentations on subjects related to ICT & cyber security.

1.3 Course requirements and grading

Format

This course is a combination of lectures and seminars taking nine weeks. Each class starts with a lecture on the week's main topic presented by the lecturer. The lecture is followed by a seminar featuring presentations by students or groups of students on the assigned topics. Presenters are expected to prepare in advance and communicate with the lecturer if necessary and to use visual materials when appropriate. Students will take three in-class written tests focused on the topics of several lectures and aimed to assess their understanding of key issues and knowledge of reading materials. Students will be notified about the results of these tests within 7-10 days.

Attendance of the classes is required and contributes to the overall grading

Reading
Reading of assigned materials and being prepared to engage in class discussions is required, reading supplementary materials is commended. Most readings are available online and accessing them should not be an issue. Students are encouraged to do their own research and use additional materials. Participation in class has an impact on grading and is crucial for effective learning. Students are also expected to stay up to day with current news related to ICT and cyber security and are encouraged to present things they found out about in the beginning of each class.

Grading
The final grade is calculated as follows:

- Class attendance – 15%;
- Class participation and seminar presentation – 25%;
- Three in-class written tests – 60% (20% each).

Points from various assignments will be converted to a letter grade ranging from A (exemplary) to F (failure).

Academic integrity
Students should be committed to academic integrity and honesty. Cheating in any form is unacceptable, which includes but is not limited to plagiarism, i.e. using someone else's work without proper citation, fabrication of information, taking credit for work done by others.

PART 2:
WEEKLY SCHEDULE & READINGS

2.1 Types of work

Types of work	Academic hours
Total	**76**
Total for lectures, seminars and written tests	***36***
Lectures (and tests)	18
Seminars	18
Homework	***40***
Course Assessment	Attendance, participation, three in-class written tests, one seminar presentation

2.2. Course content and readings by topic

Resources
Students are encouraged to educate themselves on things related to information and communications technologies and cyber / information security. Below is an advisory list or resources that can be used in addition to specific reading items assigned:

- There are multiple guides and thesaurus on information security, such as Kaspersky Lab IT Encyclopedia or Sophos Threatsaurus;
- In the end on 2018, the United Nations Institute for Disarmament Research (UNIDIR) launched its Cyber Policy Portal. It is a useful interactive tool that you can use to search for specific policy documents by country. For instance, this should be useful when looking for critical infrastructure protection policies or military doctrines related to cyberspace;

- Another useful tool is the Cyber Norms Index developed by the Carnegie Endowment for International Peace. While UNIDIR's portal focuses on domestic policies, the Cyber Norms Index allows one to compare various multilateral documents dealing with ICT issues;
- The Cyber Operations Tracker is run by the Council on Foreign Relations. It covers many notable incidents, classifies them and provides available details. While specific details about some operations may be impossible to verify, the Tracker is a convenient go-to resource for information about known incidents.
- RISI Online Incident Database includes known incidents "of a cyber security nature that directly affect industrial Supervisory Control and Data Acquisition (SCADA) and process control systems", etc.
- Podcasts that might be relevant for the course: Risky Biz, Smashing Security, Wired Podcasts and Internet History Podcast.
- Google's phishing quiz can be used as a learning tool to test one's skills in identifying phishing emails that in real life can be used for malicious purposes.

Week 1. Introduction to Internet and Information Security

Aims and Content
Course introduction: the subject, the course goals and objectives. Expectations for class participation and homework. What is the Internet; key terms and concepts. Information security basics: definitions, types of malware

This course opens with an introduction to the Internet, a system of systems whose growth had a transformative effect on virtually every aspect of the world in the 21st century. We will explore its origins including the ARPANET, the World Wide Web as well as its basic technical features. Although there is no central authority on the Internet, ICANN holds a unique position as the body maintaining the Internet's address book. The ubiquity of the Internet and the ever-growing reliance on ICT worldwide call for a greater focus on information security at the national and international levels. To understand this challenge, we will begin by learning key terms and concepts used in this field.

Essential Readings

- Barry M. Leiner et al., Brief History of the Internet, Internet Society, 1997
- Okinawa Charter on Global Information Society, Kyushu-Okinawa Summit 2000
- Rus Shuler, How Does the Internet Work?
- Hacker Lexicon, Wired: Attack Surface, Phishing, DoS & DDoS Attacks, Ransomware

Supplementary Readings

- Understanding malware & other threats, Microsoft
- Information Security Handbook for Network Beginners, National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Government of JAPAN
- ICANN Beginner's Guides (Beginner's Guide to Domain Names, Beginner's Guide To Internet Protocol (IP) Addresses)
- Björn Lundgren, Niklas Möller, Defining Information Security

Week 2. Cybercrime

Aims and Content

This class continues the conversation started in the first week and introduces the phenomenon of cybercrime. This starts with a brief history, typology and demonstration of how attacks are carried out. Moving on, the discussion further addresses ways to tackle cybercrime: including the involvement of law enforcement, private sector, and technical organizations.

Seminar topics:

- Cybercrime trends: overview of cybersecurity firms' reports (2-4) firms
- International cooperation of computer emergency response teams (CERTs)

According to the World Economic Forum, by 2020 the economic loss due to cybercrime may reach $3 trillion and some cyber security companies put this number even higher. In most cases money is the main motive of the attackers, but the cybercrime landscape is evolving and getting more wide-spread. In this class, we will continue the introduction to information security and then look at a short history of cybercrime, different types of offenses and actors. On the opposite side, cybercrime is addressed by national law enforcement agencies, international organizations and groups and by Computer Emergency Response Teams that respond to incidents within specific organizations or sectors. Cybercrime has serious implications for international security not merely in and of itself, but also because skills and tools required to hack a bank may easily be repurposed for politically motivated attacks.

Essential Readings

- Understanding Cybercrime: Phenomena, Challenges and Legal Response, ITU, 2012, pp. 11-40 (skim)
- Vicente Diaz, Kaspersky Security Bulletin: Threat Predictions for 2019 (skim)
- Cisco 2018 Annual Cybersecurity Report (skim)

Supplementary Readings

- A Brief History of Cyber Crime, Florida Tech
- Robert Morgus, Isabel Skierka, Mirko Hohmann, Tim Maurer, National CSIRTs and Their Role in Computer Security Incident, New America, 2015
- Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database
- Johannes Xingan Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, 2017
- Budapest Convention on Cybercrime, Council of Europe, 2001
- Countering the use of information and communications technologies for criminal purposes, UNGA resolution, 2018

Week 3. Cyber Security of Critical Infrastructure

Aims and Content

Cyber security of critical infrastructure: concept and classification on CI, risks to major sectors. Sources of vulnerability. Critical infrastructure protection. International mitigation approaches. Case studies of cyber incidents

Seminar topics:

- Comparative approaches to securing critical infrastructure (two countries, e.g. U.S. & China)
- Case studies of major cyber incidents at critical infrastructure objects

Countries have different definitions of critical infrastructure but most often those include assets that are essential for the functioning of the economy, government and vital systems such as healthcare. One common feature of CI across the globe has been the introduction of computerized control systems over the past decades. This boosted performance of CI systems but increased connectivity made them more vulnerable to cyber attacks. On national and international levels, states strive to protect CI and reduce the risk of cyber incidents. In this class, we will examine several such incidents that have been previously reported.

Essential Readings

- Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, Organization for Security and Co-operation in Europe (OSCE) (skim)
- Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo, Cyber-Physical Systems Security – A Survey
- A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, Wired, 2015.
- Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward. Policy Memo, PIR Center

Supplementary Readings

- Cybersecurity Framework Draft Version 1.1, National Institute of Standards and Technology (NIST)
- BlackEnergy - Malware for Cyber-Physical Attacks. Analysis Report, iTrust-Analysis-001, 2016
- The Critical Infrastructure Protection in France
- Critical Infrastructure Cyber Community Voluntary Program
- The protection of critical infrastructures against terrorist attacks: Compendium of good practices

Week 4. Stuxnet Case Study

Aims and Content

During the class, students will watch the 2016 documentary Zerodays that tells a story of one of the most notorious computer attacks Stuxnet. This will be accompanied by a discussion, which will help better understand the actual attack and put information security-related concepts studied in previous weeks into an international security context.

First test on weeks 1–3

Zero Days documentary & discussion

In 2010, a computer worm has been discovered on Iranian networks and worldwide that became known as Stuxnet. A meticulous analysis of Stuxnet by cyber security experts revealed that it was an intricately crafted weapon targeting centrifuges at a uranium enrichment facility in Iran and aimed at sabotaging its nuclear program, while reporting by journalists helped piece together the political backstory of this attack. The Stuxnet attack was a pivotal moment in militarization of cyberspace. To students of information security as an international issue, it is a crucial case study demonstrating states' cyber capabilities, political and legal aspects of using and mitigating consequences of cyber attacks, and technical perspective, specifically vulnerabilities of cyber-physical systems and critical infrastructure in general.

Essential Readings

- Kim Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Wired
- David Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, New York Times

Supplementary Readings

- Kim Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, Wired
- (book) Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, 2014
- Ralph Langner, To Kill a Centrifuge, The Langner Group
- Nicolas Falliere, Liam O Murchu, Eric Chien, W32.Stuxnet Dossier, Symantec
- Alexander Gostev, The Mystery of Duqu: Part One, Part Two, Part Three, Securelist
- Boldizsár Bencsáth, Gábor Pék, Levente Buttyan, Mark Felegyhazi, The Cousins of Stuxnet: Duqu, Flame, and Gauss

Week 5. Information and Communications Technologies as an International Security Issue

Aims and Content

The lecture will address international efforts to develop common rules for interaction between states in cyberspace: different approaches, global (at the UN level), regional and group initiatives and processes. The lecture will also address the issue of the participation of non-state actors, primarily, leading technology companies, in the development of such norms, both jointly with states and by promoting their own initiatives.

Seminar topics:

- Regional agreements aimed at cooperation in information/cyberspace and reduction of the risk of cyber conflict
- Bilateral agreements related to ICT / cyber
- Private sector initiatives to regulate cyberspace

The issue of information security has formally been an international issue for more than two decades. In 1998, a Russia-sponsored resolution, Developments in the field of information and telecommunications in the context of international security, was adopted by the UN General Assembly. Since then, the United Nations has served as the main, yet not the only, platform for states to discuss rules and norms for cyberspace. This work was led by five Groups of Governmental Experts (GGE) whose substantive reports form the basis for international understanding of this field. Yet, GGE efforts fell short of producing a universal agreement on cyberspace, as many issues are still debated between states such as information vs cyber security, how international law applies to this domain, etc. Beyond the UN, this issue is dealt with by other organizations (i.e. OSCE, NATO), while states develop bilateral arrangements (i.e. Russia and the United States, United States and China) to address challenges emanating from cyberspace. As the role of private sector in international politics remains an open question, a few non-government initiatives to establish norms for cyberspace have emerged recently championed by IT companies or professional community.

Essential Readings

- A.A Streltsov, Application of international humanitarian law to armed conflicts in cyberspace, 2016
- Wolff Heintschel, Von Heinegg, International Law and International Information Security: A Response to Krutskikh And Streltsov, Tallinn Paper No. 9 2015, NATO Cooperative Cyber Defence Centre of Excellence
- Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015
- Alex Grigsby, The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased, CFR
- Luigi Martino, Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace, ISPI, 2018

Supplementary Readings

- Michael N. Schmitt, Liis Vihul, The Nature of International Law Cyber Norms, Tallinn Paper No. 5 Special Expanded Issue 2014. NATO Cooperative Cyber Defence Centre of Excellence.
- Arun M. Sukumar, The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?
- Patricia M. Lewis, Global Cyber Governance in 2017: Information Integrity, Chatham House, Council of Councils, 2017
- Global Cooperation in Cyberspace Initiative 2016-2017 Action Agenda. The EastWest Institute, 2016
- FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security, White House, 2013

- Ilona Stadnik, Cybersecurity Diplomacy: Business and Tech Replacing the States?, 2018
- Thomas Remington, Chris Spirito, Elena Chernenko, Oleg Demidov, and Vitaly Kabernik, Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity, Working Group on the Future of U.S.-Russia Relations, 2016
- Ilona Stadnik, Discussing state behaviour in cyberspace: What should we expect?, Diplo Foundation, 2019

Week 6. Military and Strategic Uses of Cyberspace

Aims and Content

The class will be focused on the use of cyberspace by the military of different countries. This will include issues of an organizational, doctrinal and legal nature, as well as the applicability of the law of war in conflicts in cyberspace and the attribution of attacks / incidents.

Second test on weeks 4–5

Seminar topics:

- Military doctrines related to cyberspace
- Case studies of offensive or defensive cyber operations

Cyberspace lacks solid international regulation, specifically as regards to the use of offensive tools. This, however, does not preclude states' cyber engagements. Indeed, we have seen numerous cases of reported operations conducted by states via computer networks. With the caveat in mind that attribution of actions in cyberspace is uncertain, it is still possible to study the diverse military uses of ICT by actors ranging from defense and intelligence agencies to proxy groups. A de-facto militarization of cyberspace may well be underway, but characteristics of cyber warfare are not yet clearly understood. This has mixed implications for attempts to use cyberspace to achieve strategic goals and to reduce the risk of incidents in this domain.

Essential Readings

- Oleg Demidov, Yelena Chernenko, The Game of Rules, Russia in Global Affairs, 2015
- Richard J. Harknett, United States Cyber Command's New Vision: What It Entails and Why It Matters, 2018
- Christopher Bing, Joel Schectman, Inside the UAE'S Secret Hacking Team of American Mercenaries, Reuters
- Will Dunn, Can nuclear weapons be hacked?, New Statesman, 2018
- Thomas Rid, Think Again: Cyberwar, Foreign Policy, 2012

Supplementary Readings

- Arthur P.B. Laudrain, France's New Offensive Cyber Doctrine, 2018
- Piret Pernik, Preparing for Cyber Conflict – Case Studies of Cyber Command, ICDS, 2018
- Kodar, Erki. Applying the Law of Armed Conflict to Cyber Attacks: from the Martens Clause to Additional Protocol I" ENDC Proceedings, Volume 15, 2012, pp. 107–132
- Herbert Lin, Cyber Conflict and International Humanitarian Law
- Schmitt, Michael N. Rewired Warfare: Rethinking the Law of Cyber Attack. In International Review of the Red Cross 96, no. 893 (2014): 189–206
- C. Robert Kehler, Herbert Lin, Michael Sulmeyer, Rules of engagement for cyberspace operations: a view from the USA, Journal of Cybersecurity, Volume 3, Issue 1, March 2017

Week 7. Cyber Deterrence

Aims and Content

As a continuation of the previous class, this week's discussion will focus on deterrence in cyberspace. What are theories of deterrence? How do they broadcast on the ICT environment? What evidence is there that speaks in favor or against the application of the theory of deterrence to this given domain.

Debate: Will deterrence work in cyberspace?

Deterrence is premised on the idea that threat can be used to dissuade one's opponent from behaving in certain ways, specifically from taking aggressive actions. Deterrence as a military concept has a long history in conventional warfare and it has played a prominent role in strategic thinking since the creation of nuclear weapons. But does this concept apply to cyberspace? The underlying assumptions of deterrence are challenged by such features of this domain as global scope, anonymity, diversity of capable actors, etc. While the utility of cyber deterrence is debated, many countries already rely on this concept in their military and diplomatic strategies and in practical responses.

Essential Readings

- Mariarosaria Taddeo, The Limits of Deterrence Theory in Cyberspace. Philosophy&Technology, Volume 31, Issue 3, September 2018, pp. 339-355
- Liam Nevill, Deterrence in cyberspace: different domain, different rules
- Martin Libicki, Would deterrence in cyber space work even without attribution?
- Michael Sulmeyer, How the U.S. Can Play Cyber-Offense, Belfer Center, 2018
- Jason Healey, Not The Cyber Deterrence the United States Wants, CFR, 2018
- Jack Goldsmith, Robert D. Williams, The Failure of the United States' Chinese-Hacking Indictment Strategy, Lawfare, 2018

Supplementary Readings

- Martin C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, 2009 (skim Chapter Three)
- Clorinda Trujillo, The Limits of cyber space deterrence
- Joseph S. Nye Jr., Deterrence and Dissuasion in Cyberspace, 2017

Week 8. Internet-Enabled Information Threats

Aims and Content

In recent years, the threat of information influence enabled by ICT, has become a much talked about topic among policy makers, tech companies whose services are used as platforms, and among individual citizens. How much does digitalization change the nature of informational confrontation? How are states and businesses trying to counter this challenge? What legal and ethical questions arise as a result?

Third test on weeks 6–7

Seminar topics:

- Case study of ISIS propaganda and anti-ISIS information efforts
- Are platforms responsible? Debate about social media companies' policies

Fake news, propaganda and extremism are not technology problems per se as they existed long before the arrival of the digital era. Yet ICT seems to contribute to the increased prominence of these and other challenges related to the content of information. Concerns about what information is shared online, be it terrorists' recruitment videos, divisive messages or state-sponsored attempts to influence public opinion, translate into government regulation, diplomatic and military efforts and technology responses. They also provoke debates about broader issues such as freedom of expression, privacy and sovereignty. In this class we will explore ways in which information might be manipulated using digital tools and discuss how to live in this environment.

Essential Readings

- Sean Illing, How social media became a weapon of war (Interview with Peter W. Singer, co-author of LikeWar: The Weaponization of Social Media), Vox, 2018
- Brendan I. Koerner, Why ISIS Is Winning the Social Media War, Wired, 2016,
- Oleg Shakirov, "Russian Propaganda": On Social Networks, in Eastern Europe, and Soon Everywhere, RIAC, 2018
- Stuart Macdonald, How tech companies are successfully disrupting terrorist social media activity, The Conversation, 2018

Supplementary Readings

- Julie Bort, Meet the little-known group inside of Google that's fighting terrorists and trolls all across the web, Business Insider, 2018
- The Conduct of Information Operations, Department of the U.S. Army, 2018
- Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard, Government Responses to Malicious Use of Social Media, NATO STRATCOM COE, 2018
- Emily Taylor, Stacie Walsh, Samantha Bradshaw, Industry Responses to the Malicious Use of Social Media, NATO STRATCOM COE, 2018

Week 9. Data and Privacy

Aims and Content

Why have data and privacy related issues become so important? How does this relate to international security? What is the role of private companies, national governments and international groupings in making sure that data is treated properly?

Guest speaker (?)

How often do you think about your digital privacy? Stats show that people do not really care much about it. But companies and governments do. Data privacy has become important both in the corporate world and international relations. For some, it is a mandatory requirement, while for others it represents a new field for regulation and enforcement. In this class, we will uncover five truths about data privacy: contested issues, main trends, the role of companies and governments, and its correlation with cyber security. All of this will help you understand your digital footprint and make you care about your data privacy.

Essential Readings

- Keynote address from Tim Cook, CEO, Apple Inc
- The World's most valuable resource is no longer oil but data, Economist
- Google fine launches new era in privacy enforcement, Politico Europe
- About Data Localization, CSIS

Supplementary Readings

- The Strava Heat Map and the End of Secrets, Wired
- Dylan Curran, Are you ready? Here is all the data Facebook and Google have on you, The Guardian
- Henry Farrell, Abraham Newman, The Transatlantic Data War, Foreign Affairs
- Chris Ip, Who controls your data?, Engadget
- Gabriel J.X. Dance, Michael LaForgia, Nicholas Confessore, As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants