SYLLABUS

CYBER SECURITY AND CYBER DIPLOMACY

COURSE DESCRIPTION

Title	Cyber Security and Cyber Diplomacy
Credit	
Lecturer	Marina Kaljurand, GCSC
Language	English
Classroom work	
Bibliography	There is no single textbook for the course. Readings will be distributed by the lecturer
Mode of examination	Combination of attendance, participation, presentation

Annotation

The course examines the theory and practice of cyber security and cyber diplomacy. Cyber revolution/use of ICTs came to stay. ICTs continue to provide immense opportunities for social and economic development. However, wider use of ICTs is accompanied by new challenges and negative trends, including the increase in incidents involving the malicious use of ICTs by States, their proxies and other non-State actors and spread of malicious ICT capabilities. These negative trends hold risks for all States and carry serious implications for international peace and security. Cyber security has become an integral part of national, regional and global security. The aim of the lecture/course is to introduce and reflect on discussions taking place in different internatonal foras, including UN, OSCE, NATO, EU, with special emphasis on applicability of international law to cyber space and norms of responsible State behviour in cyber space.

The course will also focus on the lessons learned from Estonia's experience. Estonia has had the luxury of experiencing the benefits of the use of ICTs, e-lifestyle for more than 20 years. But Estonia was also the first country in the world to fall under politically motivated cyber attacks aiming at influencing Estonian domestic affairs, disrupting e-services and disturbing the whole society. The questions that were raised during and after the 2007 cyber attacks remain topical and timely also in 2018: role of Government in providing cyber security, attribution, counter-measures, applicability of international law to cyber space, norms of responsible

behavior, responsibility of a state for supporting cyber attacks originating or transiting through its territory, responsibility of states for the acts of proxies and other non-State actors, cooperation with industry/private sector, multistakeholder approach and international cooperation.

The course will include group work analyzing/discussing practical aspects that States face in everyday activities in cybersecurity sphere – deterrence, attribution and responsibility of States (for their activities and for the activities of non-State actors). The groups will be assigned with specific cases and the conclusions of the group discussion will be presented to the whole group.

COURSE OUTLINE

The course will cover following topics

1. Definition of cyber security. Existing and emerging threats.
2. Cyber security as part of national and international security.
3. Applicability of international law to cyber
4. Deterrence, attribution, countermeasures, offensive capabilities.
5. International cooperation – bilateral, regional global.
6. Role of different institutions and organizations: UN, G7, G20, OSCE, NATO, EU.
7. Role of Governments.
8. Role of MFA and cyber diplomacy.
9. Multistakeholder model: role of other stakeholders
10. Future trends in cyber security and cyber diplomacy.