

Cybersecurity

Policy, Strategy and Geopolitical Ramifications

At the time increasingly digitized societies when the cyber-domain is recognized as the fifth domain of military operations and warfare (along with land, sea, air and space) cybersecurity cannot be addressed just from its technological angle. It has evolved into a discipline with essential policy, strategy and geopolitical ramifications.

For policy practitioners, cybersecurity policy studies have opened the way to a new focus area of diplomacy and international engagement, called cyber-diplomacy. Diplomats and policy professionals are currently engaged at UN level in the Governmental Group of Experts (UN-GGE) on cybersecurity and the Open Ended Working Group on Cyber Policy, at EU level in the Digital Diplomacy Network, while national diplomats, along with private sector experts are engaged in a multi-stakeholder approach in supporting various initiatives such as The Paris Call for peace and stability in Cyberspace. This course draws a lot on the practical experience and analysis of international policy and strategy developments and is addressed to those who are interested to understand this development and potentially to engage in these critical and complex strategic cyber policy endeavours.

The course introduces the key concepts related to cybersecurity, addressing the different types of actors, motivations and aims, types of cyber-attacks and attack vectors, as well as impact analysis and categorisation. The seminars offer the possibility to analyse concrete case studies and reflect the impact and strategic conclusions.

The deeper conceptual analysis of the course links cybersecurity policy and strategy first to “soft policy” essential linked to so called “cyber-hygiene”, best practices, information and analysis exchanges etc. and expands the link of cyber operations linked to hybrid attacks (against digital infrastructure, information space) and up the escalation ladder to the level of deploying cyber-attacks, linked to military operations. This creates the path towards linking key security strategy concepts such as escalation management or deterrence to the cyber domain.

The course addresses cybersecurity approaches, policies and strategies, at the level of international organizations, such as NATO, EU, OSCE, United Nations. Cybersecurity strategies of a number of individual countries are addressed at the seminar.

The applicability of existing International Law to cyberspace is analysed throughout the course both for the situation of cyber operations below the threshold of armed attack and above that threshold while addressing, in the latter case, the key aspects linked both to “*Jus ad bellum*” and those related to “*Jus in bellum*”.

Given some important “grey areas” in the applicability of International Law to the cyber domain, the course also addressed international initiative at UN, OSCE or in other multilateral for a, aim at development of norms of responsible behaviour in cyberspace as well as transparency and confidence building measure in cyberspace.

A recent addition to the Cybersecurity course is related to the impact of the ground-breaking AI technologies upon the resilience and security of digital infrastructure, and the need for international engagement on AI governance as well as responsible use.