ITSS
International Team
For the Study of Security
Verona

Summer School Track: A Cyber World

Module Convenors: Martina Gambacorta (martina.gambacorta@studio.unibo.it)
Julia Hodgins (julia.hodgins@kcl.ac.uk)

Module Description

Join this track to explore the fascinating and ubiquitous Cyberspace and the many socio-political, military, and technical challenges that interconnectivity and cyber reliance pose to individuals, businesses, states, critical infrastructure, online venues, etc. We will walk you through strategy and cybersecurity, remarking the relevance of sensitive policymaking oriented to keep cyberspace and our society safe and operative.

The track will thus help students develop analytical capacities to understand the cyber domain as both a new battlefield and an operational space where new actors, mostly non-state organizations, have been mobilizing power. Our modules provide deeper knowledge of several of the canonical cases that continue to influence the study and practice of international security today.

Aims

Through a combination of frontal lectures, seminars, live interviews, and presentations by world-leading experts, students are invited to embrace and appreciate the comprehensiveness and complexity entailed in cybersecurity. The track provides students with an in-depth understanding of the main underlying themes in cybersecurity studies. In doing so, the module aims to **inspire** participants to **think as holistically as possible, to challenge common wisdom,** and to express themselves in the debates that will arise throughout the lessons.

Learning outcomes

By the end of the course, participants will be able to demonstrate the following:

Knowledge and understanding of:

- The nature of cyberspace and the challenges of the application of strategy
- Strategy and strategic thought, and Cyber deterrence
- Relevance of cybersecurity, including the security by design approach
- Pressing issues on cyberspace (attribution, obscureness) and be able to challenge traditional concepts.
- The cyberwarfare battlefield in terms of current and future cyber threats
- Opportunities and risks associated with new technologies
- A critical attitude towards the most problematic and controversial aspects of cybersecurity

Skills (specific to the module):

- Socio-political and strategic analysis of cyberspace and cybersecurity
- Technical analysis of cyber attacks and cyber defense tools
- Mind mapping the characteristics and challenges of cyberspace
- Case study analysis

Transferable/employability skills (through the seminars):

- Communication and presentational skills
- Balance in crafting an argument by appreciating complexity, avoiding jumping to uncorroborated conclusions
- Mental flexibility – members are to think as critically and as holistically as possible
- Respect – for every actor's research, work, and overall perspective

Teaching arrangements

The module is divided into **eight lessons** spread across **four weekends** on Saturday morning and afternoon for four consecutive weekends, equalling **12 hours total.** Teaching sessions will be delivered remotely. Lessons feature **frontal lectures** (1 hour) and **short seminars** (30 minutes). Frontal teaching prevails in the first class where students are provided with the needed theoretical background on cyber security and warfare. Images, videos, online material, as well as live interviews with world-leading experts, will facilitate interactive and practical lectures. Q&A and debates will follow the presentation, where students are encouraged to present their doubts and questions.

Hence, this is how the module is specifically divided:

Saturday, June 11th, 2022

Lesson #1: **"Introduction to Strategy"**

The lecture on Introduction to Strategy will briefly examine the evolution of strategic thought before focusing on how strategy is used within cyberspace. To expand on this, an overview of cyberspace, its characteristics, and challenges will be explained. Then, by drawing on examples of various cyber incidents, the concept of how strategy may work in cyberspace will be tied together. In this session, Julia M. Hodgins and Mariam Qureshi (ITSS Verona) take on core cases like Ukraine and Estonia and the Russian Cyber Subversion during the US Presidential Elections of 2016.

Lesson #2: **"Cybersecurity challenges: socio-political implications"**

Cyberspace offers malign actors a range of technical features which compromise security – such as obscureness, non-territoriality/territoriality, relentless innovation, the amplification of power, scale, and speed of operations, and the disproportionate effect that can be achieved by non-state actors. Whilst these may appear technical challenges to a cyber-security strategy, the threats they pose manifest as the political or social effects of attacks on the infrastructure that characterises, enables, and perhaps even defines much modern society. As such, these pose very different, and equally demanding, challenges to the resilience of the societies in question. Considering recent case studies which generated both technical and social effects, students will be invited to identify and consider potential solutions that can be orchestrated to mitigate/manage those challenges, guided by our expert speaker Dr. Andrew Corbett (KCL).

Saturday, June 18th, 2022

Lesson #3: **"Cybersecurity: challenges, complexity, and trade-offs"**

Challenges in cybersecurity derive from the technical nature of cyberspace, – i.e. the securitization of technological devices, the Internet-of-Things, and its regulation through standardization and licenses. This session will focus on the technical IT/OT aspect, in the wider sense of making connections between concrete issues of cybersecurity and implications for policy and decision-making. This vertical articulation brings cybersecurity to the forefront when making managerial and business decisions, assessing and managing risks and costs, defining policy, and strategy. Expert Oleg Goldshmidt (Fortinet) will lead the class to round up these aspects of cybersecurity within a broader statecraft and leadership context.

Lesson #4: **"AI for cybersecurity"**

Artificial intelligence endeavors to simulate human intelligence. It has immense potential in cybersecurity. If harnessed correctly, Artificial Intelligence or AI systems can be trained to generate alerts for threats, identify new types of malware, and protect sensitive data for organizations. We explore the potential implications of AI in cybersecurity with expert speaker Andrea Rigoni (Deloitte).

Saturday, June 25th, 2022

Lesson #5 & 6: **"The cyber domain as the new worldwide battlefield"**

Today's cyberwarfare has integrated a full spectrum of sensors, weapon systems, computers, telecommunications, data collection, and processing activities into the military environment, with the battlefield resulting in a new digitalized field. Despite being boundless, the new battlefield must be defined. Cyber-attacks have demonstrated that many countries are developing strong cyber capabilities in the frame of an 'arms race', showing that technologies can potentially be used to undermine international stability and security. Through the analysis of the most famous cyberattacks, some important features will emerge: what a cyber-weapon looks like, the steps of an ongoing cyberattack, the actors behind cyberwar, causes and motivations, the basic forms of cyber defense, the operational and strategic levels of cyber-warfare. In these sessions, Martina Gambacorta (ITSS Verona) will explore these issues in-depth and present core case studies – including Stuxnet, Black Energy, and Solarwinds.

Saturday, July 2st, 2022

Lesson #7: **"Cyber Deterrence"**

Although the means might vary, interstate confrontations all seek to serve political ends. This was as true of the face-to-face fights of the Peloponnesian wars 2500 years ago as it is in the globalised, multimedia, grey zone, high technology environment of the 21st century. Psychological issues such as coercion, compellence, and deterrence, as well as the violence of war and the use of force, are familiar aspects of these confrontations. Cyberattacks appear to promise a disruption on a scale similar to that of conventional warfare, but cyber-specific issues such as attribution and credibility, and ethical constraints associated with the more familiar control of the use of force, pose particular challenges to traditional concepts of deterrence by denial and deterrence by punishment. Using a number of contemporary case studies, expert speaker Dr. Andrew Corbett (KCL) will explore notions of cyber security alongside long-standing theories of deterrence to enable students to consider how modern deterrence strategies might accommodate the 'cyber threat' in this fast-moving area of strategy.

Lesson #8: **"Technical matters of cybersecurity"**

As organizations and companies face cyber-attacks by malicious threat actors, they have to design strategies to counter malicious attacks. Students are introduced to the world of consulting in the field of cybersecurity by our expert speaker Andrea Rigoni (Deloitte) to better understand the potential pitfalls and requirements of such a multifaceted domain. The focus is on the types of analysis aimed at developing cyber strategies and skills for the government and public sector. This allows students to better understand and research the approaches, tools, and techniques that are used in cyberspace for unlawful purposes – and where we go from here.

Module requirements

There are no formal requirements for this module. Everyone with an interest in the aforementioned topics is welcome.

Referenced sources/Supplemental materials

A full list of reading/viewing materials will be provided in due course. Some initial readings are:

- Brantly, A. (2014). *Cyber Actions by State Actors: Motivation and Utility*, International Journal of Intelligence and CounterIntelligence, 27:3, 465-484, DOI: 10.1080/08850607.2014.900291

- Czosseck, C & Geers, K (Eds.). (2009). *The virtual battlefield: perspectives on cyber warfare* (Vol. 3). Ios Press.

- Ďulík M. and Ďulík M. jr. (2019). Cyber Security Challenges in Future Military Battlefield Information Networks. *Advances in Military Technology*. Vol. 14, No. 2 (2019), pp. 263-277 ISSN 1802-2308, eISSN 2533-4123 DOI 10.3849/aimt.01248

- Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, *11*(4), 541-562.

- Lobel H. (2012) Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict, *Texas International Law Journal*, Vol. 47, Iss. 3,. 617-640.

- Shimeall J. T. (2016) From cybercrime to cyberwar: indicators and warnings. Strategic Studies Institute, *US Army War College*.