DISCIPLINA: **INTERNATIONAL LAW AND POLITICS OF CYBERSPACE**	CÓDIGO: **GRDDIRATCE0459**
PROFESSOR: **BARRIE SANDER**	CARGA HORÁRIA: **10h**

EMENTA

1.Foundational Concepts of Cyberspace. 2.State Responsibility and Cyberattacks. 3.Cyber Espionage and Human Rights. 4.Cyber Crime and Cyber Terrorism. 5. Use of Force and Cyber War

OBJETIVOS GERAIS

Emerging as a new domain of human interaction in the second-half of the twentieth century, cyberspace has become woven into the fabric of societies around the world. But for all its benefits, cyberspace has also given rise to new opportunities for harm and disruption. As the cyber threat landscape has become multifaceted, characterised by an increasing number of threats and vulnerabilities, the question of how cyberspace should be governed has become a global priority. This course examines the extent to which international law provides a vocabulary for regulating cyberspace. For this purpose, the course examines a broad range of issue-areas, including cyberattacks, cyber crime, cyber espionage, cyber terrorism and cyber warfare. Each session will draw on contemporary case-studies to illuminate the tensions and controversies that arise when applying international law to the unique context of cyberspace.

OBJETIVOS ESPECÍFICOS

By the end of this course, students will develop:

- an in-depth understanding of international law and the challenges encountered when applying international law to cyber activities; and
- an ability to critically discuss some of the central tensions and controversies that have arisen when determining whether/how international law applies to cyber activities.

NB: A prior knowledge of public international law is NOT required for this course.

METODOLOGIA

The course will be delivered through 10 hours of lectures and seminars, divided into 5 two-hour sessions. Detailed online Prezis will be developed to structure each session. Classes will combine traditional lectures with interactive discussions concerning the most contentious issues examined within each thematic.

PROGRAMA

Session 1: Foundational Concepts of Cyberspace

In our opening session, we will discuss what is meant by cyberspace, the extent to which cyberspace constitutes a unique domain of politics and power, different regulatory analogies that have been drawn in order to determine whether/how cyberspace should be governed, what is meant by cybersecurity and cyberthreats, and the different modalities by which international lawyers have been engaging with the question of regulating cyberspace.

Session 2: State Responsibility and Cyberattacks

This session will examine the application of the international law of state responsibility to cyber activities, including the challenge of attributing cyber conduct to particular actors, the principle of due diligence, and the law on counter-measures, reprisals, retorsion and necessity. The session will examine these issues by discussing two case studies: the 2016 cyberattack on the US Democratic National Committee, by which Russia is alleged to have attempted to influence the outcome of the 2016 US presidential election; and the 2014 cyberattack on Sony Pictures Entertainment alleged to have been orchestrated by North Korea in response to the release of the film, *The Interview*.

Session 3: Cyber Espionage and Human Rights

The disclosures by whistleblower Edward Snowden from mid-2013 onwards about alleged widespread cyber espionage practices, including extraterritorial surveillance and interception of communications, generated considerable alarm within the international community. The first-half of this session will examine whether cyber espionage is permitted under international law and, if so, to what extent. The second-half of the session will examine the application of international human rights law to cyber activities – including privacy rights and the right to be forgotten – as well as how cyberspace is transforming human rights fact-finding processes.

Session 4: Cyber Crime and Cyber Terrorism

Hacked computers, spam, virus attacks, online fraud and cyberstalking. Cyberspace has given rise to a new and increasingly common phenomenon: cybercrime. With offenders and victims of harmful cyber activities often located across different jurisdictions, cybercriminal activities are often deterritorialized in nature. The first half of this session will examine the legal responses to cybercrime which have also increasingly taken on an international or transnational dimension. The second-half of the session will examine cyber terrorism, encompassing acts of terrorism that are cyber-enabled through propaganda, financing, training, planning, execution, and cyberattacks. The session will examine some of the tensions that arise through governmental attempts to counter cyber terrorist activities, including the potential of hate speech legislation to encroach on the right to freedom of expression.

Session 5: Use of Force and Cyber War

In recent decades, alarmist accounts depicting an increasingly threatening cyber landscape have emerged, with references to "cyber-doom scenarios", "cybergeddons", and even a "digital pearl harbour". Although these threats have yet to be realised, significant attention has been devoted by scholars and policymakers to the question of whether and how cyber warfare is regulated under international law. In our final session, we will examine some of the tensions that arise from applying the law on the use of force and the law of armed conflict to cyber activities. The session will include a critical discussion of whether the extensive cyberattacks against Estonia in 2007, which led to the shutdown of its financial institutions, met the threshold to be considered a "use of force" or "armed attack" under international law.

CRITÉRIOS DE AVALIAÇÃO

The course will be evaluated through two assessments:

- Participation (50%): Students are required to demonstrate engagement with the allocated readings for each session through in-class discussions;

- Written Assignment (50%): Students are required to submit a blog post, 500-1,000 words in length, related to any topic discussed during the course. More details on the requirements of the written assignment will be provided at the beginning of the course.

BIBLIOGRAFIA OBRIGATÓRIA

TSAGOURIAS N., and BUCHAN, R. (eds.), Research Handbook on International Law and Cyberspace (Edward Elgar, 2015)

KITTICHAISAREE, K., Public International Law of Cyberspace (Springer, 2017)

SINGER, P.W., and FRIEDMAN, A., Cybersecurity and Cyberwar (Oxford University Press, 2014)

BIBLIOGRAFIA COMPLEMENTAR

CHOUCRI, N., Cyberpolitics in International Relations (MIT Press, 2012)

OHLIN, J.D. et al. (eds.), Cyber War: Law and Ethics for Virtual Conflicts (Oxford University Press, 2015)

ROSCINI, M., Cyber Operations and the Use of Force in International Law (Oxford University Press, 2014)

ZIOLKOWSKI, K. (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (NATO CCD COE Publication, 2013)

SCHMITT, M.N. (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP, 2017)