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.

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)