Université Paris Cité

DU LLM International Law
2023/2024

CYBER LAW

Course informations :

Degree level	○ DU LLM International Law ~~○ Master 2 Droit international général~~[1]
Semester	
Course duration	15h
ECTS delivered upon completion	7

Instructor information:

Name	AUDE GÉRY
Status	Senior researcher
Institution	GEODE (French Institute of Geopolitics, University Paris 8)
Email	gery.aude@gmail.com

Course description :

Cybersecurity and information security have been an important topic in international negotiations for more than 20 years now. International law has become a key topic and States and regional organizations are developing a politics of international law. The course aims at understanding the politics around cybersecurity and international law as well as the content of cyber law. Based on real examples, the course will allow students to understand the different issues around the interpretation and application of international law to cybersecurity and information operations, including the different views of States.

Course learning outcomes:

Upon completion of this course, students will demonstrate their ability to:

- Understand the specificities of cyberspace: architecture, actors, threats, geopolitical context, *etc.*
- Understand and apply the rules of general international law to cyberoperations.
- Analyze the legal difficulties of applying international law to cyberoperations.
- Understand the UN processes and other international processes related to cyber issues.

Student evaluation plan:

The evaluation will be based upon oral participation and on a final exam as described hereafter in the course schedule.

[1] Only for *Law and Practice of International Courts and Tribunals*; *International Law and Global Governance*; *International Commercial Arbitration*.

Course schedule :

Date	Session	Topic	Description	Assignment
2023-01-04	1	Internet Governance and Cyber Diplomacy	The objective of the course is to understand the nature of cyberspace, the nature of the threats, as well as to provide an overview of the international bodies involved in Internet governance and cyber diplomacy.	
2023-01-09	2	General International Law and Cyber Operations (Part 1)	The objective of the course is to understand how rules of general international law apply to cyberoperations; the issues of interpretation raised by the characteristics of cyberspace; State's views on the interpretation of international law to cyberoperations.	Reading for the course: UN doc. A/76/136.
2023-01-11	3	General International Law, Human Rights Law, and Cyber Operations (Part 2)	The objective of the course is to understand how rules of general international law apply to cyberoperations; the issues of interpretation raised by the characteristics of cyberspace; State's views on the interpretation of international law to cyberoperations.	
2023-01-16	4	International Responsibility of States and Cyber Operations	The objective of the course is to understand how cyber operations can be attributed to States, both from a technical and legal perspectives, and the problems raised by the characteristics of cyberspace. Legal remedies available in case of an international wrongful cyberoperations are also being studied.	Exercise to be handled in writing at the beginning of the course.
2023-01-18	5	International Humanitarian Law and Cyber Operations	The objective of the course is to understand the challenges brought by cyberoperations to the application of international humanitarian law. Through case studies, specific obligations will be analyzed.	Reading for the course : L GISEL, T. RODENÄUSER, K. DÖRMANN, "Twenty years on:International humanitarian law and the protection of civilians against the effects of

				cyber operations during armed conflicts", *International Review of the Red Cross* (2020), 102 (913), 287–334. Final exam to be handled in writing a few weeks after the last course.

Books:

M. N. SCHMITT, L. VIHUL (eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

S. Bortzmeyer, *Cyberstructure : L'Internet, un espace politique*, C&F Editions, 2018.

M. GRANGE, A-Th. NORODOM (eds.), *Cyberattaques et droit international. Problèmes choisis*, Pedone, 2019.

B. BUCHANAN, T*he Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press, 2020.

F. DELERUE, *Cyber Operations and International Law*, Cambridge University Press, 2020.

"Géopolitique de la Datasphère", *Hérodote*, n°177-178, 2020.

P. CORNISH (ed.), *The Oxford Handbook of Cyber Security*, OUP, 2021.

N. TSAGOURIAS, R. BUCHAN, *Research Handbook on International Law and Cyberspace*, E. Elgar Publishing, 2021.

Journal articles:

P. JACOB, « La gouvernance de l'Internet du point de vue du droit international public », A.F.D.I., vol. 56, 2010, 543-563.

T. MAURER, *Cyber Norms Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber Security*, Belfer Center for Science and International Affairs, 2011.

C. RUHL, D. HOLLIS, W. HOFFMAN, T. MAURER, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, Washington DC: Carnegie Endowment for International Peace, 2020.

D. HOLLIS, M. FINNEMORE, "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity", *E.J.I.L.*, vol. 31, n°3 2020, 969-1003.

F. DELERUE, F. DOUZET, A. GERY, *The Geopolitical Representations of International Law in the International Negociations on the Security and Stability of Cyberspace*. Brussels, Paris: EU Cyber Direct, IRSEM, 2020.

T. MIKANAGI, K. MACAK, "Attribution of cyber operations: an international law perspective on the *Park Jin Hyok* Case", *Cambridge International Law Journal*, vol. 9, n°1, 2020, 51-75.

N. TSAGOURIAS, M. FARRELL, "Cyber Attribution: Technical and Legal Approaches and Challenges", *E.J.I.L.*, vol. 31, n°3 2020, 941-967.

A. COCO, T. DE SOUZA DIAS, "Cyber Due Diligence : A Patchwork of protective Obligations in International Law", *EJIL*, vol. 32, n°3, 2021, 771-806.

R. Geiss, H. Lahmann, *Protection the global information space in times of armed conflict*, Working paper, Geneva Academy, 2021.
K. Macak, “Unblurring the lines: military cyber operations and international law”, *Journal of Cyber Policy*, 2021, vol. 6, n° 3, 411-428.
A. Géry, « Les discours des États sur l’application du droit international dans le cyberespace. Entre renforcement et contournement du droit international », *AFRI*, vol. XXIII, 2022, pp. 823-838.
K. Macak, T. Rodenhäuser, « Towards common undertandings: the aplication of established IHL principles to cyber operations », *ICRC*, 2023 https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/.
W. C. Biggerstaff, « The Status of the Ukraine's "IT Army" Under the Law of Armed Conflict », *Articles of War*, 10 mai 2023, https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/.
M. Milanovic, « Revisiting Coercion as an Element of Prohibited Intervention in International Law », *SSRN*, 17 juillet 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4504816.
Y. E. Gül, « The application of the principle of precautions to cyber operations », *The Military Law and the Law of War Review*, vol. 61, n°1, pp. 3-38.

Supplement resources:
Inside Cyber Diplomacy, Podcast dédié aux questions de cyberdiplomatie, https://www.csis.org/podcasts/inside-cyber-diplomacy?page=0.
Vidéo de présentation de la gouvernance d’Internet : https://eurossig.eu/eurossig/2020-edition/self-study/.