



TEL AVIV
UNIVERSITY

אוניברסיטת
תל אביב

Full Syllabus



Course Title

Foreign Policy and Geopolitics in A Cyber Age (1020-4012-01)

Lecturer

Dr. Nir Hassid

Semester

1st semester, 2027

Course requirements

N/A

Final grade components

1. Presence – at least 9 classes out of 12 (five points will be reduced for less than 9) – 20%
2. Case study/class presentation –30%
3. Submission of a Final paper – 50%

Course schedule

Class no. / Date	Subject and Requirements (assignments, reading materials, tasks, etc.)
1. (23/10/26)	International security and global order An introduction to existing global security arrangements that enhance cooperation through international regimes and the role of hegemony in structuring and maintaining these regimes.
2. (30/10/26)	The Challenge of Cyber to Traditional Security Regimes Why do cyber capabilities challenge traditional arms control regimes, deterrence models, and international law? Discussion on attribution, strategic stability, and the limitations of classical security architectures.
3. (06/11/26)	Major Cyber Powers: The United States Exploring how major cyber powers shape cyberspace to serve strategic interests, and how global legal frameworks enable or constrain their cyber policies.
4. (13/11/26)	Major Cyber Powers: China Analyzing China's approach to cyberspace governance and its bid to shape global cyber norms as an emerging norm entrepreneur amid strategic competition with the United States
5. (20/11/26)	Major Cyber Powers: Russia Assessing Russia's cyber strategy and its impact on the prospects for establishing a global cybersecurity regime.
6. (27/11/26)	Major Cyber Powers: The European Union

Full Syllabus



	Examining how the EU balances security imperatives, economic interests, and digital sovereignty in shaping its cyber policy.
7. (04/12/26)	Non-binding norms and the UN GGE dialogue An overview of global cybersecurity regulation challenges, focusing on UN GGE progress and current obstacles.
8. (18/12/26)	Selling Capability: Knowledge Industries, Cyber Exports and the Limits of Leverage Digital middle powers derive standing from a civilian knowledge industry, but exporting that capability exposes them to the regulatory and reputational pressure of larger powers. The class examines the Israeli case against US and EU export-control regimes, and asks when a state's technological advantage translates into influence and when it becomes a liability. * <u>Part of the time will be dedicated to student presentations.</u>
9. (25/12/26)	International Cooperation in Space: Shared Platforms and Chokepoints As activity in space expands, more states share satellite infrastructure out of necessity, and in doing so become sensitive to their partners or dependent on them. The class examines technological cooperation between states, the gap between legal instruments and control over the technical chokepoints of the platform, and how system architecture creates those chokepoints in the first place. * <u>Part of the time will be dedicated to student presentations.</u>
10. (01/01/27)	Commercial Chokepoints: Private Infrastructure and State Autonomy in Conflict States increasingly conduct security operations on infrastructure they do not own: cloud services, connectivity, and data platforms supplied by a handful of firms. The class asks who holds the control points when the provider is commercial rather than sovereign, drawing on the war in Ukraine, Israel, and Taiwan scenarios, and what this leaves of the regulatory tools discussed earlier in the course. * <u>Part of the time will be dedicated to student presentations.</u>
11. (08/01/27)	Regimes Without Verification: The Problem of Not Knowing Arms control has always depended on verification: states could count missiles, inspect facilities, and confirm that others were keeping their commitments. In cyberspace nothing of the kind exists. Capabilities are software, they are kept secret, and their use is often discovered late or not at all — and the same is true of the shared technological infrastructure discussed in the previous classes. The class asks how states are supposed to cooperate, deter, and build regimes when they cannot verify what others hold or what they have already done, and revisits the substitutes for verification that appeared throughout the course: non-binding norms, public attribution, export controls, and architectural separation.



Full Syllabus



	* <u>Part of the time will be dedicated to student presentations.</u>
12. (15/01/27)	This class will be dedicated to individual consultations, providing academic guidance and feedback on students' final papers. <u>Final paper topics must be approved prior to submission.</u>

Required course reading

Class #1

Petersen, Niels. How Rational is International Law?. *European Journal of International Law* 20.4 (2009): 1247-1262.

Class #2

Johnson, J. (2021). The end of military-techno *Pax Americana*? Washington's strategic responses to Chinese AI-enabled military technology. *The Pacific Review*, 34(3), 351–378.
<https://doi.org/10.1080/09512748.2019.1676299>

Class #3

Waddell, S., et al. (2024). Charting Digital Domain: The US's Evolving Approach to Cyberspace and Critical Infrastructure." *Security and Intelligence*, 9(1).

Class #4

- Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur?. *International Affairs*, 100(6), 2419–2440 .
- Singh, N. K., et al. (2025). Navigating the nexus: US-China cyber strategic competition. *Cogent Social Sciences*, 11(1).

Class #5

Hassid, N., & Matania, E. (2024). A global regime for cybersecurity and the obstacles to future progress. *Global Governance*, 30(1), 13–40.

Class #6

Zaad, V., & Christou, G. (2024). The new geopolitics of EU cybersecurity: Security, economy and digital sovereignty. *International Affairs*, 100(6), 2379–2398.

Class #7

- Radanliev, P. (2024). *Journal of Cyber Security Technology*, 9(1), 28–78.
- Nye, J. S. (2014). *The regime complex for managing global cyber activities*. Belfer Center.

Class #8

Hassid, N., & Matania, E. (2024). "Civilian knowledge industries and the ascendance of small and medium-sized states in world politics." *Humanit Soc Sci Commun*, 11, 1394.

Full Syllabus



Class #9

Keohane, R. O., & Nye, J. S. (1977). *Power and Interdependence: World Politics in Transition*. Little, Brown. Ch. 1, "Interdependence in World Politics" (Chapter 1, pp. 11–19)

Class #10

Javadi, M. (2025). Infrastructural entanglement and cloud hyperscalers in contemporary warfare: Insights from Ukraine, Israel and Taiwan. *Contemporary Security Policy*. doi:10.1080/13523260.2025.2593247

Class #11

Oppenheimer, H. (2024). How the process of discovering cyberattacks biases our understanding of cybersecurity. *Journal of Peace Research*, 61(1), 28–43. doi:10.1177/00223433231217687

Optional course reading

Class #11

Dunn Cavelty, M., Pulver, T., & Smeets, M. (2024). The evolution of cyberconflict studies. *International Affairs*, 100(6), 2317–2339.

Comments

The course website will be used to post updates, announcements, and supplementary learning materials throughout the term.