CYBER STRATEGY AND CYBER WARFARE

GINS 4090 Section B

Fall 2025

Carleton University

Kroeger College of Public Affairs

Bachelor of Global and International Studies

Seminar:
Wednesdays, 8:30 a.m. – 11:30 a.m.
See Brightspace for location

Instructor:
Tyler Welch
TylerWelch4@cunet.carleton.ca
Dunton Tower 2120
office hours

COURSE DESCRIPTION

This course explores how cyber strategy and cyber warfare impact international affairs. It tells the story of the development of global cyber capabilities ranging from early cyber weapons like Stuxnet, all the way to present-day cyber threats from actors such as the PRC's Volt Typhoon and anti-Western non-state cyber groups.

It also details the ways in which state cyber programs deploy cyber tools for espionage, sabotage, disruption, and destruction – even including kinetic cyber weapons and cyber-enabled information operations. Finally, it will survey the specific roles played by (and the perspectives held by) state intelligence agencies, organized military units, cybercriminals, and politically motivated hacktivists. We will also explore the ecosystem of high-tech researchers, front companies, and private sector firms that underpin the global cyber threat environment.

LEARNING OUTCOMES

By the end of the course, students will be able to:

- **Explain the evolution of global cyber capabilities**
    - Trace developments from early cyber weapons (e.g., *Stuxnet*) to contemporary threats by state and non-state actors.
    - Define core concepts in cyber strategy such as espionage, sabotage, disruption, and cyber-enabled influence operations.

- **Analyze the objectives, actors, and contexts of cyber operations**
    - Compare the motives, methods, and structures of state, criminal, and hacktivist groups.
    - Examine how geopolitical, economic, and strategic considerations shape cyber campaigns.

- **Evaluate the roles and capabilities of key organizations**
  - Assess the functions and limitations of intelligence agencies, military units, and private-sector actors in offensive and defensive cyber operations.
  - Identify the influence of the wider cyber ecosystem, including researchers, front companies, and technology suppliers.

- **Interpret and assess real-world case studies**
  - Link technical execution to strategic and political outcomes in major cyber incidents.
  - Weigh ethical and policy implications of cyber weapon use and defense.

- **Communicate informed perspectives on cyber strategy**
  - Synthesize strategic and geopolitical insights.
  - Present clear, persuasive analyses in written and oral formats.
-

TEXTS AND COURSE MATERIALS

The core texts for this course are books and journal articles that are all available online via the Carleton MacOdrum Library OMNI system and academic databases. All other course materials are openly available on the internet, usually with a link provided in the syllabus.

COURSE CALENDAR – OVERVIEW

Week 1 – September 3rd – Welcome, Introductions, Outline Review

Week 2 – September 10th – Introduction to Cyber Strategy and Cyber Warfare

Week 3 – September 17th – "Year Zero" and the Origins of Modern Cyberspace

Week 4 – September 24th – Espionage

Week 5 – October 1st – No class

Week 6 – October 8th – Cyber Sabotage, and Cyber-Enabled Influence Operations

Week 7 – October 15th – Disruptions, Destruction, Cyber Weapons, and Hybrid Warfare

Week 8 – October 22nd – Fall Break, no classes

Week 9 – October 29th – State Cyber Programs (Intelligence and Military)
* Research Paper Proposal Due

Week 10 – November 5th – Non-State Actors (Hacktivists and Cybercriminals)

Week 11 – November 12th – The Private Sector and National Cyber Ecosystems

Week 12 – November 19th – Contemporary Cyber Threats

Week 13 – November 26th – The Future of Cyber Strategy and Warfare
*Research Paper Due

Week 14 – December 3rd – Guest Speaker: Working in cyber and national security

EVALUATION

- **Seminar Participation (40%) – ongoing**
  Seminar attendance is expected and attendance will be taken. The participation grade will reflect the extent to which students contribute to class discussions in an informed and critical manner, not only attendance. Participants are expected to arrive each week having completed the readings and prepared to discuss the material.

- **Seminar Icebreaker (20%) – ongoing**
  Each week one or more students will each give a 10-12 minute presentation meant to kick-off that week's session. The presentation will be on a topic of the student's choosing but must relate to the subject of that week's discussion. It can be a breakdown of a case study, an exploration of a complicated legal/ethical issue, or anything analytically interesting to the student.

  The student will then lead a short discussion among the class by coming up with engaging discussion questions, reflecting back on the content from previous weeks, and walking the class through the discussion.

- **Research Paper Proposal (10%) – due Week 9**
  Students will write a 1-3 page proposal and abstract in anticipation of the main research paper or project. The proposal should display the ability to weave ideas together from across the syllabus, and the pursuit of interesting primary and secondary sources. The proposal should include a short description, a tentative thesis, and a bibliography.

- **Research Paper (30%) – due Week 13**
  Students will write an 8-13 page research paper on one aspect/theme/trend of the historical, present-day, or future cyber threat environment.

Final Grade Approval: Standing in a course is determined by the course instructor subject to the approval of the Faculty Dean. This means that grades submitted by the instructor may be subject to revision. 4 No grades are final until they have been approved by the Dean.

Submitting Work: Always keep a copy of all essays, term papers, written assignments, or take-home tests submitted in your courses. You may be asked to submit drafts and rough notes, or to re-submit work for evaluation or for extension requests.

- *Submission of Term Work***:** Upload assignments to Brightspace. All assignments are due by 11:59 p.m. unless otherwise specified. If the assignment portal has closed we are under no obligation to accept emailed assignments. Please do not email late assignments without contacting the Instructor first**.**

- *Late penalties***:** Late assignments will receive a -5% deduction for the first day, -5%/day thereafter, weekends count as one day. Please see extension policy below.

- *Policy on Extensions*: Extensions are granted solely at the discretion of the Instructor. While medical notes, appeals from the Registrar and PMC, etc., may be considered, please note that extensions are not guaranteed.

STATEMENT OF ACADEMIC INTEGRITY

- The University Academic Integrity Policy defines plagiarism as "*presenting, whether intentionally or not, the ideas, expression of ideas or work of others as one's own."* This includes reproducing or paraphrasing portions of someone else's published or unpublished material, regardless of the source, and presenting these as one's own without proper citation or reference to the original source. Examples of sources from which the ideas, expressions of ideas or works of others may be drawn from include but are not limited to: books, articles, papers, literary compositions and phrases, performance compositions, chemical compounds, art works, laboratory reports, research results, calculations and the results of calculations, diagrams, constructions, computer reports, computer code/software, material on the internet and/or conversations. Examples of plagiarism include, but are not limited to:
    - any submission prepared in whole or in part, by someone else, including the unauthorized use of generative AI tools (e.g., ChatGPT);
    - using ideas or direct, verbatim quotations, paraphrased material, algorithms, formulae, scientific or mathematical concepts, or ideas without appropriate acknowledgment in any academic assignment;
    - using another's data or research findings without appropriate acknowledgement;
    - submitting a computer program developed in whole or in part by someone else, with or without modifications, as one's own; and
    - failing to acknowledge sources through the use of proper citations when using another's work and/or failing to use quotations marks.
- Plagiarism is a serious offence that cannot be resolved directly by the course's instructor. The Associate Dean of the Faculty conducts a rigorous investigation, including an interview with the student, when an instructor suspects a piece of work has been plagiarized. Penalties are not trivial. They can include a final grade of "F" for the course or even suspension or expulsion from the University.

USE OF AI TOOLS

- Students may use technology, including generative artificial intelligence tools, to contribute to their understanding of course materials.

- Students may use artificial intelligence tools, including generative AI, in this course as learning aids. However, students are ultimately accountable for the work they submit. Students will be responsible for any errors or omissions provided by the tool.
- Students may choose to use generative artificial intelligence tools as they work through the assignments in this course; this use must be documented in an appendix for each assignment. The documentation should include what tool(s) were used, how they were used, and how the results from the AI were incorporated into the submitted work, and a list of all prompts used.
- Students must also include a short reflection describing how they made use of generative artificial intelligence tools for each assignment
- Any content produced by an artificial intelligence tool must be cited appropriately. Many organizations that publish standard citation formats are now providing information on citing generative AI
- The instructor reserves the right to ask students to explain their process for creating their assignment.
- As a result, this course purposefully prioritizes evaluations that are based on demonstrating a depth of thinking, preparation, and the ability to communicate and engage with ideas.

INTELLECTUAL PROPERTY

Student or professor materials created for this course (including presentations and posted notes, labs, case studies, assignments and exams) remain the intellectual property of the author(s). They are intended for personal use and may not be reproduced or redistributed without prior written consent of the author(s). I maintain the copyright to all course materials; they may not be posted, uploaded, transferred, or sold without my express written consent in advance.

COURSE COMMUNICATIONS

All email communication to students from BGInS will be via official Carleton university e-mail accounts and/or Brightspace. As important course and University information is distributed this way, it is the student's responsibility to monitor their Carleton email and Brightspace accounts.

STUDENT MENTAL HEALTH

As a student you may experience a range of mental health challenges that significantly impact your academic success and overall well-being. If you need help, please speak to someone. There are numerous resources available both on- and off-campus to support you. For more information, please consult https://wellness.carleton.ca/

Emergency Resources (on and off campus)

- Crisis/Urgent Counselling Support: 613-520-6674 (Mon-Fri, 8:30-4:30)
- Suicide Crisis Helpline: call or text 9-8-8, 24 hours a day, 7 days a week.
- For immediate danger or urgent medical support: call 9-1-1

Carleton Resources

- Mental Health and Wellbeing: https://carleton.ca/wellness/
- Health & Counselling Services: https://carleton.ca/health/
- Paul Menton Centre: https://carleton.ca/pmc/

- Academic Advising Centre (AAC): https://carleton.ca/academicadvising/
- Centre for Student Academic Support (CSAS): https://carleton.ca/csas/
- Equity & Inclusivity Communities: https://carleton.ca/equity/

Off Campus Resources

- Distress Centre of Ottawa and Region: call 613-238-3311, text 343-306-5550, or connect online at https://www.dcottawa.on.ca/
- Mental Health Crisis Service: call 613-722-6914 or toll-free 1-866-996-0991, or connect online at http://www.crisisline.ca/
- Good2Talk: call 1-866-925-5454 or connect online at https://good2talk.ca/
- The Walk-In Counselling Clinic: for online or on-site service https://walkincounselling.com

ACADEMIC ACCOMODATIONS

Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes, including information about the Academic Consideration Policy for Students in Medical and Other Extenuating Circumstances, are outlined on the Academic Accommodations website (students.carleton.ca/course-outline)

WEEKLY SYLLABUS

Week 1 – September 3rd – Welcome, Introductions, Outline Review

Week 2 – September 10th – Introduction to Cyber Strategy and Cyber Warfare
Topic: Defining key concepts and context

Readings:

- Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. **Chapter 1: The Hacked World Order**
- Perkovich, G., & Levite, A. E. (Eds.). (2017). *Understanding cyber conflict: 14 analogies*. Georgetown University Press. **Introduction.**
  - o (Available via the Carnegie Endowment)
- S&P Global. (n.d.). *What is cyber warfare?* S&P Global. https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk/cyber-warfare
- *Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939*

Week 3 – September 17th – "Year Zero" and the Origins of Modern Cyberspace
Topic: The development of cyber tools in statecraft. Stuxnet as a case study**.**

Readings:

- Review Segal Chapter from last week

- Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown. **Chapter 1 and 2.**
- Perkovich, G., & Levite, A. E. (Eds.). (2017). *Understanding cyber conflict: 14 analogies*. Georgetown University Press. **Chapter 4: Cyber, Drones, and Secrecy.**
    - o (Available via the Carnegie Endowment)
- **(*Optional*)** Lindsay, J. R. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. *Journal of Strategic Studies*. Advance online publication. https://doi.org/10.1080/01402390.2025.2481447

Week 4 – September 24th – Espionage
Topic: How states use cyber tools for espionage and intelligence gathering

Readings:

- Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. **Chapter 5: Everybody Spies**
- BBC News. (2023, May 23). *Inside the Salt Typhoon cyber espionage campaign targeting critical infrastructure*. https://www.bbc.com/news/articles/c86w2evj05do
- Baker, K. (2025, January 16). *What is cyber espionage?* CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/
- Proofpoint. (2021, July 19). *I knew you were trouble: TA456 targets defense contractor with alluring social media persona*. Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media
- U.S. Department of Justice. (2019, November 7). *Two former Twitter employees and a Saudi national charged as acting as illegal agents of Saudi Arabia*. https://www.justice.gov/archives/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia

Week 5 – October 1st – No class

Week 6 – October 8th – Cyber Sabotage, and Cyber-Enabled Influence Operations
Topic: Case studies of cyber sabotage and the role of cyber tools in influence operations and democratic interference.

Readings:

- Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. **Chapter 7: Let Slip the Twitter Followers of War.**
- Microsoft Threat Intelligence. (2024, February 26). *Iran surges cyber-enabled influence operations in support of Hamas*. Microsoft Security Insider. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas

- Brangetto, P., & Veenendaal, M. A. (2016). *Influence cyber operations: The use of cyberattacks in support of influence operations*. In N. Pissanidis & H. Rõigas (Eds.), *Cyber Power: Proceedings of the 8th International Conference on Cyber Conflict* (pp. 422–?). NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf
- Perkovich, G., & Levite, A. E. (Eds.). (2017). *Understanding cyber conflict: 14 analogies*. Georgetown University Press. **Chapter 5: Cyber War and Information War a la Russe.**
  - (Available via the Carnegie Endowment)
- ***(Optional)*:** Whyte, C. (2025). The subversion aversion paradox: Juxtaposing the tactical and strategic utility of cyber-enabled influence operations. *Journal of Global Security Studies, 10*(2), Article ogaf006. https://doi.org/10.1093/jogss/ogaf006

Week 7 – October 15th – Disruptions, Destruction, Cyber Weapons, and Hybrid Warfare

Topic: Cyber in the physical world, the integration of cyber tools into military operations.

Readings:

- Perkovich, G., & Levite, A. E. (Eds.). (2017). *Understanding cyber conflict: 14 analogies*. Georgetown University Press. **Chapter 9: Why a Digital Pearl Harbor Makes Sense… and is Possible.**
  - (Available via the Carnegie Endowment)
- Canadian Centre for Cyber Security. (2022, June 22). *Cyber Threat Activity related to the Russian invasion of Ukraine*. Government of Canada. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf
- Greenberg, A. (2022, May 12). *The case for war crimes charges against Russia's Sandworm hackers*. WIRED. https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/
- Halpern, S. (2019, July 18). *How cyber weapons are changing the landscape of modern warfare*. *The New Yorker*. https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare

Week 8 – October 22nd – Fall Break, no classes

Week 9 – October 29th – State Cyber Programs (Intelligence and Military)

Topic: The elements of a successful state cyber program

Readings:

- Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs. **Chapter 2: The Anatomy of Cyber Power.**
- Canadian Centre for Cyber Security. (2025). *National Cyber Threat Assessment 2025–2026*. Government of Canada.

https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026 **Page 10, especially Figure 1: State cyber program ecosystem.**
- Voo, J., Hemani, I., & Cassidy, D. (2022, September). *National Cyber Power Index 2022*. Cyber Project, Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

Week 10 – November 5th – Non-State Actors (Hacktivists and Cybercriminals)
Topic: The roles and impacts of hacktivists and cybercriminals in the cyber threat environment

Readings:

- Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press. https://doi.org/10.1017/9781108569308 **Chapters: Cyber Proxies: an Introduction; Cyber Proxies on a Loose Leash : Iran and Syria**
- Canadian Centre for Cyber Security. (2025). *National Cyber Threat Assessment 2025–2026*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026 **Section on Cybercrime Threats.**
- Greenberg, A. (2025, April 14). *CyberAv3ngers: The Iranian saboteurs hacking water and gas systems worldwide*. WIRED. https://www.wired.com/story/cyberav3ngers-iran-hacking-water-and-gas-industrial-systems/
- Silobreaker. (2025, July 13). *Hacktivism in the Israel-Iran conflict*. https://www.silobreaker.com/blog/geopolitical/hacktivism-in-the-israel-iran-conflict/
- Miller, M. (2023, October 15). *How hackers piled onto the Israeli-Hamas conflict*. Politico. https://www.politico.eu/article/israel-hamas-war-hackers-cyberattacks/

Week 11 – November 12th – The Private Sector and National Cyber Ecosystems
Topic: How the private sector enables and hinders cyber strategy and cyber warfare

Readings:

- Farrow, R. (2022, April 18). *How democracies spy on their citizens*. *The New Yorker*. https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
- Amnesty International. (2021, July 18). *The Pegasus Project: How governments use NSO spyware to target activists*. Amnesty International. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/
- Mozur, P. et al (2024, February 22). *China's leaked files expose internal struggles and secrets*. *The New York Times*. https://www.nytimes.com/2024/02/22/business/china-leaked-files.html
- Knockel, J., Kato, K., & Dirks, E. (2023, April 26). *Missing links: A comparison of search censorship in China* (Citizen Lab Research Report No. 166). University of Toronto—Citizen Lab. https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/
- Canadian Centre for Cyber Security. (2025). *National Cyber Threat Assessment 2025–2026*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026 **Trend 4:**

Vendor concentration is increasing cyber vulnerability and Trend 5: Dual-use commercial services are in the digital crossfire

- **Optional**: "Mythical Beasts and where to find them." A project from The Atlantic Council.

Week 12 – November 19th – Contemporary Cyber Threats

Topic: The "Big Four", emerging states, VOLT TYPHOON and beyond.

Readings:

- Canadian Centre for Cyber Security. (2025). *National Cyber Threat Assessment 2025–2026*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026. **Section 1 - Cyber Threat from State Adversaries**
- Forno, R. (2024, April 1). *What is Volt Typhoon? A cybersecurity expert explains the Chinese hackers targeting US critical infrastructure*. UMBC Stories. University of Maryland, Baltimore County. https://umbc.edu/stories/what-is-volt-typhoon-a-cybersecurity-expert-explains-the-chinese-hackers-targeting-us-critical-infrastructure/
- National Cyber Security Centre. (2023, November 14). *Case study: Russia – an acute and chronic cyber threat*. In *Annual Review 2023*. National Cyber Security Centre. https://www.ncsc.gov.uk/collection/annual-review-2023/threats-risks/case-study-russia
- Hakala, J., & Melnychuk, J. (2021, June). *Russia's strategy in cyberspace* (NATO StratCom CoE). NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf **Section on "Activities in Cyberspace"**

Week 13 – November 26th – The Future of Cyber Strategy and Warfare

Topic: Emerging trends, technologies, and challenges

Readings:

- Canadian Centre for Cyber Security. (2025). *National Cyber Threat Assessment 2025–2026*. Government of Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026. **Section 3 - Trends Shaping Canada's Cyber Threat Landscape**
- Humble, K. (2024, July 12). *War, artificial intelligence, and the future of conflict*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/
- Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing. **Epilogue**.

Week 14 – December 3rd – Guest Speaker: Working in cyber and national security