EURR 4201A/5201A / PSCI 4801B/5915B

Russia and The West: Hybrid Warfare and Transatlantic Security

Draft Course Outline

Fall 2025

Thursdays 11:30-14:30; check location on Carleton Central

Institute of European, Russian and Eurasian Studies (EURUS), Carleton University

Instructor: Dr. Mikhail A. Polianskii

Office: 3315 Richcraft Hall
Office Hours: Thursdays, 14.30-15.30. Other times available via appointment (in person or online).
Email: MikhailPolianskii@cunet.carleton.ca

Course Description:

This course provides an in-depth analysis of Russia's hybrid warfare tactics and their implications for transatlantic security. In the current era of evolving conflict, Moscow employs a sophisticated blend of active measures (*aktivnye meropriyatiya*), including cyber disruption, targeted disinformation, deepfakes, proxy mobilization, economic coercion, and covert sabotage, to challenge the transatlantic security architecture. These methods are deliberately designed to undermine collective defense mechanisms and blur the distinction between peace and war, compelling the West to formulate effective counterstrategies.

Through a rigorous examination of Russia's doctrine and operational techniques, the course utilizes case studies from various geographical settings and domains, offering students a comprehensive understanding of contemporary hybrid warfare. The curriculum integrates memoirs and firsthand accounts from Soviet and Russian intelligence operatives with expert literature and official documents, promoting an evidence-based analysis of Russian operations. Students will develop essential methodological skills by applying diverse analytical approaches to assess and anticipate Russian strategies.

Delivered through a combination of lectures, interactive seminars, and collaborative projects, this course enables participants to explore modern Russian hybrid operations and evaluate strategic countermeasures available to Western countries. Ultimately, the course sharpens analytical abilities and strategic insight, fostering a deep, nuanced understanding of today's complex and multifaceted security challenges.

Preclusions

This course has no preclusions.

Learning Outcomes

This course equips students with the conceptual, strategic, and methodological foundations needed to analyse—and counter—Russia's hybrid warfare campaigns. After mapping the intellectual debates on "hybrid" and "gray-zone" conflict, participants will dissect the full spectrum of Russian coercive instruments (cyber, disinformation, proxy forces, economic leverage, legal warfare) across various regions (Europe, the Arctic etc.) and the Western responses built around deterrence, resilience, and competitive statecraft. Case-driven seminars, in-class discussions and presentations will cultivate the analytic dexterity and strategic judgement demanded of contemporary security professionals. Drawing on varied disciplinary lenses—from strategic studies and intelligence analysis to sociology, economics, and international relations—the module encourages participants to capitalise on their own interdisciplinary backgrounds while honing evidence-based policy skills.

By the end of the module, students will therefore be able to demonstrate:

- a sophisticated grasp of the concept of hybrid warfare and its relevance to Russia-West strategic competition;
- detailed knowledge of Russian doctrine, operational practice, and regional case studies spanning Europe, the Arctic, and the Global South;
- an ability to integrate qualitative and quantitative methods (OSINT, cyber forensics, scenario planning) in analysing hybrid threats;
- critical insight into the political, legal, and ethical challenges of crafting deterrence and resilience policies for NATO and the EU;
- proficiency in producing clear, policy-oriented outputs (briefing memos, group presentations);
- confidence in leading and contributing to structured debates, simulations, and negotiations that mirror real-world decision environments;
- a capacity to translate strategic analysis into actionable recommendations that strengthen transatlantic security in the face of evolving hybrid tactics.

Overview:

Thematically, the course is organized in two halves: Part I covers conceptual, doctrinal, and operational foundations of Russian hybrid conflict, and Part II explores regional and thematic case studies. Throughout the course, students will engage in active learning – debates, simulations, and policy exercises – to foster strategic thinking and policy analysis skills. Assessments include policy memos, group presentations, and short papers tied to each block's themes.

Date	**Theme**
Part I: Foundations of Russian Hybrid Warfare	
09/04	1. Introduction. The Hybrid Conflict Landscape: Concepts & Theory
09/11	2. Learning from History? From Soviet "Active Measures" to Modern Adaptations
09/18	3. Modern Russian Strategy and Doctrine: "Non-linear Warfare" and Beyond
09/25	4. Disinformation and Influence Operations (Information Warfare)
10/02	5. Cyber and Technological Warfare
10/09	6. Sabotage, and Subversion: Plausible Deniability in Action?
10/16	7. (Counter-)Intelligence and Methodologies for Analysis of Hybrid Threats
10/23	*8. Fall Break – Reading Week*
Part II: Regional & Thematic Case Studies	
10/30	9. Ukraine: War on Two Fronts
11/06	10. Resilience and Adaptation in Europe's Hybrid Battlespace
11/13	11. The High North and the Arctic: New Strategic Frontier
11/20	12. Africa, Middle East and the Global South
11/27	13. NATO and Allied Responses: Counter Hybrid Warfare?
12/04	14. The Endgame? Navigating Strategic Competition with Russia

Readings

Texts will be made available through Brightspace. Due to the very vibrant political context, assigned readings might change. A comprehensive list of core and additional readings is provided below. Students are not required to purchase textbooks or other learning materials for this course.

Preparation

Read the core texts. Follow up on different sources.

You are strongly encouraged to keep up to date with the latest developments in Russian-Western relations following reputable news sources from around the world of your choosing. In addition to following the news, it is advised to regularly read sources of analysis from Russia.[1] These include, but not limited to

Russian Media, Journals and Think-tanks: Meduza, Carnegie Politika, Novaya Gazeta Europe, The Insider, Russia in Global Affairs (Journal), Russian International Affairs Council (Think-Tank); Valdai (Think-Tank) *In Russian only*: Kommersant, Vedomosti, RBK, TASS, Nezavisimaya Gazeta, Vyorstka Media.

Podcasts: In Moscow's Shadows (Mark Galeotti), Carnegie Politika Podcast (Sasha Gabuev), The Naked Pravda (Kevin Rothrock at Meduza); War on the Rocks (Ryan Evans/Michael Kofman/Dara Massicot).

X(ex-Twitter)-Accounts[2]: @KofmanMichael, @RALee85, @CooleyOnEurasia, @jakluge, @sguriev, @kirlant, @AndrKolesnikov, @baunov, @KadriLiik, @Stanovaya, @ElenaChernenko, @christogrozev, @BBCSteveR; @irgarner; @olliecarroll

Requirements and Grading

Undergraduate Students:

Class Participation 25%
Oral Presentation 20%
Feedback Papers 20%
Term Paper 35%

Graduate Students:

Class Participation 30%

[1] The recommended list of Russian media, journals, and think tanks encompasses a wide ideological spectrum. It includes sources known for their independent or critical stance (such as Meduza and The Insider) as well as prominent state-affiliated outlets and think tanks (like TASS and the Valdai Club). The purpose of providing this range is to expose students to the different sides of contemporary debates and encourage a critical analysis of the Russian information landscape.
[2] The listed accounts are primarily referenced via Twitter/X because this remains the most active and consistent platform for their commentary and analysis. While some of these individuals or institutions may also maintain a presence on platforms like Bluesky or Mastodon, their Twitter/X feeds typically still offer the most up-to-date content. If you prefer alternative platforms, it's worth searching for their profiles there—but be aware that posting frequency and content may vary.

Oral Presentation 15%
Feedback Papers 20%
Term Paper 35%

Oral Participation and Attendance Policy

Active participation is a central component of this course and will play a significant role in your final grade (see above). Success in this class depends not only on completing the readings and assignments but also on engaging thoughtfully during in-class discussions.

Attendance is mandatory, and classes will not be recorded or made available online. Unexcused absences will affect your participation grade. Specifically, each absence without a valid explanation will result in a deduction from your overall participation score. Please make every effort to attend consistently, as repeated absences can significantly impact your final grade.

While very occasional insignificant lateness is understandable, frequent or extended late arrivals may negatively affect your participation grade, especially if they disrupt the flow of the class or result in missing key discussions.

Use of mobile phones, browsing unrelated content, or other disruptions during class will also be considered when determining your participation mark. Students who demonstrate particular focus and engagement during class will receive a 10% bonus on their participation grade as a recognition of their activity

In cases of valid reasons (limited to one or two occasions), students may have the opportunity to make up participation credit by submitting a brief reflection paper on the week's readings (200 – 300 words).

Participation will be assessed based on both attendance and the quality of your engagement. Strong participation involves being attentive, contributing meaningfully to discussion, demonstrating knowledge of the readings, and offering thoughtful analysis of the topics at hand.

Presentations

Students will be allocated into team of 2-3 people. Each student team will give one presentation (approx. 12–17 minutes) during the semester as an introduction to the class discussion (usually in the beginning of the second half of the class). For some topics, two presentations may be scheduled together. Students will be randomly assigned to teams in the first week, along with a list of possible topics. You can slightly change/adapt the topic of your presentation by coordinating with the course instructor.

Presentations should be ideally based on a research question (i.e. "Why" type of questions)—to encourage analytical thinking and discussion. Topics will focus on debates around Russian hybrid warfare, its forms and ways to counter them.

Please structure your presentation according to the criteria outlined in the table below, which covers the introduction, main body, and conclusion—focusing on clarity, structure, relevance to the research question, and engagement with the topic. The assessment criteria of presentations are also listed below.

Introduction	**35**
Definition of the topic/justification of the time frame/definition of terms	20
Relevant research question	15
Main body	**35**
Logical structure of the argument/well-structured	30
Examples	5
Conclusion	**30**
Relevance to the research question posed	15
Appropriateness of the conclusions to the content	10
Suggestions for further research on the topic	5
Total	**100**

Feedback Papers

To deepen engagement with course content, students are required to submit two feedback papers over the semester (in total they account for 20% of the final note). These short papers offer space for critical reflection on individual sessions and help consolidate understanding through analytical writing. You may choose which sessions to reflect on, ideally those most relevant to your interests or ongoing work.

Each paper (ca. 1000 words) may address the following points:

1. Session Summary

Briefly summarize the key themes, concepts, actors, or cases discussed. How does the session fit into the broader structure of the course?

2. Critical Reflection on the content of the session

- What did you find most compelling or problematic?
- Were there arguments or interpretations you disagreed with? Why?
- How did the material challenge or reinforce your understanding?

3. Questions and Further Inquiry

- Identify open questions or areas you would like to explore further.
- What remains unclear or contested?
- How might the topic relate to current events, your research interests, or policy debates?

Term paper

The term paper accounts for 50% of the final course grade and should take the form of a traditional written essay. Students are welcome to further develop the topic their presented on during the semester or select a new one—just be sure to check with the course leader if choosing a different topic.

Length requirements:

- Undergraduate students: 3,500–4,500 words
- Graduate students: 5,000–6,000 words
  (Word count includes references)

Formatting guidelines:

- Font: Times New Roman, size 12
- Line spacing: 1.15 -1.5
- No cover sheet
- Include the word count at the top of the first page

Papers will be assessed based on the quality of the research question, structure and clarity of argument, engagement with relevant literature, and the ability to critically analyze the topic.

Syllabus

September 4 (week 1): Introduction. The Hybrid Conflict Landscape: Concepts & Theory

1. What defines "hybrid warfare," and how does it differ from conventional or insurgent warfare? What are the key definitional debates surrounding this term?
2. How have scholars and analysts critiqued or refined the concept of hybrid warfare since its emergence? What happened after 2014?
3. Is hybrid warfare inherently an autocratic tool against democracies? Are democracies *a priori* more vulnerable to hybrid threats?
4. What are the analytical and policy implications of different conceptual approaches to hybrid warfare?

Core Readings:

- Hoffman, F. G. (2009). Hybrid warfare and challenges. Joint Force Quarterly, 52(1), 34-48.
- Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. Journal of Strategic Studies, 46(4), 858-880.
- Wither, J. K. (2023). Hybrid warfare revisited: A battle of 'buzzwords'. Connections, 22(1), 7-27.

Additional Readings:

- Atkinson, C. (2018). Hybrid warfare and societal resilience: Implications for democratic governance. *Information & Security*, *39*(1), 63–76.
- Sahin, K. (2016). Liberal democracies hybrid war. *International Institute for Strategic Studies*. https://www.iiss.org/online-analysis/military-balance/2016/12/liberal-democracies-hybrid-war/
- Polyakova, A., & Boyer, S. P. (2018). The future of political warfare: Russia, the West, and the coming age of global digital competition. *Brookings Institution*. https://www.brookings.edu/articles/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/

September 11 (week 2): Learning from History? From Soviet Active Measures to Modern Adaptations

1. Is hybrid warfare a new phenomenon?
2. What were the techniques and objectives of Soviet active measures during the Cold War?
3. Which elements of Soviet-era active measures remain influential in modern Russian practice?
4. What lessons do historical counter-disinformation campaigns offer for today's defense strategies?

Core Readings:

- Gioe, D. V., Lovering, R., & Pachesny, T. (2020). The Soviet legacy of Russian active measures: New vodka from old stills? International Journal of Intelligence and Counterintelligence, 33(3), 514–539.
- Bittman, L. (1984). The KGB and Soviet disinformation: An insider's view (Ch. 1 & Epilogue). Pergamon-Brassey's.
- Romerstein, H. (2001). Disinformation as a KGB weapon in the Cold War. Journal of Intelligence History, 1(1), 54–67.

Additional Readings:

- Haynes, J. E., & Klehr, H. (2024). "Operation Snow": A history-changing Soviet "agent of influence" success or KGB propaganda? International Journal of Intelligence and CounterIntelligence. https://doi.org/10.1080/08850607.2024.2408647
- Hosaka, S. (2022). Repeating history: Soviet offensive counterintelligence active measures. International Journal of Intelligence and CounterIntelligence, 35(3), 429–458.
- USIA. (1992). Soviet active measures in the "post-Cold War" era 1988–1991. United States Information Agency. http://intellit.muskingum.edu/russia_folder/pcw_era/index.htm
- Kalugin, O. (2009). Spymaster: My thirty-two years in intelligence and espionage against the West (Introduction Chapter Only). Basic Books

September 18 (week 3): Modern Russian Strategy and Doctrine: "Non-linear Warfare" and Beyond

1. What is the "Gerasimov Doctrine," and how accurately does this concept capture Russian military thinking and strategic planning?
2. Does Russia have a comprehensive hybrid warfare strategy?
3. How do Russian conceptions of "non-linear warfare" differ from Western understandings of hybrid conflict?
4. How does the hybrid warfare connect to Russia's broader geopolitical objectives?

Core Readings:

- Gerasimov, V. (2013). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. Military Review (translated by Robert Coalson), January–February 2016, 23–29. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

- Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? Small Wars & Insurgencies, 27(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170
- Fabian, S. (2019). The Russian hybrid warfare strategy – Neither Russian nor strategy. Defense & Security Analysis, 35(3), 308–325.
- Pynnöniemi, K., & Jokela, M. (2020). Perceptions of hybrid war in Russia: Means, targets and objectives identified in the Russian debate. Cambridge Review of International Affairs, 33(6), 828–845.

Additional Readings:

- Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. Small Wars & Insurgencies, 32(3), 415–440.
- Galeotti, M. (2019). Russian political war: Moving beyond the hybrid (Intro & Part IV only). Routledge.
- Burkholder, R. (2023). Tackling Russian gray zone approaches in the post–Cold War era. Journal of Advanced Military Studies, 14(2), 151–157.
- Polianskii, M. (2024). Russian foreign policy research and war in Ukraine: Old answers to new questions? Communist and Post-Communist Studies, 57(2), 156–172. https://doi.org/10.1525/cpcs.2024.2112378

September 25 (week 4): Disinformation and Influence Operations (Information Warfare)

1. What techniques characterize modern Russian disinformation campaigns?
2. Do historical narratives and memory politics amplify or blunt Russian disinformation efforts?
3. Which countermeasures (fact-checks, platform policies, media literacy) can be successful against Russian disinformation?
4. How can policymakers balance rapid and resolute response to disinformation and fact-twisting with protection of free speech and media freedom?

Core Readings:

- Ivan, C., Chiru, I., & Arcos, R. (2023). Hybrid security threats and the information domain: Concepts and definitions. In Routledge Handbook of Disinformation and National Security (pp. 9-19). Routledge.
- Arribas, C. M., et al. (2023). Information manipulation and historical revisionism: Russian disinformation and foreign interference through manipulated history-based narratives. Open Research Europe, 3, 1–29. https://doi.org/10.12688/openreseurope.16087.1

- Rid, T. (2020). Active measures: The secret history of disinformation and political warfare (Chapter "What Is Disinformation?" (6-16)
- and "Century of Disinformation" (414-426)). Farrar, Straus and Giroux.
- Belogolova, O., Foster, L., Rid, T., & Wilde, G. (2024). Don't hype the disinformation threat. Foreign Affairs, May 3, 2024.
- Wagnsson, C., Hellman, M., & Hoyle, A. (2024). Securitising information in European borders: How can democracies balance openness with curtailing Russian malign information influence? European Security, 34(1), 127–147. https://doi.org/10.1080/09662839.2024.2321906

Additional Readings:

- Zilinsky, J., et al. (2024). Justifying an invasion: When is disinformation successful? Political Communication, 41(6), 965–986. https://doi.org/10.1080/10584609.2024.2352483
- Burda, R., & Bundzíková, V. (2025). Tailoring narratives on war in Ukraine: Cross-national study of Sputnik News. Nationalities Papers, 1–22. https://doi.org/10.1017/NPS.2024.89
- Jankowicz, N. (2024). The coming flood of disinformation. Foreign Affairs, February 7, 2024. https://www.foreignaffairs.com/united-states/coming-flood-disinformation

October 2 (week 5): Cyber and Technological Warfare

1. How do cyber operations integrate with Russian broader hybrid warfare strategies?
2. Why did Russian cyber operations in Ukraine not achieve the devastating effects many analysts predicted? What factors contributed to Ukrainian cyber resilience?
3. How emerging technologies (like AI) reshape cyber-hybrid tactics?
4. What are main challenges of responding to cyber-attacks?

Core Readings:

- Giles, K. (2023). Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine. Chatham House.
- Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Kolodii, R. (2024). Unpacking Russia's cyber-incident response. Security Studies, 33(4), 640–669. https://doi.org/10.1080/09636412.2024.2391757
- Neuberger, A. (2025). Spy vs. AI: How artificial intelligence will remake espionage. Foreign Affairs, January 15, 2025.
- Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.

- Zegart, A., Rovner, J., Warner, M., Lindsay, J., Maschmeyer, L., Fischerkeller, M. P., … & Kollars, N. A. (2023). Deter, disrupt, or deceive: Assessing cyber conflict as an intelligence contest. Georgetown University Press.
-

Additional Readings:

- Givens, A. D., Gorbachevsky, M., & Biernat, A. C. (2023). How Putin's cyberwar failed in Ukraine. Journal of Strategic Security, 16(2), 96–121. https://doi.org/10.5038/1944-0472.16.2.2099
- Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. Journal of Strategic Studies, 46(3), 570–594. https://doi.org/10.1080/01402390.2022.2104253
- Lin, H. (2022). Russian cyber operations in the invasion of Ukraine. Cyber Defense Review, 7(4), 31–46. https://doi.org/10.2307/48703290

October 9 (week 6): Sabotage and Subversion: Plausible Deniability in Action?

1. What are the main characteristics of Russian subversion tactics?
2. Is Russia successful in achieving plausible deniability in its hybrid warfare operations?
3. How do energy dependencies and critical infrastructure vulnerabilities create opportunities for hybrid warfare?
4. Should Western democratic states start responding in kind to Russia's proxy operations (i.e. Operation "Spiderweb")?

Core Readings:

- Cline, L. E. (2019). Partisans, hybrids, and intelligence. International Journal of Intelligence and Counterintelligence, 32(2), 248–271.
- Radin, A., Demus, A., & Marcinek, K. (2020). Understanding Russian subversion: Patterns, threat and responses. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE331/RAND_PE331.pdf
- Geri, M. (2024). Understanding Russian hybrid warfare against Europe in the energy sector and in the future "energy-resources-climate" security nexus. Journal of Strategic Security, 17(3), 15–34. https://doi.org/10.2307/48793907
- Soldatov, A., & Borogan, I. (2024). Putin's new agents of chaos. Foreign Affairs, August 2024. https://www.foreignaffairs.com/ukraine/paris-olympics-putin-agents-chaos-andrei-soldatov-irina-borogan

Additional Readings:

- Górka, M. (2023). The Wagner Group as a tool of Russian hybrid warfare. Polish Political Science Yearbook, 52(2), 83–98.
- Lauder, M. A. (2024). State, non-state or chimera? Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-33-state-non-state-or-chimera-the-rise-and-fall-of-the-wagner-group-and-recommendations-for-countering-russias-employment-of-complex-proxy-networks/
- Bondar, K. (2025). How Ukraine's Operation "Spider's Web" redefines asymmetric warfare. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

October 16 (week 7): (Counter-)Intelligence and Methodologies for Analysis of Hybrid Threats

1. Which OSINT, HUMINT, SIGINT/IMINT methods are best suited for predicting hybrid-threat attacks?
2. How do intelligence agencies and scholarly community adapt their collection and analysis methods to address the challenges posed by hybrid threats that blur traditional conflict boundaries?
3. What role does counterintelligence play in defending against hybrid warfare, and how has this evolved since the Cold War?

Core Readings:

- Varzhanskyi, I. (2024). Reflexive control as a risk factor for using OSINT: Insights from the Russia–Ukraine conflict. International Journal of Intelligence and Counterintelligence, 37(2), 419–449.
- Roell, P. (2020). Hybrid warfare: Challenges for intelligence services. ISPSW Strategy Series, No. 687. https://www.ispsw.com/wp-content/uploads/2020/04/687_Roell.pdf
- Kotaridis, I., & Benekos, G. (2023). Integrating Earth observation IMINT with OSINT data: A case study of the Ukraine-Russia war. Security and Defence Quarterly, 43(3), 1–21. https://doi.org/10.35467/sdq/170901
- Walton, C. (2023). The new spy wars: How China and Russia use intelligence agencies to undermine America. Foreign Affairs, July 19, 2023.

Additional Readings:

- Thomas, T. (2004). Russia's reflexive control theory and the military. Journal of Slavic Military Studies, 17(2), 237–256. https://doi.org/10.1080/13518040490450529
- Golitsyn, A. (1984). New lies for the old: The communist strategy of deception and disinformation (Part 1, pp. 1–10). GSG & Associates.

- Gates, R. (2011). From the shadows: The ultimate insider's story of five presidents and how they won the Cold War (pp. 24–33). Simon & Schuster.
- Driedger, J. J., & Polianskii, M. (2023). Utility-based predictions of military escalation: Why experts forecasted Russia would not invade Ukraine. Contemporary Security Policy, 44(4), 544–560. https://doi.org/10.1080/13523260.2023.2259153

October 23 (week 8): No Class - Reading Week

October 30 (Week 9): Ukraine: War on Two Fronts

1. Did Russia's invasion of Ukraine in February 2022 become the first XXI century hybrid war as many predicted?
2. What factors contributed to Ukraine's resilience against Russian hybrid warfare campaigns?
3. How has the full-scale invasion of Ukraine since February 2022 changed the nature of hybrid warfare and the relationship between hybrid and conventional operations?
4. What are the ongoing lessons of the war for studying Russia's hybrid warfare? How can these insights be used in the West?

Core Readings:

- Brantly, A. F., & Brantly, N. D. (2024). The blitzkrieg that was and wasn't: The military and intelligence implications of cyber operations during Russia's war on Ukraine. Intelligence and National Security, 39(3), 475–495. https://doi.org/10.1080/02684527.2024.2321693
- Helmus, T. C., & Holynska, K. (2024). Ukrainian resistance to Russian disinformation: Lessons for future conflict. RAND. https://www.rand.org/t/RRA2771-1
- Bachmann, S.-D., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy, 14(5), 858–869.

Additional Readings:

- Kalensky, J., & Osadchuk, R. (2024). How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/
- Bojor, L., Petrache, T., & Cristescu, C. (2024). Emerging technologies in conflict: The impact of Starlink in the Russia-Ukraine War. Land Forces Academy Review, 29(2), 185–194. https://doi.org/10.2478/raft-2024-0020

- Davies, P. H. J. (2024). Counterintelligence and escalation from hybrid to total war in the Russo-Ukrainian conflict 2014–2024. Intelligence and National Security, 39(3), 496–514.

November 6 (Week 10): Resilience and Adaptation in Europe's Hybrid Battlespace

1. What were/are the most successful Russian hybrid operations in Western and Eastern Europe, and how have target states responded?
2. How have the European states developed resilience strategies against Russian hybrid threats, and what are main differences between these approaches?
3. What role does EU play in deterring hybrid attacks, and how do alliance mechanisms adapt to gray zone challenges?

Core Readings:

- Eurovision News (2025). Playing with Fire: Are Russia's hybrid attacks the new European war? https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/?
- Hoyle, A., Hellman, M., & Hoyle, A. (2024). Weapons of mass division: Sputnik Latvia's Russophobia narratives and testing the rejection-identification model in Russian speakers in Latvia. Political Psychology, 45(4), 753–772. https://doi.org/10.1111/POPS.12964
- Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. European View, 20(1), 23–33.
- Stoian, V. (2023). The EU Approach to Combating Disinformation: Between Censorship and the "Market For Information". In Routledge Handbook of Disinformation and National Security (pp. 311-327). Routledge.

Additional Readings:

- Gorawantschy, B., Lenzner, M., & Körner, T. (2024). Hybrid threats – European security at stake. Konrad-Adenauer-Stiftung. https://www.kas.de/documents/284153/0/KAS+Security+Snapshot+II+-+Hybrid+Threats+-+December+2024.pdf/0138af9b-c62c-4790-694b-7daab48090bb?version=1.0&t=1733929043967
- Morkūnas, M. (2023). Russian disinformation in the Baltics: Does it really work? Public Integrity, 25(6), 599–613.
- Praks, H. (2025). Russia's hybrid attacks in Europe: From deterrence to attribution to response. ICDS. https://icds.ee/en/russias-hybrid-attacks-in-europe-from-deterrence-to-attribution-to-response/
- Kayali, L., Banse, D., & Schweppe, C. (2024). Europe is under attack from Russia. Why isn't it fighting back? Politico. https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/

November 13 (Week 11): The High North and the Arctic: New Strategic Frontier

1. What unique challenges do Arctic conditions and geography present for both hybrid operations and defensive measures?
2. How did the Arctic Countries react to Russian hybrid warfare?
3. How has NATO expansion in the High North change the importance of hybrid warfare for regional powers?
4. How should Canada respond to increasing Russian hybrid threats?

Core Readings:

- Kertysova, K., & Cricius, G. (2023). Countering Russia's hybrid threats in the Arctic. European Leadership Network. https://europeanleadershipnetwork.org/wp-content/uploads/2023/12/23_11_22_Countering-Russias-Hybrid-Threats-in-the-Arctic15_ES_EK40.pdf
- Schalin, J., & Fjäder, C. (2024). Building resilience to hybrid threats: Best practices in the Nordics. Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-31-building-resilience-to-hybrid-threats-best-practices-in-the-nordics/
- Jackson, N. (2019). Deterrence, resilience and hybrid wars: The case of Canada and NATO. Journal of Military and Strategic Studies, 19(4).

Additional Readings:

- Gjørv, G. H. (2024). Security and geopolitics in the Arctic: The increase of hybrid threat activities in the Norwegian High North. Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-30-security-and-geopolitics-in-the-arctic-the-increase-of-hybrid-threat-activities-in-the-norwegian-high-north/
- Dalziel, A. (2024). Critical resilience. Macdonald-Laurier Institute. https://macdonaldlaurier.ca/wp-content/uploads/2024/06/20240613_Undersea-cables-Dalziel_PAPER-v8-FINAL.pdf
- Albertus, M. (2025). The coming age of territorial expansion: Climate change will fuel contests—and maybe wars—for land and resources. Foreign Affairs. https://www.foreignaffairs.com/united-states/climate-change-coming-age-territorial-expansion

November 20 (Week 12): Africa, Middle East and the Global South

1. What historical precedents from Cold War operations in the developing world inform contemporary hybrid warfare strategies?

2. How do Russian influence operations in the Global South differ from their approaches in other regions?
3. What role do proxy forces and private military companies play in Russian hybrid strategies across Africa and other developing regions?

Core Readings:

- McGarr, P. M. (2021). Fake news, forgery, and falsification: Western responses to Soviet disinformation in Cold War India. The International History Review, 43(1), 34–53. https://doi.org/10.1080/07075332.2019.1662471
- Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare (pp. 298–311). Farrar, Straus and Giroux. (Chapter "AIDS Made in the USA").
- Beccaro, A. (2021). Russia, Syria and hybrid warfare: A critical assessment. Comparative Strategy, 40(5), 482–498.
- Šćepanović, J. (2024). Subversive narratives and status-seeking: A look at Russia's outreach to the developing world. International Journal, 79(2), 250–274. https://doi.org/10.1177/00207020241257630

Additional Readings:

- Kakachia, K., & Kakabadze, S. (2024). Beyond cyber and disinformation: Russian hybrid warfare tactics in Georgia. In Russian warfare and influence states in the intersection between East and West (pp. 129–153). Bloomsbury Academic.
- Peruchon, L. (2024). Propaganda machine: Russia's information offensive in the Sahel. Forbidden Stories. https://forbiddenstories.org/propaganda-machine-russias-information-offensive-in-the-sahel/
- Potočňák, A., & Mareš, M. (2022). Russia's private military enterprises as a multipurpose tool of hybrid warfare. The Journal of Slavic Military Studies, 35(2), 181–204.

November 27 (Week 13): NATO and Allied Responses: Counter Hybrid Warfare?

1. How have transatlantic frameworks evolved to address hybrid threats, and what institutional adaptations are still necessary?
2. What are the key challenges in developing collective defense mechanisms against hybrid attacks that fall below traditional Article 5 thresholds?
3. Does NATO need one-catches-all strategy to counter Russian hybrid threats or should the answers be more nuanced? Should NATO member-states have more room for maneuver in elaborating their responses?
4. Should NATO member states mirror Russia's hybrid attacks? What are the advantages and risks of this approach?

Core Readings:

- Bilal, A. (2024). NATO Review – Russia's hybrid war against the West. NATO Review. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html
- Bajarūnas, E. (2025) Using NATO's Article 5 Against Hybrid Attacks, CEPA. https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/
- Genini, D. (2024). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. New Perspectives. https://doi.org/10.1177/2336825X251322719

Additional Readings:

- Wiedemar, S. (2023). NATO and Article 5 in cyberspace. Center for Security Studies, ETH Zürich. https://doi.org/10.3929/ethz-b-000610328
- Kumar, S., et al. (2025). NATO self-defense – Is Article 5 the right framework for responding to sub-kinetic cyber aggression? Texas A&M University School of Law Legal Studies Research Paper. https://doi.org/10.2139/SSRN.5216954
- Seely, B. (2023). The Russian way of war: Moscow wants to weaken NATO in Ukraine, not just win battles. Foreign Affairs. https://www.foreignaffairs.com/ukraine/russian-way-war
- Claver, A. (2018). Governance of cyber warfare in the Netherlands: An exploratory investigation. The International Journal of Intelligence, Security, and Public Affairs, 20(2), 155–180
- NATO (2025) NATO's approach to counter information threats, NATO Website. https://www.nato.int/cps/en/natohq/topics_219728.htm

December 4 (Week 14): The Endgame? Navigating Strategic Competition with Russia

1. How should transatlantic actors balance deterrence, dialogue, and sanctions?
2. What plausible tactics are most promising in countering Russian hybrid attacks against the backdrop of Cold War experience? Are we in a new Cold War?
3. Reflecting on broader lessons of the course: what institutional reforms or strategic innovations are most urgent in transatlantic institutions in light of hybrid threats?

Core Readings:

- Ferguson, N. (2025). How to win the new Cold War: To compete with China, Trump should learn from Reagan. Foreign Affairs.
- Kendall-Taylor, A., & Kofman, M. (2024). Putin's point of no return: How an unchecked Russia will challenge the West. Foreign Affairs, 1–9.
- Walton, C. (2022). What's old is new again: Cold War lessons for countering disinformation. Texas National Security Review, 5(4). https://doi.org/10.55540/0031-1723.1388

Additional Readings:

- Soldatov, A., & Borogan, I. (2025). Arsonist, killer, saboteur, spy: While Trump courts him, Putin is escalating Russia's hybrid war against the West. Foreign Affairs. https://www.foreignaffairs.com/russia/arsonist-killer-saboteur-spy-vladimir-putin-donald-trump
- Whyte, J. (2024). Soviet active measures and the Second Cold War: Security, truth, and the politics of self. International Political Sociology, 18(3), 24–24. https://doi.org/10.1093/IPS/OLAE024
- Glimore, D. (2024). The rising threat of ransomware in manufacturing. Threat Intelligence. https://www.threatintelligence.com/blog/manufacturing-ransomware
- Johnson, L. K. (2022). The Third Option: Covert Action and American Foreign Policy (pp. 1–19, 252–278). Oxford University Press.

Appendix

Student Mental Health

As a university 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.

Here is a list that may be helpful:

Emergency Resources (on and off campus): https://carleton.ca/health/emergencies-andcrisis/emergency-numbers/

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: (613) 238-3311 or TEXT: 343-306-5550, https://www.dcottawa.on.ca/
- Mental Health Crisis Service: (613) 722-6914, 1-866-996-0991, http://www.crisisline.ca/
- Empower Me: 1-844-741-6389, https://students.carleton.ca/services/empower-me-counsellingservices/
- Good2Talk: 1-866-925-5454, https://good2talk.ca/

- The Walk-In Counselling Clinic: https://walkincounselling.com

Requests for Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request, the processes are as follows:
Pregnancy accommodation: Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For accommodation regarding a formally-scheduled final exam, you must complete the Pregnancy Accommodation Form (click here).

Religious accommodation: Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details click here.
Accommodations for students with disabilities: If you have a documented disability requiring academic accommodations in this course, please contact the Paul Menton Centre for Students with Disabilities (PMC) at 613-520-6608 or pmc@carleton.ca for a formal evaluation, or contact your PMC coordinator to send your instructor your Letter of Accommodation at the beginning of the term. You must also contact the PMC no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, reach out to your instructor as soon as possible to ensure accommodation arrangements are made. For more details, click here.

Accommodation for student activities: Carleton University recognizes the substantial benefits, both to the individual student and to the university, that result from a student participating in activities beyond the classroom. Reasonable accommodation will be provided to students who engage in student activities at the national or international level.

Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more information, please click here.

For more information on academic accommodation, please contact the departmental administrator or visit: students.carleton.ca/course-outline/.

Sexual Violence Policy

As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated. Survivors are supported through academic accommodations as per Carleton's Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit: carleton.ca/sexual-violence-support.

Academic Integrity

Academic integrity is an essential element of a productive and successful career as a student. Carleton's Academic Integrity Policy addresses academic integrity violations, including plagiarism, unauthorized collaboration, misrepresentation, impersonation, withholding of records, obstruction/interference, disruption of instruction or examinations, improper access to and/or dissemination of information, or violation of test and examination rules. Students are required to familiarize themselves with the university's academic integrity rules.

Plagiarism

The Academic Integrity Policy defines plagiarism as "presenting, whether intentional 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, websites, 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;
- 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.

Use of Artificial Intelligence

Written work produced for this course must not be produced by generative AI tools such as Chat GPT, Perplexity etc. The instructor may decide to make the grade for an assignment dependent on an oral discussion with the student to confirm their knowledge of the material and sources. If the instructor has evidence for the use of AI tools, an academic integrity investigation will be initiated as per Carleton's Academic Integrity Policy.

Procedures in Cases of Suspected Violations

Violations of the Academic Integrity Policy are serious offences which cannot be resolved directly with the course's instructor. When an instructor suspects a violation of the Academic Integrity Policy, the Associate Dean of the Faculty conducts a rigorous investigation, including an interview with the student. Penalties are not trivial. They may include a mark of zero for the assignment/exam in question or a final grade of "F" for the course. More information on the University's Academic Integrity Policy can be found at: https://carleton.ca/registrar/academic-integrity/.

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).

Submission and Return of Term Work

Papers must be submitted directly to the instructor according to the instructions in the course outline. The departmental office will not accept assignments submitted in hard copy.

Grading
Standing in a course is determined by the course instructor, subject to the approval of the faculty Dean. Final standing in courses will be shown by alphabetical grades. The system of grades used, with corresponding grade points is:

Percentage Letter grade 12-point scale

90-100	A+	12
85-89	A	11
80-84	A-	10
77-79	B+	9
73-76	B	8
70-72	B-	7
67-69	C+	6
63-66	C	5
60-62	C-	4
57-59	D+	3
53-56	D	2
50-52	D-	1
>50	F	0

Standing in a course is determined by the course instructor subject to the approval of the Faculty Dean. This means that grades submitted by an instructor may be subject to revision.

No grades are final until they have been approved by the Dean.

Carleton E-mail Accounts

All email communication to students from the Department of Political Science 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 University email accounts and Brightspace.