INTA 4050

International Affairs and Technology Policy Making

Term: Spring 2026 **Credit Hours:** 3
Time: Mondays, 6:30–9:15 PM **Location:** Skiles 269

Instructor Information

Instructor: Dr. Juljan Krause jkrause@gatech.edu
Office Hours and Location: TBA

Core IMPACTS

This is a Core IMPACTS course that is part of the Social Sciences area.

Core IMPACTS refers to the core curriculum, which provides students with essential knowledge in foundational academic areas. This course will help master course content, and support students' broad academic and career goals.

This course should direct students toward a broad Orienting Question:

- How do I understand human experiences and connections?

Completion of this course should enable students to meet the following Learning Outcomes:

- Students will effectively analyze the complexity of human behavior, and how historical, economic, political, social or geographic relationships develop, persist or change.

Course content, activities and exercises in this course should help students develop the following Career-Ready Competencies:

- Intercultural Competence
- Perspective-Taking
- Persuasion

Course Description

A growing number of geopolitical struggles today are fought through *infrastructure*: chips and compute, undersea cables and satellites, standards and supply chains, and the cloud platforms that increasingly mediate economic and military power. This course examines how international technology policy is made in practice when *interdependence is inescapable* but *security stakes are rising*. We focus on the policy instruments that translate technical capability into political leverage: export controls and industrial policy, platform regulation and content governance, cybersecurity strategies and alliance coordination, and the management of high-consequence transitions (e.g., post-quantum cryptography). While the course focuses primarily on the fast-evolving relationships among the United States, Europe, and China, the dynamics we study routinely extend beyond this core and shape technology policy worldwide.

The course is deliberately applied. Students learn to read strategies and policy documents as instruments of power, to identify assumptions and implementation risks, and to produce decision-grade outputs under real-world constraints. Assessment emphasizes professional policy writing, one in-class crisis simulation, and a final portfolio (submitted as an alternative final assessment) rather than in-class exams.

The course is organized around three recurring propositions:

- *Infrastructure creates leverage.* The most durable advantages often come from chokepoints, dependencies, and switching costs, not just "innovation."
- *Governance happens in the plumbing.* Standards, procurement policies, compliance regimes, liability rules, and interoperability constraints can lock in power and shape conflict.
- *Dual-use is normal.* "Civilian" systems routinely become security-relevant because they are widely deployed, privately operated, and difficult to replace quickly.

By the end of the course, students should be able to (i) explain how material and digital infrastructures (re)shape the international system, (ii) evaluate competing policy strategies across jurisdictions, and (iii) communicate clear recommendations to decision-makers under uncertainty and time pressure.

Learning Outcomes

Upon successful completion of this course, you will be able to:

1. **Diagnose** an international technology policy problem by identifying the key actors, incentives, institutions, and strategic dynamics.
2. **Translate** technical change into policy-relevant claims by distinguishing what is measurable, what is uncertain, and what is hype.
3. **Select and justify** appropriate policy instruments, including standards, regulation, procurement, industrial policy, export controls, alliances, and norms/treaties.
4. **Write like a practitioner** by producing concise, decision-grade memos that present options, trade-offs, a recommendation, and an implementation pathway.
5. **Stress-test** strategies using cases and in-class simulations, with attention to cascades, escalation risk, and unintended consequences.
6. **Communicate across organizational cultures** (e.g., engineering, diplomacy, regulation) without sacrificing analytical precision.

Course Requirements and Assessment

Assessment at a glance

What	What you do (and when)	Weight
No in-class exams	There is no midterm and no in-class final exam. Assessment is based on applied writing, one in-class crisis simulation, and a final portfolio submitted during the Registrar-scheduled final assessment window.	—
Participation & in-class work	Ongoing. Includes preparation, discussion, and completion of in-class analytic artifacts.	15%
Policy Analysis Brief (individual)	2–3 pages analyzing *one* policy/strategy document (problem definition, instruments, trade-offs, enforceability, and evidence). **Due Fri 13 Feb 2026, 5:00pm.**	10%
Policy Memo (individual)	4–6 pages, decision-grade memo (options, recommendation, implementation, risks). **Due Fri 13 Mar 2026, 5:00pm.**	20%
Simulation: Undersea Infrastructure Crisis + After-Action Memo	In-class crisis simulation (Week 11) + 2-page memo (individual). **After-Action Memo due Fri 10 Apr 2026, 5:00pm.**	20%
Final Portfolio (Alternative Final Assessment)	Portfolio package (analysis + risk register + feasibility/cost note + briefing slides). **Due during the Registrar-scheduled final exam slot for INTA 4050** (time TBA when posted; currently expected Mon 4 May 2026, 6–8.50pm).	35%

Deadline visibility: All due dates are bolded above and repeated below. Missing a deadline because it was "hard to find" will not be an acceptable reason for late submission.

1) Participation & in-class labs/discussion (15%)

A great mark comes from consistent preparation and contributions that improve the class's collective analysis. This includes demonstrating careful reading, asking informed questions, and translating technical constraints into institutional and political realities.

2) Policy Analysis Brief (10%)

A great mark comes from disciplined, document-centered analysis. Your job is to make a policy/strategy document intelligible as a *policy instrument*: what it claims to solve, what it actually does, how it expects compliance, what it assumes about technology, and where its implementation risks are.

3) Policy Memo (20%)

A great mark comes from writing like a practitioner: a clear problem statement, a small number of plausible options, explicit trade-offs, a justified recommendation, and an implementation

pathway that takes politics and capacity seriously. Your memo should be concise, evidence-based, and explicit about uncertainty.

4) Simulation: Undersea Infrastructure Crisis + After-Action Memo (20%)

A great mark comes from disciplined crisis reasoning: prioritizing under uncertainty, managing escalation risks, and communicating clearly under time pressure. The After-Action Memo should explain (i) what you did and why, (ii) what you learned about alliance politics and escalation management, and (iii) what you would do differently.

5) Final Portfolio (Alternative Final Assessment) (35%)

A great mark comes from integration, professionalism, and decision-readiness. It requires multiple complementary artifacts rather than a single essay. Your portfolio must include:

- **Core analysis** (4–6 pages): problem, stakes, options, recommendation, implementation.
- **Risk register** (1 page): top risks, likelihood/impact, mitigations, residual risk.
- **Feasibility / cost note** (1–2 pages): timeline, dependencies, who pays, what breaks.
- **Briefing slides** (5–7 slides): decision-ready summary that is targeted and inviting both in terms of content and presentation, crafted with your (imaginary) audience of senior decision-makers in mind.

6) How your final course grade is calculated

Your course grade is computed as a weighted average of the five components listed above. Each component is graded on a 0–100 scale, multiplied by its weight, and then summed to produce a final percentage out of 100.

- Participation & in-class work: 15%
- Policy Analysis Brief: 10%
- Policy Memo: 20%
- Simulation + After-Action Memo: 20%
- Final Portfolio (Alternative Final Assessment): 35%

Your final grade will be assigned as a letter grade according to the following scale:

A	90–100%
B	80–89%
C	70–79%
D	60–69%
F	0–59%

Key due dates

PLEASE NOTE: These are hard deadlines.

- **Fri 13 Feb 2026, 5:00pm:** Policy Analysis Brief due
- **Fri 13 Mar 2026, 5:00pm:** Policy Memo due
- **Mon 6 Apr 2026 (in class):** Undersea Infrastructure Crisis Simulation
- **Fri 10 Apr 2026, 5:00pm:** Simulation After-Action Memo due
- **Registrar-scheduled final exam slot (TBA):** Final Portfolio due (currently expected Mon 4 May 2026, 6–8.50pm, but please double-check)

Late work, extensions, and unexpected events

Deadlines are part of the learning design in this course: they help you plan, help me grade fairly, and keep the class moving together. If something disrupts your ability to meet a deadline, please email me *as soon as reasonably possible* (ideally before the deadline) with a brief description of the situation and a proposed plan.

Extensions. I can often grant short extensions for good-faith reasons when requested in advance. In most cases, I will ask for documentation. You do not need to share sensitive details; when documentation is requested, a brief note from an appropriate authority (e.g., Student Health Services, a medical provider, the Dean of Students, or an accessibility/academic support office) confirming the situation is sufficient.

Late submissions. Unless an extension is approved, late work will receive a penalty of 5 percentage points per 24 hours (including weekends), up to 72 hours. After 72 hours, the assignment will receive a zero, except in cases of documented emergencies or official accommodations.

Final portfolio. The Final Portfolio is the course's alternative final assessment and must be submitted during the Registrar-scheduled final assessment window (see syllabus). Late final-portfolio submissions can only be accepted in line with Institute policy and official accommodations.

Course Policies, Expectations, & Guidelines

Subject to Change Statement

The syllabus and course schedule may be subject to change. Changes will be communicated via email and/or the Canvas announcement tool. It is your responsibility to check your email messages and keep an eye on course announcements.

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information from their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Important: Make sure your email is set up to receive course announcements through Canvas.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/ as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible to set up a time to discuss your learning

needs (of course you won't need to disclose any medical or otherwise sensitive information to me).

Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. Review Georgia Tech's Honor Code and the student Code of Conduct.

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Use of Generative AI

You may use AI tools (such as ChatGPT or Claude) as research aids and for brainstorming, but all submitted work must be your own. If you use AI assistance, you must acknowledge it and explain how you used it. Entirely AI-generated text submitted as your own work constitutes an academic integrity violation.

If you use AI assistance, please include a brief disclosure (1–3 sentences) at the end of the document describing what tool you used and how.

Attendance and Participation

Regular attendance is expected and contributes significantly to your grade. Given the evening timing and small class size, your presence and engagement are essential to the learning environment. If you must miss a class, please notify the instructor in advance. More than two unexcused absences will affect your participation grade.

Student Resources

Georgia Tech provides numerous resources to support your success. Visit success.gatech.edu for undergraduate academic support, including tutoring and advising. Graduate students can find resources at grad.gatech.edu/current-students. For wellness support, visit students.gatech.edu/student-resource-guide.

Course Materials

There is no required textbook. Readings will be drawn from academic articles, policy reports, government strategy documents, think tank analyses, and current affairs publications, and are accessible online and available on Canvas (see links in the Weekly Schedule section below).

Optional/additional readings are exactly that: optional. Some weeks list more than others to offer a wider menu of sources, not to increase the expected workload, though you are always encouraged to read beyond the required minimum.

Weekly Schedule

Calendar notes: No class on Mon, Jan 19 (Institute holiday). No class on Mon, Mar 23 (Spring Break).

Week 1: Technology policy as international order — Mon, Jan 12

How do infrastructures and security framings reconfigure the global balance of power?

Required readings:

- The White House (November 2025). *National Security Strategy of the United States of America*. PDF.
- Farrell, Henry and Abraham L. Newman (2019). "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44(1): 42–79. Link.

Additional/optional readings:

- Ministry of Foreign Affairs of the People's Republic of China (27 October 2025). *The 2025 PRC Global AI Governance Initiative (Update).* Link.
- European Commission & High Representative (20 June 2023). *Joint Communication on "European Economic Security Strategy"* (JOIN(2023) 20 final). PDF (EUR-Lex).
- UK Cabinet Office (March 2023). *Integrated Review Refresh 2023: Responding to a more contested and volatile world*. PDF.
- Bakonyi, Jutta and May Darwich (2024). "Infrastructures and International Relations: A Critical Reflection on Materials and Mobilities." *International Studies Review* 26(4): viae046. Open-access PDF.

Week 2: How technology policies form — Mon, Jan 26

How do technology policies and strategies actually get made (and why do they look the way they do)?

Required readings:

- UK Government (November 2025). *The UK's Modern Industrial Strategy*. PDF.
- Cairney, Paul and Michael D. Jones (2016). "Kingdon's Multiple Streams Approach: What Is the Empirical Impact of This Universal Theory?" *Policy Studies Journal* 44(1). Author PDF.

Additional/optional readings:

- UK Government (March 2023). *The UK's International Technology strategy*. PDF.
- Frank, Aaron B., and Elizabeth M. Bartels. (2022). *Designing a Robust Decision-Based National Security Policy Process.* RAND Corporation. PDF.

Week 3: The Global Core: Internet & Standards — Mon, Feb 2

Why are technical standards bodies the "invisible" battleground of modern geopolitics?

Required readings:

- Internet Society (ISOC) (2020). *Discussion Paper: An Analysis of the "New IP" Proposal to the ITU-T.* PDF.
- DeNardis, Laura (2013). *Internet Points of Control as Global Governance*. CIGI Paper No. 2. PDF.

Additional/optional readings:

- U.S. Department of State (April 2022). *Declaration for the Future of the Internet*. PDF.
- Mueller, Milton L. and Karim Farhat (2022). *Regulation of platform market access by the United States and China: Neo-mercantilism in digital services*. Policy & Internet, vol. 14 no. 2. PDF.

Week 4: Chokepoints: Chips, Cables, & Clouds — Mon, Feb 9

How does physical infrastructure create inescapable switching costs and political leverage?

Required readings:

- European Commission (8 March 2024). *Commission Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures*. PDF.
- Bassens, David, Cheng Fang, and Ulysses Pascal (2025). *Striving for sovereignty across the cloud finance stack: A relational comparison of the United States, the European Union, and China*. Finance and Society (FirstView), pp. 1–21. DOI: 10.1017/fas.2025.10019. PDF.

Additional/optional readings:

- The White House (March 2025). *Amended National Strategy on Microelectronics Research*. PDF.
- European Parliament and Council (18 September 2023). *Regulation (EU) 2023/1781 establishing a framework of measures for strengthening Europe's semiconductor ecosystem ("Chips Act")*. PDF.
- Runde, Daniel F., Erin L. Murphy, and others (CSIS) (August 2024). *Safeguarding Subsea Cables: Protecting Cyber Infrastructure Amid Great Power Competition*. PDF.
- European Court of Auditors (2025). *Special Report 12/2025: The EU's strategy for microchips*. PDF.

Week 5: Shadow Wars: Cyber Conflict & Norms

Mon, Feb 16

Can international rules actually restrain state behavior in a domain largely designed for anonymity?

Required readings:

- United Nations General Assembly (July 2021). *Advancing responsible State behaviour in cyberspace in the context of international security: Report of the Group of Governmental Experts* (A/76/135). PDF.
- Lindsay, Jon R. (2025). *Stuxnet revisited: From cyber warfare to secret statecraft*. Journal of Strategic Studies, vol. 48 no. 4. DOI.

Additional/optional readings:

- U.S. Department of State (May 2024). *United States International Cyberspace & Digital Policy Strategy*. PDF.
- UNIDIR (2022). *Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics*. PDF.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (December 2020). *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN(2020) 18 final). PDF.
- Egloff, Florian J. (2020). *Public attribution of cyber intrusions*. Journal of Cybersecurity, vol. 6 no. 1. DOI. PDF.

Week 6: The Platform Governance Clash

Mon, Feb 23

How do states balance trade and security when domestic rules reach across borders to govern global digital platforms?

Required readings:

- U.S. Congress (codified in U.S. Code; current through 2021 ed.). *47 U.S.C. §230: Protection for private blocking and screening of offensive material* (the statutory baseline for limited platform liability obligations in U.S. federal law). PDF.
- European Parliament and Council (19 October 2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)* (OJ L 277, 27 Oct 2022). Long version: PDF. Summary explainer: Page.
- Gorwa, Robert (2019). *The platform governance triangle: conceptualising the informal regulation of online content*. Internet Policy Review, vol. 8 no. 2. DOI. PDF.

Additional/optional readings:

- Congressional Research Service (CRS) (February 2024). *Section 230: A Brief Overview* (IF12584). PDF.
- UK Government, Department for Science, Innovation and Technology (24 April 2025). *Online Safety Act 2023: explainer*. Page.

- European Data Protection Board (12 November 2019). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (final, after public consultation). PDF.

Week 7: The Compute Race: AI & Industrial Policy — Mon, Mar 2

Is AI governance about the algorithms, or the infrastructure required to run them?

Required readings:

- The White House (July 2025). *Winning the Race: America's AI Action Plan*. PDF.
- Ministry of Foreign Affairs of the People's Republic of China (July 2025). *Global AI Governance Action Plan* (in English). Page.
- State Council of the People's Republic of China (July 2017). *Next Generation Artificial Intelligence Development Plan* (English translation). PDF.
- Sastry, Girish, Lennart Heim, Haydn Belfield, et al. (February 2024). *Computing Power and the Governance of Artificial Intelligence*. arXiv:2402.08797. Page. PDF.

Additional/optional readings:

- OECD (November 2025). *Competition in Artificial Intelligence infrastructure*. PDF.
- Chan, K., Smith, G., Goodrich, J., DiPippo, G., & Pilz, K. F. (June 2025). *Full Stack: China's Evolving Industrial Policy for AI*. RAND. Page.
- Wang, T., Chen, Q., Wei, S., & Zhang, Z. (2025). *Industry policies and technological innovation in artificial intelligence clusters: are central positions superior? Humanities and Social Sciences Communications*, 12:1262. PDF. DOI.

Week 8: Algorithmic Security: AI in the Military — Mon, Mar 9

What happens to stability when the speed of AI deployment outruns the speed of oversight?

Required readings:

- U.S. Department of Defense (25 January 2023). *DoD Directive 3000.09: Autonomy in Weapon Systems*. PDF.
- UK Ministry of Defence (June 2022). *Ambitious, Safe and Responsible: Our approach to the delivery of AI-enabled capability in Defence*. PDF.
- Johnson, James (2026). *Can AI behave ethically during military crises? Preserving human moral agency*. International Affairs, vol. 102 no. 1, pp. 63–83. DOI. Page. PDF.

Additional/optional readings:

- North Atlantic Treaty Organization (22 October 2021). *Summary of the NATO Artificial Intelligence Strategy*. Page.
- U.S. Department of Defense (June 2024). *Responsible Artificial Intelligence Strategy and Implementation Pathway*. PDF.

- International Committee of the Red Cross (May 2021). *ICRC position on autonomous weapon systems and background paper*. PDF.
- State Council Information Office of the People's Republic of China (July 2019). *China's National Defense in the New Era* (National Defense White Paper; includes discussion of "intelligentization" and modernisation priorities). PDF. Official page.

Week 9: The Quantum Transition

Mon, Mar 16

How do states coordinate on an existential security transition with an immensely uncertain timeline?

Required readings:

- National Science and Technology Council (NSTC) (September 2018). *National Strategic Overview for Quantum Information Science*. PDF.
- Cyberspace Administration of China (CAC) (December 2021). *14th Five-Year Plan for National Informatization* (English translation, DigiChina / Stanford Cyber Policy Center; original published Dec. 28, 2021). PDF.
- Kong, Ini, Marijn Janssen, and Nitesh Bharosa (2024). *Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions*. Government Information Quarterly, vol. 41 no. 1, 101884. DOI. PDF.

Additional/optional readings:

- National Institute of Standards and Technology (NIST) (November 2024). *NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards*. PDF.
- Krause, Juljan (February 2024). *The Quantum Race: U.S.-Chinese Competition for Leadership in Quantum Technologies*. UC Institute on Global Conflict and Cooperation (IGCC) Policy Brief. PDF.
- European Commission (April 2024). *Commission Recommendation (EU) 2024/1101 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*. PDF.
- UK Government, Department for Science, Innovation and Technology (March 2023). *National Quantum Strategy*. PDF.

Week 10: The New High Ground: Space & Satellites

Mon, Mar 30

How do mega-constellations redefine the boundaries between private enterprise and national security?

Required readings:

- U.S. Department of Defense (April 2024). *DoD Commercial Space Integration Strategy*. PDF.
- Indian Space Research Organisation (ISRO) / Government of India (April 2023). *Indian Space Policy – 2023*. PDF.

- Koplow, David A. (2024). *Large Constellations of Small Satellites: The Good, the Bad, the Ugly, and the Illegal*. Harvard National Security Journal, vol. 15 no. 2, pp. 257–292. PDF. Page.

Additional/optional readings:

- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (March 2023). *European Union Space Strategy for Security and Defence* (JOIN(2023) 9 final). PDF.
- UK Ministry of Defence (February 2022). *Defence Space Strategy: Operationalising the Space Domain*. PDF.
- U.S. Space Force (April 2024). *U.S. Space Force Commercial Space Strategy*. PDF.
- Defense Science Board (May 2024; public release July 2024). *Commercial Space System Access and Integrity* (Task Force Report). PDF.

Week 11: [Simulation] The Undersea Infrastructure Crisis

Mon, Apr 6

How do alliances manage escalation when vital physical links are severed?

Required readings:

- Heads of State or Government of Denmark, Estonia, Finland, Germany, Latvia, Lithuania, Poland and Sweden (14 January 2025). *Joint Statement of the Baltic Sea NATO Allies Summit* (Helsinki). PDF.
- European Commission and High Representative of the Union for Foreign Affairs and Security Policy (21 February 2025). *EU Action Plan on Cable Security* (JOIN(2025) 9 final). PDF.
- Bueger, Christian and Tobias Liebetrau (2021). *Protecting hidden infrastructure: The security politics of the global submarine data cable network*. Contemporary Security Policy, vol. 42 no. 3, pp. 391–413. DOI. Page.

Additional/optional readings:

- Atlantic Council (26 November 2025). *How the Baltic Sea nations have tackled suspicious cable cuts*. Page.
- Finnish Institute of International Affairs (FIIA) (February 2025). *The EU and NATO in pursuit of better deterrence* (Briefing Paper). PDF.
- European Commission (June 2023). *EU–NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report – Digital*. PDF.
- North Atlantic Treaty Organization (29 October 2025). *Alliance Maritime Strategy*. Page.

Week 12: Economic Statecraft & Supply Chain Resilience — Mon, Apr 13

How do states weaponize "plumbing" (minerals, manufacturing, and shipping) to force political outcomes?

Required readings:

- The White House (13 August 2025). *Executive Order 14336: Ensuring American Pharmaceutical Supply Chain Resilience by Filling the Strategic Active Pharmaceutical Ingredients Reserve*. PDF.
- European Parliament and Council of the European Union (3 May 2024). *Regulation (EU) 2024/1252 establishing a framework for ensuring a secure and sustainable supply of critical raw materials (Critical Raw Materials Act)*. PDF.
- Chen, Ling S. and Miles M. Evers (Fall 2023). *"Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft*. International Security, vol. 48 no. 2, pp. 164–204. DOI. PDF.

Additional/optional readings:

- The White House (December 2025). *National Security Strategy 2025* (sections on economic security, supply chains, and critical materials). PDF.
- OECD (September 2024). *OECD Inventory of Export Restrictions on Industrial Raw Materials 2024: Monitoring the use of export restrictions amid market and policy tensions*. OECD Publishing. PDF.
- World Bank (11 April 2024). *Dire Strait: The Far-Reaching Impact of the Red Sea Shipping Crisis* (MENA FCV Economic Series Brief; short, data-rich overview of rerouting, costs, and spillovers). PDF.
- Congressional Research Service (8 May 2024). *Red Sea Shipping Disruptions: Estimating Economic Effects* (In Focus IF12657). PDF.

Week 13: Final Portfolio Workshop — Mon, Apr 20

How do you turn 12 weeks of analysis into decision-grade advice: a clear recommendation, a risk register, a feasibility/cost note, and a briefing deck?

Required readings:

- Harvard Kennedy School (January 2018). *How to Write a Policy Memo*. PDF.
- HM Treasury (May 2023). *The Orange Book: Management of Risk – Principles and Concepts*. PDF.
- Avey, Paul C. and Michael C. Desch (2014). *What Do Policymakers Want From Us? Results of a Survey of Current and Former Senior National Security Decision Makers*. International Studies Quarterly, vol. 58 no. 2, pp. 227–246. DOI. PDF.

Additional/optional readings:

- Office of the Director of National Intelligence (2 January 2015). *Intelligence Community Directive (ICD) 203: Analytic Standards*. PDF.

- HM Treasury / UK Government (March 2015). *The Aqua Book: Guidance on producing quality analysis for government*. PDF.
- UK Cabinet Office (2015). *Working with Ministers: A Practical Handbook on Advising, Briefing & Drafting*. PDF.
- Australian Government (December 2024). *Government writing handbook* (accessible PDF). PDF.

Week 14: Infrastructure, Interdependencies, and (In)Security: The Big Picture

Mon, Apr 27

How do states pursue security and prosperity when critical infrastructures are transnational, privately operated, and increasingly contested?

Required readings:

- North Atlantic Treaty Organization (29 June 2022). *NATO 2022 Strategic Concept*. PDF.
- Ministry of Foreign Affairs of the People's Republic of China (21 February 2023). *The Global Security Initiative Concept Paper*. PDF.
- Gjesvik, Lars (2023). *Private infrastructure in weaponized interdependence*. *Review of International Political Economy*, vol. 30 no. 2, pp. 722–746. DOI. Page.

Additional/optional readings:

- European Commission (24 January 2024). *Advancing European economic security: an introduction to five new initiatives* (COM(2024) 22 final). PDF.
- Bercero, Ignacio G. (December 2025). *From strategy to doctrine: the next steps for European economic security*. Bruegel Policy Brief 32/2025. PDF.
- McCarthy, Daniel R. (2024). *Infrastructure and the integral state: Internal Relations, processes of state formation, and Gramscian state theory*. *Review of International Studies*, vol. 50 no. 4, pp. 619–637. DOI. PDF.
