School for International Training | 1 Kipling Road, PO Box 676 | Brattleboro, VT 05302-0676 USA
Tel 888 272-7881 | Fax 802 258-3296 | studyabroad.sit.edu

Intelligence and Cyber Security

SECU-3000 (3 credits)

South Korea: International Relations and Security

This syllabus is representative of a typical semester. Because courses develop and change over time to take advantage of unique learning opportunities, actual course content varies from semester to semester.

Course Description

This course examines how intelligence and information shape security and diplomacy. Focusing on South Korea's regional context, students analyze how states gather, interpret, and share information to anticipate threats and build trust. The course explores intelligence cooperation, open-source data analysis, and disinformation campaigns alongside cybersecurity policy and digital governance. Comparative case studies, ranging from North Korean cyber operations to U.S.–Korea intelligence sharing and regional technology competition, highlight the intersection of information, strategy, and diplomacy.

Learning Outcomes:

Upon completion of the course, students will be able to:

- **Analyze** the role of intelligence in national security strategy and foreign policy decision-making in South Korea and the region
- **Evaluate** North Korea's cyber capabilities, tactics, and strategic objectives in the context of asymmetric warfare
- **Assess** frameworks for U.S.-ROK intelligence cooperation and information sharing in alliance management
- **Examine** cybersecurity governance structures, policies, and regulatory approaches in South Korea
- **Apply** open-source intelligence (OSINT) techniques to analyze security challenges and evaluate the ethical, legal, and oversight frameworks governing intelligence activities

Language of Instruction

This course is taught in English.

Instructional Methods

This course is designed around the principle that learning is an active, holistic process that extends well beyond the classroom. Seminars introduce key concepts and interpretive frameworks that are then examined, complicated, and enriched through direct engagement with people, places, and contexts — field visits, expert briefings, guided observation, and community-based learning. Field-based learning is integrated into course design rather than treated as enrichment: faculty prepare students for each engagement, guide interpretation on location, and facilitate the reflection that connects experience to course themes. Students move through cycles of experience, observation, and analysis, progressively taking greater ownership of their own inquiry. This process is not always linear, and that is by design — developing the capacity to learn from unpredictable, context-dependent situations is itself a transferable skill and a foundation for lifelong learning.

Assignment Descriptions and Grading Criteria

Evaluation is based on successful completion of multiple components designed to build analytical, strategic thinking, and communication skills progressively throughout the program. Assignments combine fieldwork observation, intelligence analysis, and policy simulation to develop well-rounded international security practitioners.

Assignment Overview

- In-Class Participation and Field Engagement: 15%
- Threat Assessment Analysis: 25%
- Open-Source Intelligence (OSINT) Analysis Project: 30%
- Cybersecurity Policy Proposal: 30%

1. In-Class Participation and Field Engagement (15%)

Active participation is essential for learning in this course. Students are expected to engage meaningfully in class discussions, field activities, security briefings, and interactions with guest speakers from intelligence agencies, cybersecurity firms, technology companies, and civil society organizations. Students will be evaluated on the quality of their contributions, critical thinking skills, respectful engagement with security professionals, ability to connect field experiences to theoretical concepts, and professionalism during sensitive briefings. This includes coming prepared with completed readings, asking thoughtful questions of guest lecturers and intelligence professionals, participating constructively in analytical exercises and simulations, and demonstrating appropriate discretion during classified or sensitive discussions.

2. **Threat Assessment Analysis (25%)**

Students will select one cyber threat or security challenge and conduct research to understand its nature, how it works, and why it matters for regional security. This project builds research and analytical skills while introducing students to cybersecurity concepts.

Requirements:

- Select one threat/challenge from provided list: North Korean hacking groups, ransomware attacks on hospitals/schools, election disinformation campaigns, Chinese technology espionage, cryptocurrency theft, supply chain vulnerabilities
- Research basic information: Who is behind it? What do they do? How do they do it? (in accessible terms)
- Identify 3-5 real examples/incidents with specific dates and impacts
- Explain strategic objectives: What is the attacker trying to achieve? Political, economic, or military goals?
- Analyze responses: How have governments and companies tried to stop or prevent these attacks?
- Assess effectiveness: What's working? What isn't? Why?
- Create presentation (12-15 minutes) with clear visuals, real examples, and non-technical explanations
- Submit 5-7 page written analysis with citations

3. **Open-Source Intelligence (OSINT) Analysis Project (30%)**

Students will learn to gather and analyze publicly available information on a regional security topic, developing skills in finding reliable sources, verifying information, and drawing analytical conclusions from open-source materials.

Requirements:

- Select one security topic (e.g., North Korean missile tests, regional military exercises, cyber incidents, diplomatic negotiations, technology developments)
- Identify 3-4 reliable information sources: news media, official government statements, think tank reports, academic publications, verified social media accounts
- Collect information over 4 weeks, maintaining an organized source log
- Write bi-weekly analysis memos (2 total, 500 words each) documenting what you found and what it means
- Create visual presentation (timeline, map, or infographic) showing key developments
- Submit mid-semester source evaluation (Week 5, 2 pages) explaining which sources are most reliable and why
- Final 1,500-1,800 word analytical report synthesizing findings and strategic implications

4. **Cybersecurity Policy Proposal (30%):** Working in teams of 3–4 students, develop a policy brief recommending a diplomatic or institutional response to a regional cybersecurity challenge facing South Korea.

Policy Scenarios (choose one):

- Propose a framework for trilateral cyber cooperation between the U.S., South Korea, and Japan
- Recommend a South Korean position on international norms for state-sponsored cyber operations
- Design a confidence-building mechanism to reduce cyber escalation risk with a regional adversary
- Develop a strategy for responding to a major North Korean cyberattack through diplomatic and intelligence channels

Assignment Components:

- Strategic context: What is the challenge and why does it matter for South Korea's international position?
- Stakeholder analysis: Which actors are involved and what are their interests?
- Policy recommendation: A clearly argued diplomatic or institutional response
- Tradeoffs and risks: Likely objections or unintended consequences
- Preliminary presentation (Week 6, 10 minutes): Problem framing and initial recommendation
- Final presentation (Week 10, 15 minutes): Policy briefing with Q&A
- Written brief (8-10 pages) with all components above

Grading Scale

94-100%	A	74-76%	C
90-93%	A-	70-73%	C-
87-89%	B+	67-69%	D+
84-86%	B	64-66%	D
80-83%	B-	Below 64	F
77-79%	C+		

Note on Attendance and Participation: Consistent participation in classes, site visits, and required program activities is essential to the academic experience. Students are expected to participate fully and may not opt out of required components, as these activities are integral to course learning and collective discussion. If circumstances such as illness affect attendance, students must communicate promptly with the Center Director or a designated staff member. Absences may affect academic performance and course grades, and repeated or unexcused absences may result in additional academic or programmatic consequences. When absences are unavoidable, alternative academic work may be required.

Program Expectations
To support a respectful, engaging, and academically rigorous learning environment, students are expected to approach this program with professionalism, preparation, and openness. Because this is an intensive, field-based program, individual conduct directly shapes the quality of the shared academic experience.

- **Learning Community:** Students are expected to engage respectfully with differing perspectives, including those of classmates, guest speakers, and local partners. Agreement is not required, but attentive listening, intellectual openness, and respectful dialogue are essential.
- **Content Considerations:** Course materials and activities may engage sensitive or challenging topics. The classroom is a space for thoughtful, respectful engagement with complex ideas. When possible, faculty will flag particularly intense content in advance. Students who find that course content affects their ability to participate or keep up with coursework are encouraged to communicate with faculty and seek appropriate support.
- **Participation and Engagement:** Students are expected to come prepared and to engage actively in classes, discussions, and site-based learning. This includes contributing thoughtfully to discussion, asking questions, and engaging respectfully with faculty, peers, and guest speakers. Meaningful participation supports collective learning and is an essential part of the program experience.
- **Flexibility and Adaptability:** Because this is a multi-country, field-based program, schedules and activities may change in response to local conditions or logistical realities. Students are expected to approach such adjustments with flexibility and professionalism. Adaptability is considered part of meaningful engagement in the program.
- **Academic Integrity:** Students are expected to complete all work honestly and ethically, in accordance with academic integrity standards outlined in course and program policies.
- **Managing Academic Work:** Students are responsible for maintaining reliable access to their academic work by keeping multiple copies using secure storage methods (e.g., cloud-based platforms or the learning management system). Technical issues such as lost files or device failures do not excuse late or missing work.
- **Personal Technology Use:** Personal devices may be used for note-taking and course-related activities. Off-task use is not acceptable, particularly during discussions, site visits, or guest presentations, as it detracts from collective engagement.
- **Course Communication:** Course materials, assignments, and updates will be posted on Canvas. While the course calendar provides a general structure, adjustments may occur based on program flow or site-based learning opportunities. Students are responsible for checking the course site regularly and communicating promptly about access issues.
- **Recording Policy:** To support open discussion, recording of classes or program activities is not permitted without prior written approval from the instructor. Approved

recordings are for personal academic use only. Documented academic accommodations may supersede this policy.

SIT Policies and Resources

Please refer to the SIT Study Abroad Handbook and the Policies section of the SIT website for all academic and student affairs policies. Students are accountable for complying with all published policies. Of particular relevance to this course are the policies regarding: academic integrity, Family Educational Rights and Privacy Act (FERPA), research and ethics in field study and internships, late assignments, academic status, academic appeals, diversity and disability, sexual harassment and misconduct, and the student code of conduct.

Please refer to the SIT Study Abroad Handbook and SIT website for information on important resources and services provided through our central administration in Vermont, such as Library resources and research support, Accessibility Services, Counseling Services, Title IX information, and Equity, Diversity, and Inclusion resources.

Credit Hours: SIT adheres to the standard that 1 credit hour equals no less than 45 hours of coursework. The calculation is based on the standard 50-minute academic hour. The number of credits each course carries determines how many total hours each course involves in a semester. Of the 45-hours for 1-credit hour, one third is designated for direct faculty instruction. Direct faculty instruction includes all learning activities led by the faculty whether in the classroom or in the field — lectures, guest speakers, site visits, hands-on field activities, etc.

Note on Late Assignments: Because this program integrates classroom learning with site visits and debriefs, assignments are designed to build on one another and connect directly to learning on location. *Timely submission is therefore important for maintaining continuity and full participation in the academic experience*. Extensions may be granted *in limited circumstances and on a case-by-case basis* with approval from the Program Director or a designated staff member. Requests should be made in writing as early as possible and no later than 12 hours before the posted due date. Students are expected to communicate proactively if challenges arise. Work submitted after an approved extension period may receive a reduced or failing grade, depending on the circumstances.

Note on the Use of Generative AI Tools: In this course, students may use generative AI tools only in ways that support their own intellectual work. Acceptable uses may include brainstorming questions, organizing notes, clarifying concepts, or supporting revision at the sentence or structure level. Students may not use AI tools to generate substantive analysis, strategic arguments, written sections, or oral responses that are presented as their own work. Because assignments emphasize applied reasoning, comparative judgment, and place-based analysis, students are expected to remain the primary source of ideas, interpretation, and decision-making.

Expectations for AI use may vary by assignment and will be discussed explicitly with faculty. In some cases, students and faculty may collaboratively establish guidelines for appropriate AI use for a particular task. Students are responsible for following the agreed-upon expectations and for seeking clarification if boundaries are unclear.

When generative AI tools are used in the preparation of an assignment, students are expected to acknowledge their use clearly and transparently, noting the tool used and the nature of its contribution (e.g., brainstorming, outlining, or language revision). This acknowledgment supports academic transparency and does not, on its own, imply inappropriate use.
Policies on AI use may differ across courses and instructors within the program. Students should attend carefully to course-specific guidance and understand that responsible AI use is defined at the course level.

Sample AI Acknowledgment Statement: I used [tool name] for [purpose, e.g., brainstorming or sentence-level revision]. All analysis, interpretation, and conclusions are my own.

Course Schedule

**Please be aware that topics and excursions may vary to take advantage of any emerging events, to accommodate changes in our lecturers' availability, and to respect any changes that would affect student safety. Students will be notified if this occurs.*

Module 1: Intelligence Fundamentals and the Korean Context

This opening module introduces core theoretical frameworks for understanding intelligence in national security and foreign policy, establishing foundational concepts that will be explored throughout the course. Students examine how states collect, analyze, and share information to anticipate threats and inform decision-making, with particular focus on South Korea's intelligence architecture and regional challenges.

Session 1: Introduction—Intelligence and Information Power

Possible topics covered:

- Defining intelligence: collection, analysis, dissemination, covert action
- Intelligence cycle and decision-making processes
- Information power in international relations: persuasion, influence, disruption
- Intelligence failures and pathologies: groupthink, politicization, mirror-imaging
- Course overview and assignment introduction

Required Readings:

- Nye, J. S. (2011). The future of power. PublicAffairs. (https://www.files.ethz.ch/isn/154756/issuesinsights_vol11no08.pdf)

- Warner, M. (2002). Wanted: A definition of "intelligence." *Studies in Intelligence, 46*(3), 15-22.

Session 2: South Korea's Intelligence Architecture and Regional Threats

Possible topics covered:

- National Intelligence Service (NIS): structure, mandate, reforms
- Defense Intelligence Agency and military intelligence
- Cyber Command and digital security units
- Intelligence sharing with United States: agreements, liaison relationships, joint operations

Required Readings:

- International Crisis Group. (2014). *Risks of intelligence pathologies in South Korea* (Asia Report No. 259). https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/259-risks-intelligence-pathologies-south-korea
- Boo, H. (2017). An Assessment of North Korean Cyber Threats. *The Journal of East Asian Affairs*, *31*(1), 97–117. http://www.jstor.org/stable/44321274

Optional Readings:

- Gioe, David. 'The History of Fake News', The National Interest (July 1, 2017), https://nationalinterest.org/feature/the-history-fake-news-21386
- Voo, J. (2024). Driving wedges: China's disinformation campaigns in the Asia-pacific. In *Asia-Pacific Regional Security Assessment 2024* (pp. 108-123). Routledge.

Module 2: North Korean Cyber Operations and Asymmetric Warfare

This module examines North Korea's cyber capabilities as a model of asymmetric warfare, analyzing how a resource-constrained state uses cyber operations to achieve strategic objectives. Students explore technical capabilities, organizational structure, strategic logic, and international responses.

Sessions 3 and 4: North Korean Cyber Capabilities and Organization

Possible topics covered:

- Training programs and overseas deployment of cyber operators
- Technical capabilities: malware development, network intrusion, cryptocurrency theft

- Revenue generation through cryptocurrency theft and cybercrime
- Cyber operations as strategic tool: coercion, deterrence, revenue

Required Readings:

- Horschig, D. (2024, July 31). How Are Cyberattacks Fueling North Korea's Nuclear Ambitions? Center for Strategic & International Studies. https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1-2), 4-37.
- U.S. Department of Justice. (2021). Three North Korean military hackers indicted in wide-ranging scheme to commit cyberattacks and financial crimes across the globe. Press release.

Module 3: Intelligence Cooperation and Alliance Management

This module examines intelligence sharing as a foundation for alliance relationships, with focus on U.S.-ROK cooperation and regional partnerships. Students explore frameworks for sharing classified information, technical cooperation on cyber threats, joint operations, and challenges of trust, security, and sovereignty in intelligence alliances. The module addresses both bilateral cooperation and multilateral initiatives.

Session 5: U.S.-ROK Intelligence Sharing and Alliance Coordination

Possible topics covered:

- History of intelligence cooperation: Korean War to present
- Bilateral intelligence agreements and security classifications
- Combined intelligence operations center and liaison structures
- Signals intelligence cooperation: SIGINT sharing, joint facilities

Required Readings:

- Bronza, R., & Podoler, G. (2025). Historical Gulfs, Strategic Bridges: A Pragmatic-Symbolic Analysis of the GSOMIA Between Japan and South Korea. *East Asia*, *42*(2), 131-155.
- Park, H. R. (2024). What Made South Korea–Japan Security Cooperation Retreat During the Moon Jae-in Administration?. *Journal of Asian Security and International Affairs*, *11*(1), 94-121.

- Seo, H. (2018). Intelligence Politicization in the Republic of Korea: Implications for Reform. *International Journal of Intelligence and CounterIntelligence*, *31*(3), 451–478. https://doi.org/10.1080/08850607.2018.1466566

Session 6: Regional Intelligence Partnerships and Five Eyes Engagement

Possible topics covered:

- Five Eyes intelligence alliance: U.S., UK, Canada, Australia, New Zealand
- South Korea's observer status and potential membership debates
- Intelligence sharing with Japan: GSOMIA controversies, trilateral cooperation
- ASEAN Regional Forum and confidence-building measures

Required Readings:

- Gallagher, M. (2025). Recalibrating the Five Eyes Alliance. *The Washington Quarterly*, *48*(3), 163-185.
- Cooper, Z. (2021, October 4). *Five Eyes Wide Shut*. American Enterprise Institute - AEI. https://www.aei.org/op-eds/five-eyes-wide-shut/
- Panda, J. (2020, August 24). *Is Seoul Prepared to Join a Five Eyes Plus Framework?* 38 North: Informed Analysis of North Korea. https://www.38north.org/2020/08/jpanda082420/

Module 4: Cybersecurity Governance and Digital Threats

This module examines cybersecurity policy frameworks, digital governance structures, and emerging threats in South Korea's highly connected society. Students explore critical infrastructure protection, election security, disinformation campaigns, and the challenge of balancing security with democratic freedoms. The module addresses regulatory approaches, public-private partnerships, and civil society perspectives on digital rights.

Session 7: Critical Infrastructure Protection and Cyber Defense Policy

Possible topics covered:

- National Cybersecurity Strategy and implementation
- Ministry of Science and ICT cybersecurity mandate
- Critical infrastructure sectors: energy, finance, telecommunications, transportation

Required Readings:

- Wood, N. (2024). South Korea's 2024 Cyber Strategy: A Primer | Strategic Technologies Blog | CSIS. Center for Strategic and International Studies. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer
- Kim, S. (2024). ROK's New National Cybersecurity Strategy and Its Implications. 106(3). https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf

Optional Readings:

- Pytlak, A. (2026, February 9). Toward Strategic Agility: A Case for South Korea's Evolving and Adaptive Approach to Cybersecurity • Stimson Center. Stimson Center. https://www.stimson.org/2026/toward-strategic-agility-a-case-for-south-koreas-evolving-and-adaptive-approach-to-cybersecurity/
- Heiding, F., O'Neill, A., & Price, L. (2025, March 27). Cybersecurity Strategy Scorecard. The Belfer Center for Science and International Affairs. https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard

Session 8: Election Security and Disinformation Campaigns

Possible topics covered:

- Election infrastructure vulnerabilities: voter registration, voting systems, results reporting
- Foreign interference campaigns: Russian, Chinese, North Korean activities
- Disinformation and influence operations on social media
- Deepfakes and synthetic media threats

Required Readings:

- Sheehy, B., Choi, S., Khan, M. I., Arnold, B. B., Sang, Y., & Lee, J. J. (2025). Truths and tales: Understanding online fake news networks in South Korea. *Journal of Asian and African Studies*, *60*(4), 2612-2639.
- Lee, S. H. (2024, May 13). AI and Elections: Lessons From South Korea. Thediplomat.com; The Diplomat. https://thediplomat.com/2024/05/ai-and-elections-lessons-from-south-korea

Module 5: Emerging Technologies and Future Challenges

This final module examines how emerging technologies transform intelligence collection, analysis, and operations while creating new vulnerabilities. Students analyze artificial intelligence, quantum computing, surveillance technologies, and biotechnology through security and ethical lenses. The module culminates in student presentations of their Cybersecurity Policy Proposals and course synthesis.

Session 9 & 10: AI, Surveillance, Ethics and Technology

Possible topics covered:

- Artificial intelligence in intelligence analysis: pattern recognition, predictive analytics, automation
- Machine learning for cyber defense and offensive operations
- Surveillance technologies: facial recognition, behavioral analysis, social credit systems
- China's technology development and export of surveillance tools

Required Readings:

- Bae, S., & Kim, S. J. (2025). AI Security Strategy and South Korea's Challenges. Center for Strategic and International Studies. https://www.csis.org/analysis/ai-security-strategy-and-south-koreas-challenges
- Hwang, W., Paik, W., & Lim, H. (2024). The US–China competition, restructuring the global supply chain, and economic security. *Journal of East Asian Studies*, *24*(3), 324-342.
- Greitens, S. C. (2020). Dealing with demand for China's global surveillance exports. *Brookings Institution Global China Report*.
- Park, J. (2023). Is Economic Security National Security? Defining South Korea's Economic Security for Future Industries. *KEI Editorial Board*, 52.

Final Discussion: Synthesizing course themes: How should democracies balance security and privacy in the digital age? What are the most pressing intelligence challenges facing South Korea? How can intelligence cooperation strengthen alliances while respecting sovereignty?