SA.501 (TECHNOLOGY AND INNOVATION)

Courses

SA.501.100. News Media & International Affairs. 4 Credits.
The purpose of this course is to provide deeper understanding of the interaction between the operations of the news media and the conduct of international relations. This will include an emphasis on how rapidly the major medium of exchange has passed in barely 50 years from newspapers to broadcast to the internet. The instruction will be through a combination of lectures, guest lectures, student discussion and papers. There will be an emphasis on clear and good writing. Student evaluation will be based on participation in discussion and papers.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.600.755[C]

SA.501.104. Artificial Intelligence: The Science, Ethics, and Politics. 4 Credits.
Artificial intelligence (AI) and machine learning (ML) have emerged as increasingly significant areas of inquiry and debate in science, technology, and society. From search engines, advertising, and chatbots to autonomous weapon systems, driverless vehicles, financial risk management, law enforcement, and medical diagnosis, AI and ML are being integrated within many services and products across a range of industries. At the same time, AI-enabled technologies are facilitating discrimination, raising questions on privacy and transparency, fueling fears about labor shortages, and feeding competition on the international stage. The challenge of today and tomorrow is taking a human-centered approach to filling the gap between technology, ethics, and policymaking. We will review and discuss industry use cases to better understand the complexity and evolution of AI. Students will work on a semester-long group research policy project on a topic of their choice.

SA.501.105. Technology and Geopolitical Risk Practicum. 4 Credits.
From the printing press and nuclear reactor to the internet, advancements in technology have historically been major drivers of geopolitical shifts. Today, technologies such as blockchain, artificial intelligence, and nanotechnology, have become indistinguishable from national and inter-state interests. This course gives students the tools to understand and integrate disruptive technologies in their analysis of geopolitical risks in the twenty-first century; examine how technology affects our societies, international development, and the use of force; and the demands on regulatory institutions in a world increasingly reliant on machines.
The course is interactive and employs a suite of learning techniques, including academic scholarship, business case studies, and discussion with subject-matter experts. Simultaneously, students collaborate on a group consulting project with an outside client related to a relevant set of social, political, and/or economic risks concerning a technology solution. Findings are presented as an oral pitch and final whitepaper. Students aspiring for careers in government, technology, or political risk consulting will find this practicum especially beneficial.

SA.501.106. Technology, Innovation, and Public Policy. 4 Credits.
Technology and governance are in perpetual tension. Relative power and wealth can be created, destroyed, enabled, denied, checked, and balanced when technologies emerge, and governments react. In this course students will prepare and present business case studies focusing on the role of governments in each case and how policy related to innovation altered the trajectory of markets, domestic politics, and international relations. The case studies will be a starting point for discussions of alternative strategies that firms and states might have employed to their respective advantage and any case specific lessons with broader application for innovators, investors, policymakers, and citizens.

SA.501.107. Clashing Information Orders. 4 Credits.
People thought until recently that global information flows would lead to the global spread of liberal values and democracy, as social media platforms allowed citizens to talk and organize freely. Now, we are starting to understand that global information politics doesn't have predetermined winners. States - both democratic and authoritarian contending with each other over who should set the rules for information flows, each trying to impose its own national information order on others. In this class, we will examine where the different information orders of the major powers—the U.S., the E.U. and China—come from, and how each sees the politics of information as bound up with the survival of its own regime. We will examine the different vulnerabilities of democracies and autocracies to global information flows, and how each looks to shore up these vulnerabilities, as well as how each tries to project and spread its own approach to information to other countries, creating a new realm of global power politics.

SA.501.108. Media Wars. 4 Credits.
Is social media making our politics more extreme? How does the circulation of “fake news” differ from propaganda efforts of the pre-digital age? Does it affect our politics in the long-term? How are states using media today not only to inform their own citizens, but as a weapon in larger geo-political contests? Are algorithms racists, and what does that say about the future we are building? This course will take a critical look at the production, circulation, and consumption of media in the contemporary world. We’ll particularly focus on the development of technology, surveillance, cyberwar, militarized media, social movements, and the social life of algorithms. We will explore cases through the Americas, Europe, Middle East, and Africa.

SA.501.109. Technology, Innovation and Strategy. 4 Credits.
The class intends to help students understand the connection between strategy, technology and innovation. The class relies on the literature in international relations and security studies, management science and economics as well as on policy reports and business cases. The multidisciplinary focus of the class stems from the need to understand complex processes and dynamics characterizing an age of great powers competition (strategy) focused on technological superiority (technology) pursued and advanced by start-ups and Big Tech companies (innovation). After deepening the meaning of strategy, technology and innovation, the class looks at the interaction between strategy and technology, technology and innovation as well as innovation and strategy both at the abstract or theoretical level and through empirical or historical instances.The ultimate goal of the class consists of preparing students for understanding the challenges that private or public organizations may face when working in competitive environments characterized by rapid technological change and the need to generate or adopt innovations.

SA.501.110. Data Analytics and Visualization (using R). 4 Credits.
Data analytics and visualization skills are in high demand in today's complex international affairs, geopolitics, and public policy more broadly. This course introduces students to the fundamentals of data science using the R statistical software. The course consists of three main components. The first part builds fluency in basic data manipulation, description, and analysis. The second part focuses on the principles and practical applications of data visualization. In the third part, students generate, analyze, and visualize a large dataset to answer a research question of their choice.

SA.501.111. Introduction to Trust and Safety. 4 Credits.
In an era where digital and social media platforms shape global interactions, a field referred to as "trust and safety" has emerged inside primarily US technology companies aimed at identifying and addressing the risks and harms individuals face online, including but not limited to fraudulent activities, cyberbullying, misinformation, hate speech, identity theft, privacy breaches, and exploitative content. This course explores the evolving landscape of trust and safety (T&S) within technology companies, including the history of the field, contemporary challenges, and tying it to the practice of global affairs. Through a multidisciplinary lens, students will explore how T&S intersects with topics such as national security, foreign policy, and tech policy, gaining insights into the complex dynamics shaping digital governance and online safety. Students will examine the strategies employed by T&S practitioners to anticipate, manage, and mitigate these risks, critically evaluating their efficacy in safeguarding digital spaces and fostering a climate of trust and integrity. This course will also explore the cultural, regulatory, and ethical considerations that inform T&S practices. Students will delve into the legal and regulatory frameworks that govern trust and safety practices in various jurisdictions, including laws such as Section 230, General Data Protection Regulation (GDPR), The Digital Services Act (DSA), Children's Online Privacy Protection Act (COPPA), and their implications for content moderation and user privacy. By examining case studies and real-world examples, students will see what it is like to attempt to address thorny questions facing content moderators, policy makers, product managers, and leaders at technology companies.

SA.501.113. Information Policy Strategy and Design in the Age of AI. 4 Credits.
Information and digital technologies have transformed the way modern societies operate over the last 20 years and introduced unprecedented opportunities as well as thorny policy challenges such as privacy, ethics, data rights, and competition. The meteoric rise of artificial intelligence in the last year has reinvigorated many of these recurring information policy challenges, and heightened tensions between the drive for rapid innovation alongside calls for regulation. Students will develop a foundational understanding of key concepts within information policy issues and apply it to information-intensive emerging technologies including AI/Generative AI, digital platforms and social media, smart devices/Internet of Things, and AR/VR/Metaverse. Students will build technical knowledge necessary to diagnose and remedy policy issues at hand, be able to discuss the ethical tradeoffs and nuances of contested issues from multiple perspectives, and curate a toolkit of policy approaches and regulatory options available for emerging tech. Relevant current events and technological developments will be incorporated into the course throughout the semester, and students will be expected to interact with many of the technologies discussed throughout to spark class discussion and inform future practice. This course will leave students with knowledge that will allow them to feel equally comfortable traversing the boardrooms of Silicon Valley and corridors of power within Washington DC.

SA.501.114. Technology and International Competition. 4 Credits.
This course would focus on technology, particularly military technology and dual use technology, as a variable in international relations. It will consider questions such as how does technology drive security competition and how does it create or obstruct opportunities for cooperation. The course will identify attributes of technology that impact the coercive application of military power in world politics, from damage imposition to coercive leverage in bargaining. The analytic approach will be grounded in case studies of several major technology categories, most likely (1) nuclear technology, notably atomic weapons and power plants; (2) rockets, including precision strike capabilities, hypersonics, ballistic missiles, and space launch vehicles; (3) space systems, primarily satellites and other orbital platforms such as spacecraft and anti-satellite (ASAT) weapons; (4) chemical and biological and (5) artificial intelligence.

SA.501.115. Digitalization and Decarbonization of the Energy Systems. 4 Credits.
This course will examine two concurrent megatrends: the digitalization and decarbonization of the energy sector. With a particular emphasis on artificial intelligence approaches, students will engage in an in-depth exploration of the evolving dynamics within energy generation, transportation, consumption, and storage. Topics of study will encompass a wide spectrum, including the utilization of autonomous and electric vehicles, the assessment of energy consumption in data centers, the digital monitoring of emissions, cybersecurity threats to energy infrastructure, and various strategies for managing energy demand and implementing demand response initiatives. Furthermore, the course will critically assess the policies and frameworks necessary to facilitate robust digital solutions for achieving decarbonization objectives.

SA.501.116. Artificial Intelligence & Epistemic Security. 4 Credits.
This course will explore how the emergence of generative AI is affecting issues of epistemic security (misinformation, influence operations, media consumption, academic integrity, etc.) and how advances in AI could shape our epistemic futures. Students will learn the basics of how foundation models, LLMs, image generation models, and multimodal models work, and how choices across the AI lifecycle, from development to deployment, can cause harmful outputs and/or could contribute to epistemic decline (e.g.: quality of sources on the Internet, issues with model confabulations, academic integrity). Furthermore, students will apply their knowledge of influence operations and misinformation gained from previous courses to understand how malicious actors could use AI to threaten epistemic security, as well as learn more about the current AI malicious actor ecosystem (for both state and non-state actors). Lastly, the course will delve deep into potential solutions to mitigate epistemic crises, from technical mitigations within AI models, content authentication approaches, to broader whole of society efforts (participatory governance, information literacy, etc.). Students put themselves in the shoes of various actors in the current AI ecosystem, specifically: large AI developers, social media platforms, and policymakers across the US government, to produce targeted outputs for the course. In addition, students will engage with and use generative AI tools to understand various types of harms and will also learn unique insights into the challenges of trust & safety in the AI space. Course outputs could include: an internal policy enforcement protocol for disinformation for a large AI developer, a policy memo for the Director of OSTP on AI and information integrity, an exercise to generate known mis/disinformation narratives using generative AI models, and more.

SA.501.117. The Intersection of Space Systems Engineering and International Public Policy. 4 Credits.
This course straddles the boundary between engineering and public policy related to Outer Space. It presents space policy and the effects that policy has on engineering decisions. It presents the underlying space systems engineering principles that necessitate space policy. Space is a highly technical and nonintuitive domain. Professionals working in any space-related field should have a basic understanding of the relationship between engineering and international public policy.

SA.501.118. Biotech, Artificial Intelligence, and Health Security. 4 Credits.
This course explores the link between security (national and international) and public health. Its primary target audience are students who may not have health security as a primary work responsibility in the future, but will need an understanding of how public health, biotechnology, emerging technologies like AI, and infectious diseases have national or international security implications. Students will gain an understanding of the impact disease has on security, and will have an opportunity to examine the policy, ethical, historical, and economic issues that surround biological sciences and security, including the development of medical countermeasures. Trends and advances in the biological sciences, their societal and health benefits, the potential threat of deliberate or accidental misuse, and preparations for a future pandemic will be explored. Students will gain an understanding of how past disease emergencies have intersected with national and international security from a US perspective, including COVID-19, Ebola (2014), and anthrax (2001), and ongoing US preparations for future health security events. While classes will be taught by Hopkins faculty, class sessions will also engage experts across the US Government, industry, and relevant policy organizations for lecture discussion and student interaction and networking.

SA.501.119. AI and National Security. 4 Credits.
The course examines one of the topics most central for the future of national security policy: artificial intelligence (AI). We will begin first by examining what AI is and isn't, and discuss how the underlying technology works. We will then proceed to survey the national security landscape and consider how AI will impact key policy and strategy decisions in the near future. Topics discussed include autonomous weapons, intelligence collection and analysis, cyber attacks, disinformation, and technology competition. We will also focus on the AI strategies of the US and China. No technical background is required for this class, though we will introduce some important ideas that are relevant to how AI works. Students will be evaluated through a key concepts quiz that assesses understanding of important ideas. They will also be assigned one final paper in which they will take a stand on a proposition regarding AI's policy impact. In addition, class participation is a vital component of this class, as a substantial portion of each week will be oriented towards discussion.

SA.501.120. Unleashing Prometheus: Technology and Development. 4 Credits.
The seminar will examine three major issues. First, how technology has, and can be, leveraged to address major development challenges, from strengthening human capital to alleviating pollution to adapting to climate change as well as the core challenge of production and jobs in a developing economy. Second, how will the "Fourth Industrial Revolution" (IoT, 5G, AI) affect the economic prospects of developing countries. Finally, what are the main policy instruments (from industrial policy to standards), that can help developing countries better leverage technology for development.

SA.501.121. Ghost in the Machine: The Intellectual History of AI and its Risks. 4 Credits.

SA.501.122. Cyber Operations: How and Why States Compete in Cyberspace. 4 Credits.
How, and why, do states compete in cyberspace? Scholars of war and conflict have long divided their subject into three segments: the strategic, the operational, and the technical. The most widely discussed of these, strategy, focuses on big questions like deterrence. Technical analysis is also common in specialized courses and, in a topic like cybersecurity, requires a fair amount of computer science knowledge. In contrast, with its focus on the operational dynamics at play, this course bridges the gap between strategic concepts and technical details. Over the course of the semester, we will establish a model for offensive and defensive cyber operations and introduce key terms and concepts that can be flexibly deployed to understand a wide range of incidents, actors, and pressing policy debates. We will use these models and concepts to examine how different groups of hackers performed their missions and what outcome resulted. With this solid foundation established, we will use our operational understanding to re-examine strategic ideas and policy debates like deterrence, attribution, resilience, and persistent engagement in a new and more informed light.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.154[C]

SA.501.123. Semiconductors: Industry, Security, and Geopolitics. 4 Credits.
Semiconductors are the quintessential foundational, and therefore geostrategic, technology. They are simultaneously essential for (a) military and defense technology, weaponry, and equipment; (b) geopolitically significant technologies, such as Artificial Intelligence (AI); and (c) the critical infrastructure and services upon which the daily functioning of societies rest, such as 5G networks and satellite communications. It is this breadth of use-cases that has raised the semiconductor industry from 'important' to the level of 'national security imperative'. This course will take students beyond the buzzwords to examine the technology (and technologies) in question, the supply chains underpinning them, the use-cases they enable as well as the ways in which those same use cases (most notably AI) are reshaping the industry, and the evolving and diverging security and economic interests animating the global policy landscape.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.176[C]

SA.501.124. Evolution of Cyberpolicy. 4 Credits.
This class will explore the different economic, political, and civil tensions that have shaped cyber policy over the last 20 years. Too many practitioners of cyber policy and operations have not thought deeply about the underlying assumptions and history that current policies are based on. Similarly, there is minimal appreciation for how other countries experience the US-dominated approach to the development of the internet economy and how this shapes their own approach to cyber policy. Students will finish the class with an understanding of the fundamental principles of US cyber policy that have remained constant and emerging trends that are leading the US and other countries to assert greater dominance. The class will dive deeper into the accepted wisdom of established cyber norms and principles and determine whether the assumptions these are based on are flawed. Students will also gain a deeper understanding of the domestic and international dynamics that shape Russian and Chinese approach to cyber policy.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.178[C]

SA.501.125. Introduction to Applied Machine Learning for Threat Intelligence Analysis. 4 Credits.
Students will be introduced to applied machine learning (ML) to support cyber and other threat intelligence investigations and analysis. The course covers fundamental machine learning concepts, approaches, and best practices, including topics on classification, clustering, and model building and evaluation. These will be applied using Python through substantive examples within the realm of intelligence investigations and analysis to help students become familiar with how such approaches might be put to practice. The course will not be heavily focused on theory or the underlying math of models, but instead focus on developing student familiarity with basic applications of common ML approaches —geared towards students who have no, or very little, prior exposure to coding. students will be expected to do substantial work to develop their Python skills. Python and introduction to ML are typically taught as two separate classes, so tackling them both in a single course will be an ambitious undertaking for you, but a rewarding one. (Course is not for students with significant Python experience, as it will be too slow paced—contact professor if you have questions.)
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.191[C]

SA.501.128. Cyber-Enabled Intelligence and Covert Action. 4 Credits.
On a practical level, state-nexus cyberspace ("cyber") operations have become a ubiquitous element of contemporary intelligence activities. To that end, this course presents cyber operations through a traditional intelligence tradecraft lens. This includes the specific role and function of cyber operations when they are employed to support intelligence collection, counterintelligence, covert action, and operational enablement activities. Students will also be exposed to how unique elements of cyber activity (such as cybercrime tactics) can and have been leveraged in an intelligence context, the ethics of cyber operations as an intelligence activity, and case studies regarding how different countries approach the conduct of such activities. Students who complete this course will be prepared to interpret state-nexus cyber operations in the context of traditional intelligence contests between states.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.157[C]

SA.501.129. Global Cyber Threats. 4 Credits.
Who are the hackers that dominate headlines? This course will answer that question not just with broad terms like "Russia" and "China" but with more focused and nuanced analysis. We will focus on known hacking groups, their methods, motivations, and relationship to greater geopolitical developments. The course will focus primarily on state-affiliated threats, though it will touch other realms of the cyberthreat ecosystem as well. Students completing this course will have a foundational knowledge of what nations are doing in cyberspace, an important step towards subject matter expertise.No background in computer science is necessary for this class, though you should be willing to push yourself out of your technical comfort zone and be persistent in learning new skills. We will examine many case studies of historic and contemporary adversary behavior. Students will gain strategic perspective by examining reporting that will include tactical, operational, and strategic insights. Many of these examples are available in the open source literature, but additional context will be provided in class discussion.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.110[C]

SA.501.130. Influence Operations in the Digital Age. 4 Credits.
This course will explore how global actors have weaponized false or misleading information and personas to shape public perceptions, achieve strategic geopolitical goals, make money, and pollute the information environment. Students will study the new tools being used by state and non-state actors and examine the reach/effectiveness of disinformation campaigns in shaping public dialogue. In particular, this course will explore how the practice of influence operations has changed in the information age, how both state and non-state actors weaponize technology, social networks, and other tools for dissemination, and what makes human beings and societies vulnerable to influence operations. In addition to covering state- sponsored influence operations, this course will also dive into financially motivated operations, the role of traditional media and state media, and the inadvertent spread of viral false information, otherwise known as misinformation. Students will study how to detect influence campaigns using open-source investigative techniques and discuss the difficulties of attribution particular to the influence operations space. Finally, this course will explore regulatory, diplomatic, technological, and societal mitigations and interventions aimed at protecting the information environment, assessing their effectiveness.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.140[C]

SA.501.131. The Combined Threat: Counterintelligence and Cyber. 4 Credits.
The traditional counterintelligence and cyber threats posed to the United States by nation-state and cyber-criminal actors is at an unprecedented level. Our nation state adversaries and criminal cyber enterprises routinely target United States-based companies, academic institutions, and various other organizations for their own gain. These gains are for the purpose of economic and political advantages and come in the form of Intellectual Property theft, surreptitious collection of policy positions, and financial extortion. But, how (and why) do our adversaries select their United States-based targets and how effective are our adversaries at accomplishing their strategic objectives? In understanding how our adversaries select their targets, we can begin to understand our adversaries' strategic intent. In this course, you will learn not only about these threats and how they manifest in the United States – both at the strategic and tactical level – but also how the Intelligence Community understands the strategic intent of our adversaries and combats their actions in our country.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.170[C]

SA.501.132. Cyber: Intelligence and Policy. 4 Credits.
The US cyber apparatus is an oft-discussed but little understood instrument of US national power. This course will define the defensive and offensive cyber elements of the USG and private sector and explain the historical evolution of the terms and concepts. This will include a basic overview of the evolution of the internet, the concepts of computer network exploitation vs computer network attack, and a study of nation state and non-nation state cyber threats. This baseline understanding will then allow students to understand the economic, military, and counter-intelligence threat posed by adversary cyber actors and methods for the USG and private sector to counter these threats. Finally, with this knowledge on-hand, students will debate the efficacy of recently published National Cyber Strategy and associated policies and pending legislation.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.175[C]

SA.501.133. Digital Counterintelligence. 4 Credits.
The rise of computer network operations is an increasingly well-known story. This course explores the missing flip-side of cyber espionage: the neglected twenty-year story of one of the most momentous and radical shifts in the entire history of intelligence—the rise of digital counterintelligence. This hidden revolution was powered by a tripod of forces, all coming to the fore in the mid-2010s: the explosive growth of digital espionage; the extraordinary rise of an alternative, entrepreneurial investigative community that cut across sectors and borders; and by the drip-drip of three vast, unprecedented, and unique intelligence leaks. The class traces the evolution of some of the core conceptual frameworks and essential tools of threat intelligence and digital forensics, such as the "advanced persistent threat," the cyber kill chain, indicators of compromise, network monitoring, malware analysis, and attribution. The class will, unlike any other class anywhere, illustrate and contrast the rise of private sector APT hunting with a detailed chronological look at how Five Eyes intelligence agencies pioneered "counter computer network exploitation." We will explore core intelligence concepts of passive collection, active-passive integration, signals intelligence development, implant frameworks, and fourth party collection.
Prerequisite(s): Students may not register for this class if they have already received credit for SA.502.199[C]

SA.501.134. Shaping the Next Industrial Revolution: Biotechnology Innovation Policy. 4 Credits.
The world is embarking on a biotechnology revolution, with new biological tools that impact not just human health but also energy, climate change, food systems, supply chains, and national security. Over the past 3 years, multiple federal biotechnology policies have accelerated the expansion of the bioeconomy, and our nation finds itself at an inflection point. This course aims to inspire a new generation of bio-literate policy leaders by exploring the current and future impacts of biotechnology, the biotech policy ecosystem, and the pathways by which policy ideas are implemented. The course is designed for non-technical students interested in pursuing policy roles that influence the rapidly evolving field of biotechnology. The first third of the course is focused on developing a foundational understanding of key concepts in biology, providing the knowledge necessary to engage effectively with technical subject matter experts. The remainder of the course leverages the case study method to help students examine the impact of policy (i.e., industrial policy, regulation, standards, etc.) on the advancement of biotech. This will include a focus on the startup ecosystem and considerations that impact investor decisions on financing biotech startups. Additionally, students will examine the ways in which policies such as the Bioeconomy Executive Order came to fruition. By the end of the course, students will not only understand the magnitude of biotechnology's potential but also feel empowered to shape its future through thoughtful and informed policy making.

SA.501.135. Democratic Strategies in an Age of Information Conflict. 4 Credits.
This course examines how democracies can respond to propaganda, covert influence, and political warfare. Co-taught by instructors with experience in journalism, intelligence, and policy, the course combines theory with practice, asking what democratic resilience looks like in an era of global information confrontation. Drawing on historical and contemporary case studies—from World War II black radio and Cold War psyops to modern-day Ukraine and recent U.S. elections—the course explores tools and strategies that can be employed today across government, technology platforms, and civil society.

SA.501.136. Political Economy of AI. 4 Credits.
The political economy of AI explicitly or implicitly shapes arguments about the consequences of AI for politics and policy. Will AI continue to scale until it produces super-human intelligence? Will it continue to need enormous amounts of human generated data? What consequences will it have for the working of the economy and bureaucracy? And how will its benefits and costs be distributed among different social groups? In this seminar class, we will explore emerging debates over how the technology of AI intersects with classic debates in political economy.