Information Sheet
Eisenhower School – Cyber Domain/Advanced Computing Industry Study (January-May 2020)
30 September 2019

Course/Mission: The Cyber Domain/Advanced Computing Industry Study ('Cyber IS') is one of 18 industry studies at the Eisenhower School, National Defense University (NDU), that examines the resourcing component of national security. As such, it supports Eisenhower's mission of "[preparing] select military officers and civilians for strategic leadership and success in developing a national security strategy and in evaluating, marshaling, and managing resources in the execution of that strategy."[1]

Overview/Scope of Study: The Cyber IS is a 1-semester spring course in a 10-month, full-time program for students completing a Master of Science in National Resource Strategy. Through readings, case studies, seminars, research, policy papers, guest speakers, and visits to firms/agencies in the United States and abroad, IS students will learn about market structures and business strategies, compare business environments, and gain industry-specific insights. They will also develop a strategic perspective on U.S. and global industrial bases, and their role in supporting the resource requirements for national security. This course is about industry, innovation, and resourcing, primarily in four areas—(1) cyber-security/cyberspace operations (e.g., equipping cyberspace forces), (2) artificial intelligence (AI), (3) advanced computing (quantum and neuromorphic), and (4) 5G telecommunications (specifically, the expanding Internet of Things (IoT) and its implications). We will engage with researchers, educators, operators, legislative staff, lobbyists, startups, investors, accelerators, and firms of many kinds. Most course content will be unclassified; cleared students will attend some sessions with classified content.

Students: The Eisenhower School student body includes approx. 300 mid-career U.S. and international military officers, interagency civilians, and private sector executives. The Cyber IS class will have about 17 students: 13 U.S. military officers (O5-O6) and U.S. government civilians, and four international officers from allied/partner nations. In the future, many of our graduates will play a role in acquiring new capabilities, influencing policy development, and resourcing U.S./allied national security strategies.

Faculty: The Faculty Lead for the Cyber IS is Col Andrew Nichols, USAF (andrew.h.nichols.mil@ndu.edu), and the #2 is CAPT R.A. (Rambo) Torruella, Jr., USN (ramberto.a.torruella.mil@ndu.edu).

The Industry. The primary business areas and markets served by firms in this ecosystem include:

Enterprise Software/Applications	IT Infrastructure	Devices/Mobile Phones
Consumer Software/Applications	High-Performance Computers	Autonomous Vehicles
Internet Media/Social Media	Personal Computers	Human Capital
Data Aggregators/Sellers	Semiconductors & Processors	Cyber Risk Insurance
IT Services	Telcos (Wireless & Fixed-Line)/ISPs	E-Waste Management

Industry Context: The cyber domain is a vast, expanding network of more than 20 billion devices[2]—hardware, software, data, and more—that has improved our lives and enabled tremendous wealth creation. The top 10 largest technology firms alone have amassed $4.8 trillion in market capitalization, with eight U.S. firms accounting for $4.1 trillion (85%).[3] In terms of revenue, these 10 firms earn $856 billion annually, and U.S. firms capture a 69% share.[4] In the telecommunications area, by comparison, the top 300 firms globally earn a little more—about $1.4 trillion per year.[5] Among the defense prime contractors, the top 12 earn $290 billion per year, and U.S. firms capture about 32%.[6] Among the cyber-security software firms, the top 10 earn $16.5 billion annually, and U.S. firms capture a 67% share.[7]

Approach: After analyzing a dozen and a half cyber case studies, the class will turn its attention to industry players, key technologies, and the competitive environment. The topics discussed will include: business-government relations, the national innovation system, supply chain management, human capital as a source of competitive advantage, agile software development, industrial security (protection of critical technology), U.S.-Russia and U.S.-China trade and security concerns, and finally, mobilization—specifically, how to leverage industry capabilities/contributions to respond to a potential national crisis.

Policy Challenges (not all-inclusive). Among the issues we will discuss during the course are these:

- What actions should be taken, and by whom, to promote continued innovation, corporate and industrial competitiveness, and economic growth in the technology sector?
- What actions should U.S. strategic leaders take in collaboration with domestic and international partners in government, industry, and academia to defend and advance national interests?
- What actions should future national security leaders take to address the challenges and opportunities presented by AI, advanced computing, and telecom technologies (esp. 5G) over the next 5-10 years?

Domestic Field Studies. The U.S.-based hosts and guest speakers are tentatively projected to include:

a16z	CrowdStrike	FireEye	In-Q-Tel	Northrop Grumman	The Capital Factory
ARL:UT	CTIA	Google	Intel	NSA	Univ. of Maryland
AT&T	DISA	HP	MassChallenge	NVIDIA	Univ. of Texas at Austin
BSA	Enlighten	IBM	Microsoft	SparkCognition	U.S. Cyber Command
Cisco	FBI	Illumio	NASA ARC	Symantec	Verizon

Overseas Field Studies: Plans are currently under development for an overseas visit to either (1) Israel (multiple locations) (18-24 April 2020), or (2) Tokyo, Japan, and Taipei, Taiwan, ROC (20-29 April 2020). We are also considering dividing the students into two travel groups (*I* and *T*) to send *I* to (1) and *T* to (2).

Student Deliverables: During the course, the students will produce an individual research paper and a group research paper to address strategic industry and policy issues examined during the course. They will also receive practice drafting a policy recommendation memo for a senior government official. The course will culminate in late May 2020 with a student-led presentation (with recommendations) to a distinguished panel of senior government and industry executives.

Non-Attribution Policy: To support candid discussions among speakers, hosts, and students, speakers' remarks will not be attributed to them in any student product without their expressed consent.

Representative Questions for Host Firms (on topics we would like to learn about during a visit):

- What factors most influence your strategic business decisions, and how do you think about them?
- What legal/policy changes would you like to see to enhance competitiveness, innovation & growth?
- In what ways could the govt. improve acquisition methods and system performance/affordability?
- In the event of a national crisis, how should strategic leaders leverage your firm's capabilities?

Representative Questions for Host Research Institutions and Universities:

- What opportunities & challenges will AI/quantum/neuromorphic computers offer in the next 10 yrs.?
- What should future national security leaders do to better leverage AI/quantum/5G technologies?

Representative Questions for Visited Government Agencies:

- What else should be done with domestic and int'l partners to defend & advance national interests?
- What else should be done to secure data and reduce illegal transfers of critical data/technologies?
- What new authorities, capabilities, or actions would significantly enhance your mission effectiveness?

Notes

1. The Eisenhower School, https://es.ndu.edu/About/Mission/ (accessed 28 September 2019).

2. Munich Security Conference Foundation GmbH, "Munich Security Report 2018: To the Brink and Back?" (2018), pg. 51. https://dynamic.faz.net/download/2018/MunichSecurityReport2018.pdf (accessed 19 September 2019). Munich Security Conference analysis/graphic based on Gartner, "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," 7 February 2017, https://www.gartner.com/newsroom/id/3598917, and United States Census Bureau, International Data Base, https://www.census.gov/data-tools/demo/idb/informationGateway.php (accessed 11 January 2018). According to the projections in the 2018 Munich Security Conference graphic (p. 51), in 2020, the global population will reach 7.636 billion people, and there will be about 20.415 billion connected devices in the world, or about 2.7 per person, on average.

3. Jonathan Ponciano, "The Largest Technology Companies in 2019: Apple Reigns as Smartphones Slip and Cloud Services Thrive," *Forbes* (May 15, 2019). https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#437d6ab1734f (accessed 28 September 2019).

4. Market share estimates based on industry revenue data provided by Bloomberg.

5. Ibid.

6. Ibid.

7. Ibid.