U.S. House of Representatives
COMMITTEE ON ETHICS

Employee Post-Travel Disclosure Form

☐ *Original* ☐ *Amendment*

This form is for disclosing the receipt of travel expenses from private sources for travel taken in connection with official duties. This form does not eliminate the need to report privately-funded travel on the annual *Financial Disclosure Statements* of those employees required to file them. In accordance with House Rule 25, clause 5, you must complete this form and *file it with the Clerk of the House, B-81 Cannon House Office Building*, within 15 days after travel is completed. Please *do not* file this form with the Committee on Ethics.

NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.

1. Name of Traveler: Sarah Moxley

2. a. Name of Accompanying Relative: _____ *OR* None ☑
   b. Relationship to Traveler: ☐ Spouse ☐ Child ☐ Other (specify): _____

3. a. **Dates:** Departure: 8/26/2019 Return: 8/29/2019
   b. Dates at Personal Expense, if any: _____ *OR* None ☑

4. Departure City: Washington, DC Destination: San Francisco, CA Return City: Syracuse, NY

5. Sponsor(s), Who Paid for the Trip: Stanford University

6. Describe Meetings and Events Attended: See attached.

7. Attached to this form are *each* of the following, *signify that each item is attached by checking the corresponding box*:
   a. ☐ a completed *Sponsor Post-Travel Disclosure Form*;
   b. ☑ the *Primary Trip Sponsor Form* completed by the trip sponsor *prior* to the trip, *including all* attachments *and* the *Grantmaking* or *Non-Grantmaking Sponsor Forms*;
   c. ☑ page 2 of the completed *Traveler Form* submitted by the employee; *and*
   d. ☑ the letter from the Committee on Ethics approving my participation on this trip.

8. a. I represent that I participated in each of the activities reflected in the attached sponsor's agenda.
   Signify statement is true by checking the box: ☑
   b. If not, explain: _____

I certify that the information contained on this form is true, complete, and correct to the best of my knowledge.

Signature of Traveler: _____ Date: 9/3/2019

I authorized this travel in advance. I have determined that all of the expenses listed on the attached *Sponsor Post-Travel Disclosure Form* were necessary and that the travel was in connection with the employee's official duties and would not create the appearance that the employee is using public office for private gain.

Name of Supervising Member: Mike Rogers Date: 9/3/2019

Signature of Supervising Member: _____

Version date 12/2018 by Committee on Ethics

U.S. House of Representatives
COMMITTEE ON ETHICS

Sponsor Post-Travel Disclosure Form

☑ *Original* ☐ *Amendment*

This form must be completed by an officer of any organization that served as the primary trip sponsor in providing travel expenses or reimbursement for travel expenses to House Members, officers, or employees under House Rule 25, clause 5. A completed copy of the form must be provided to each House Member, officer, or employee who participated on the trip *within ten days of their return*. You must answer all questions, and check all boxes, on this form for your submission to comply with House rules and the Committee's travel regulations. Failure to comply with this requirement may result in the denial of future requests to sponsor trips and/or subject the current traveler to disciplinary action or a requirement to repay the trip expenses.

NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.

1. Sponsor(s) who paid for the trip: Stanford University
2. Travel Destination(s): Stanford University, Stanford, CA
3. Date of Departure: August 26, 2019 Date of Return: August 29, 2019
4. Name(s) of Traveler(s): Attached list

   Note: You may list more than one traveler on a form only if ***all*** information is ***identical*** for each person listed.
5. **Actual amount** of expenses paid on behalf of, or reimbursed to, each individual named in Question 4:

	Total Transportation Expenses	Total Lodging Expenses	Total Meal Expenses	Total Other Expenses (dollar amount per item and description
Traveler	$599.45	$600 ($200/night)	$191.07	$86.68 ground transportation
Accompanying Family Member	N/A	N/A	N/A	N/A

6. All expenses connected to the trip were for actual costs incurred and not a *per diem* or lump sum payment. *Signify statement is true by checking box:* ☑

I certify that the information contained in this form is true, complete, and correct to the best of my knowledge.

Signature: Russell Wald Date: 09/05/2019

Name: Russell Wald Title: Senior Manager, External Affair

Organization: Stanford University

I am an officer of the above-named organization. Signify statement is true by checking box: ☑

Address: 434 Galvez Mall, Stanford, CA 94305

Telephone: 650-850-9034 Email: rwald@stanford.edu

Committee staff may contact the above-named individual if additional information is required.

If you have questions regarding your completion of this form, please contact the Committee on Ethics at 202-225-7103.

U.S. House of Representatives
COMMITTEE ON ETHICS

TRAVELER FORM

1. Name of Traveler: Sarah Moxley
2. Sponsor(s) who will be paying for the trip: Stanford University
3. City and State OR Foreign Country of Travel: Stanford, CA
4. a. Date of Departure: 8/26/19 Date of Return: 8/29/2019
   b. Will you be extending the trip at your personal expense? ☐ Yes ☑ No
   If yes, list dates at personal expense: _____
5. a. Will you be accompanied by a family member at the sponsor's expense? ☐ Yes ☑ No **If yes:**
   (1) Name of Accompanying Family Member: _____
   (2) Relationship to Traveler: ☐ Spouse ☐ Child ☐ Other (specify): _____
   (3) Accompanying Family Member is at least 18 years of age: ☐ Yes ☐ No
6. a. Did the trip sponsor answer "Yes" to Question 8(c) on the *Primary Trip Sponsor Form* (i.e., travel is sponsored by an entity that employs a registered federal lobbyist or a foreign agent)? ☐ Yes ☑ No
   b. **If yes**, and you are requesting lodging for two nights, explain why the second night is warranted:
7. *Primary Trip Sponsor Form* is attached, including agenda, invitee list, and any other attachments and contributing sponsor forms: ☑ Yes ☐ No
   NOTE: The agenda should show the traveler's individual schedule, including departure and arrival times and identify the specific events in which the traveler will be participating.
8. Explain why participation in the trip is connected to the traveler's individual official or representational duties. **Staff should include their job title and how the activities on the itinerary relate to their duties.**
   See attached.
9. Is the traveler aware of any registered federal lobbyists or foreign agents involved planning, organizing, requesting, or arranging the trip? ☐ Yes ☑ No
10. For staff travelers, to be completed by your employing Member:

ADVANCED AUTHORIZATION OF EMPLOYEE TRAVEL

I hereby authorize the individual named above, an employee of the U.S. House of Representatives who works under my direct supervision, to accept expenses for the trip described in this request. I have determined that the above-described travel is in connection with my employee's official duties and that acceptance of these expenses will not create the appearance that the employee is using public office for private gain.

Signature of Employing Member M Rogers Date 7/19/19

U.S. House of Representatives
COMMITTEE ON ETHICS

Primary Trip Sponsor Form

This form should be completed by private entities offering to provide travel or reimbursement for travel to House Members, officers, or employees under House Rule 25, clause 5. A completed copy of the form (and any attachments) should be provided to each invited House Member, officer, or employee, who will then forward it to the Committee together with a *Traveler Form* **at least 30 days before the start date of the trip.** The trip sponsor should *NOT* submit the form directly to the Committee. The Committee website (ethics.house.gov) provides detailed instructions for filling out the form.

NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001. Failure to comply with the Committee's Travel Regulations may also lead to the denial of permission to sponsor future trips.

1. Sponsor who will be paying for the trip: Stanford University

2. I represent that the trip will not be financed, in whole or in part, by a registered federal lobbyist or foreign agent. *Signify that the statement is true by checking box:* ☑

3. ***Check only one.*** I represent that:
   a. The primary trip sponsor has not accepted from any other source, funds intended directly or indirectly to finance any aspect of the trip: ☑ OR
   b. The trip is arranged without regard to congressional participation and the primary trip sponsor has accepted funds only from entities that will receive a tangible benefit in exchange for those funds: ☐ OR
   c. The primary trip sponsor has accepted funds from other source(s) intended directly or indirectly to finance all or part of this trip and has enclosed disclosure forms from each of those entities. ☐
   If "c" is checked, list the names of the additional sponsors: _____

4. Provide names and titles of **ALL** House Members *and* employees you are inviting. **For each House invitee, provide an explanation of why the individual was invited** (include additional pages if necessary): Attached list of staffers have been chosen to attend due to their background or interest in the policy areas being discussed.

5. Is travel being offered to an accompanying family member of the House invitee(s)? ☐ Yes ☑ No

6. Date of Departure: August 26, 2019 Date of Return: August 29, 2019

7. a. City of departure: Washington, DC
   b. Destination(s): Stanford University, Stanford, CA
   c. City of return: Washington, DC

8. ***Check only one.*** I represent that:
   a. The sponsor of the trip is an institution of higher education within the meaning of section 101 of the Higher Education Act of 1965: ☑ OR
   b. The sponsor of the trip does not retain or employ a registered federal lobbyist or foreign agent: ☐ OR
   c. The sponsor employs or retains a registered federal lobbyist or foreign agent, but the trip is for attendance at a one-day event *and* lobbyist / foreign agent involvement in planning, organizing, requesting, or arranging the trip was *de minimis* under the Committee's travel regulations. ☐

9. ***Check only one of the following:***
   a. I checked 8(a) or (b) above: ☑
   b. I checked 8(c) above but am not offering any lodging: ☐
   c. I checked 8(c) above and am offering lodging and meals for one night: ☐ OR
   d. I checked 8(c) above and am offering lodging and meals for two nights: ☐ If you checked this box, explain why the second night of lodging is warranted: _____

U.S. House of Representatives
COMMITTEE ON ETHICS

10. Attached is a detailed agenda of the activities House invitees will be participating in during the travel (i.e., an hourly description of planned activities for trip invitees). *Indicate agenda is attached by checking box:* ☑

11. ***Check only one of the following:***
    a. I represent that a registered federal lobbyist or foreign agent will not accompany House Members or employees on any segment of the trip. *Signify that the statement is true by checking box:* ☐ OR
    b. *Not Applicable.* Trip sponsor is a U.S. institution of higher education: ☑

12. For ***each*** sponsor required to submit a sponsor form, describe the sponsor's interest in the subject matter of the trip ***and*** its role in organizing and/or conducting the trip:
    Stanford University is the sole sponsor of the trip, and is 501(C)3 and institution of higher education that seeks to promote the public welfare by excercising an influence in behalf of humanity and civilization through teaching and rigorous scholarship.

13. ***Answer parts a and b. Answer part c if neccessary:***
    a. Mode of travel: Air ☑ Rail ☐ Bus ☑ Car ☐ Other ☐ (specify: _____)
    b. Class of travel: Coach ☑ Business ☐ First ☐ Charter ☐ Other ☐ (specify: _____)
    c. If travel will be first class, or by chartered or private aircraft, explain why such travel is warranted:

14. I represent that the expenditures related to local area travel during the trip will be unrelated to personal or recreational activities of the invitee(s). *Signify that the statement is true by checking box:* ☑

15. ***Check only one.*** I represent that either:
    a. The trip involves an event that is arranged or organized *without regard* to congressional participation and that meals provided to congressional participants are similar to those provided to or purchased by other event attendees: ☐ OR
    b. The trip involves events that are arranged specifically *with regard* to congressional participation: ☑
    If "b" is checked:
    1) Detail the cost *per day* of meals (approximate cost may be provided): Meals will be planned to comply with the $64 per diem.
    2) Provide the reason for selecting the location of the event or trip: The location of stanford's campus will allow more California-based scholars to participate.

16. Name, nightly cost, and reasons for selecting each hotel or other lodging facility:
    Hotel Name: Schwab Residence Center City: Stanford, CA Cost Per Night: $200
    Reason(s) for Selecting: Owned and operated by Stanford, complies with per diem, and is close to events
    Hotel Name: _____ City: _____ Cost Per Night: _____
    Reason(s) for Selecting: _____
    Hotel Name: _____ City: _____ Cost Per Night: _____
    Reason(s) for Selecting: _____

17. I represent that all expenses connected to the trip will be for actual costs incurred and not a per diem or lump sum payment. *Signify that the statement is true by checking box:* ☑

U.S. House of Representatives
COMMITTEE ON ETHICS

18. **Total Expenses for each Participant:**

☐ Actual Amounts ☑ Good Faith Estimates	Total **Transportation** Expenses per Participant	Total **Lodging** Expenses per Participant	Total **Meal** Expenses per Participant
For each Member, Officer, or Employee	$599.45	$600	$231
For each Accompanying Family Member			

	Other Expenses (dollar amount per item)	Identify Specific Nature of "Other" Expenses (e.g., taxi, parking, registration fee, etc.)
For each Member, Officer, or Employee	$200	Ground transportation
For each Accompanying Family Member		

NOTE: Willful or knowing misrepresentations on this form may be subject to criminal prosecution pursuant to 18 U.S.C. § 1001.

19. *Check only one:*
    a. I certify that I am an officer of the organization listed below: ☐ OR
    b. *Not Applicable.* Trip sponsor is an individual or a U.S. institution of higher education. ☑
20. I certify that I am not a registered federal lobbyist or foreign agent for any sponsor of this trip. ☑
21. I certify by my signature that the information contained in this form is true, complete, and correct to the best of my knowledge.

Signature: Russell Wald Date: July 18, 2019

Name: Russell Wald

Title: Senior Manager, External Affairs

Organization: Stanford University

Address: 434 Galvez Mall, Stanford, CA 94305

Telephone: 202-760-3200

Email: rwald@stanford.edu

If there are any questions regarding this form, please contact the Committee at the following address:

Committee on Ethics
U.S. House of Representatives
1015 Longworth House Office Building, Washington, D.C. 20515
Phone: 202-225-7103 General Fax: 202-225-7392

ONE HUNDRED SIXTEENTH CONGRESS

U.S. House of Representatives

COMMITTEE ON ETHICS

1015 Longworth House Office Building
Washington, D.C. 20515–6328
Telephone: (202) 225–7103
Facsimile: (202) 225–7392

August 23, 2019

Ms. Sarah Moxley
Committee on Homeland Security
H-2 117 Ford House Office Building
Washington, DC 20515

Dear Ms. Moxley:

Pursuant to House Rule 25, clause 5(d)(2), the Committee on Ethics hereby approves your proposed trip to Stanford, California, scheduled for August 26 to 29, 2019, sponsored by Stanford University.

You must complete an Employee Post-Travel Disclosure Form (which your employing Member must also sign) and file it, together with a Sponsor Post-Travel Disclosure Form completed by the trip sponsor, with the Clerk of the House within 15 days after your return from travel. As part of that filing, you are also required to attach a copy of this letter and both the Traveler and Primary Trip Sponsor Forms (including attachments) you previously submitted to the Committee in seeking pre-approval for this trip. If you are required to file an annual Financial Disclosure Statement, you must also report all travel expenses totaling more than $390 from a single source on the "Travel" schedule of your annual Financial Disclosure Statement covering this calendar year. Finally, Travel Regulation § 404(d) also requires you to keep a copy of all request forms and supporting information provided to the Committee for three subsequent Congresses from the date of travel.

If you have any further questions, please contact the Committee's Office of Advice and Education at extension 5-7103.

Sincerely,

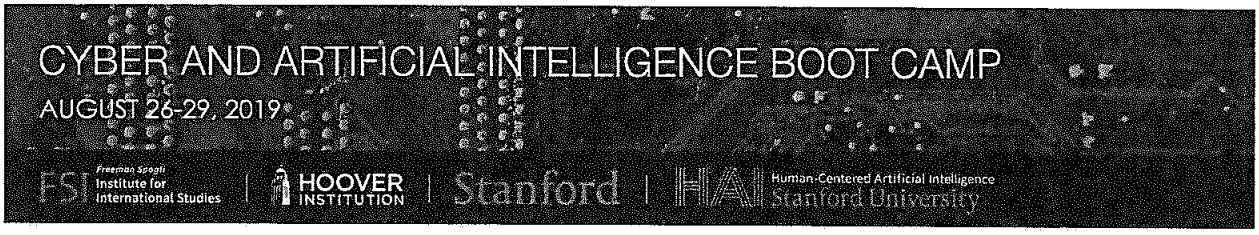
Theodore E. Deutch
Chairman

Kenny Marchant
Ranking Member

TED/KM:jls

I participated in meetings and discussions artificial intelligence and cybersecurity as it related to government and industry which improves my knowledge and allows me to better serve the Members of the Homeland Security Committee.

As the Subcommittee Director for the Cybersecurity, Infrastructure Protection and Innovation Subcommittee on the Committee on Homeland Security participating in this trip will allow me to have hands on experience with cybersecurity such as through the simulated ransomware attack. It will also allow for diverse policy conversations with experts in cybersecurity and AI space which will increase my knowledge and allow me to better advise the members of the committee.



July 18, 2019

Dear Ms. Moxley,

We are pleased to inform you that you have been selected to participate in the Stanford Cyber and Artificial Intelligence Boot Camp at Stanford University in Palo Alto, CA, on August 26th – 29th. This intensive 3-day program includes seminars, simulations, a keynote dinner event with industry stakeholders, and a field trip.

These sessions will challenge you to learn from and debate key philosophical and policy issues with some of the nation's leading thinkers and practitioners. As a participant you will receive round-trip airfare and ground transportation to Stanford University from Washington, DC, housing on Stanford's campus, and those meals that are part of the program.

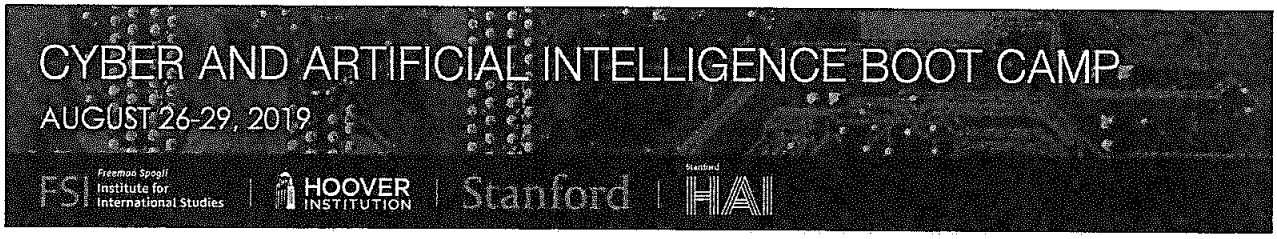
To proceed, please confirm your agreement to attend by completing this form by the close of business on Monday, July 22nd. Due to ethics rules, to maintain your spot, it is imperative that you submit the proper paperwork. Please complete the paperwork provided and items listed below **to your ethics committee for review by Wednesday, July 24th**. Your submission packet must include:

- Ethics Traveler Form (attached for you to fill out)
- Private Sponsor Form (completed for you and attached)
- Syllabus
- House Boot Camp Offers
- Copy of this invitation letter

If you have any questions, do not hesitate to contact me (rwald@stanford.edu). Thank you in advance for your prompt response so we can ensure your seat in the boot camp. We look forward to and expect an excellent program.

Sincerely,

Russell C. Wald
Senior Manager, External Affairs
Hoover Institution, Stanford University



Cyber and Artificial Intelligence Boot Camp

August 26-29, 2019

The Hoover Institution, Annenberg Conference Room 105, Lou Henry Hoover Building
434 Galvez Mall, Stanford, CA 94305

LEADERSHIP

Andrew Grotto
Program Director, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute
William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC)
Research Fellow, Hoover Institution
Dr. Herb Lin
Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

CONTACTS

Danielle Jablanski, djablanski@stanford.edu +1(650) 725-4839
Cyber Program Manager, Program on Geopolitics, Technology, and Governance, Stanford Cyber Policy Center, Freeman Spogli Institute
Russell Wald, rwald@stanford.edu +1 (202) 760-3204
Senior Manager for External Affairs
Hoover Institution, Stanford University

COURSE DESCRIPTION

Threats in cyberspace, innovations in emerging technology, complex digital interdependence and challenges for security, governance, privacy and safety capture headlines across the globe. Nations, companies and individuals are increasingly dependent on information and information technology for societal functions. Ensuring the security of information and information technology — defined as cybersecurity — against a broad spectrum of hackers, criminals, terrorists, propagandists and state actors is a critical task for the nation. Challenges are evolving rapidly, with threats facing the nation and its infrastructure changing by the day.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, international relations, and a host of other disciplines. This Boot Camp draws upon the expertise of cyber and artificial intelligence scholars in academia as well as senior business leaders and security professionals in Silicon Valley and beyond to provide perspectives on the many dimensions of this dynamic set of issues.

Artificial intelligence developments and are likewise being documented all over the world, with advances for medicine, automation, mobile apps, IoT devices, robotics, and more. In collaboration with the Stanford Institute for Human-Centered Artificial Intelligence (HAI) recently launched at Stanford, the Boot Camp will introduce fundamentals of machine learning and AI. As the HAI mission states, the development of artificial intelligence should be paired with an ongoing study of its impact on human society and guided accordingly.

The 2019 Cyber and Artificial Intelligence Boot Camp for Congressional Staffers will incorporate multiple viewpoints and interactive sessions to provide an understanding of the fundamentals of cybersecurity and artificial intelligence, the nature of international security challenges and threats, various approaches to addressing these threats, and the development and use of capabilities to advance national interests. The Boot Camp seeks to give Congressional Staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the converging technology and policy issues of tomorrow.

- **Scope**: The security implications and challenges of the nation's use of information technology. The course focuses specifically on topics relevant for international security and policymaking. We will not dive deep on any technological security products or processes for protecting or attacking systems and networks.
- **Framing Theme #1**: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem posed requires understanding the perspectives of various actors, their interests and incentives. Boot Camp sessions are designed to allow staffers to better understand the perspectives of different stakeholders

and key players, including attackers, researchers, industry experts, and corporate executives.

- **Framing Theme #2**: The non-technical dimensions of offensive and defensive cybersecurity (politics, organizational and cultural dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.
- **Framing Theme #3**: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.
- **Framing Theme #4**: The expected global and multisector impacts of artificial intelligence cannot be understated. AI experts will provide fundamental primers for how algorithms and autonomous systems are built, how incorporation of this technology will affect society, and frameworks for how governments and publics thinking about the uses and misuses of technology in this new reality will evolve.

DAY 1 (Monday, August 26): Cyber Offense and Defense

11:30 am – 12:00 pm INTRODUCTION AND PROGRAM OVERVIEW

Faculty:

- **Andrew Grotto,** *William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

12:00 pm – 12:30 pm LUNCH KEYNOTE & WELCOME

Opening Remarks:

- **H.R. McMaster,** *Fouad and Michelle Ajami Senior Fellow, Hoover Institution; Former assistant to the president for National Security Affairs; Retired Lieutenant General, U.S. Army*

12:30 pm – 1:30 pm THINKING LIKE AN ATTACKER

Faculty:

- **Dr. Greg Conti,** *Senior Security Strategist, IronNet Cybersecurity*
- **Dr. Herb Lin,** *Stanford University*
- **Andrew Grotto,** *Stanford University (Moderator)*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

Assignment: **While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.**

Learning Objectives: Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

1:30 pm – 1:45 pm BREAK

1:45 – 3:00 pm KEYNOTE: CURRENT THREAT LANDSCAPE

- **Kevin Mandia,** *CEO, FireEye*
- **Sean Kanuck,** *Visiting Fellow, Hoover Institution; Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Threat actors and their specific activity signatures, global hot spots and trends, are analyzed daily by various security agencies, governments, and organizations. This keynote will direct our attention to today's principal threat actors, providing a bird's eye view of the threat landscape, current trends and capabilities, future outlook of malicious cyber activity, and seeks to bust certain myths sometimes circulated or recounted incorrectly about cyber operations. Speakers will also provide first-hand examples of experiences tracking threats and bad actors, and share insights about working in this field.

3:00 pm – 3:15 pm BREAK

3:15 pm – 4:15 pm THREATS TO CYBERSECURITY

Faculty:

- **Carey Nachenberg,** *Chief Scientist, Chronicle; Adjunct Assistant Professor of Computer Science, UCLA*
- **Dr. Tom Berson,** *Visiting Scholar, Stanford CISAC; Advisory Board Member, Salesforce; Founder, Anagram Laboratories*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. This session examines various known techniques and vulnerabilities in information technology that allow them to happen, painting a picture of a well-known cybersecurity theme: offense dominance. This session will include forensic case studies that illuminate the spectrum of the attack surface, key challenges, and trends.

Learning Objectives: Security-relevant principles of information technology; types of

compromises; inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

4:15 pm – 4:30 pm BREAK

Dinner available in Annenberg Conference Room

4:30 pm – 5:30 pm DINNER: OFFENSIVE DIMENSIONS OF CYBERSECURITY

Faculty:

- **Dr. Herb Lin,** *Stanford University*
- **Jason Kichen,** *Vice President, Advanced Security Concepts, eSentire*
- **Andrew Grotto,** *Stanford University (Moderator)*

Offensive activities — including those conducted for espionage and attack purposes — serve a variety of national goals. This discussion will summarize the operational and strategic requirements, intelligence needs, organizational structure and policy considerations necessary for offensive cyber operations.

Learning Objectives: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture, signaling, and other purposes; the differences between penetration and exploitation and their important distinctions; the scope and nature of U.S. command and control of offensive operations in cyberspace.

5:30 pm – 6:00 pm BREAK

Walk to Stanford Graduate School of Business, meet in room G101, Dunlevie Classroom

6:00 pm – 8:30 pm HOSPITAL RANSOMWARE SIMULATION

The hospital has been the victim of a cyber-attack in the form of ransomware which successfully encrypts 250,000 files and holds at least one system hostage, demanding a ransom payment in Bitcoin (BTC) in return for a decryption key which will unlock its systems and restore access and functionality to the system. The hospital has a timeline of 72 hours to pay the ransom before their files become permanently encrypted and inaccessible, or are moved off their network.

Subject matter experts will act as the hospital's Chief Executive Officer and Chief Strategy Officer during the simulation, and staffers will be divided into teams to assist with directing action items, press releases, and critical decisions on how to manage the attack and response.

Each team will have a coach aiding their organization and strategy. All names and information will be fictional, however, the simulated attack is based on previous real life scenarios. The information made available to participants is subject to change throughout the simulation. At the end of the exercise, teams will present their decision making processes to the hospital's CEO and Board of Trustees, and debrief on what it is like to face this type of cyber scenario in the real world.

DAY 2 (Tuesday, August 27): Technical & Nontechnical Approaches

8:30 am – 9:00 am BREAKFAST AND DAY 1 DEBRIEF

- **Andrew Grotto,** William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:00 am – 11:00 am HANDS ON HACK LAB

Faculty:

- **Alex Stamos,** *Visiting Scholar, Hoover Institution; Adjunct Professor, Stanford University; Director, Internet Observatory, Cyber Policy Center, Freeman Spogli Institute*

Stamos' course provides an introduction to the most common types of attacks used in cybercrime and cyberwarfare. As a long-time security practitioner, he covers the basics of an area of technology and how it has been misused. Participants will complete a lab session from his Stanford course in which they will be guided through attacking a known insecure system using techniques and tools seen in the field.

Participants will be required to bring a Windows or Mac laptop and will be provided with basic information for the exercise 2 weeks prior to the session. No computer science background is necessary for this session.

11:00 am – 11:15 pm BREAK

Lunch available in Annenberg Conference Room

11:15 am – 12:15 pm LUNCH: CYBER RISK, ECONOMICS, AND ORGANIZATIONAL DIMENSIONS OF CYBERSPACE

Faculty:

- **Dr. Tyler Moore,** *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*
- **Dr. Greg Falco,** *Security Researcher, Stanford CISAC*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Known cybersecurity measures are often not fully adopted due to a variety of economic and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. The insurance sector is working to provide accurate and adequate coverage for this market. This session examines how these factors often discourage the adoption of sound security practices.

Learning Objectives: The importance of economic and organizational factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

12:15 pm – 12:30 pm BREAK

12:30 pm – 1:30 pm PRIVACY & SECURITY FOR CONSUMERS, CUSTOMERS, AND CRITICAL INFRASTRUCTURE

Faculty:

- **Robert Chesney,** *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*
- **Ted Gizewski,** *Vice President, Product Legal, Salesforce*
- **Andrew Grotto,** *Stanford University (Moderator)*

Privacy and security risks manifest differently in different business sectors. They also share important interdependencies that require integrated risk management and policy-making strategies.

Learning objectives: Gaining insight into how privacy and security risks affect different sectors, how risk management strategies must be tailored to the risk environment, and why an integrated approach to managing privacy and security risks is imperative.

1:30 pm – 1:45 pm BREAK

1:45 pm – 2:45 pm INTERNATIONAL LAW AND CYBERSECURITY

Faculty:

- **Dr. Tess Bridgeman,** *Senior Fellow, Center on Law and Security, NYU*
- **Dr. Herb Lin,** *Stanford University*
- **Andrew Grotto,** *Stanford University (Moderator)*

Technological change has far outpaced updates to laws and regulatory frameworks, and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technologies. Furthermore, nations have cooperative and competitive (and sometimes adversarial) interests that play out in cyberspace, devoid of national borders, giving an international dimension to every cybersecurity and policy challenge.

Learning Objectives: The implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing international law to technological circumstances not contemplated at the time of initial passage. These include the law of armed conflict, human rights, proposals for internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

2:45 pm – 3:45 pm FUNDAMENTALS OF DEFENSE FOR CYBERSECURITY

Faculty:

- **Dr. Irving Lachow,** *Visiting Fellow, Hoover Institution; Affiliate, CISAC; Portfolio Manager, International Cybersecurity, MITRE*
- **Andrew Grotto,** *Stanford University*
- **Dr. Herb Lin,** *Stanford University (Moderator)*

Cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and

blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity, understanding interdependencies, and how to use fundamentals and understanding collectively to improve security.

3:45 pm – 4:00 pm BREAK

4:00 pm – 5:00 pm CYBER ENABLED INFORMATION WARFARE AND INFLUENCE OPERATIONS

Faculty:

- **Dr. Rosanna Guadagno,** *Director, Information Warfare Working Group, Stanford University*
- **Dr. Herb Lin,** *Stanford University*
- **Andrew Grotto,** *Stanford University (Moderator)*

Cyber-enabled information warfare is fundamentally different than cyber war and cyber conflict, at least as the latter are generally understood today in the policy world. Cyber war and cyber conflict target information and information technology systems, whereas cyber-enabled information warfare targets human minds. Russia did not "hack" Facebook and YouTube and Twitter by penetrating their security—it used those platforms exactly as they were designed to be used. This session delves into these differences, placing the emphasis on the psychological vulnerabilities of **people** that the Russians (and other institutional users of social media) exploit for gain.

Learning Objectives: Understanding the fundamental differences between cyber war and cyber-enabled information warfare; the psychology underlying cyber-enabled information warfare; and the present inadequacies of the U.S. government in coping with such warfare.

5:00 pm BREAK

Please make your way to Blount Hall at the David and Joan Traitel Building for dinner

6:30 pm – 8:30 pm KEYNOTE RECEPTION/DINNER – ARTIFICIAL INTELLIGENCE

- **Dr. John Etchemendy,** *Co-Director, Stanford Institute for Human-Centered Artificial Intelligence; Provost Emeritus, and Patrick Suppes Family Professor in the School of Humanities, Stanford University*
- **Reid Hoffman**, *Partner, Greylock Partners; Co-founder and former Executive Chairman, LinkedIn*
- **Ambassador Michael McFaul,** *Senior Fellow, Freeman Spogli Institute for International Studies; Senior Fellow, Hoover Institution, Stanford University (Moderator)*

Artificial intelligence technologies are augmenting human capability and efficiency, changing the way we think about and interact with information, and creating new governance challenges and opportunities for policy makers and business leaders. Please join two distinguished thought leaders to discuss critical issues facing the future of human-centered AI development, innovation, and governance.

DAY 3 (Wednesday, August 28): Industry Voices, and the Future of Artificial Intelligence

9:00 am – 9:30 am BREAKFAST AND DAY 2 DEBRIEF

- **Andrew Grotto,** *William J. Perry International Security Fellow, Center for International Security and Cooperation (CISAC), Research Fellow, Hoover Institution*
- **Dr. Herb Lin,** *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

9:30 am – 10:45 am INDUSTRY PERSPECTIVES PANEL

- **Dr. Sameer Bhalotra (Chair),** *Co-Founder and CEO, ActZero.ai; Affiliate, CISAC; Senior Associate of the Strategic Technologies Program, CSIS; former Senior Director for Cybersecurity, National Security Council*
- **Frank Chen,** *Partner, Andreessen Horowitz*
- **Michelle Finneran Dennedy,** *Vice President, Chief Privacy Officer, Cisco*
- **Rick Howard,** *Chief Security Officer, Palo Alto Networks*
- **Dr. Mark Rosekind,** *Chief Safety Innovation Officer, Zoox*

Market forces have a critical role in enhancing or weakening security and privacy considerations. This session examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "ground truths" about the security problems facing the private sector.

Learning Objectives: Various private sector perspectives on technology and relations beyond Silicon Valley from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity and AI.

10:45 am – 11:00 am BREAK

11:00 am – 12:00 pm FUNDAMENTALS OF AI AND MACHINE LEARNING

Faculty:

- **Dr. Emma Brunskill,** *Assistant Professor, Computer Science, Stanford University; Stanford AI for Human Impact Lab*
- **Dr. Jeff Clune,** *Harris Associate Professor, Computer Science, University of Wyoming; Senior Research Manager, Uber AI Labs*
- **Andrew Grotto,** *Stanford University, (Moderator)*

Machine learning and the algorithms that fuel its applications have important principle foundations including deep learning neural networks, increased complexity in evolving neural networks, and robotics developments which are increasingly intelligent, adaptable, and resilient. Also known as reinforcement learning, algorithms can learn from experience to make decisions or provide diagnostics in applications such as educational software, healthcare decision making, robotics, or people-facing applications. This session will explain the basic elements of machine learning, and the typical environment for building and testing neural networks and reinforcement learning.

Learning Objectives: Practical applications and limits of machine learning, the broad strokes of development of deep neural networks, and the overall veracity of both development and applications of this technology. Faculty will also speak to the trajectory of the technology, and any risks it may pose from a technical perspective.

12:15 pm – 1:15 pm KEYNOTE LUNCH: ARTIFICIAL INTELLIGENCE AND SAFETY

- **Dr. Fei-Fei Li,** *Co-Director, Stanford Human-Centered Artificial Intelligence Initiative, Stanford University; Professor, Computer Science, Stanford University*
- **Mykel Kochenderfer,** *Assistant Professor of Aeronautics and Astronautics, Stanford University; Director, Stanford Intelligent Systems Laboratory*
- **Andrew Grotto,** *Stanford University (Moderator)*

Building robust decision making systems is challenging, especially for safety critical systems such as unmanned aircraft and driverless cars. Decisions must be made based on imperfect information about the environment and with uncertainty about how the environment will evolve. In addition, these systems must carefully balance safety with other considerations, such as

operational efficiency. Typically, the space of edge cases is vast, placing a large burden on human designers to anticipate problem scenarios and develop ways to resolve them.

Learning Objectives: We will discuss ways in which artificial intelligence can be applied to the design of these safety critical systems. This approach has the potential to significantly improve robustness of these systems, but there are two major challenges. The first is in ensuring computational tractability, and the other is establishing trust in their correct operation when deployed in the real world. We will outline some methodologies for addressing these challenges.

1:15 pm – 1:30 pm BREAK

1:30 pm – 2:30 pm ETHICS AND GOVERNANCE FOR AI

Faculty:

- **Dr. John Villasenor,** *Visiting Fellow, Hoover Institution; Professor of Electrical Engineering, Law, Public Policy, and Management, University of California Los Angeles*
- **Dr. Patrick Lin,** *Director, Emerging Sciences Group, California Polytechnic State University*
- **Dr. Herb Lin, Stanford** *University (Moderator)*

Advances in AI are raising a set of fundamentally important questions that go well beyond technology. This session will explore key AI ethics and governance issues, such as the nuances and challenges of addressing questions like: What should the rules be when machines make decisions with ethical implications, and who writes those rules? How can the issue of bias in AI be addressed?

Learning Objectives: The sorts of governance structures that can best ensure a climate of innovation in the AI ecosystem while also protecting against its potential misuses. What special issues are raised by AI in defense and security specifically.

Walk to Hoover Tower

2:40 pm – 3:50 pm HOOVER TOWER AND ARCHIVES TOUR (Staffers only)

Founded by Herbert Hoover in 1919, the Hoover Institution Library & Archives are dedicated to documenting war, revolution, and peace in the twentieth and twenty-first centuries. With nearly one million volumes and more than six thousand archival collections from 171 countries, Hoover

supports a vibrant community of scholars and a broad public interest in the meaning and role of history.

Travel to Stanford Center for Automotive Research
SHUTTLE ARRIVES AT 3:50PM TO END OF GALVEZ ST.

4:15 pm – 5:30 pm VISIT TO CENTER FOR AUTOMOTIVE RESEARCH AT STANFORD

Faculty:

- **Dr. Stephen Zoepf,** *Executive Director, Center for Automotive Research, Stanford University*
- **Bryan Casey,** *Lecturer in Law, Stanford University*
- **Marco Pavone,** *Associate Professor, Aeronautics and Astronautics, Stanford University*

The Center for Automotive Research at Stanford (CARS) brings together researchers, students, industry, government and the community to enable a future of human-centered mobility. Understanding how people and machines work together has never been so important than when building vehicles of the future. CARS supports educational experiences for students, infrastructure for research and events that bring students and campus researchers together with industry professionals and the broader community. Researchers and vehicles affiliated with CARS are housed at the Automotive Innovation Facility, which houses the Volkswagen Automotive Innovation Lab (often referred to as 'VAIL'), a state-of-the-art vehicle research facility where interdisciplinary teams can work on projects that move vehicle human-centered mobility forward.

Participants will visit CARS' Automotive Innovation Facility and hear from researchers on the cutting edge of the development of autonomous vehicles. Experts will brief the group on trends in the field, ongoing legal and ethical debates, and provide a tour of the facility showcasing vehicles and a driving simulator used for research.

***Ride to Stanford Golf Course* - SHUTTLE ARRIVES AT 5:45PM TO THE SDDL**

6:00 pm – 8:00 pm DINNER AND REFLECTIONS – (Staffers only)

Coupa Café – Stanford Golf Course
198 Junipero Serra Blvd, Stanford, CA, 94305

***Ride to Schwab Residential Hall* - SHUTTLE ARRIVES AT 8:15pm**

Thursday, August 29: Shuttle will arrive to Schwab Residential Hall at 6:30am to depart for San Francisco International Airport

Last Name	First Name	Middle Na	Job Title	Current Office or Committee
Anderson	Wendy	D	Chief of Staff	Rep Val Demings
Carithers	Charles	Anderson	Professional Staff Member	Committee on Homeland Security
Fullerton	Laura	Funderbur	Deputy Staff Director	House Foreign Affairs
Hagens-Jorda	Jessica	Rene	Defense and Foreign Policy Advisor	Rep. Jim Himes (HPSCI)
Heinemann	John	Douglas	Counsel	Financial Services Committee, Oversight and Investigations Subcommittee
Matt	Svetlana		Legislative Assistant	Office of Rep. Jerry McNerney (CA-09)
Moxley	Sarah	Whiting	Staff Director	Committee on Homeland Security, Subcommittee on Cybersecurity, infrastructure Protection and Innovation
Ramzanali	Asad		Senior Advisor, Technology Policy	Office of Rep. Eshoo
Seeds	Michael	William	Deputy Chief of Staff & Legislative Director	Rep. Mac Thornberry
Smith	Alicia	M	Counsel	Committee on Homeland Security
Tai	Katherine	Chi	Chief Trade Counsel, Trade Subcommittee St	Ways and Means