STANFORD CONGRESSIONAL CYBER BOOT CAMP

Hoover Institution | Center for International Security and Cooperation | Stanford University

AUGUST 18 - 20, 2014

TABLE OF CONTENTS

Note from the Conveners 1

Conference Agenda and Schedule 3

Map of Stanford 5

Keynote Speaker Biographies 6

Session Descriptions 13

Overview of Google Visit 23

Staffer Biographies 24

A NOTE FROM THE CONVENERS

Cybersecurity represents one of the most pressing challenges that the United States will face in the coming decades. Ensuring continued economic prosperity and defense readiness requires improving the security of the computing devices, systems, and networks that have become essential to the nation's commerce and defense. Moreover, the United States has at its disposal powerful offensive capabilities in cyberspace—how can and should it use these capabilities in support of national interests? These and other cyber issues are important, complex, and here to stay.

While technological capabilities are moving ahead at lightning speed, policy and legal frameworks in cybersecurity are lagging behind. Historically, governments have safeguarded citizens and national interests from external threats. In cyber, however, traditional boundaries are fuzzy. What constitutes an internal threat? An external one? How do we even know a threat when we see it? The roles and missions in cyberspace of various government agencies are also unclear. What is clear is that the government cannot go it alone: the private sector holds key capabilities and owns vital assets that make public/private cooperation essential, demanding, and often problematic.

Stanford University's Hoover Institution and the Center for International Security and Cooperation (CISAC) are natural partners for tackling cybersecurity challenges across sectors and academic disciplines. The world's growing interconnectedness and the "Internet of things" raise key questions about privacy, individual liberty, the appropriate role of government, international peace and national security, and economic freedom – issues that lie at the heart of Hoover's mission to develop "ideas defining a free society." CISAC has a unique and successful model of bringing together scientists and social scientists to address pressing international security issues through rigorous scholarship, policy outreach, and Track II diplomacy. Both institutions are dedicated to developing policy relevant knowledge by bridging academic divides, convening leading thinkers across sectors, and training the next generation.

The spirit of cross-disciplinary collaboration and drive for innovation run deep at Stanford, and help explain why the university ranks as one of the best in the world, with top departments ranging from computer science to classics and scholars and alumni who include 5 Pulitzer Prize winners, 21 astronauts, 27 MacArthur Fellows, 28 current billionaires, and 22 living Nobel Laureates. Stanford's interdisciplinary programs include new undergraduate joint majors combining computer science with English or music, and research collaborations between doctors, scientists, and engineers that have generated breakthrough discoveries in medicine. Companies founded by Stanford faculty, researchers, and former students—including Cisco Systems, Google, Hewlett-Packard, LinkedIn, Sun Microsystems, and Yahoo!—today generate more than $2 trillion annually in revenues, a figure equivalent to the GDP of the world's 7th largest economy. Stanford's location and ties to Silicon Valley put us at the heart of the technological ecosystem that is driving transformative international change.

Breaking out of intellectual stovepipes is crucial to developing a better understanding of cyber challenges and how to address them. Cyber threats involve political, legal, organizational, economic, and psychological factors that technical experts often do not fully understand or appreciate. On the other hand, these conflicts in cyberspace may also involve technologies that social scientists and policymakers often do not fully grasp. In the policy world, current priorities leave little time for longer term thinking. In the academic world, research on cyber policy and security is siloed and embryonic. While there is great consensus on the importance of cyberspace from the standpoint of international security, there is surprisingly little consensus on appropriate strategy, doctrine, tactics, theory, or data that might be brought to bear to understand the relevant issues. Indeed, there is little consensus even about which issues constitute the most important ones deserving attention. These gaps and questions provide an opportunity for CISAC, Hoover, and Stanford more broadly to play an early and significant role in thought leadership and cross-sector convening.

Hosting this inaugural cyber boot camp for congressional staff—the first program of its kind at Stanford—is an important step forward. Our aim was to bring together senior legislative staff across political parties, chambers, and committees for three action- packed days of workshops, simulations, and discussions with leading academic and industry thinkers away from the pressures of daily business in Washington. The next 72 hours will be all about connecting—generating ideas, insights, questions, and relationships that we hope will better inform both policy and academic research to improve American cybersecurity.

We would like to thank Hoover Institution Director John Raisian and Mariano-Florentino Cuéllar, Director of CISAC's parent institute, the Freeman Spogli Institute for International Studies, for their indispensable support. Thanks also to Leisel Bogan, Heather Campbell, Ryan Mayfield, and Russell Wald for taking this boot camp from idea to reality. Finally, we are grateful to each of you for sharing your most precious resource: time. We are thrilled that you could join us for this inaugural boot camp and look forward to working together.

Sincerely,

Dr. Amy Zegart
Co-Director, CISAC
Associate Director, Davies Family Senior Fellow, Hoover Institution
Professor of Political Science (by courtesy)

Dr. Herb Lin
Consulting Scholar, CISAC
Chief Scientist, Computer Science and Telecommunications Board, National Academies (until December 2014)
Senior Research Scholar, CISAC, and Research Fellow, Hoover Institution (effective January 2015)

CONFERENCE AGENDA

CYBER ATTACKS AND RESPONSES

Day 1 – Monday, August 18, 2014

10.00 am Congressional staffers arrive at San Francisco Airport

11.45 pm **Welcome: Framing Session**
Faculty Speakers: Dr. Amy Zegart (CISAC, Hoover), and Dr. John Villasenor (UCLA, CISAC, Hoover)

12.00 pm **Lunch and Keynote Address: Dr. Jane Holl Lute (Council of Cybersecurity, CISAC)**

1.00 pm **Session 1: Security as a Concept**
Faculty: *Professor Tadayoshi Kohno (University of Washington)*
Discussant: *Dr. Herb Lin (National Research Council, CISAC, Hoover)*

2.30 pm Break

2.45 pm **Session 2: Threats to Cybersecurity**
Faculty: *Professor Carey Nachenberg (UCLA, Symantec)*
Discussant: *Dr. Tim Junio (CISAC, Hoover)*

4.15 pm Break

4.30 pm **Session 3: Offensive Dimensions of Cybersecurity (dinner served during presentation)**
Faculty: *Col. Matteo Martemucci (U.S. Air Force) and Oren Falkowitz (Area 1 Security)*
Discussant: *Dr. Tim Junio (CISAC, Hoover)*

6.00 pm Break

6.15 pm **Session 4: Simulation**
Dr. Lucas Kello (Harvard University)

9.15 pm Return to Stanford Guest House

DEEP DIVE: TECHNICAL & NONTECHNICAL ASPECTS OF CYBER

Day 2 – Tuesday, August 19, 2014

7.15 am Depart from Stanford Guest House for Stanford University

7.45 am Breakfast and debrief from previous day

8.30 am **Session 5: Fundamental Principles of Cybersecurity**
Faculty: *Dr. Drew Dean (SRI International Computer Science Laboratory)*
Discussant: *Dr. Herb Lin (National Research Council, CISAC, Hoover)*

10.00 am Break

10.15 am **Session 6: Economic, Psychological, and Organizational Dimensions of Cybersecurity**
Faculty: *Professor Tyler Moore (South Methodist University), Dr. Janice Stein (University of Toronto), Paul Rosenzweig (George Washington)*
Discussant: *Jonathan Mayer (Stanford, CISAC)*

AND SCHEDULE OF EVENTS

12.00 pm **Lunch and Keynote Address: Dr. John Hennessy (Stanford) and Larry Kramer (Hewlett)**
Stauffer Auditorium, Hoover Institution

1.30 pm Break

2.00 pm **Session 7: Domestic and International Law**
Faculty: *Lynn St. Amour (Internet Matters), Professor Orin Kerr (George Washington School of Law) and Professor Matthew Waxman (Columbia Law School)*
Discussant: *Elaine Korzak (CISAC)*

3.45 pm Return to Stanford Guest House (change for dinner)

5.30 pm Return to Hoover Institution

6.00 pm **Dinner and Keynote Address: Dr. Condoleezza Rice (Stanford) and Dr. Eric Schmidt (Google)**

8.30 pm Return to Stanford Guest House

CIVIL LIBERTIES, CORPORATE INTERESTS, AND SECURITY

Day 3 – Wednesday, August 20, 2014

7.15 am Depart from Stanford Guest House for Stanford University

7:45 am Breakfast and debrief from previous day

8.30 am **Session 8: Cybersecurity and Civil Liberties**
Faculty: *Jennifer Granick (Stanford) and Benjamin Wittes (Brookings and Hoover)*

10.00 am Break

10.15 am **Session 9: Corporate Perspectives on Cybersecurity**
Chair: Raj Shah (Palo Alto Networks)
Speakers: *Scott Charney (Microsoft), Melody Hildebrandt (Palantir), David Liddle (U.S. Venture Partners), and Ellen Richey (Visa)*

11.45 pm Break

12.00 pm **Lunch and Keynote Address: Joe Sullivan (Facebook)**

1.30 pm Break

2.00 pm Depart for Google Headquarters

2.30 pm **Google Headquarters tour**

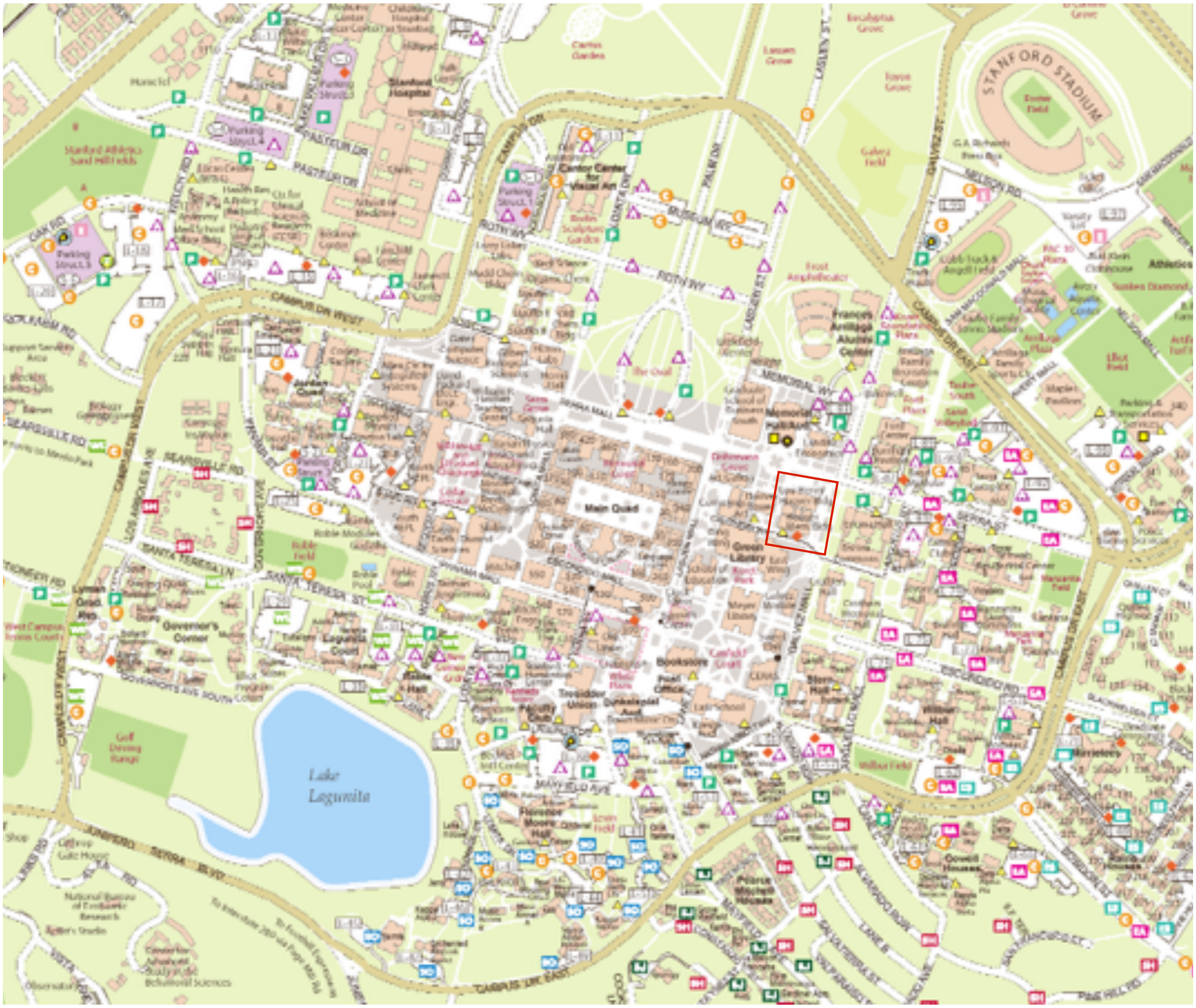
5.45 pm Dinner at Mandarin Roots Restaurant (3345 El Camino Real, Palo Alto, CA 94306)

8.30 pm Return to Stanford Guest House

Day 4 – Thursday, August 21, 2014

5.15 am Depart from Stanford Guest House for San Francisco Airport (SFO)

GETTING TO STANFORD



From Highway 101 North & South

Exit onto Embarcadero Road and travel west, following the signs directing you to Stanford University. About three miles after you exit the freeway, Embarcadero Road becomes Galvez Street as you cross El Camino Real. Turn left at the Stadium and make a right into the Visitor Center Lot onto Nelson Road.

From Highway 280 North & South

Exit onto Sand Hill Road and follow the signs for Stanford University. Heading east, drive approximately 3 miles to the Stanford Shopping Center. Turn right onto Arboretum Road (Nordstrom is on your right). Stay on Arboretum until it ends, then turn right onto Galvez Street. Move to the left lane and continue past the stadium. The entrance to the Visitor Center Lot is on the left just beyond Nelson Road.

JANE HOLL LUTE

AUGUST 18 LUNCH KEYNOTE

Jane Holl Lute is the President and Chief Executive Officer of the Council on Cyber Security, and she is responsible for the overall direction and activities of the organization. She most recently served as Deputy Secretary for the Department of Homeland Security. As the Department's Chief Operating Officer, she was responsible for the day-to-day management of the Department's efforts to prevent terrorism and enhance security, secure and manage the nation's borders, administer and enforce U.S. immigration laws, strengthen national resilience in the face of disasters, and ensure the nation's cybersecurity. From 2003-2009, she served as Assistant Secretary General of the United Nations, and was responsible for comprehensive on-the-ground support to U.N. peace operations worldwide, including rapid-response efforts in support of development and humanitarian operations and crises. Lute also served as Assistant Secretary-General for Peacebuilding. In that post, here she was responsible for coordinating efforts on behalf of the Secretary General to build sustainable peace in countries emerging from violent conflict.

Prior to joining the U.N., Lute was Executive Vice President and Chief Operating Officer of the United Nations Foundation and the Better World Fund and worked with David A. Hamburg, former president of the Carnegie Corporation of New York and Cyrus Vance, former U.S. Secretary of State, on the Carnegie Commission on Preventing Deadly Conflict, a global initiative that pioneered the cause of conflict prevention.

Lute has served on the National Security Council staff under both President George H.W. Bush and President William Jefferson Clinton, and she has also had a distinguished career in the United States Army, including service in the Persian Gulf during Operation Desert Storm. She holds a Ph.D. in political science from Stanford University and a J.D. from Georgetown University.

JOHN HENNESSY

AUGUST 19 LUNCH KEYNOTE

John L. Hennessy joined Stanford's faculty in 1977 as an assistant professor of electrical engineering. He rose through the academic ranks to full professorship in 1986 and was the inaugural Willard R. and Inez Kerr Bell Professor of Electrical Engineering and Computer Science from 1987 to 2004.

From 1983 to 1993, Dr. Hennessy was director of the Computer Systems Laboratory, a research and teaching center operated by the Departments of Electrical Engineering and Computer Science. He served as chair of computer science from 1994 to 1996 and, in 1996, was named dean of the School of Engineering. In 1999, he was named provost, the university's chief academic and financial officer. As Provost, he continued his efforts to foster interdisciplinary activities in the biosciences and bioengineering and oversaw improvements in faculty and staff compensation. In October 2000, he was inaugurated as Stanford University's 10th president. In 2005, he became the inaugural holder of the Bing Presidential Professorship.

A pioneer in computer architecture, in 1981 Dr. Hennessy drew together researchers to focus on a computer architecture known as RISC (Reduced Instruction Set Computer), a technology that has revolutionized the computer industry by increasing performance while reducing costs. In addition to his role in the basic research, Dr. Hennessy helped transfer this technology to industry. In 1984, he cofounded MIPS Computer Systems, now MIPS Technologies, which designs microprocessors.

Dr. Hennessy is a recipient of the IEEE John von Neumann Medal, the ASEE Benjamin Garver Lamme Award, the ACM Eckert-Mauchly Award, the Seymour Cray Computer Engineering Award, a NEC C&C Prize for lifetime achievement in computer science and engineering, a Founders Award from the American Academy of Arts and Sciences and the IEEE Medal of Honor, IEEE's highest award.

LARRY KRAMER

AUGUST 19 LUNCH KEYNOTE

Larry Kramer became president of The William and Flora Hewlett Foundation in Menlo Park, California, in September 2012. Before joining the Foundation, Mr. Kramer served from 2004 to 2012 as Richard E. Lang Professor of Law and Dean of Stanford Law School. During his tenure, he spearheaded significant educational reforms (which pioneered a new model of multidisciplinary legal studies while enlarging the clinical education program), a public service ethos, and developed the international law program to support a growing emphasis on globalization in legal practice. His teaching and scholarly interests include American legal history, constitutional law, federalism, separation of powers, the federal courts, conflict of laws, and civil procedure.

At the start of his career, Mr. Kramer served as law clerk to U.S. Court of Appeals Judge Henry J. Friendly of the Second Circuit and U.S. Supreme Court Justice William J. Brennan Jr.

Following his clerkships, Mr. Kramer was Professor of Law at the University of Chicago and University of Michigan Law Schools. He joined the faculty of New York University School of Law in 1994, where he served as Associate Dean for Research and Academics and as Russell D. Niles Professor of Law until leaving for Stanford in 2004. He has also served as a special consultant for Mayer, Brown, Rowe & Maw LLP.

Mr. Kramer is a Fellow of the American Academy of Arts and Sciences, a member of the American Philosophical Society, and a member of the American Law Institute. He serves as a director on the boards of a number of nonprofit organizations, including the National Constitution Center and the ClimateWorks Foundation.

Mr. Kramer received an A.B. in Psychology and Religious Studies from Brown University, and a J.D. from the University of Chicago Law School.

CONDOLEEZZA RICE

AUGUST 19 DINNER KEYNOTE

Condoleezza Rice is currently a Professor of Political Economy in the Graduate School of Business; the Thomas and Barbara Stephenson Senior Fellow on Public Policy at the Hoover Institution; and a Professor of Political Science at Stanford University. She is also a founding partner of RiceHadleyGates.

From January 2005-2009, Rice served as the 66th Secretary of State of the United States, the second woman and first African-American woman to hold the post. Rice also served as President George W. Bush's Assistant to the President for National Security Affairs (National Security Advisor) from January 2001-2005, the first woman to hold the position.

Rice served as Stanford University's Provost from 1993-1999, during which she was the institution's chief budget and academic officer. As Provost, she was responsible for a $1.5 billion annual budget and the academic program involving 1,400 faculty members and 14,000 students. In 1997, she also served on the Federal Advisory Committee on Gender-Integrated Training in the Military.

From 1989 through March 1991, Rice served on President George H.W. Bush's National Security Council staff. She served as Director, Senior Director of Soviet and East European Affairs, and Special Assistant to the President for National Security Affairs. In 1986, while an international affairs fellow of the Council on Foreign Relations, Rice also served as Special Assistant to the Director of the Joint Chiefs of Staff.

As Professor of Political Science, Rice has been on the Stanford faculty since 1981 and has won two of the highest teaching honors – the Walter J. Gores Award for Excellence in Teaching and the School of Humanities and Sciences Dean's Award for Distinguished Teaching. She has authored and co-authored numerous books, including two bestsellers, *No Higher Honor: A Memoir of My Years in Washington* (2011) and *Extraordinary, Ordinary People: A Memoir of Family* (2010).

You can follow Dr. Rice on Twitter at @CondoleezzaRice.

ERIC SCHMIDT

AUGUST 19 DINNER KEYNOTE

Since joining Google in 2001, Eric Schmidt has helped grow the company from a Silicon Valley startup to a global leader in technology. As executive chairman, he is responsible for the external matters of Google: building partnerships and broader business relationships, government outreach and technology thought leadership, as well as advising the CEO and senior leadership on business and policy issues.

From 2001-2011, Eric served as Google's chief executive officer, overseeing the company's technical and business strategy alongside founders Sergey Brin and Larry Page. Under his leadership, Google dramatically scaled its infrastructure and diversified its product offerings while maintaining a strong culture of innovation.

Prior to joining Google, Eric was the Chairman and CEO of Novell and Chief Technology Officer at Sun Microsystems, Inc. Previously, he served on the research staff at Xerox Palo Alto Research Center (PARC), Bell Laboratories, and Zilog. He holds a bachelor's degree in electrical engineering from Princeton University as well as a master's degree and Ph.D. in computer science from the University of California, Berkeley.

Eric is a member of the President's Council of Advisors on Science and Technology and the Prime Minister's Advisory Council in the U.K. He was elected to the National Academy of Engineering in 2006 and inducted into the American Academy of Arts and Sciences as a Fellow in 2007.

He also chairs the board of the New America Foundation, and since 2008 has been a trustee of the Institute for Advanced Study in Princeton, New Jersey. In May 2012, Eric became a member of Khan Academy's board of directors and in 2013 he joined the board of *The Economist*.

You can follow Dr. Schmidt on Twitter at @ericschmidt.

JOE SULLIVAN

AUGUST 20 LUNCH KEYNOTE

Joe Sullivan is the Chief Security Officer at Facebook, where he manages the company's teams responsible for information security, product security, investigations, and law enforcement relations. In addition to spending most of his time promoting safety and security for Facebook users, Joe also works on other regulatory and privacy-related legal issues. Joe is on the boards of the National Cyber Security Alliance and the Action Alliance for Suicide Prevention.

Prior to joining Facebook in 2008, Joe spent over six years working in a number of different security and legal roles at PayPal and eBay, including overseeing user safety policies and company relations with law enforcement agencies around the world, guiding eBay's regulatory compliance efforts, and managing PayPal's North America legal team.

Before entering the private sector, Joe spent eight years with the U.S. Department of Justice. He was the first federal prosecutor in a U.S. Attorney's office dedicated full-time to fighting high-tech crime, working on many high profile internet cases, ranging from the digital evidence aspects of the 9/11 investigation to child predator, computer intrusion, and economic espionage cases. He was a founding member of a special unit based in Silicon Valley dedicated exclusively to high-tech crime prosecution.

Joe has spoken extensively on internet security and criminal investigations at law enforcement and industry conferences around the world, has testified on two occasions before the U.S. Congress on online safety and security, has appeared many times on television, radio and print media to promote internet safety, has trained prosecutors and judges from many countries on electronic evidence and other cyber-related legal issues, and is very active in promoting internet safety in schools.

FRAMING SESSION

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the boot camp. Cybersecurity means different things and poses different challenges to different stakeholders. This boot camp is centered on the security implications and challenges of the nation's information and technology use. We do not address topics such as consumer security, although many of these concepts are relevant. Our aim is to integrate multiple perspectives and disciplines to provide a fuller understanding of the underpinnings of cybersecurity, the nature of cybersecurity threats, various approaches to address them, and the use of offensive cyber capabilities to advance national interests. In preparing for the future, the boot camp endeavors 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 the problems of tomorrow.

Faculty

Professor John Villasenor, UCLA, CISAC, Hoover Institution

John Villasenor is Professor of Electrical Engineering and Public Policy at UCLA, Vice Chair of the World Economic Forum's Global Agenda Council on the Intellectual Property System, a CISAC affiliate, and a Hoover Institution National Fellow. His work addresses the intersection of technology, policy and law. Villasenor's research considers the broader impacts of key technology trends including the move to the cloud, the globalization of technology product design and manufacturing, advances in digital communications and electronics, and the increasing complexity of today's networks and systems. He has authored or co-authored nearly 200 peer-reviewed technical publications and has also written for the *Atlantic*, *Billboard*, *Forbes*, *Scientific American*, and the *Washington Post*. Prior to joining the UCLA faculty, Villasenor was with the NASA Jet Propulsion laboratory, where he developed methods of imaging earth from space. He holds a B.S. in electrical engineering from the University of Virginia and an M.S. and Ph.D. in electrical engineering from Stanford University. *You can follow Dr. Villasenor on Twitter at @JohnDVillasenor.*

Dr. Amy Zegart, CISAC, Hoover Institution, Stanford University

Amy Zegart is the Davies Family Senior Fellow and Associate Director for Academic Affairs at the Hoover Institution. She is also Co-Director of Stanford's Center for International Security and Cooperation (CISAC) and Professor of Political Science (by courtesy). Before coming to Stanford in 2011, she spent twelve years at UCLA, where she was Professor of Public Policy. Zegart's research examines organizational development, adaptation, and innovation in national security policy. Her most recent book is *Eyes on Spies: Congress and the United States Intelligence Community*. She has also authored the award-winning books *Flawed by Design* and *Spying Blind*, testified before the Senate Intelligence Committee, and published commentary in *Foreign Policy*, the *New York Times*, *Washington Post*, *Los Angeles Times* and elsewhere. Prior to her academic career, she spent several years as a management consultant at McKinsey & Company, advising firms on strategy and organizational effectiveness. She has served on the National Academies of Science Panel to Improve Intelligence Analysis, as a foreign policy advisor to the Bush 2000 presidential campaign, and currently serves on the Secretary of Energy Advisory Board Task Force on Nuclear Nonproliferation. Zegart received an A.B. in East Asian studies from Harvard University and an M.A. and Ph.D. in political science from Stanford University. *You can follow Dr. Zegart on Twitter at @AmyZegart.*

SESSION 1

SECURITY AS A CONCEPT

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, that is, 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. Examples of the security mindset (and how to combat it) from non-cyber contexts in everyday life can be used to advance cybersecurity.

Faculty and Discussant

Professor Tadayoshi Kohno, University of Washington

Tadayoshi Kohno is an Assistant Professor in the Department of Computer Science and Engineering at the University of Washington. His research focuses on computer security and privacy, broadly defined. In fact, he believes that almost every topic in computer science can have an exciting security-related twist. Although he was originally trained in applied and theoretical cryptography, his current research spans secure cyber-physical systems (including wireless medical devices and automobiles) to private cloud computing. Kohno is the recipient of a National Science Foundation CAREER Award, an Alfred P. Sloan Research Fellowship, an MIT Technology Review TR-35 Young Innovator Award, and multiple best paper awards. He received his Ph.D. in computer science from the University of California at San Diego. *You can follow Dr. Kohno on Twitter at @yoshi_kohno.*

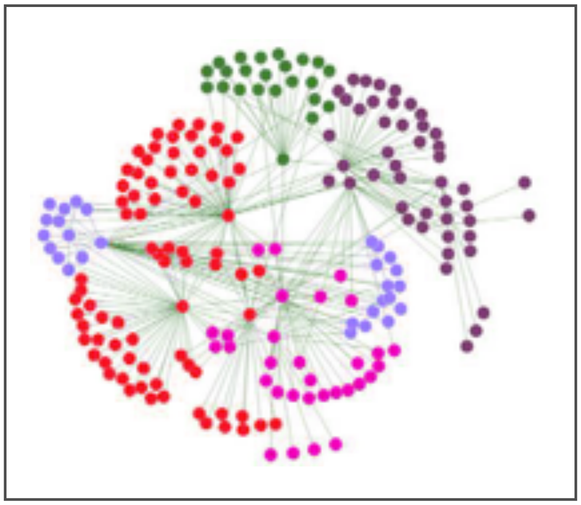
Discussant: Dr. Herb Lin, National Research Council, CISAC, Hoover

Dr. Herbert Lin is chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT. Apart from his CSTB work, he is published in cognitive science, science education, biophysics, and arms control and defense policy. He also consults on K-12 math and science education.

SESSION 2

THREATS TO CYBERSECURITY

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends. In this session, staffers will learn about security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology and the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.



Faculty and Discussant

Professor Carey Nachenberg, UCLA and Symantec

Carey Nachenberg, chief architect of Symantec's Security Technology and Response (STAR) division, has been an innovator at Symantec Corporation for the past 18 years. As a chief architect, Nachenberg drives the technical strategy for all of Symantec's core security technologies and security content, which in total protect over 100M customers around the world. During his time at Symantec, Nachenberg has led the design and development of many of Symantec's core antivirus and intrusion prevention technologies, as well as key aspects of Symantec's LiveUpdate system. His work in these areas has garnered 25 United States patents. Nachenberg has earned both B.S. and M.S. degrees from the University of California at Los Angeles, where he continues to serve as a lecturer of Computer Science.

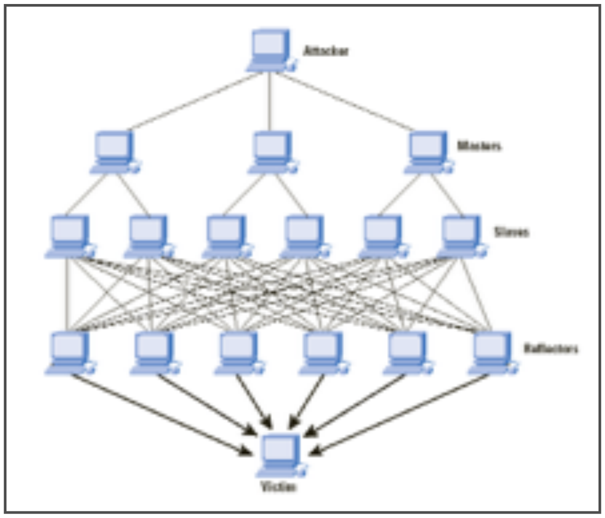
Discussant: Dr. Tim Junio, CISAC, Stanford, and Hoover Institution

Junio was a cybersecurity postdoctoral fellow at CISAC for 2012-2014. He received his Ph.D. from the University of Pennsylvania in 2013. His research is on information technology and national security, and he continues testing his theories with comparative fieldwork on how the U.S., South Korea, and Taiwan produce and project cyber power. In his spare time, Junio develops new cyber capabilities at the Defense Advanced Research Projects Agency (DARPA). Before his Ph.D. studies, he received his M.A. from Johns Hopkins University's School of Advanced International Studies (SAIS), and his B.A. from Johns Hopkins University. He worked on cybersecurity strategy for the Office of the Secretary of Defense, RAND Corporation, US intelligence community, and Johns Hopkins' Information Security Institute.

SESSION 3

OFFENSIVE DIMENSIONS OF CYBERSECURITY

Offensive activities—including those conducted for espionage or for attack—serve a variety of national goals. These goals include, but are not limited to, cyber defense. Col. Martemucci will present on strategy and policy. Mr. Falkowitz will continue this conversation with a presentation on planning offensive cyber operations and the nature of intelligence required for success.



Faculty

Colonel Matteo Martemucci, U.S. Air Force and Hoover Institution

Colonel (select) Matteo Martemucci, representing the U.S. Air Force, was a National Security Affairs Fellow for 2011-2012 at the Hoover Institution. He is a career intelligence officer and cyberspace operator. He recently completed command of the 315th Network Warfare Squadron, the Air Force's premier Computer Network Attack unit based at Fort Meade, Maryland. In addition to his numerous stateside assignments, he has served in Korea, Iraq, Saudi Arabia, France, and the Czech Republic. He is fluent in Czech and conversant in Italian. His work on strategic communication has been published in the *Iosphere*, the professional journal of Joint Information Operations. His research will focus on US government policy and strategy in the cyberspace domain.

Oren Falkowitz, Area 1 Security

Oren Falkowitz serves as the co-founder and CEO of Area 1 Security. Mr. Falkowitz was a co-founder of Sqrrl Data, Inc. and served as its CEO and President until March 2013. Previously, he served as Chief Data Scientist at United States Cyber Command and held a number of positions at the National Security Agency focused on Big Data and Computer Network Operations. *You can follow Mr. Falkowitz on Twitter at @orenfalkowitz.*

Discussant: Dr. Tim Junio, CISAC, Stanford, and Hoover Institution

See biography on page 15.

SESSION 4

SIMULATION

This session will lead participants through an exercise in which they assume the roles of various decision makers in the Executive Branch trying to respond to cyber events of initially unknown origin and significance. In this session, the simulation will emulate the chaotic environment in which decision makers operate when facing a cyber crisis. This will allow staffers to have a hands-on feel for the key policy, organizational, and political challenges they are likely to confront and will lay out the options for handling them.

Cyber conflict presents formidable challenges of crisis management. Lines of authority that serve well in a traditional crisis may break down in a cyber crisis. Information sharing among relevant actors can become fractured. Leaders may be unaware of the full operational theater; at best, they may have only partial knowledge of their own situation. Cyber events blur the lines between the physical and virtual worlds, state and non-state action, local and distant conflict. Threats move at the speed of electrons; policy responses to them move at the sluggish pace of bureaucracy. Decision-makers with a strong awareness of cyber conflicts' challenges will be best prepared to manage them during a national emergency. This exercise seeks to foster such awareness: it applies theories and concepts discussed in the classroom to the management of a major cyber crisis. The exercise exposes participants to the difficulties of effective decision-making, escalation control, and crisis termination in this new domain of conflict. It develops and applies participants' knowledge of existing policy techniques and facilitates the identification of shortcomings in current capacities. Originally designed at Harvard University's Belfer Center for Science and International Affairs, the exercise is modeled on Tallinn CIIP 2010—Estonia's first cross-ministerial cyber defense simulation, which drew on the country's unique experience defending against a cyberattack in 2007.

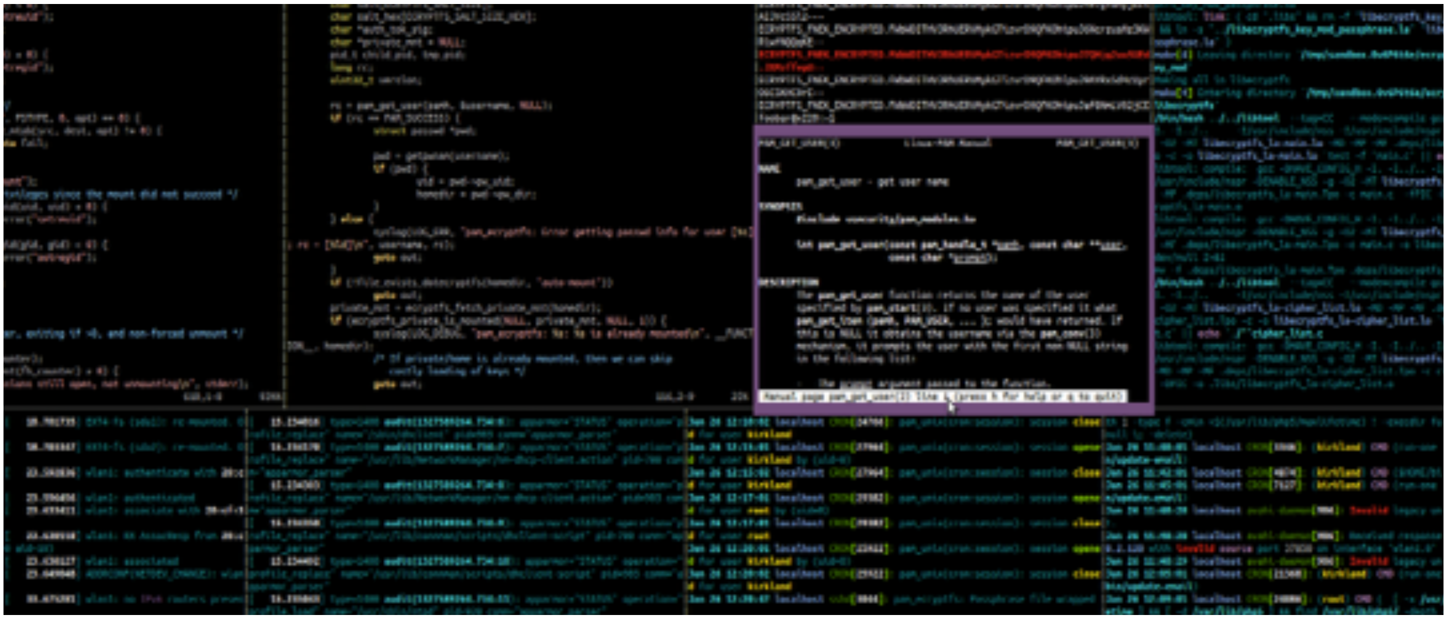
Faculty

Dr. Lucas Kello, Belfer Center, Harvard University

Lucas Kello is a joint postdoctoral research fellow in the International Security Program and the Science, Technology, and Public Policy Program. He is exploring the implications of cyber weapons for international relations and security. One aspect of his work involves the design of a conceptual framework for the analysis of deterrence and escalation dynamics in the cyber domain, while his policy research focuses on European and NATO institutional responses to emergent cyber threats. Kello has served as a consultant to European Union (EU) authorities and the Estonian Government on cyber defense strategy. He has also worked with the Spanish Ministry of Defense in various areas of security policy, including post-conflict stabilization in the Middle East. Kello holds a bachelor's degree from Harvard College as well as a master's and doctorate in International Relations from Oxford University. *You can follow Dr. Kello on Twitter at @KelloLucas.*

SESSION 5

FUNDAMENTAL PRINCIPLES OF CYBERSECURITY



Although cybersecurity can be a deeply technical subject, especially in the implementation of cybersecurity solutions, a few fundamental principles underlie most such solutions. This session takes a deeper dive into understanding the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology; detecting cybersecurity compromises; blocking and limiting the impact of compromise. Additional items of discussion include authentication, access control, and forensics; recovery, containment, and resilience; and active defense.

Faculty and Discussant

Dr. Drew Dean, SRI International Computer Science Laboratory

Dr. Drew Dean is the Senior Computer Scientist at SRI International Computer Science Laboratory, and has previously held research and program management positions at Yahoo!, the Defense Advanced Research Projects Agency (DARPA), and the Palo Alto Research Park (PARC). He holds a B.Sc. in mathematics and computer science at Carnegie Mellon University and a Ph.D. in computer science from Princeton University.

Discussant

Dr. Herb Lin, National Research Council, CISAC, Hoover Institution

See biography on page 14.

SESSION 6

ECONOMIC, PSYCHOLOGICAL, AND ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY

Even when useful cybersecurity measures are known, often they are not adopted fully, effectively, or at all due to a variety of economic, psychological, and organizational factors. These factors are usually non-technical in nature and are often underappreciated by the technical community in places like Silicon Valley and by the policy community in Washington. Economics describes the incentives that apply to cyber defenders and adversaries, including the extent and nature of cybersecurity market failure and how to handle collective action problems. Psychology addresses the deception that underlies nearly all cybersecurity threats and decision making under uncertainty. Organizational aspects address the organizational structure and needs for cybersecurity and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practice.

Faculty and Discussants

Professor Tyler Moore, Southern Methodist University

Tyler Moore is an Assistant Professor of Computer Science at SMU, and his research focuses on the economics of information security, the study of electronic crime, and the development of policy for strengthening security. He directs the Security Economics Lab within HACNet (High Assurance Computing and Networking Labs), a research group working in different areas related to security. Prior to joining SMU, he was a postdoctoral fellow at Harvard University. He received his Ph.D. at the University of Cambridge.

Professor Janice Gross Stein, University of Toronto

Janice Gross Stein is the Belzberg Professor of Conflict Management in the Department of Political Science and the Director of the Munk School of Global Affairs at the University of Toronto. Her most recent publications include *Networks of Knowledge: Innovation in International Learning* (2000); *The Cult of Efficiency* (2001); and *Street Protests and Fantasy Parks* (2001). She is a contributor to *Canada by Picasso* (2006) and the co-author of The *Unexpected War: Canada in Kandahar* (2007).

Paul Rosenzweig, George Washington, Homeland Security

Paul Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He is a Professorial Lecturer in Law at George Washington University, an Adjunct Professor at the National Defense University, and a Visiting Fellow at The Heritage Foundation. Mr. Rosenzweig is a graduate of the University of Chicago Law School, has an M.S. in Chemical Oceanography from the Scripps Institute at U.C. San Diego and a B.A from Haverford College. *You can follow Mr. Rosenzweig on Twitter at @RosenzweigP.*

Discussant: Jonathan Mayer, CISAC, Stanford University

Jonathan Mayer is a Ph.D. candidate in computer science at Stanford University, where he received his J.D. in 2013. Mayer's research and commentary frequently appear in national publications, and he has contributed to federal and state law enforcement actions. Mayer is a Junior Affiliate Scholar at the Center for Internet and Society, a Stanford Interdisciplinary Graduate Fellow, and was a Cybersecurity Fellow at the Center for International Security and Cooperation. He earned his A.B. at Princeton University. *You can follow Mr. Mayer on Twitter at @jonathanmayer.*

SESSION 7

DOMESTIC AND INTERNATIONAL LEGAL IMPLICATIONS OF CYBERSECURITY

This session examines both the domestic and international legal dimensions of cybersecurity. Technological change has far outpaced changes in law and almost certainly will continue to do so in the future. This lag creates legal challenges and makes it difficult for Congress to craft future legislation that is likely to be appropriate ten years down the road. Furthermore, nations also have cooperative and competitive (and sometimes adversarial) interests that play out in cyberspace. Communications through the Internet do not inherently respect national borders, giving an international dimension to every cybersecurity challenge, blurring lines in unprecedented ways between economics and security, and changing the relationships between civil societies, transnational actors, and states.

Faculty and Discussants

Professor Orin Kerr, George Washington University School of Law

Professor Kerr is a scholar of criminal procedure and computer crime law. He has authored more than 50 articles, and his scholarship has been cited in almost 2000 academic works. Before teaching, Professor Kerr was a trial attorney in the Computer Crime and Intellectual Property Section at the U.S. Department of Justice and Special Assistant U.S. Attorney in the Eastern District of Virginia. In 2013, Chief Justice Roberts appointed him to serve on the Advisory Committee for the Federal Rules of Criminal Procedure. *You can follow Dr. Kerr on Twitter at @OrinKerr.*

Professor Matthew Waxman, Columbia University School of Law

Matthew Waxman is an expert in national security law and international law, including issues related to international human rights, conflict resolution, and terrorism. Before joining the Columbia faculty, he served in senior positions at the U.S. State Department, Department of Defense and National Security Council. He is a member of the Council on Foreign Relations, and he is the Co-Chair for the Cybersecurity Center at the Columbia Institute for Data Sciences and Engineering. He holds a J.D. from Yale Law School.

Lynn St. Amour, Internet Matters

Lynn St. Amour is President/CEO of Internet Matters. Previously, she was president and CEO of the Internet Society (ISOC), an international organization dedicated to open development and use of the Internet. She became ISOC's global Executive Director and COO in 1999 and held that position until her appointment as President and CEO in March of 2001. Her background includes positions at the highest levels in international marketing, strategic planning, partner management and manufacturing. *You can follow Ms. St. Amour on Twitter at @LynnStAmour.*

Discussant: Elaine Korzak, CISAC, Stanford University

Elaine Korzak is a Ph.D. student in the Department of War Studies at King´s College London. She joined CISAC in September 2013 as a pre-doctoral cybersecurity fellow. Her thesis examines the applicability and adequacy of two key international legal frameworks to the emerging phenomenon of cyber attacks. During her time at CISAC, Korzak is conducting empirical research examining states´ responses to the legal challenges created by cyber attacks.

SESSION 8

CYBERSECURITY & CIVIL LIBERTIES

Many measures intended to support cybersecurity can also threaten certain civil liberties. At the same time, what cybersecurity means depends in part on whose security you are concerned with—a threat to civil liberties resulting from greater use of information technology might be construed as cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace. The session features a discussion between Jennifer Granick, one of the country's leading civil liberties advocates, and national security law expert Benjamin Wittes, where they will examine perspectives at the nexus of civil liberties and cybersecurity, and how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

Faculty

Benjamin Wittes, Brookings, Hoover Institution

Benjamin Wittes is a Senior Fellow in Governance Studies at The Brookings Institution. He co-founded and is the editor-in-chief of the Lawfare blog, which is devoted to sober and serious discussion of "Hard National Security Choices," and is a member of the Hoover Institution's Task Force on National Security and Law. He is the author of *Detention and Denial: The Case for Candor After Guantanamo* (2011) and editor of *Campaign 2012: Twelve Independent Ideas for Improving American Public Policy* (Brookings Institution Press, May 2012). He is also writing a book on data and technology proliferation and their implications for security. Between 1997 and 2006, he served as an editorial writer for *The Washington Post* specializing in legal affairs. Before joining the editorial page staff of *The Washington Post*, Wittes covered the Justice Department and federal regulatory agencies as a reporter and news editor at *Legal Times. You can follow Mr. Wittes on Twitter at @benjaminwittes.*

Jennifer Granick, Center for Internet & Society, Stanford Law School

Jennifer Granick is the Director of Civil Liberties at the Stanford Center for Internet and Society. She returns to Stanford after working with the internet boutique firm, Zwillgen PLLC. Before that, she was the Civil Liberties Director at the Electronic Frontier Foundation. Granick practices, speaks and writes about computer crime and security, electronic surveillance, consumer privacy, data protection, copyright, trademark, and the Digital Millennium Copyright Act. Before teaching at Stanford, Jennifer spent almost a decade practicing criminal defense law in California. She earned her law degree from University of California, Hastings College of the Law and her undergraduate degree from the New College of the University of South Florida. *You can follow Professor Granick on Twitter at @granick.*

SESSION 9

CORPORATE PERSPECTIVES ON CYBER SECURITY

Market forces play a critical role in enhancing or weakening cybersecurity. Session 9 examines how these forces play out at the level of the individual firm. Bay Area senior executives and engineers will give their "cyber-ground truths" about the security problems facing the private sector.

Speakers

Panel Chair: Raj Shah

Senior Director of Cyber Security, Palo Alto Networks

Raj Shah is the Senior Director of Cybersecurity at Palo Alto Networks. Prior to that, he was a Special Assistant in the Office of the Secretary of Defense where he worked on technology acquisition issues. He began his business career as a consultant with McKinsey & Co., and he also served as a reserve F-16 pilot in the USAF where he completed multiple combat tours in Iraq and Afghanistan. Shah holds an A.B. from Princeton University's Woodrow Wilson School and an M.B.A. from The Wharton School, University of Pennsylvania.

Scott Charney, Corporate VP, Trustworthy Computing, Microsoft

Scott Charney leads Microsoft's engagements with governments, partners and customers on security and privacy issues. Before joining Microsoft in 2002, he led PricewaterhouseCoopers' Cybercrime Prevention and Response Practice, and served as Chief of the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. He serves on the U.S. President's National Security and Telecommunications Advisory Committee Studies. He holds degrees in history, English and law.

Melody Hildebrandt, Global Head of Cyber Security, Palantir

Melody Hildebrandt is one of two founding females in Palantir's New York office, and currently works as a Deployment Strategist, leading Palantir's commercial cyber business. She works with some of the world's largest financial institutions and commercial enterprises on diverse data analysis problems ranging from cybersecurity, fraud, compliance and insider threat to data breach investigations. She received a B.A. in economics from Tufts University. *You can follow Ms. Hildebrandt on Twitter at @mhil1.*

David Liddle, Venture Partner, U.S. Venture Partners

David Liddle is co-founder of Interval Research Corporation, consulting Professor of Computer Science at Stanford University, and credited with heading development of the groundbreaking Xerox Star computer system. He was chair of the board of trustees of the Santa Fe Institute from 1994 to 1999, and he holds a B.S. in computer science from the University of Michigan. In January 2012, he joined the board of directors of SRI International.

Ellen Richey, Executive Vice President, Visa

Ellen Richey serves as Global Head of Enterprise Risk at Visa U.S.A., Inc. and has been its Chief Enterprise Risk Officer since October 2007. She serves as Chief Enterprise Risk Officer of Visa International Service Association. She served as Senior Vice President, Enterprise Risk Management and Executive Vice President, Cards Services at Washington Mutual, Inc. from October 2005 to June 2006. Ms. Richey holds a B.A. in Linguistics and Far Eastern Languages from Harvard University and a J.D. degree from Stanford Law School.

GOOGLE CAMPUS VISIT

Google's mission is to organize the world's information and make it universally accessible and useful. In this tour of one of the world's most famous companies in internet related services, staffers will learn about Google's cybersecurity efforts and its newest developments at Google [X]. This session includes a seminar and Q&A with Eric Grosse, Google's VP of Security, and Rick Salgado, Director of Information Security.

SCHEDULE OF EVENTS

2.30 pm	Tour of Google Campus
3.00 pm	Welcome; Cybersecurity Chat
4.15 pm	Google [X] Overview
5.15 pm	Depart for Palo Alto (dinner)

Speakers

Eric Grosse, Vice President, Security Engineering

Eric Grosse is the Vice President of Security Engineering at Google, where he leads a team of 250 members to ensure that systems and data stay safe and users' privacy remains secure. Improved and wider use of SSL, stronger consumer authentication technology, detection and blocking of foreign espionage, transparency on government request for data, sophisticated malware analysis, tools and frameworks for safer building of web applications are among the achievements of the Google Security Team. Grosse is a former Fellow at Bell Labs in Murray Hill and holds a Ph.D. in computer science from Stanford University.

Richard Salgado, Director, Information Security & Law Enforcement

Richard Salgado serves as Google's Director for information security and law enforcement matters. Prior to joining Google, Salgado was with Yahoo!, focusing on international security and compliance work. He also served as senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. He is a senior instructor with the SANS Institute, and a lecturer in law with Stanford Law School. Salgado received his J.D. from Yale Law School.

CONGRESSIONAL STAFF BIOGRAPHIES

Nate Adler, Senate Select Committee on Intelligence

Nate Adler is a professional staff member on the Senate Select Committee on Intelligence, where he covers cybersecurity issues for Senator John D. Rockefeller IV. Prior to joining the Committee, Nate was the defense and foreign policy advisor to Senator Rockefeller and was a Rosenthal Fellow on the Senate Foreign Relations Committee. Nate received an M.P.A. with a concentration on international relations at the Woodrow Wilson School, and an A.M. in East Asian Studies at Harvard University. Nate has been a James A. Kelly Fellow and a Project on Nuclear Issues Scholar, both at the Center for Strategic and International Studies (CSIS). A San Francisco native, Nate was a Fulbright Scholar to South Korea in 2005.

Tom Corcoran, House Permanent Select Committee on Intelligence

Tom Corcoran has been the Chairman's Senior Policy Advisor on the House Permanent Select Committee on Intelligence since January 2011, where he is the Committee's lead for cybersecurity issues. In this position, Corcoran has drafted and negotiated cyber threat information sharing legislation that passed the floor of the House by broad bipartisan margins. Corcoran served as an intelligence officer for the Defense Intelligence Agency, and he is a Navy Reserve intelligence officer with active duty service in Bosnia, Guantanamo Bay, and Afghanistan. Corcoran has a B.A. from George Washington University, and an M.A. from Johns Hopkins University's School of Advanced International Studies (SAIS).

Brett DeWitt, House Committee on Homeland Security

Brett DeWitt is currently the Senior Policy Advisor for Cybersecurity at the House Committee on Homeland Security. He currently advises Chairman Michael McCaul (R-TX) and the Committee on all Federal legislation involving cybersecurity, privacy, and security technologies. Prior to working for this committee, Mr. DeWitt served as a Legislative Aide to both Congressman Michael Turner (R-OH) and Congressman Phil English (R-PA). He also served as an Assistant to the Speaker of the House, J. Dennis Hastert. He is a graduate of UCLA, the U.S. Naval War College, College of Naval Command and Staff, and is currently pursuing a Masters of Arts in National Security and Strategic Studies.

Drenan Dudley, Senate Committee on Appropriations, Homeland Security

As professional staff, Drenan has oversight responsibilities of over $10 billion in annual Department of Homeland Security programs for the National Protection and Programs Directorate (main component responsible for cybersecurity programs), the Federal Emergency Management Agency, the Federal Protective Service, and the Office of Health Affairs. Prior to her current position, she was the Director of Projects and Grants for U.S.Senator Fritz Hollings. Before working in D.C., Dudley worked for two years in Arizona, at the Maricopa Association of Governments on regional coordination. She has earned a B.A. from the University of South Carolina and a M.P.A. from the University of Georgia.

CONGRESSIONAL STAFF BIOGRAPHIES

Brandon Eden, Office of Majority Whip Kevin McCarthy

Brandon Eden is the Senior Legislative Assistant and Military Legislative Assistant to the Majority Whip Kevin McCarthy. Prior to joining Congressman McCarthy's office, Eden was the Military Legislative Assistant to Congressman Richard Hanna (NY), the Victory Director of the Republican National Committee, and the New York Political Coordinator of the National Republican Congressional Committee. Eden has also served in the United States Marine Corps for six years. He holds a B.S. in history from Liberty University.

Michael Fischer, Senate Judiciary Committee

Prior to serving as Counsel to the Senate Judiciary Committee, Michael Fischer was an Associate with the law firm of Kellogg, Huber, Hansen, Todd, Evans & Figel in Washington, D.C. He was an Assistant U.S. Attorney in Philadelphia, PA. He is a graduate of Princeton University and Columbia Law School, where he served as an editor for the Columbia Law Review.

Joe Graupensperger, House Judiciary Committee

Joe Graupensperger serves as Democratic Counsel for the House Judiciary Committee. After graduating from the University of Virginia School of Law, he practiced in Washington, DC prior to working at the U.S. Department of Justice in the Office of Legislative Affairs, where he handled a range of legislative and oversight issues primarily related to federal criminal law. Having built relationships with Congressional staff during his time at the Department of Justice, Graupensperger was asked by the House Judiciary Committee Democrats to join their staff as a counsel to work on crime policy issues, particularly white collar crime, cybersecurity, computer crime, and domestic surveillance.

Stephanie Hall, Office of Senator John McCain

Stephanie Hall, as Counsel to Senator John McCain, handles legal and ethics issues, as well as legislation and policy developments in the areas of cybersecurity, telecommunications, technology, transportation, and judiciary-related topics. Prior to this position, Stephanie served as counsel on the Permanent Subcommittee on Investigations, working primarily on financial services and tax-related investigations. She previously worked as a law clerk on oversight and investigations at the Senate Judiciary Committee. Stephanie attended law school at the George Washington University School of Law and college at the University of Florida.

CONGRESSIONAL STAFF BIOGRAPHIES

Anne Harrington, Congressional Research Service

Anne I. Harrington is a Cybersecurity Fellow at the Congressional Research Service. Since earning her Ph.D. from the University of Chicago in 2010, Dr. Harrington has held fellowships at Stanford University and the Center for Nonproliferation Studies. In 2013 she was awarded an American Political Science Association Fellowship to work on Capitol Hill where she staffed for Senator Kirsten Gillibrand (D-NY). In Senator Gillibrand's office, she worked on military personnel issues. She also handled the Senator's cyber portfolio, focusing on DOD cyber workforce issues and critical infrastructure protection. Currently, she is working at the Congressional Research Service, co-authoring a report on U.S. Cyber Command with Catherine Theohary.

Jamil Jaffer, Senate Committee on Foreign Relations

Jamil N. Jaffer currently serves as the Republican Chief Counsel and Senior Advisor to the United States Senate Committee on Foreign Relations, where he advises the Committee on a range of foreign policy and national security matters, and as an Adjunct Professor and Director of the Homeland and National Security Law Program at the George Mason University School of Law. Immediately prior to joining the Senate Foreign Relations Committee, Jaffer served as Senior Counsel to the House Permanent Select Committee on Intelligence, where he worked on range of intelligence and national security issues, including cybersecurity, counterterrorism, and surveillance matters. He holds degrees from UCLA, the University of Chicago Law School, and the United States Naval War College.

Kerry Kinirons, House Committee on Homeland Security

Kerry A. Kinirons serves as Staff Director of the Subcommittee on Emergency Preparedness, Response, and Communications at the House Committee on Homeland Security where she advises Committee Members on policy pertaining to bioterrorism, grants, communications, and emergency management, including response efforts relating to the physical consequences of a cyber attack. Prior to joining the Committee, she served as Counsel to Congressman Peter T. King of New York. She received her Juris Doctorate from the Catholic University Columbus School of Law and her Bachelor of Arts in Political Science with honors from American University. She is admitted to practice law in the Commonwealth of Virginia.

Heather Molino, House Permanent Select Committee on Intelligence

Heather Moeder Molino is the Minority Staff Director for the House Permanent Select Committee on Intelligence. She and her team were critical in helping Intelligence Committee leadership pass four Intelligence Authorization Acts in four years, as well as the most prominent cyber legislation in the House of Representatives, the Cyber Intelligence Sharing and Protection Act by wide bipartisan margins. Before coming to Capitol Hill, she worked in the broadcast news world for more than ten years. She was a TV Reporter and Anchor in Washington, D.C., Virginia, and North Carolina. The Cornell University graduate and her husband, Michael Molino, a West Point graduate and former military officer, have three children.

CONGRESSIONAL STAFF BIOGRAPHIES

John Ohly, House Committee on Energy and Commerce

John Ohly is a Professional Staff Member for the House Committee on Energy and Commerce where he is responsible for conducting oversight and investigations related to energy, cybersecurity, automotive safety and other issues within the Committee's jurisdiction. Prior to joining Energy and Commerce, he served on the House Committee on Oversight and Government Reform where he focused on a wide range of issues and federal programs, including: U.S. security and foreign policy interests; energy; cybersecurity; nuclear power and security; telecommunications; and government administration. A native of Northern Virginia, Ohly graduated from the University of Pennsylvania with a degree in Diplomatic History.

Wyndee Parker, Office of the House Democratic Leader

Wyndee Parker is the National Security Advisor for the Office of the Democratic Leader of the U.S. House of Representatives. Her responsibilities include advising the Leader on national security and international affairs matters, and overseeing the activities of the Armed Services, Intelligence, Foreign Affairs and Homeland Security Committees, and their Appropriations Committee counterparts. She served in the same role in her capacity as National Security Advisor to the Speaker of the House from 2009-2011. Immediately prior to joining the Speaker's office, Ms. Parker was the Deputy Staff Director and General Counsel of the House Permanent Select Committee on Intelligence. Earlier in her career, Ms. Parker served as an assistant state prosecutor, and as an attorney at the Central Intelligence Agency and the Federal Bureau of Investigation.

Cherilyn Pascoe, Senate Committee on Commerce, Science, and Transportation

As Professional Staff Member and Investigator for the Senate Committee on Commerce, Science, and Transportation, Cherilyn Pascoe handles investigations and oversight activities and develops technology and consumer protection policy and strategy on behalf of Committee Ranking Member John Thune of South Dakota. She is a key staffer on cybersecurity, having drafted and negotiated bipartisan cybersecurity legislation and handled investigations into cybersecurity management in the public and private sectors. Pascoe received her M.A. in International Science and Technology Policy from the George Washington University and her B.S. Chem. with Highest Honors in Chemistry from the University of Michigan.

Daniel Pomeroy, Office of Senator Edward Markey

Daniel Pomeroy is AGU's 40th Congressional Science Fellow and will work in the office of Senator Edward Markey. He completed his Ph.D. in High Energy Experimental Physics at Brandeis University in 2012. His training as a physicist and recent work at the National Academy of Sciences focused on understanding U.S. nuclear safety and security. This gives him a valuable perspective in preparation of serving his term as a fellow in Congress. As a Congressional Science Fellow, he hopes to bridge communications between policymakers and scientists.

CONGRESSIONAL STAFF BIOGRAPHIES

Rebecca Seidel, Senate Committee on Commerce, Science, and Transportation

As General Counsel for the Commerce Committee, Rebecca Seidel handles cybersecurity issues as well as data breach, data security and privacy issues. Prior to joining the Committee, she has served as counsel on the Senate Impeachment Trial Committee regarding the impeachment of Judge G. Thomas Porteous, as Deputy Assistant Attorney General for Legislative Affairs at the U.S. Department of Justice, and as Senior Counsel on the Senate Judiciary Committee. Her public service was preceded by her extensive experience in private law practice in the Boston area doing civil litigation defense in the areas of products and premises liability.

Nicole Tisdale, House Committee on Homeland Security

Nicole Tisdale is the Democratic Subcommittee Director and Counsel to the United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence. She is the primary advisor to Ranking Member Bennie G. Thompson (MS), Subcommittee Ranking Member Brian Higgins (NY) and other Democratic Members of the Committee on policy matters and legislation related to intelligence, cyber counterterrorism, countering violent extremism, and law enforcement information sharing. Throughout her tenure on Capitol Hill, Tisdale has created strategic partnerships between the private sector and the Committee. She received both her Juris Doctorate (2009) and Bachelor's of Art (2006) from the University of Mississippi.

Shaun West, House Committee on Homeland Security

As a Professional Staff Member for the Committee on Homeland Security in the U.S. House of Representatives, Shaun West is responsible for policy development and departmental oversight in the areas of Counterterrorism and Intelligence. West has also served as a Special Agent in the U.S. Secret Service conducting multiple high level criminal investigations and several protection details for national leaders and foreign heads of state. West served a previous stint as Oversight Investigator for the Committee on Homeland Security. He earned his Bachelor of Criminal Justice and Master of Applied Social Sciences in Public Administration from Florida A&M University in 2005 and 2007, respectively.

Jessica Wilkerson, House Committee on Energy and Commerce

Jessica Wilkerson graduated from Syracuse University with a degree in Policy Studies and minors in both Computer Science and Mathematics. During her time there, she completed two internships with the Air Force's Information Directorate at the Air Force Research Laboratory in Rome, NY, where she studied formal verification of cyber systems. As a staff member of the House Committee on Energy and Commerce, she leverages this technical background to better understand and craft policy responses to the cybersecurity issues faced by the Committee.

CONGRESSIONAL CYBER BOOT CAMP

A CONVERSATION ON INDUSTRY AND POLICY CHALLENGES IN CYBERSECURITY
AUGUST 18-20, 2014

HOOVER INSTITUTION | Stanford University | CISAC STANFORD | CENTER FOR INTERNATIONAL SECURITY AND COOPERATION