CYBERSECURITY FOR A NEW AMERICA: BIG IDEAS AND NEW VOICES

The Ronald Reagan Building and International Trade Center
February 23, 2015

#NewAmCyber
Thank you to our sponsor

Please use this information to connect to the wifi.

username: NEWAMERICA
password: na2015
ANNOUNCING NEW AMERICA’S CYBERSECURITY INITIATIVE

There is perhaps no issue that has grown more important, more rapidly, on so many different levels, than cybersecurity. It affects personal privacy, business prosperity and the wider economy, as well as national security and international relations. It is a field that matters for everything from human rights and corporate profits to fundamental issues of war and peace. And with the rapid growth in both the number of people and devices coming online across the globe, the security of information systems is only going to grow in importance. Yet, while ever more amounts are spent each year, our collective understanding of the problem remains immature and both public policy and private sector efforts have failed to match the scale or complexity of this challenge for us all. The Internet has connected us, but the policies and debates that surround the security of our networks are too often disconnected, disjoint, and stuck in an unsuccessful status quo.

This is what New America’s new Cybersecurity Initiative is designed to address. We believe that it takes a wider network to face the network of diverse security issues. Success in this endeavor will require collaboration - across organizations, issue areas, professional fields and business sectors, as well as local, state, and international borders. By highlighting bold new ideas, bringing in new voices with fresh perspectives, breaking down issue and organizational barriers while building up a new field of study, encouraging new research approaches to the next generation of cybersecurity issues, connecting and creating new constituencies, and providing vibrant media and policy platforms to support that creativity, we can aid in pushing forward the cyber policy needed right now and better set us up for success tomorrow.

The nature of this new kind of approach to a new kind of 21st century problem is exactly why New America was built. We are a new kind of think tank, entrepreneurial in its ethos, nonpartisan in its research and advocacy, transparent in its funding, that specializes in bringing together individuals from a wide range of different backgrounds on the new set of opportunities and challenges facing America in the 21st century. Not only are we the only such organization with technologists on staff, but we also bring to the discussion world-renown experts in fields that range from international and national security strategy to privacy and human rights. We also take an approach that is focused on partnership building, notably beyond the DC Beltway (we also have an office in New York and are building a presence in California), connecting the next generation of leaders and experts from across the world into a network of offices and global media partnerships.

Initially the new Cybersecurity Initiative at New America will have three major elements:

- Networks: Supported by our partnership with The William and Flora Hewlett Foundation, we will build
  - A network of National Cyber Fellows, pulling together thinkers from across the United States, from in and outside the cyber policy community, to write and contribute new thinking to the policy debate.
  - An International Cyber Network to write and comment on cybersecurity issues from a range of vantage points, providing a unique set of foreign perspectives to what is an inherently global field.
  - A series of media partnerships to connect the above networks into and push forward wider public discourse. These include New America’s relationship with Slate Magazine and its Future Tense blog, a new cybersecurity focused podcast co-hosted with Christian Science Monitor, its “Future of War” programming with Defense One/The Atlantic, and launch event with CNN.

- Events: We are excited to work with our networks and other partners - both in DC and across our wider footprint - to support events that promote the initiative’s objectives.
  - A Policy/Business Roundtable aimed at bringing together some of the best thinkers from the policy and business communities to discuss common approaches to emerging or under-addressed cybersecurity policy issues. This thinking will then form the basis of further work to drive the policy agenda.
  - An Annual Conference bringing together diverse expert communities and policy leaders, while highlighting bold new ideas.
  - A series of public events addressing both emerging issues and especially highlighting the work of our Fellows and network members.

- Research and Advocacy: We will continue to build on our extensive policy research and focus especially on developing cybersecurity policy approaches that are realistic, yet scalable and impactful.
  - A series of reports and papers featuring original research, designed to push forward the next generation of ideas and thinkers.
  - A suite of new online resources and databases, such as the cyber definitions database recently completed by New America’s cyber team, made available for media, government, and other researchers to leverage in their own work.
  - Through the wider partnerships and a focus on impact, we will engage both the wider public and policy makers directly, building a networked case for action on topics that will range from the protection of civil liberties within cyber debates to new military thinking about cybersecurity topics. As a network, our building community will often represent a range of opinions on any particular issues, but will always be designed for widening the engagement of communities and pushing the debate forward.
How can we secure the least secure among us? Though most Americans equate privacy with security, safety, and protection, the population most likely to do anything to keep themselves safe and secure online are college-educated, white men. But what about other groups, especially members of disadvantaged groups with low levels of digital literacy? What prevents more people from adopting secure technologies and being mindful of security risks online? And what needs to change in order to ensure that personal security online is accessible and available to everyone?

Cyber incidents will happen. They are likely to occur in spite of the important international efforts to strengthen norms governing and limiting the malicious use of cyberspace. We need a Cyber Red Cross, cyber humanitarians working across borders to respond to such incidents and to provide assistance where needed at times of war and peace. Can Computer Emergency Response Teams (CERTs) play this role? What other institutions and networks exist? What would the ICRC’s humanitarian principles of neutrality, independence, and impartiality look like for cyberspace?
have resources to direct sustained, sophisticated hacking campaigns for financial or political gain, what is our best defense? How should the targets, the security vendors that assist them, and the policymakers that serve them react to an ever more hostile Internet environment that’s starting to look more like a failed state than the info-utopia we once envisioned? And how do we combat these threats while also preserving the openness of the Internet and the privacy of Internet users?

NEW AMERICA’S CYBERSECURITY TEAM

Kevin Bankston is the Policy Director of the New America’s Open Technology Institute (OTI), where he works in the public interest to promote policy and regulatory reforms to strengthen communities by supporting open communications networks, platforms, and technologies, with a focus on issues of Internet surveillance and censorship. Prior to leading OTI’s policy team, Kevin was a Senior Counsel and the Director of the Free Expression Project at the Center for Democracy & Technology. Since 2005, he has served on the board of the First Amendment Coalition, a non-profit public interest organization dedicated to advancing free speech and a more open and accountable government, and previously was a nonresident fellow at the Stanford Law School’s Center for Internet & Society. Prior to CDT, he worked at the Electronic Frontier Foundation, where, as a Senior Staff Attorney at EFF, he was a lead counsel in EFF’s lawsuits against the National Security Agency and AT&T, challenging the legality of the NSA warrantless wiretapping program first revealed in 2005. He originally joined EFF as an Equal Justice Works/Bruce J. Ennis First Amendment Fellow, studying the impact of post-9/11 anti-terrorism surveillance initiatives on online privacy and free expression. Before joining EFF, he litigated Internet-related free speech cases at the national office of the American Civil Liberties Union in New York City as a Justice William Brennan First Amendment Fellow. He received his JD at the University of Southern California Law School after receiving his BA at the University of Texas at Austin.

Alan Davidson is New America’s Vice President for Technology Policy and Strategy and Director of the Open Technology Institute. He is also a Research Affiliate at MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL), where he is a co-founder of the new MIT Information Policy Project. Until 2012 Alan was the Director of Public Policy for Google in the Americas. He opened Google’s Washington, D.C. office in 2005, and led the company’s public policy and government relations efforts in North and South America. Prior to joining Google, Alan was Associate Director of the Center for Democracy and Technology, a public interest group promoting civil liberties and human rights online. He has testified before Congress, written, and spoken widely on a range of Internet policy issues including free expression, privacy, content regulation, encryption, network neutrality and copyright online. Alan started professional life as a computer scientist. He was a senior consultant at Booz Allen & Hamilton, where he helped design information systems for NASA’s Space Station Freedom Project. Alan has a bachelor’s degree in mathematics and computer science and a master’s degree in technology and policy from MIT. He is also a graduate of the Yale Law School, where he was Symposium Editor of the Yale Law Journal.

Seeta Peña Gangadharan is a Senior Research Fellow at the New America’s Open Technology Institute. Her work lies at the intersection of technology, civil society, and communication policy. She focuses on the nature of digital inequalities, data and discrimination, social dynamics of technology adoption, communication rights, and media justice. Since joining OTI in July 2011, she has written and spoken widely about digital inclusion, privacy, surveillance, and data profiling of marginalized populations. Her work has identified privacy and surveillance norms and practices among members of underserved groups and exposed the lack of privacy and surveillance knowledge among frontline staff at digital literacy organizations. Prior to OTI, she was a postdoctoral fellow at the Information Society Project at Yale Law School, where she initiated a project on the tension between digital inclusion and data profiling. Her PhD work, completed at Stanford University, investigated the politics of communication policymaking, with a focus on the rulemaking process at the Federal Communications Commission. She is a research fellow of the Data & Society Research Institute and a visiting fellow of the Information Society Project at Yale Law School.
Anne-Marie Slaughter is currently the President and CEO of New America, a think tank and civic enterprise with offices in Washington and New York. She is also the Bert G. Kerstetter ’66 University Professor Emerita of Politics and International Affairs at Princeton University. From 2009-2011 she served as director of Policy Planning for the United States Department of State, the first woman to hold that position. Upon leaving the State Department she received the Secretary’s Distinguished Service Award for her work leading the Quadrennial Diplomacy and Development Review, as well as meritorious service awards from USAID and the Supreme Allied Commander for Europe. Prior to her government service, Dr. Slaughter was the Dean of Princeton’s Woodrow Wilson School of Public and International Affairs from 2002–2009 and the J. Sinclair Armstrong Professor of International, Foreign, and Comparative Law at Harvard Law School from 1994-2002. Dr. Slaughter has written or edited six books, including A New World Order (2004) and The Idea That Is America: Keeping Faith with Our Values in a Dangerous World (2007), and over 100 scholarly articles. She was the convener and academic co-chair, with Professor John Ikenberry, of the Princeton Project on National Security, a multi-year research project aimed at developing a new, bipartisan national security strategy for the United States. In 2012 she published the article “Why Women Still Can’t Have It All,” in The Atlantic, which quickly became the most read article in the history of the magazine and helped spawn a renewed national debate on the continued obstacles to genuine full male-female equality. Dr. Slaughter writes a monthly column for Project Syndicate. She provides frequent commentary for both mainstream and new media and curates foreign policy news for over 80,000 followers on Twitter. Foreign Policy magazine named her to their annual list of the Top 100 Global Thinkers in 2009, 2010, 2011, and 2012. She received a B.A. from Princeton, an M. Phil and D.Phil in international relations from Oxford, where she was a Daniel M. Sachs Scholar, and a J.D. from Harvard. She is married to Professor Andrew Moravcsik; they live in Princeton with their two sons.

Ian Wallace is a Senior Fellow in the International Security Program, and also Co-Director of New America’s Cybersecurity Initiative. His research is mainly focused on the international security and military dimensions of cybersecurity policy. He is also a member of the ‘Future of War’ project. Ian joined New America from the Brookings Institution where he spent two years in the Foreign Policy Program as a Visiting Fellow for Cybersecurity. He was previously a senior official at the British Ministry of Defence (MOD). From 2009-2013 Wallace was as the British Embassy, Washington’s defense policy and nuclear counselor. There he helped develop new UK/US mil/mil cyber link at both the operational and policy levels. Before joining the embassy he was a fellow at the Weatherhead Center at Harvard University where his research included working on the military implications of cyber capabilities. During his UK MOD career, he combined strategy and planning positions with operational postings to Pristina (2001-2002), Basra (2005) and Baghdad (2007-2008). He also served as the head of policy at the UK’s operational HQ (2002-2003). His Whitehall appointments included Deputy Director of Capability, Resource and Scrutiny and Assistant Director of Defence Resources (with day-to-day responsibility for the UK MOD’s overall resource planning process). From 2000-2001 he was the Assistant Private Secretary to the UK Defence Secretary. Wallace has a degree in ancient and modern history from Christ Church, Oxford University.

Tim Maurer is a Research Fellow at New America where he focuses on cyberspace and international affairs and co-leads New America’s Cybersecurity Initiative. He is part of New America’s Future of War project and serves as a member of the Research Advisory Network of the Global Commission on Internet Governance, the Freedom Online Coalition’s cybersecurity working group “An Internet Free and Secure”, and co-chair of the Civil Society Advisory Board for the Global Conference on Cyberspace. His research projects center on cyberwarfare and the global cyber-security norms process, transatlantic cooperation on security and freedom in the digital age, Internet Freedom especially in the context of U.S. sanctions and export controls, and research on swing states in the international Internet governance debate. In 2013 and 2014, Mr. Maurer spoke about cyber-security at the United Nations in New York and Geneva in addition to other national and international conferences. He conducts his academic research as a non-resident research fellow at the Citizen Lab and serves as a reviewer for academic journals. Prior to joining New America, Mr. Maurer worked at the Center for Strategic and International Studies and gained experience with the United Nations in Rwanda, Geneva, and New York focusing on humanitarian assistance and the coordination of the UN system. He holds a Master in Public Policy concentrating on international and global affairs from the Harvard Kennedy School.

Peter W. Singer is a Strategist and Senior Fellow at New America. He is considered one of the world’s leading experts on 21st century security issues and is the author of multiple award-winning books. He has been named by the Smithsonian Institution-National Portrait Gallery as one of the 100 leading innovators in the nation, by Defense News as one of the 100 most influential people in defense issues, and by Foreign Policy magazine to their Top 100 Global Thinkers List. His books include Corporate Warriors: The Rise of the Privatized Military Industry, Children at War, and Wired for War: The Robotics Revolution and Conflict in the 21st Century. His most recent book, Cybersecurity and Cyberwar: What Everyone Needs to Know, was named to both the US Army and US Navy professional reading list. Singer is a contributing editor at Popular Science magazine and the founder of NeoLuddite, a technology advisory firm. He has consulted for the US military, Defense Intelligence Agency, and FBI, as well as advised a wide-range of technology and entertainment programs, including for Warner Brothers, Dreamworks, Universal, HBO, and the video game series Call of Duty, the best-selling entertainment project in history. He is a member of the US State Department’s Advisory Committee on International Communications and Information Policy. His past work included serving as coordinator of the Obama-08 campaign’s defense policy task force, in the Balkans Task Force at the Office of the Secretary of Defense, and as the founding director of the Center for 21st Century Security and Intelligence at The Brookings Institution, where he was the youngest senior fellow in its 100 year history.

Ian Wallace

Tim Maurer

Anne-Marie Slaughter

Peter W. Singer
Aileen Alexander is a Principal in the Washington, D.C. office of Korn Ferry, where she co-leads the Firm's Cybersecurity Center of Expertise and specializes in the Aerospace, Aviation & Defense Sector. She also has expertise in the financial services, government services and board services sectors as it adheres to military veteran talent. In delivering integrated talent management solutions, Ms. Alexander partners with a diverse client base as an advisor focused on building and developing effective leadership teams at the C-suite and senior executive levels. She has been certified in Korn Ferry, powered by Lominger, Leadership Architect®. Previously, Ms. Alexander was with another international search firm, where she served clients in the aerospace & defense, professional services, financial services, and nonprofit sectors. Prior to entering the talent management profession, Ms. Alexander worked in national security, most recently as a Professional Staff Member on the Committee of Armed Services in the U.S. House of Representatives. In this role, she consulted Members of Congress in their oversight activities as they related to the Department of Defense and some elements within the Department of Energy. Her expertise included global defense issues related to Asia, Africa, and Latin America as well as nonproliferation and homeland defense programs and activities. She has also traveled around the world with a focus on military operations and drafted legislation in the annual National Defense Authorization Act. Previously, Ms. Alexander was a Presidential Management Fellow in the Office of the Secretary of Defense. Earlier in her career, she served as a Captain in the U.S. Army as a communications officer. Ms. Alexander holds a master’s degree in public policy from Harvard University’s Kennedy School of Government and earned a bachelor of arts degree from The Johns Hopkins University. She is a Term Member with the Council on Foreign Relations and is a regularly coaches retiring General/Flag Officers.

Lieutenant General Edward C. Cardon is the Commanding General, United States Army Cyber Command. He was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. LTG Cardon has commanded at every level from company through division. Prior to assuming command of the United States Army Cyber Command, he was the commander of the 2nd Infantry Division based in South Korea. His education includes a Bachelor’s of Science Degree from the United States Military Academy and two Master’s Degrees - one from the National War College and the other from the United States Naval Command and Staff College, both in National Security and Strategic Studies. Lieutenant General Cardon is married and has three children.

Nate Fick is CEO of Endgame. He has more than a decade of experience in the security community, and is an operating partner at Bessemer Venture Partners, where he focuses on defense and intelligence technologies. Before joining Endgame, Nate was CEO of the Center for a New American Security, a national security research organization. He served as a Marine Corps infantry officer, including combat tours in Afghanistan and Iraq. His book about that experience, One Bullet Away, was a New York Times bestseller, a Washington Post “Best Book of the Year,” and one of the Military Times’ “Best Military Books of the Decade.” He graduated with high honors in Classics from Dartmouth College and holds an MPA from the Harvard Kennedy School and MBA from the Harvard Business School. Nate serves as a Trustee of Dartmouth and a Director of the Marine Corps Scholarship Foundation, and he is a member of the Council on Foreign Relations.

Daniel Kahn Gillmor is a Technology Fellow with the ACLU’s Speech, Privacy and Technology Project. He is an active developer for Debian, one of the oldest and largest free software operating systems, in addition to other free software projects, with a focus on cryptographic tools. Daniel is also a participant in the development of Internet protocols for secure communications with groups like the IETF and W3C. He has served on the Leadership Committee of May First/People Link, a mutual aid Internet organization for social justice advocates, and is a mutual aid Internet organization for social justice advocates, and is an advocate and trainer for wider adoption of secure communications tool.

Siobhan Gorman is a Director of the Brunswick Group, focus on corporate data and privacy issues. She formerly served as a reporter for The Wall Street Journal covering intelligence, terrorism, cybersecurity, and surveillance issues. Prior to joining The Journal in 2007, Ms. Gorman was a Washington correspondent for The Baltimore Sun, covering intelligence and security. From 1998 to 2005, she was staff correspondent for National Journal covering homeland security, justice, and intelligence; and in 1997 was also a research associate for “Bob Levey’s Washington,” at The Washington Post. Ms. Gorman won the 2006 Sigma Delta Chi Award for Washington Correspondence for her coverage of the National Security Agency and in 2000 received a special citation in national magazine writing from the Education Writers Association. Ms. Gorman received her bachelor’s arts in government from Dartmouth College.

Seda Gürses is a post-doctoral research fellow in the Media, Culture and Communications Department working on privacy, security, surveillance studies and requirements engineering. She is also a member of the Intel ISTC Center on Social Computing. Previously Seda was a post-doctoral researcher at COSIC (Computer Security and Industrial Cryptography) in the Department of Electrical Engineering of the KU Leuven, where she acted as the coordinator of the interdisciplinary project SPION (Security and Privacy in Online Social Networks) funded by the Flemish Agency for Innovation in Science and Technology (IWT). Seda received her PhD at the Department of Computer Science of the KU Leuven, her Master’s degree in Informatics at the Humboldt University Berlin (Germany), her B.S. in Mathematics and BA in International Relations and Peace from the University of Redlands in the USA.

Shane Harris is a Sr. Intelligence and National Security Correspondent for The Daily Beast and an ASU Future of War Fellow at the New America. He is the author of two books: @War: The Rise of the Military-Internet Complex, and The Watchers: The Rise of America’s Surveillance State, which won the New York Public Library’s Helen Bernstein Book Award for Excellence in Journalism. Prior to joining The Daily Beast, Shane was a senior writer at Foreign Policy magazine. He has also written for Washingtonian Magazine, the National Journal and Government Executive Magazine. Shane is the 2010 winner of the Gerald R. Ford Prize for Distinguished Reporting on National Defense. He has been a finalist four times for the Livingston Awards for Young Journalists, which honor the best reporters in America under 35. He graduated from Wake Forest University with a B.A. in Politics in 1998.

Will Harvey is the Lead for Public Sector Networks & Cyber Security Incident Management at the UK Cabinet Office’s Office of Cyber Security and Information Assurance. He joined the Civil Service after undertaking varied roles in the private sector. Through the Fast Stream he undertook a number of different roles and projects covering a range of issues from policy, communications, technology delivery and business performance management. He became involved in the delivery of government information security and business continuity, and over the past five years has led functions in different security disciplines from personnel and physical security to education and awareness, through to responding to cyber crime. In 2012 he joined the Office of Cyber Security and Information Assurance as their lead on both the security issues facing public sector networks and cyber incident response. Will holds a BA (Hons) in Psychology, Philosophy and Physiology from Oxford, and is a CESG Certified Professional security and risk advisor.
Duncan B. Hollis is the James E. Beasley Professor of Law and the Associate Dean for Academic Affairs at the Temple University School of Law in Philadelphia. Professor Hollis’s scholarship focuses on treaties and international regulation of cyber threats. He is the editor of the award-winning Oxford Guide to Treaties (OUP, 2012) and National Treaty Law and Practice (Martinus Nijhoff, 2005) as well as a series of articles on the extent to which international law does (and does not) regulate governance and behavior in cyberspace. He is a senior team member of METANORM: A Multi-disciplinary Approach to the Analysis and Evaluation of Norms and Models of Governance for Cyberspace, an MIT-led project that is funded by the Minerva Research Initiative. A former legal adviser for treaty affairs in the U.S. Department of State’s Office of the Legal Adviser, Professor Hollis serves on the Executive Council of the American Society of International Law, as an elected member of the American Law Institute, and as a regular contributor to Opinio Juris, a leading blog on international law and international relations.

Morgan Marquis-Boire is a Senior Researcher and Technical Advisor at the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is the Director of Security for First Look Media. Prior to this he worked on the security team at Google. He is a founding member of The Secure Domain Foundation, a non-profit, free, adversary intelligence group. He is a Special Advisor to the Electronic Frontier Foundation in San Francisco and an Advisor to the United Nations Inter-regional Crime and Justice Research Institute. In addition to this, he serves as a member of the Free Press Foundation security advisory board. A native of New Zealand, He was one of the original founders of the KiwiCON hacker conference. His research on surveillance and the digital targeting of activists and journalists has been featured in numerous print and online publications.

Cheri McGuire is the Vice President Global Government Affairs and Cybersecurity Policy at the Symantec Corporation. She leads Symantec’s global public policy agenda and government engagement strategy that includes cybersecurity, critical infrastructure protection (CIP), and privacy. With more than twenty years of government and industry experience, she leads a team of professionals spanning the U.S., Canada, Europe, and Asia. Ms. McGuire serves on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of the Information Technology Industry Council, the US Information Technology Office in China, and the National Cyber Security Alliance. From 2010 to 2012, she served as Chair of the US IT Sector Coordinating Council – one of 16 critical sectors identified by the President and DHS to partner with the government on CIP and cybersecurity. Ms. McGuire is a frequent presenter on technology policy issues, including testifying numerous times before Congress. Past positions include: Director for Critical Infrastructure and Cybersecurity in Microsoft’s Trustworthy Computing Group; Acting Director and Deputy Director of the DHS National Cyber Security Division and US-CERT; program manager at Booz Allen Hamilton; and Congressional staffer.

Angela McKay is Director of Cybersecurity Policy and Strategy in the Global Security Strategy and Diplomacy team at Microsoft. She focuses on driving strategic change, both within Microsoft and externally, to advance trust in the computing ecosystem. Ms. McKay leads Microsoft’s cybersecurity policy work in the U.S., and engages internationally with industry, governments, and civil society to improve security and stability of cyberspace for users around the world. Ms. McKay combines technical expertise and public policy acumen to develop policies that support development, growth, and innovation, and advance security, privacy, and trust in the Information Age. Ms. McKay served as Microsoft’s POC for the National Security Telecommunications Advisory Committee (NSTAC), a Presidential advisory committee focused on maintaining secure and resilient communications and as Chair of the IT Sector Coordinating Council, a public private partnership between the IT industry and the U.S. Government focusing on critical infrastructure protection and cybersecurity. Prior to joining Microsoft, she worked at Booz Allen Hamilton and BellSouth Communications. Ms. McKay holds a Bachelor’s of Industrial and Systems Engineering from the Georgia Institute of Technology.

Thomas R. Millar is the United States Computer Emergency Readiness Team’s (US-CERT) Chief of Communications, a role which finds him at the intersection of outreach, awareness, standards development, and technical interoperability initiatives. In this role, Mr. Millar is focused on modernizing US-CERT’s approaches to information sharing, knowledge exchange and coordination. Since joining US-CERT in 2007, he has played a significant role in US-CERT’s response activities during major cyber events such as the Distributed Denial of Service (DDoS) attacks on Estonia in 2007, the outbreak of the Conficker worm, and the DDoS attacks on major U.S. Government and commercial Web sites in 2009. Mr. Millar has previously worked as a team lead for intrusion detection and analysis at the FBI’s Enterprise Security Operations Center. Prior to his cybersecurity career, he served as a linguist with the 22nd Intelligence Squadron of the United States Air Force. Mr. Millar has a Master’s of Science in Engineering Management from the George Washington University.

Katie Moussouris is the Chief Policy Officer for HackerOne, a platform provider for coordinated vulnerability response & structured bounty programs. She oversees the company’s philosophy on vuln disclosure, advises customers & researchers, & works to legitimize & promote security research to help make the internet safer for everyone. Katie’s earlier Microsoft work encompassed industry-leading initiatives such as Microsoft’s bounty programs & Microsoft Vulnerability Research. She is also a subject matter expert for the US National Body of the International Standards Organization (ISO) in vuln disclosure (29147), vuln handling processes (30111), secure development (27034), and penetration testing (2004). Katie is a visiting scholar with MIT Sloan School, doing research on the vulnerability economy and exploit market. She is an ex-hacker, ex-Linux developer, & persistent hugger. Follow her and HackerOne on Twitter http://twitter.com/klemo and http://twitter.com/hacker0x01

Dlshad Othman is a Syrian activist and IT engineer who provides Syrians with digital security resources and assistance so that they can utilize online communications and advocacy freely and securely in spite of increased online government repression in the form of censorship, sophisticated cyber attacks, and intense surveillance. He started supporting local coordination committees in Syria as an IT consultant from the beginning of the Syrian revolution but was obliged to flee Syria at the end of 2011 when his name became known to Syrian intelligence following the arrest of British documentary filmmaker Sean McAllister. Dlshad designed and is still working on the data protection system of the Center for Documentation of Violations in Syria, which is used by the media and NGOs worldwide. He started working with the Institute for War and Peace Reporting as a cyber-security trainer in December 2011. He has given many data security training courses for Syrian activists in Lebanon and in Jordan. He has succeeded in detecting malware developed by the Syrian regime to monitor Syrian activists and has been able to guide international organizations active in helping opponents of the Syrian regime. He was chosen as a 2012 Internet freedom fellow by the US State Department and he collected the 2012 Front Line Defenders Award for Syrian human rights activist Razan Ghaazawi in her absence (she’s in jail in Syria awaiting trial). Dlshad holds a degree in operating systems and online publications.

Dr. Heather Roff is currently a Visiting Professor at the Josef Korbel School of International Studies at the University of Denver. She is a research fellow at the Eisenhower Center for Space and Defense Studies at the United States Air Force Academy, and has held faculty posts at the University of Waterloo and the United States Air Force Academy. Her research interests pertain to international ethics, security and emerging military technologies, particularly cyber warfare, lethal autonomous weapons, and unmanned systems. She is also interested in the Responsibility to Protect doctrine, international humanitarian law, and the philosophy of Immanuel Kant. She is author of Global Politics, Kant and the Responsibility to Protect (Routledge, 2013) and over a dozen articles, including “The Strategic Robot Problem” Journal of Military Ethics,(2014), and “Gendering a Warbot” International Feminist Journal of Philosophy (2015, forthcoming), and currently writing a monograph on autonomous weapons systems.

Duncan B. Hollis

Morgan Marquis-Boire

Cheri McGuire

Angela McKay

Thomas R. Millar

Katie Moussouris

Dlshad Othman

Dr. Heather Roff
Admiral Michael Rogers is the Commander of the U.S. Cyber Command and the Director of the National Security Agency. A native of Chicago, Rogers attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986. He assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency/Chief, Central Security Service in March 2014. Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as commander, U.S. Fleet Cyber Command/U.S. 10th Fleet. Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of commander, Carrier Group 2/John F. Kennedy Carrier Strike Group; and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lassen (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean. Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and, has served at Naval Security Group Department; NAVCOMSTA Rota, Spain; Naval Military Personnel Command; Commander in Chief, U.S. Atlantic Fleet; the Bureau of Personnel as the cryptologic junior officer detailer; and, Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander. Rogers’ joint service both afloat and ashore has been extensive and, prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman’s Action Group, and a leader of the JCS Joint Strategic Working Group. Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow; Harvard Senior Executive in National Security alum; and holds a Master of Science in National Security Strategy.

Molly Sauter is a doctoral student at McGill University in Montreal in the department of Art History and Communication Studies. She holds a masters degree in Comparative Media Studies from MIT, and is an affiliate researcher at the Center for Civic Media at the MIT Media Lab and the Berkman Center for Internet and Society at Harvard University. Her research is situated in socio-political analyses of technology and technological culture, and is broadly focused on hacker culture, transgressive digital activism, and depictions of technology in the media. Her work has been published in The Atlantic, HiLow Brow, 109, The American Behavioral Scientist, and the MIT Technology Review. Her research has been featured by Popular Mechanics, BoingBoing, the BBC, NPR, the CBC, Der Spiegel, Salon, and the Christian Science Monitor. She is the author of The coming Swarm: DoDo Actions, Hacktivism, and Civil Disobedience on the Internet. She resides in Montreal, Quebec, and lives on the internet, blogging at oddletters.com and tweeting @oddletters.

Bruce Schneier is a Fellow at the Harvard’s Berkman Center for Internet and Society. He is an internationally re-nowned security technologist, called “a security guru” by The Economist. He is the author of 12 books – including Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World – as well as hundreds of articles, essays, and academic papers. His influential newsletter “Crypto-Gram” and blog “Schneier on Security” are read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America’s Open Technology Institute, a board member of the Electronic Frontier Foundation, and an Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc.

Jim Sciutto is CNN’s chief national security correspondent. He reports and provides analysis across the network’s programs and platforms on all aspects of U.S. national security, including foreign policy, the military and the intelligence community. This year, he traveled to Ukraine to cover the country’s violent election, to China with U.S. Secretary of Defense Chuck Hagel and to Tehran as Iran started to implement the U.S. nuclear agreement. He twice interviewed Iranian Foreign Minister Mohammad Javad Zarif, including getting Iran’s first reaction to President Barack Obama’s 2014 State of the Union remarks. Sciutto’s work in Iran during the 2009 election protests earned him an Edvard R. Murrow award. He was also given the George Polk Award and a citation for Excellence from the Overseas Press Club for his undercover reporting from Myanmar, where he bucked government restrictions to tell the stories of that country’s repressive regime. His reporting for the series “Iraq: Where Things Stand” was recognized with an Emmy Award for two consecutive years. Most recently, Sciutto served as chief of staff and senior advisor to the U.S. Ambassador to Chi-nna, Gary Locke. Prior to ABC News, he served as the Hong Kong-based correspondent for Asia Business News. Sciutto began his career as the moderator and producer of a weekly public affairs talk show on PBS. He graduated from Yale University with a bachelor’s degree in Chinese history. Jim is married to Gloria Riviera-Sciutto, who is Asia Correspondent for ABC News.

François Stamm is the Head of Regional Delegation for the U.S. & Canada for the International Committee of the Red Cross where he oversees ICRC visits to the detention facility Guantanamo Bay, Cuba and is responsible for working relationships with the governments of the United States and Canada. He also interfaces with the National Red Cross Societies and serves as the ICRC’s representative to the public at large in both countries. Previously, from 2008 to 2012, Mr. Stamm served as Head of Regional Delegation for India, Bhutan, and the Maldives overseeing detention visits as well as carrying out a range of humanitarian activities in violence-prone areas. Between 2002 and 2008, Mr. Stamm was Head of Operations for North America, Western, Central & South Eastern Europe at ICRC Headquarters in Geneva. Mr. Stamm joined the ICRC in 1987, serving in South East Asia (Cambodia, Philippines) and Africa (Zambia, Soma- lia, Zimbabwe, Malawi). Between 1994 and 2002, he focused on various operational contexts in the Balkans (Kosovo, Montenegro, Serbia, Macedonia). He has held various positions involving the distribution of assistance to victims of conflicts, visits to persons deprived of freedom, contact and negotiations with national and international representa-tives, as well as senior operational management. Mr. Stamm is a graduate of the Lausanne Higher Business School.

Alex Stamos is the CISO of Yahoo. He was the co-founder of iSEC Partners and founder of Artemis Internet, two companies that continue to make the Internet a safer place. Alex has spent his career building or improving secure, trustworthy systems, and is a noted expert in Internet infrastructure, cloud computing and mobile security. He is a frequently request speaker at conferences such as Black Hat, DEF CON, Amazon ZonCon, Microsoft Blue Hat, FS-ISAC and Infragard. He holds a BSEE from the University of California, Berkeley and his personal security writings are available at http://unhandled.com.

Tara Whalen is a Staff Privacy Analyst at Google and a Non-Residential Fellow at the Center for Internet and Society at Stanford Law School. She obtained a Master of Laws from the University of Ottawa, with a Concentration in Law and Technology. Tara previously worked as a Privacy Engineer at Apple, and as an IT Research Analyst at the Office of the Privacy Commissioner of Canada. She conducted post-doctoral research in computer security at Carleton University, after receiving a PhD in computer science at Dalhousie University. Tara has 20 years of experience in the information security and privacy fields, including roles in research labs, academia, federal government institutions, and the private sector. Her research interests include usable security and privacy, as well as technology policy.