

# Initiative on the Future of Cyber Risk

A project of the Columbia University School of International and Public Affairs  
Technology and Policy Initiative

Director and Principal Investigator: Jason Healey

The last 12 months have been as historic as they've been shocking, and much of that conflict and tumult has been reflected in cyberspace. Throughout the 2016-2017 academic year, Columbia University's School of International and Public Affairs (SIPA) has expanded upon its efforts to understand a world increasingly dominated and defined by cybersecurity and cyber conflict. These efforts examined the effects of cyber risk on infrastructure, government, military, the economy, and narratives of information and security.

The Initiative's more prominent research brought Jason Healey (SIPA) together with Matthew Waxman (Columbia Law School) and Steven Bellovin (Columbia Computer Science Department) to jointly examine balances and trade-offs as national security imperatives increasingly intrude into cyberspace. The Initiative also supported Jason Healey and Robert Jervis' (SIPA) Department of Defense-funded research on the strategic dynamics of cyber conflict, as well as the activities of the New York Cyber Task Force (NYCTF). Comprised of New York private sector executives, the group is releasing a strategic report on making cyberspace more defensible, with technical and policy-oriented recommendations.

Through these interdisciplinary and inter-school efforts, the initiative continued to prioritize the following key questions:

- How can cyberspace be made more defensible?
- What cyber risks are likely to arise in the future?
- How might the future Internet differ – for better or worse – from today's?
- What is a nation's true cyber power and how might that power change over time?
- What are the dynamics of cyber conflict and how do they differ from its tactical and strategic dynamics?
- How can public policy mitigate cyber risk and build better digital futures?
- How does business and systemic cyber risk affect financial sector stability?

With the resources of the entire Columbia community, including world-class faculty, scholars, and students, the Initiative has inaugurated numerous remarkable thought leadership, publication, and events, helping to establish SIPA as a world-class center on thinking and learning and a destination for the next generation of cyber leaders.

The program is directed by Jason Healey, a SIPA Senior Research Scholar with nearly 20 years' cyber experience as a researcher and practitioner with the U.S. Air Force, Goldman Sachs, the Atlantic Council and the White House.

## ABOUT THE SIPA TECH & POLICY INITIATIVE

Tech & Policy @ SIPA is an ambitious effort to fuse public policy, engineering, data science, and entrepreneurship through activities including innovation competitions, start-up incubator space and interdisciplinary research.

By equipping the next generation of public policy students with a deep understanding of new technology, nurturing organizations that build novel tech-based solutions to pressing public policy problems and supporting cutting-edge interdisciplinary research, SIPA is establishing itself as a preeminent authority in technology and public policy.

## Major Achievements

### 1. State of the Field of Cyber Conflict

In June 2016, Columbia University SIPA, in conjunction with the Cyber Conflict Studies Association (CCSA), hosted a first-ever workshop to examine the existing research in the field of cyber conflict, establishing the key questions, canonical works, progress made over the past decades, and remaining gaps. This workshop brought together some of the most senior practitioners in law, history, political science, and technology. A second State of the Field event was then held in June 2017.

### 2. Bridging the Gap in Cyber Conflict Studies

In November 2016, SIPA and CCSA hosted a workshop to “bridge the gap” between junior- and senior-level academics and between academics and practitioners. This two-day workshop focused on the state of the field of cyber conflict, best practices for research design, methodology and execution, and the application and expansion of cyber research beyond academia.

### 3. New York Cyber 9/12 Student Challenge

Columbia University hosted the first-ever New York City Cyber 9/12 Competition in November 2016. This two-day policy competition required students to tackle the challenges of assessing the impact of a major cyber-attack and thinking through attribution, national responsibility, and response options for the President and private sector. The event included 16 teams from 10 universities (including Tufts-Fletcher, Princeton-Wilson, the U.S. Military Academy, Carnegie Mellon, and King’s College London) and judges from JP Morgan Chase, the Department of Defense, the U.S. Air Force, Harvard-Kennedy, the Army Cyber Institute, CNN, IBM, Palantir, and Google Jigsaw, among others. Top teams went on to compete in the national competition in Washington D.C.



*Audience at New York Cyber 9/12 Student Challenge*

### 4. Dynamics of Cyber Conflict

Jason Healey and Robert Jervis, both with the Arnold A. Saltzman Institute of War & Peace Studies, were awarded the Minerva Research Initiative 2017 University Grant. Their three-year research project, which began in June 2017, explores how the strategic dynamics of cyber conflict differ from its tactical and technical dynamics and from the dynamics characteristic of other kinds of conflict. The project will identify these differences, examine whether nations can prevail in cyber conflict, and posit how the dynamics of past cyber conflicts can inform the Department of Defense about those of the future.

### 5. New York Cyber Task Force

This year, the NYCTF will release its final report on achieving a more defensible cyberspace. The group, comprised of 30 cyber experts from New York City and the financial sector, examined ways to enhance the defensibility of companies and cyberspace as a whole. Its recommendations target companies, policymakers, and technology executives, as well as academics and think-tank experts.

## 6. The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers

Graduate students in Jason Healey's Policy Dilemmas in Cybersecurity class conducted research on zero-day vulnerabilities, culminating in group presentations on the private market for vulnerabilities and the Vulnerability Equities Process (VEP). Following the Shadow Brokers' leak regarding NSA capabilities, this research was compiled into a report and published by the *Columbia Journal of International Affairs*. The findings, including estimates on the number of vulnerabilities stockpiled by the government, were widely cited.

## 7. Air Force National Security Scholars Conference

Columbia SIPA hosted the annual National Security Scholars Conference (NSSC) for the U.S. Air Force. During this conference, the Secretary, Chief of Staff, and other Air Force leadership met with several student groups (including veterans and ROTC) and participated in panels on military innovation and agility in the face of changing national security threats.



*Photograph from Air Force National Security Scholars Conference*

## 8. Financial Stability and Cyber Risk

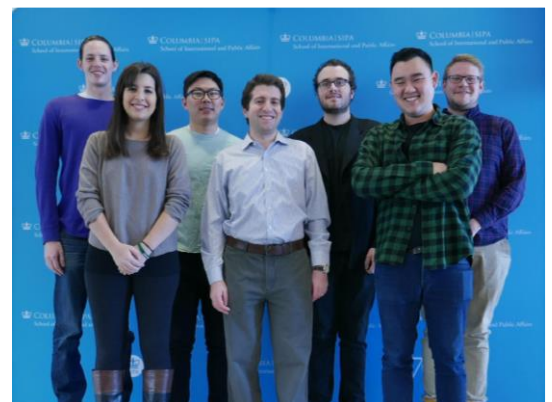
This conference aimed to tie the financial sector's cybersecurity efforts to existing academic work on financial stability and resilience. 30+ attendees (from JP Morgan Chase, the New York Federal Reserve, the Financial Systemic Analysis & Resilience Center, the Carnegie Endowment for International Peace, PwC, McKinsey, Morgan Stanley, the Department of the Treasury, and Goldman Sachs, among others) discussed the effects of cyber risk on instability, public trust, and international cooperation, as well as new solutions from the public and private sectors.

## 9. SIPA Cyber Recommendations Project

SIPA graduate students, under the direction of Jason Healey, scrutinized existing reports from think tanks as well as research and government organizations to identify and catalogue recurring cyber recommendations for the U.S. government and private sector. This ongoing project currently boasts more than 700+ unique recommendations and has culminated in memorandums to the Homeland Security Advisor, the National Institute of Standards and Technology (NIST), the Department of Homeland Security, and the office of the Federal Chief Information Officer.

## 10. Columbia SIPA Digital and Cyber Group (DCG)

This student-run initiative, formed in the fall of 2016, dramatically increased its scope this past year, becoming one of the most active and visible student groups on campus. DCG, as the primary coordinator for student-run cyber activities at SIPA, organized a number of widely attended events and facilitated several student publications on cyber regulation and conflict.



*Executive Board of SIPA Digital Cyber Group*

## Events and Panels

### In-House SIPA Events

1. Panel regarding cyber issues relating to NATO and Russia with NATO Assistant Secretary General Sorin Ducaru, moderated by Jason Healey, on 15 September 2016.
2. Dinner discussion with NATO Assistant Secretary General Sorin Ducaru and Rob Knake from the Council on Foreign Relations on 15 September 2016.
3. Panel on Columbia student VEP research on 19 September 2016.
4. Student discussion with John Hultquist of FireEye on 22 September 2016.
5. \*\*Lunch discussion with Columbia Cyber Community on 23 September 2016 at Columbia Law School.
6. Discussion on cyber risk metrics for more resilient cyber environments on 26 September 2016.
7. DCG and Cyber 9/12 Happy Hour on 29 September 2016.
8. Discussion regarding critical national security cyber issues and the implications of autonomous systems on 12 October 2016.
9. \*\*Discussion on the NSA and cyber challenges on 20 October 2016 at Columbia Law School.
10. Discussion with SEC Cybersecurity Advisor Christopher Hetner on 27 October 2016.
11. Discussion on the IANA stewardship transition and cybersecurity implications on 27 October 2016 at SIPA.
12. Student discussion with Google Jigsaw on 17 November 2016.
13. Panel and discussion on the future of Internet governance on 30 November 2016.
14. SIPA Cyber Alumni Meeting at Columbia Career Conference on 12 January 2017 in Washington D.C.
15. Discussion on systemic financial cyber resilience on 25 January 2017.
16. Panel discussion with Maryam Mujica from Twitter's Public Policy team on 7 February 2017.
17. Presentation from Lance James of Flashpoint on threat intelligence and pen testing for students in Policy Dilemmas of Cybersecurity class on 20 February 2017.
18. \*Panel on Russian-U.S. cyber relations on 2 March 2017.
19. Workshop on Brazil's use of blockchain with Internet policy specialist Ronaldo Lemos on 3 March 2017.
20. \*\*Discussion on cyber risk with Morgan Stanley on 9 March 2017 at Columbia Law School.
21. \*Panel on the infrastructure behind fake news on 20 March 2017.
22. Student discussion with Franz-Stefan Gady, Associate Editor of *The Diplomat*, on 21 March 2017.
23. Panel discussing the laws of armed conflict in the era of cyber and autonomous weaponry on 28 March 2017.
24. Discussion regarding the relationship between cybersecurity and international development on 28 March 2017.
25. K2 Intelligence internship speed interview event on 30 March 2017.
26. Panel discussion on *The Hacked World Order* with Adam Segal from Council on Foreign Relations on 6 April 2017.
27. Columbia University After Action Report (AAR) on Cyber 9/12 on 13 April 2017.
28. Workshop exploring financial stability and cybersecurity on 18 April 2017.
29. Panel discussion with Microsoft, the FCC, Trans\*H4CK, and the Ministry of Taiwan on gender in technology on 18 April 2017.



*Adam Segal (Council on Foreign Relations) spoke to SIPA students and signed copies of his book [The Hacked World Order](#)*

30. \*Panel on blockchain, cybersecurity and encryption on 20 April 2017.
31. New York “Cyber Meet and Greet” with students and professionals on 25 April 2017.
32. \*Panel on artificial intelligence and data collection on 26 April 2017.
33. \*Panel with Jared Cohen from Alphabet on the digital age on 3 May 2017.
34. Discussion on cyber weapons and vulnerabilities on 4 May 2017.
35. Global Digital Futures Forum – “A Fragmenting Internet” on 5 May 2017.

\* Designates events coordinated by SIPA Tech & Policy Initiative  
 \*\* Designates events coordinated by Columbia Law School

## Notable Speakers, Guests, and Panelists at SIPA

1. Olivier Alais (Consultant at Harvard Berkman Klein Center)
2. \*Jonathan Albright (Assistant Professor at Elon University)
3. Merritt Baer (Lead Cybersecurity Advisor for Federal Communications Commission)
4. \*David Carroll (Associate Professor at The New School)
5. Jared Cohen (President of Alphabet, Inc)
6. Greg Conti (Director of Information Security Research at IronNet)
7. Laura DeNardis (Professor and Associate Dean at American University)
8. Scott DePasquale (Chairman at Utilidata)
9. Sorin Ducaru (Assistant Secretary General for Emerging Security Challenges at NATO)
10. \*\*Major-General Dan Efrony (Former Chief Military Advocate General of Israel Defense Forces)
11. Franz-Stefan Gady (Associate Editor of *The Diplomat*)
12. Erik Gartzke (Professor at University of California, San Diego)
13. \*\*Glenn S. Gerstell (General Counsel of NSA)
14. Karl Grindal (PhD Candidate at Georgia Tech)
15. Gordon Goldstein (Managing Director at Silver Lake)
16. Ambassador David Gross (Co-Chair of Wiley Rein LLP Technology Practice)
17. Andrew Hall (Colonel (USA) and Director at Army Cyber Institute at West Point)
18. Richard Harknett (Head of Political Science Department at University of Cincinnati)
19. Royal Hansen (Senior Vice President at American Express)
20. Trey Herr (Postdoctoral Fellow at Harvard Kennedy School)
21. Drew Herrick (PhD Candidate at George Washington University)
22. Christopher Hetner (Senior Cybersecurity Advisor at Securities and Exchange Commission)
23. John Hultquist (Director of Cyber Espionage Analysis at FireEye)
24. \*Toomas Ilves (Former President of Estonia)
25. Yurie Ito (Executive Director at CyberGreen)
26. Lance James (Chief Scientist at Flashpoint)
27. Rob Knake (Senior Fellow at Council on Foreign Relations)
28. Nina Kollars (Assistant Professor of Political Science at Franklin & Marshall College)
29. Nadiya Kostyuk (Doctoral Student at University of Michigan)
30. Ronaldo Lemos (Internet Policy Specialist at ITSRio)



*Lance James, Chief Scientist at Flashpoint, speaks with SIPA cyber students*

31. Andrea Limbago (Chief Social Scientist at Endgame)
32. Ryan Maness (Visiting Fellow in Political Science at Northeastern University)
33. Oriana Mastro (Assistant Professor of Security Studies at Georgetown University)
34. Tim Maurer (Fellow at Carnegie Endowment for International Peace)
35. Rose McDermott (Professor of International Relations at Brown University)
36. Angela McKay (Senior Director, Cybersecurity Policy and Strategy at Microsoft)
37. Maryam Mujica (Head of Public Policy, Latin America at Twitter)
38. Joe Nocera (Op-Ed Columnist for *The New York Times*)
39. \*\*Noah Perlman (Global Head of Financial Crimes at Morgan Stanley)
40. Neal Pollard (Cyber Incident Response Leader at PwC)
41. Greg Rattray (Managing Director at JP Morgan Chase)
42. Katheryn Rosen (Managing Director at BlackRock)
43. Karl Schimmeck (Global Head of Vulnerability Management for Morgan Stanley)
44. Jacquelyn Schneider (Faculty Member at Naval War College Center for Cyber Conflict Studies)
45. Adam Segal (Director of Digital & Cyberspace Policy Program at Council on Foreign Relations)
46. John Soughan (Business Lead at Zurich Insurance)
47. Stephen Sparks (Senior Vice President at Bank of America)
48. Paul Twomey (Former President of ICANN)
49. Phil Venables (Partner at Goldman Sachs)
50. Ian Wallace (Co-Director of Cybersecurity Initiative at New America)
51. Josephine Wolff (Assistant Professor of Public Policy at Rochester Institute of Technology)
52. Elad Yoran (CEO of Security Growth Partners)

\* Designates events coordinated by SIPA Tech & Policy Initiative  
\*\* Designates events coordinated by Columbia Law School

### External Events featuring Jason Healey- Presenter/Speaker/Participant

1. Presentation on technologies and policies for a defensible cyberspace on 30 July 2016 hosted by Black Hat.
2. Presentation on the Federal Government and 0days after the FBI-Apple debate on 5 August 2016 hosted by DEF CON 24.
3. Keynote speaker at conference regarding cyberspace on 15 September 2016, hosted by the Army Cyber Institute.
4. Keynote speaker at conference on cyber threat intelligence on 21 September 2016, hosted by the Institute of World Politics and Booz Allen Hamilton.
5. Panelist on government hacking and policy responses on 19 September 2016, hosted by New America Open Technology Institute.
6. Speaker at board briefing regarding data breaches on 26 September 2016, hosted by New York Federal Reserve.
7. Panelist on UN First Committee panel regarding UN GGE and arms control on 4 October 2016, hosted by ICANN.
8. Moderator for panel discussion at National Security Scholars Conference on 13 October 2016, hosted by U.S. Air Force.
9. Speaker at conference regarding NYCTF material on 21 October 2016, hosted by Cyber Maryland.
10. Speaker at student conference on 24 October 2016, hosted by U.S. Air Force Academy.
11. Panelist on the cyber risk landscape on 9 December 2016, hosted by Atlantic Council.

12. Moderator for panel on cyber criminals and security exploitations on 11 January 2017, hosted by Wapack Labs Inc.
13. Presentation for NYCTF on 12 January 2016, hosted by the Deputy Assistant Secretary of Defense for Cyber Policy's Staff.
14. Discussant in conversation on the new Homeland Security Advisor on 12 January 2017, hosted by National Security Council Transition Team.
15. Participant in discussion on new Homeland Security Advisor on 17 January 2017, hosted by Atlantic Council.
16. Moderator for panel on cyberspace and U.S. foreign policy on 2 February 2017, hosted by National Committee on American Foreign Policy (NCAFP).
17. Moderator for panel on the Tallinn Manual 2.0, international law and cyber operations on 8 February 2017, hosted by Atlantic Council.
18. Moderator for cyber wargame with senior government officials and CrowdStrike on 15 February 2017, hosted by Columbia SIPA.
19. Testified before House Committee on Armed Services on Cyber Warfare in the Twenty-First Century on 1 March 2017.
20. Participant in roundtable with Andy Ozment, Co-Chief Information Security Officer (CISO) at Goldman Sachs on 19 April 2017, hosted by the Council on Foreign Relations.
21. Panelist on financial institutions and systemic cyber risks on 5 May 2017, hosted by Columbia University.
22. Participant in CyCon International Conference on Cyber Conflict from 30 May 2017 – 2 June 2017, hosted by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE).

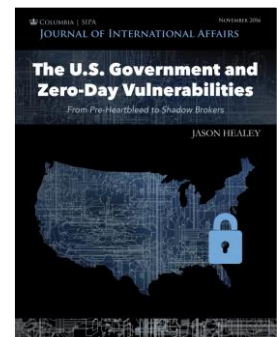
## Publications and Media

### SIPA Student Publications

1. [The Evolving Cybersecurity Regulatory Environment \(Columbia Journal of International Affairs\)](#)
2. [Terrorist Communications & Social Media Liability \(Columbia Journal of International Affairs\)](#)
3. [U.S. Response to a Russian Cyberattack \(Yale Journal of International Affairs\)](#)
4. [How Russian Attackers will Attack the U.S. Next \(DefenseOne & Quartz\)](#)
5. [The Trouble with Thailand's New Cyber Approach \(The Diplomat\)](#)
6. [Post-Action Report: The Cyber 9/12 Student Challenge 2016 \(The Hertie School Governance Page\)](#)
7. [Solving User Authentication via Artificial Intelligence \(Werken.com\)](#)

### Major Publications

1. [The U.S. Government and Zero-Day Vulnerabilities \(Columbia Journal of International Affairs\)](#)
2. [Feds and 0days: From Before Heartbleed to After FBI-Apple \(DEFCON – Presentation\)](#)
3. [Winning and Losing in Cyberspace \(NATO CCDCOE\)](#)
4. [A Nonstate Strategy for Saving Cyberspace \(Columbia Journal of International Affairs\)](#)
5. [What it'll Take to Forge Peace in Cyberspace \(CSM Passcode\)](#)
6. [NSA Hack Reveals Flaws in White House Zero-Day Process \(CSM Passcode\)](#)
7. [DNC Hack Requires Swift, Forceful Response from Washington \(CSM Passcode\)](#)
8. [Chinese Cyberespionage is Down. That's a Win for Obama's Diplomacy \(CSM Passcode\)](#)
9. [Global Implications of the U.S. – China Cyber Relationship \(RSIS CENS\)](#)
10. [Why the FBI will Eventually Reveal its iPhone Hack to Apple \(CSM Passcode\)](#)
11. [Setting Priorities on Cybersecurity \(Democracy: A Journal of Ideas\)](#)
12. [How NSA Reorganization could Squander Remaining Trust \(CSM Passcode\)](#)



13. [What it'll take to Forge Peace in Cyberspace \(Carnegie Endowment\)](#)
14. [The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities \(Journal of Cybersecurity\)](#)

### Select Interviews, Broadcasts and Media Coverage

1. [Government Software Bugs \(WIRED\)](#)
2. [Government Software Bugs \(MIT Technology Review\)](#)
3. [10 Years after Estonia \(Foreign Policy\)](#)
4. [Cyber 9/12 Competition \(Washington Exec\)](#)
5. [Government Protection of Cyberspace \(FCW\)](#)
6. [Testimony Before Congress \(The Hill\)](#)
7. [Testimony Before Congress \(New York Post\)](#)
8. [Lawmakers and Information Warfare \(Fed Scoop\)](#)
9. [Washington and Software Vulnerabilities \(CSM Passcode\)](#)
10. [Vault7 and WikiLeaks \(Washington Post\)](#)
11. [WikiLeaks and the CIA Hacking \(WIRED\)](#)
12. [Malware Attacks by U.S. Government \(The Intercept\)](#)
13. [Snowden Documents and China \(The Intercept\)](#)
14. [WikiLeaks and the CIA Hacking \(Newsweek\)](#)
15. [Trump's Cybersecurity Chief \(WIRED\)](#)
16. [Obama's Cyber Legacy \(Nextgov\)](#)
17. [Draft Trump Executive Order on Cybersecurity \(Foreign Policy\)](#)
18. [Commission on Enhancing National Cybersecurity \(CNN Money\)](#)
19. [Political Hacks and Russia \(WIRED\)](#)
20. [The DNC Hack \(Christian Science Monitor\)](#)
21. [Hacking of Democratic Emails \(PBS NewsHour\)](#)
22. [Obama on U.S. Hacking Vulnerability \(CNN Money\)](#)
23. [Macron Targeted by Hackers \(CNN\)](#)
24. [Meet Fancy Bear \(BuzzFeed News\)](#)
25. [Election Cybersecurity \(New York Times\)](#)
26. [The State of the Internet \(The Guardian\)](#)
27. [Declining Chinese Cyberattacks \(MIT Technology Review\)](#)
28. [Trump's Cybersecurity Executive Order \(Politico\)](#)



*Jason Healey Testimony before House Armed Services Committee: Cyber Warfare in the 21<sup>st</sup> Century: Threats, Challenges, and Opportunities*



## SIPA's Cyber Capstones

SIPA workshops apply SIPA students' practical skills and analytical knowledge to a real-world issue. Small student consulting teams, under faculty supervision, are assigned a substantive, policy-oriented project with an external client. Each team produces an actionable report and an oral briefing. Workshops give students a chance to refine their skills and knowledge, make a positive contribution, and build a network. This academic year, SIPA offered several cyber and cyber-related capstones, resulting in reports often published by the sponsoring organization for their own clients.

1. [Identifying Early Indicators of Radicalization on Social Media](#) (Client: US Department of State; Adjunct Faculty Advisor: Neal Pollard)
2. [Cybersecurity as an Engine for Growth](#) (Client: New America; Adjunct Faculty Advisor: Adam Segal)
3. [Identifying Correlations between Cyber Health and Socioeconomic Conditions](#) (Client: CyberGreen Institute; Adjunct Faculty Advisor: Gregory Rattray)
4. [Labor Market Drivers of Future Cyber Threat Activity](#) (Client: FireEye; Adjunct Faculty Advisor: Katheryn Rosen)
5. [Technological Change and China's Public Security System](#) (Client: U.S.-China Economic and Security Review Commission; Adjunct Faculty Advisor: Alexis Wichowski)
6. [Checkmating Russia's Assertiveness in Eastern Europe](#) (Client: RAND Corporation; Adjunct Faculty Advisor: Colin Jackson)
7. [Cyber Security, Big Data, Infrastructure, Mobile Marketing, Social Media](#) (Client: AXA Strategic Ventures; Adjunct Faculty Advisory: Bruce Taragin)
8. [Technology and the 21<sup>st</sup> Century State](#) (Client: Eurasia Group; Adjunct Faculty Advisor: Markus Jaeger)

