Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

Cyber Statecraft Initiative

2013 Year in Review: Saving Cyberspace

During 2013, the Atlantic Council's Cyber Statecraft Initiative cemented its position as the most forward-leaning think tank on cyber policy issues in Washington, DC and perhaps the world. The goal of the program is "saving cyberspace" as this most transformative technology since Gutenberg is under threat, putting at risk the national security of the United States and the economic security of the world.

Our program also became very well known for taking a strong position against overly aggressive spying by the National Security Agency and related cyber covert attacks, like Stuxnet. On this and other important issues, we held **more than sixty events**, from private dinners with senior international policymakers to large conferences like the Cyber 9/12 project with hundreds of people attending in person or online. The highlight of the Initiative's publications was the release of *A Fierce Domain, Conflict in Cyberspace, 1986 to 2012*, which as the first military history of cyberspace received widespread praise, including in the *Economist* magazine.

Led by an ideas-driven approach on these issues, this year experts had **twenty broadcast interviews** and the Cyber Statecraft Initiative has been mentioned in major national news outlets including National Public Radio, the *Washington Post*, the *New York Times*, the *Wall Street Journal*, *Foreign Policy*, Bloomberg News, *Newsweek*, CNN, the *Atlantic*, the *Financial Times*, the *Economist*, *Deutsche Welle*, and more. Director Jason Healey is a regular op-ed contributor to *US News & World Report's* "World Report" section and *Foreign Policy*'s online "National Security" blog.

In 2014, the Cyber Statecraft Initiative hopes to build on this success in several ways. First, it will continue the Cyber 9/12 series and work on Global Aggregations of Cyber Risk (aka "cyber sub-prime"). Second, the team will expand to meet the global moment, with a goal of "saving cyberspace," as the Internet is under unprecedented challenges, under threat of being torn apart by conflicting requirements, increasing complexity, and ineffectual governance.

Brian Tishuk, Executive Director of ChicagoFIRST, **Jason Healey**, Director of the Cyber Statecraft Initiative, and **Paul Twomey**, Atlantic Council Board Director and founder of Argo P@cific at the Cyber 9/12 conference at the NEWSEUM's Knight Studio.

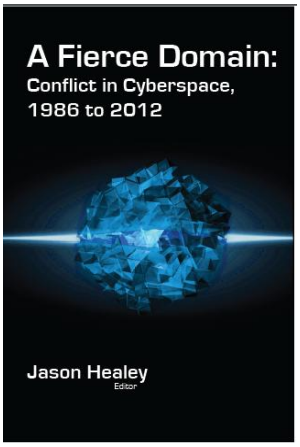
MAJOR PROJECTS for SAVING CYBERSPACE

1. Global Aggregations of Cyber Risk

The Atlantic Council, in partnership with Zurich Insurance, is managing a year-long effort to understand how concentrations of correlated risks, interconnectedness, and complexity contribute to systemic threats to the entire system and ways to mitigate these risks, such as insurance and resilience. Currently, cybersecurity professionals are looking at cyber vulnerabilities one organization or one nation at a time, without looking at the systemic risk to the overall system. This approach is similar to how the financial sector handled risks prior to the 2008 financial when financial risks were assessed one organization at a time, not recognizing how a shock to one sector—US sub-prime mortgages—might cascade to take down everyone else.

2. Cyber 9/12 Project

"Cyber 9/11" or "Digital Pearl Harbor" are common phrases with little exploration of what they actually mean or what we might do afterwards. The headline Cyber 9/12 Project, funded by Leidos, is part conference and part exercise, which presses leaders in government and private industry to explore day-after responses to a major cyber attack. A parallel event, the Cyber 9/12 Student Challenge, is a competition devoted to challenge university students to create and present high-level policy recommendations for day-after responses to a major cyber campaign. The panel of judges was drawn from the upper echelons of the White House, US Department of Defense, US Department of State, and leading cyber security firms.



3. The History of Cyber Conflict

This project focuses on capturing lasting policy lessons from the history of cyber conflict which remain largely ignored despite its occurrence for more than two decades, forcing stakeholders to re-learn old lessons and repeat mistakes. The focus of project is to demystify cyber conflict and explore how cyberspace relates to more traditional warfigting domains, both on a national and international level. This project has resulted in the first-ever cyber conflict history book*, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, which explores the twenty-six-year history of cyber conflict and analyzes case studies of the most significant cyber incidents.

4. Smart Governance for Cybersecurity and Resilience

The project explores the intersection of strong cybersecurity and maintaining an open, interoperable, secure, and reliable Internet through a series of discussions and workshops. The path to comprehensive cybersecurity requires responsible Internet governance and a balance of liberty and security in the future development of the Internet. Through events and representation at key global governance discussions, the Cyber Statecraft Initiative has been an important player in the debate.

MAJOR EVENTS

1) Private Dinner "Building a Secure Cyber Future" on February 1, 2013. Held at the Munich Security Conference.
2) Panel on "The Role of Congress in Cyber Conflict" on February 13, 2013. Public event, held at Atlantic Council. Other speakers included Derek Khanna, Cyber Security Policy Advisor, DoD, moderated by Jason Healey. The panel discussion focused on the role of Congress in cyber conflict with a particular focus on the War Powers Resolution.

Jason Healey and **Michael Hayden** addressing students at the Cyber 9/12 Student Challenge.

3) Roundtable "US Air Force and Cyberspace Operations" on February 15, 2013. The Cyber Statecraft Initiative hosted a roundtable discussion with Lt. Gen. Michael Basla, the Air Force's A6, Chief of Information Dominance and Chief Information Officer.
4) Roundtable "State of Internet and Cybersecurity Governance" on March 12, 2013. Cyber Statecraft Initiative hosted a roundtable strategy session to encourage collaboration among key stakeholders from like-minded nations, US government officials and the private sector.
5) **Book release of the *Tallinn Manual*** on March 28, 2013. Cyber Statecraft Initiative, in cooperation with the ABA Standing Committee on Law and National Security, hosted the US release of the first-ever deep analysis of how the standards of international law apply to cyber warfare. The book was funded by the NATO center in Estonia and overseen by a group of influential international lawyers. The event took place at The University Club Ballroom, and was broadcast on C-SPAN.

6) Workshop "Building on the Results of the Budapest International Cyberspace Conference" on April 9, 2013. The discussion continued the series on international Internet governance issues.
7) Conference on **International Engagement on Cyber** with Georgetown University on April 10, 2013. Held at Gaston Hall, Georgetown University Institute for Law, Science, and Global Security. Keynote speakers included Terry D. Kramer Ambassador, Head of the US Delegation for the World Conference on International Telecommunications; Eugene Kaspersky, CEO and Co-founder, Kaspersky Lab; and Teresa M. Takai, Chief Information Officer, United States Department of Defense. Representatives of the United States, Russia, Estonia, Hungary, Canada, Germany, Israel, the UK, and NATO also attended. This gathering promoted dialogue among policymakers, academics, and key industry stakeholders from across the globe, and explored the worldwide community's increasing interconnectivity in this domain.
8) Major conference "**The Cyber 9/12 Project: Cyber Statecraft After Catastrophes**" on April 12, 2013. Held at the Knight Studio, Newseum and broadcast live in high-definition. Conference featured eight experts from the technical, cyber security, and government communities discussing how to respond during and after a significant cyber conflict against the United States.
9) Conference "Zurich Classic PGA New Orleans, USA" on April 26 - 27, 2013. Panel discussion at the Zurich Classic PGA New Orleans, USA event along with an internal workshop to discuss aggregations of cyber risk.
10) Roundtable "History of Cyber Critical Infrastructure Protection: 15th Anniversary of PDD-63" on May 22, 2013. Hosted Acting Deputy Secretary of Homeland Security Suzanne Spaulding.

11) Forum with Mr. Robert Kaliňák, Deputy Prime Minister and Minister of Interior of Slovakia and Peter Kmec, Ambassador of Slovakia to the United States on May 30, 2013.
12) **Launch of *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012***. This book, edited by Jason Healey, is the first-ever military history of cyberspace.
    a. Initial launch at NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, June 6, 2013.
    b. Follow-up launch events at Chatham House in London and at NATO Headquarters, June 14, 2013.
13) Competition **Cyber 9/12 Student Challenge** on June 15, 2013. Cyber Statecraft Initiative held the first-ever student competition devoted to national security policy recommendations for day-after responses to a major cyber attack. Other competitions for students focus only on technical hack-counterhack, ignoring the policy aspects including how the nation as a whole should respond, whether the cyber attack was an "act of war," and how the attack fit into the UN Charter and NATO's Article 5. The Cyber 9/12 Student Challenge featured teams from 19 different universities including Harvard, MIT, Columbia, and Georgetown.

NPR correspondent **Tom Gjelten** moderating a panel on "Cyber Conflict and War: Yesterday, Today, and Tomorrow" with **Jason Healey**, **Richard Bejtlich**, and **Gregory Rattray**.

14) Discussion "Taking Cyber to the Hill: Future of Internet Governance" at the Capitol visitor's center on June 17, 2013. The event hosted members and staffers to discuss internet governance issues and featured Congressman James Langevin (D, RI).
15) Roundtable on "Threat of Chinese Cyber Espionage" on June 24, 2013. This discussion took place at The Army and Navy Club Ballroom and featured cyber experts with ties to the Cyber Statecraft Initiative like Dmitri Alperovitch and James Mulvenon.
16) Roundtable on "Electronic Warfare and Cyber: Increasing Interdependence?" on July 15, 2013. The event discussed the convergence between EW and cyber operations and explored its ramifications for 21st Century militaries with a roundtable discussion on cyberspace and electronic warfare.
17) **US Book Launch for *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*** on July 17, 2013. Launched at George Washington University with many dozens in attendance, followed by cocktails and a book signing.
18) Roundtable "NATO Cyber Policy" on July 24, 2013.
19) Roundtable "Iran: How a Third Tier Cyber Power Can Still Threaten the United States" on July 29, 2013. Held at the Atlantic Council and hosted by Cyber Statecraft Initiative and Iran Task Force to launch the issue brief of the same name.
20) Presented at **Black Hat**, the largest and most prestigious computer security conference in the world, presenting on "Above My Pay Grade: Incident Response at the National Level" on July 30, 2013.
21) Book signing and events at DEFCON conference on August 1, 2013.
22) Roundtable "Industrial Control Systems and Cybersecurity" on August 8, 2013. Jason Healey and Jason Thelen attended a roundtable with Ralph Langer to discuss Stuxnet.
23) Book event at Nordic Security Conference in Reykjavik, Iceland on August 30, 2013. Jason Healey presented on "Eight Cyber Conflicts Which Changed Cyberspace."
24) Event on "Cyber Rivalry in South Asia" on September 5, 2013. Held jointly with the South Asia Center discussing confidence building measures and the cyber rivalry in South Asia with Dr. Tughral Amin.

25) Roundtable "Crafting a National Cyber Agency" on September 6, 2013. Hosted a workshop with former US policymakers to discuss if a new agency should be created to lead US cyber efforts.
26) Speaking Engagement "Cyber War Will Not Take Place, Or Will It?"on September 9, 2013. Jason Healey spoke at Brookings on the likelihood of cyber war.
27) Major involvement with Zurich Insurance's "**Global Risk Management Summit**" on September 20, 2013 in Rome. The Cyber Statecraft Initiative team had six cyber experts for two meetings with Zurich clients and a panel discussion with all of Zurich's 80 or so biggest global corporate clients. To discuss Global Aggregation of Cyber Risk, the team included Paul Twomey, Jason Healey, and Jason Thelen along with senior Fellow Neal Pollard and the two new Zurich Cyber Risk Fellows, Jeff Schmidt and Tom Bossert.
28) Roundtable "Seoul Conference on Cyberspace in post-PRISM World" on September 30, 2013. The event discussed implications of PRISM revelations on Internet governance.
29) Organized a side breakfast on the "Global Aggregation of Cyber Risk" at the **Seoul Conference on Cyberspace** from October 17-18, 2013. The Cyber Statecraft Initiative organized one of only four side events allowed at this ministerial-level conference. Jason Healey and Jason Thelen organized the event which attracted ~30 attendees, including delegates (and potential funders) including Jane Holl Lute, Former Deputy Secretary of Homeland Security; Matt Tomlinson of Microsoft; Laszlo Deak, Hungary's Cyber Coordinator; Suleyman Anil of NATO and many others. We also got our history book into the hands of Amb. Dirk Brengelmann (Germany), Amb. Gordon Smith (Canada), Rune Resaland (Norway), the lead Russian cyber negotiator, and others.
30) Speaking Engagement at **Internet Governance Forum** in Indonesia on "Eight Cyber Conflicts which Changed History" from October 21-22, 2013. The IGF is the most-important annual event for Internet governance and this was a topic rarely covered there in any detail. Panel event including Bill Woodcock (US), Tim Maurer (Germany) and Yurie Ito (Japan).
31) Side dinner on "Global Aggregation of Cyber Risk" at Internet Governance Forum on October 22, 2013. Dinner discussion with global cyber leaders from the OECD, Japan, Caribbean, Hong Kong, Germany, Canada and the United States to discuss the risks from interdependence of cyber systems.

Neal Pollard and **Jason Healey** discussing global aggregation of cyber risk at the Global Risk Management Summit in Rome.

32) **Event series of "Cyber Risk Wednesday"** kickoff on October 23, 2013. Launch event of the Cyber Risk Wednesday series that bring cyber experts from government and industry together with policymakers to examine topics at the core of the Cyber Statecraft Initiative's study of interrelated cyber hazards and underlying concentrations of risks. The series is designed to expose stakeholders from the technology, policy, and risk management communities to vibrant new cyber topics and provide a venue for the exchange of ideas. The first event introduced the project and the moderated panel discussed systemic cyber risks and their implications on the future of the Internet.
33) Event "Tackling India's Cyber Threat" on November 1, 2013. Public event, held at the Atlantic Council, hosted Amb. Latha Reddy, former deputy National Security Advisor of India and was moderated by Jason Healey.
34) Briefed Zurich Latin America's 2nd annual **LATAM Risk Advisory Council** on November 11, 2013 in Sao Paulo, Brazil. Jason Thelen briefed the CEO of Zurich Brazil and CEO of Zurich Global Corporate Latin America on conventional and emerging threats and on the global aggregation of cyber risk project.

35) Panel “Cyber Conflict and War: Yesterday, Today, and Tomorrow” on November 15, 2013. Held at the Atlantic Council. Panel discussion addressed the past, present, and future of cyber conflict and featured Richard Bejtlich, the chief security officer of Mandiant, Dr. Greg Rattray, senior fellow at the Cyber Statecraft Initiative and CEO of Delta Risk and Jason Healey, and was moderated by Tom Gjelten of National Public Radio.
36) Panel "Cyber Risk Wednesday" was held on November 20, 2013 at the Atlantic Council. The second event in the series featured Catherine Mulligan**,** senior vice president of the Management Solutions Group and Specialty Products at Zurich, Matt McCabe, senior vice president of Marsh’s Network Security and Privacy Practice, and Tom Bossert Zurich Cyber Risk Fellow and was moderated by Greg Rattray, senior fellow at the Cyber Statecraft Initiative. The panel discussed cyber risk management and risk transfer and the role of insurance as a cyber risk mitigating measure.
37) Moderated panel at the **Black Sea Energy and Environment Forum** on "Systemic Risk: Finding Cyber Sub-Prime" on November 21, 2013 with Ambassadors Matt Bryza and Zalmay Khalilizad attending.

Congressman Jim Langevin with **Gregory Rattray** and **Jason Healey** discussing future of internet governance at "Taking Cyber to the Hill" event, which was a part of a series examines the success (and failures) of the multi-stakeholder model of Internet governance.

PUBLICATIONS AND MEDIA

Book

1. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*.

Issue Briefs

1. "*Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain*", January 2013 - By Jason Healey and A.J. Wilson, a Visiting Fellow with the Atlantic Council's International Security program.
2. "*How a Third Tier Cyber Power Can Still Threaten the United States*", July 29, 2013 - By Jason Healey and Barbara Slavin.

Jason Healey speaking with **Guy Johnson** on Bloomberg Television's "The Pulse" on challenges in global cyber security

Opinion Pieces

1. "Presidential Cyber Direction Looks Quite Familiar" on February 12, 2013, Jason Healey, *New Atlanticist*.
2. "How the US Should Respond to Chinese Cyber Espionage" on February 19, 2013, Jason Healey, *US News & World Report*. An article that evaluates the decade long problem of unchecked Chinese espionage and presents recommendations for the US government to press China behind closed doors and, now that the information is public, to respond publicly. The article argues that this is best opportunity in years to take direct action against Chinese cyberespionage and help to create new norms of behavior between nations.
3. "Fighting Chinese Cyber Espionage: Obama's Next Move" on February 21, 2013, Jason Healey, *US News & World Report*.
4. "Obama's Cyberwar Strategy Will Backfire" on March 08, 2013, Jason Healey, *US News & World Report* discussing how the Obama Administration's strategy of covert warfare, preemptive attacks, and clandestine intelligence will not serve US interests well in the long-term.
5. "Cyberwar Isn't a US Existential Threat" on March 20, 2013, Jason Healey, *US News & World Report*.
6. "Reason Finally Gets a Voice: The Tallinn Manual on Cyber War and International Law" on March 27, 2013, Jason Healey, *New Atlanticist*.

7. "North Korea's Cyber Stunts Aren't War, So Act Accordingly" on April 9 2013, Jason Healey, *US News & World Report*.
8. "Stuxnet and the Dawn of Algorithmic Warfare" on April 16, 2013, Jason Healey, *Huffington Post*.
9. "On China Cyber Espionage, US Should Shout but Also Listen" on April 18, 2013, Jason Healey, *Foreign Policy*.
10. "Don't Worry About Cyber Retaliation After a Syria Strike" on September 7, 2013, Jason Healey, *US News & World Report*.
11. "Time to Split the Cyber 'Deep State' of NSA and Cyber Command" on October 2, 2013, Jason Healey, *US News & World Report*.
12. "How Emperor Alexander Militarized American Cyberspace" on November 7, 2013, Jason Healey wrote for *Foreign Policy* on the militarization of American cyberspace.

Jason Healey during an interview by **Vago Muradian** on "This Week on Defense News"

13. "Our Bumbling, Fumbling Government Cybersecurity" on October 26, 2013, Jason Healey wrote for *U.S. News & World Report* on the state of US cybersecurity in the wake of leaks by Chelsea Manning and Edward Snowden.

Select Other Media Mentions

1. Review of *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* in *the Economist* article "*Digital Doomsters*" on June, 29, 2013.
2. Radio Broadcast "The Role of Cyber Warfare Tactics in Syria" on September 5, 2013, Jason Healey and Mike Huckabee discuss the role of cyber warfare tactics in Syria, and whether the United States should consider using cyber attacks against the Assad regime.
3. Quoted on September 13, 2013, Jason Healey, Cyber Statecraft Initiative director, is quoted in the *Economist* on the NSA scandal and its implications for American cyber power.
4. Article quoted Jason Healey in the *Financial Times* on proposals to "Balkanize" internet infrastructure on November 1, 2013.
5. Article quoted Jason Healey in *Newsweek* on the NSA spying scandal and its implications for America's own complaints about Chinese cyber espionage on November 1, 2013.
6. Article quoted Jason Healey in *Bloomberg News* on the need to reevaluate US surveillance programs on November 6, 2013.
7. Article quoted "Cyber Risk Wednesdays" series and Jason Healey in *Capital News Service* on November 11, 2013.

Select Interviews and Broadcasts

1. Broadcast on "Cyber Conflict" in *Federal News Radio* on February 6, 2013, Jason Healey and Francis Rose on the latest cyber intrusions into the *New York Times* and other companies.
2. Broadcast on "Pentagon's Offensive Cyber Operations" on February 11, 2013, Jason Healey on the *NPR's Morning Edition*.
3. Broadcast on "Offensive Cyber Warfare" on February 18, 2013, Jason Healey with Beat Solterman of *SRF*, the public radio network of Switzerland (in German).

4. Radio Broadcast "Preparing for Cyber Catastrophes" on April 17, 2013, Jason Healey and *Federal News Radio*'s "In Depth" host Francis Rose discussed the Council's Cyber 9/12 Project and how to prepare various sectors for cyber catastrophes.
5. Radio Broadcast on the "Private Sector and Cyber Attacks" on July 9, 2013, Jason Healey on *American Public Media*'s "Marketplace."
6. Radio Broadcast "Emerging Defense Challenges" on July 15, 2013, Jason Healey and Steve Grundman, Lund Fellow, join *Federal News Radio*'s "In Depth" program to discuss the future of US-China cyber relations and the US Department of Defense acquisition budget.
7. Interviewed by Vago Muradian on "This Week on Defense News" to discuss cyber conflict history book, August 17, 2013.

SELECT BRIEFINGS AND PRIVATE MEETINGS

1. Private Lunch with NATO Assistant Secretary General for Emerging Security Challenges, Ambassador Gabor Iklody, March 21, 2013, held at The Madison Hotel, Washington DC.
2. Private Meeting with Canadian Deputy National Security Adviser, Allan McKinnon, March 22, 2013 held at Atlantic Council.
3. Private Meeting with Victoria Woodbine and Jamie Saunders of the British Embassy, March 27, 2013 held at Atlantic Council.
4. Discussion with the German Interior Minister, Hans-Peter Friedrich, May 3, 2013 at the New America Foundation.
5. Discussion with General Keith Alexander and Atlantic Council's International Advisory Board, May 3, 2013.
6. Briefed twelve Canadian Members of Parliament's Standing Committee on National Defense on the Atlantic Council Cyber Statecraft Initiative and emerging issues in cyber defense, May 7, 2013 at the Canadian Embassy, DC.
7. Briefed Shen Yi from the Department of International Politics at Fudan University in China, May 13, 2013 on cyber issues.
8. Private Meeting with Members of Switzerland's Congress, May 14, 2013 held at Atlantic Council.
9. Briefed Colonel (Ret.) Rami Efrati, Head of the Civilian Division at the Israeli National Cyber Bureau, June 1, 2013 on emerging issues in cybersecurity.
10. Briefed Senior Fellow and Swedish colleagues on "Disruptive Technologies", June 27, 2013 in Stockholm.
11. Briefed Chief of Staff of the Air Force, General Welsh, three former Secretaries of the Air Force, plus the entire AF cyber leadership, July 17, 2013.
12. Discussed "Cyber Conflict and the Law" with Ms. Nikola Schmidt, a cybersecurity expert from the Czech Ministry of Defense, August 15, 2013.
13. Discussed "Cyber History" with a high-level finance sector computer security group at Goldman Sachs, September 5, 2013.
14. Speaking engagement "Cyber Conflict History" on September 6, 2013, Jason Thelen and Karl Grindal spoke at a luncheon at the New America Foundation.
15. Speaking engagement "Cyber War Will Not Take Place, Or Will It?" on September 9, 2013 - Jason Healey was a panelist at Brookings Institution on the likelihood of cyber war.
16. Briefed Minister-Counselor, Stephen Gee and Counselor Michael Kachel of the Australia Embassy September 13, 2013.

Tim Maurer and **Jason Thelen**, Associate Director of the Cyber Statecraft Initiative, at an event on Internet governance.

17. Briefed Takashi Kume, senior METI Japan, September 13, 2013.
18. Briefed Hyunjin Bae, Second Secretary to the Ambassador and Director Kap-soo Rim, who managed the "Seoul Conference on Cyberspace", September 13, 2013.
19. Speaking engagement "Global Aggregation of Cyber Risk: Finding Cyber Sub-Prime" on September 24, 2013, Jason Thelen delivered the morning keynote to an EU conference on Cyber Crisis Cooperation in Athens, Greece.
20. Briefed Justin Bassi, Senior Adviser for Cyber Security and International Cyber Policy and Homeland Security Division at the Department of the Prime Minster of Australia, September 30, 2103.
21. Briefed Mr. Simon Put, Defense Policy Advisor for New Flemish Alliance at the Belgian Federal Parliament, October 3, 2013.
22. Speaking Engagement at Cyber Security Policy and Research Institute at George Washington University on October 3, 2013, Jason Healey delivered a guest lecture. The Cyber Corps Program is a National Science Foundation, Department of Defense, and Department of Homeland Security cybersecurity education and workforce initiative.
23. Briefed US Representative Jim Langevin (D-RI) about "Global Aggregations of Cyber Risk" on October 10, 2013.
24. Conference "Advisen Risk Conference" on October 24, 2013, Jason Thelen and Zurich Cyber Risk Fellow, Tom Bossert were guests of Zurich Insurance at an event focusing mainly on cyber insurance and cyber threats landscape.
25. Briefed Jamie Saunders, the lead cyber envoy of the United Kingdom, via video link at the UK Embassy on November 5, 2013. Rhys Bowen, the Deputy Director for Cyber in the Cabinet Office was in attendance as well. The discussion covered national and parallel systemic cyber risk projects, and future collaboration on topics of interest.
26. Briefed Dr. Philip Kim, CEO of AhnLabs, the largest South Korea cyber security company, on November 5, 2013, on the work the Cyber Statecraft Initiative is doing on global aggregation of cyber risk.

Dmitri Alperovitch and **Gregory Rattray** discuss options for NATO's cyber policy and future capabilities.

27. Speaking engagement at a cyber warfare session at the National Committee on American Foreign Policy in New York on November 6. Jason Healey moderated a panel discussion featuring Winston Lord, Carter Booth and Mike Uretsky.
28. Private call with Atlantic Council Members on "Stabilizing Transatlantic Relations after the NSA Revelations" on November 8, 2013. Jason Healey participated in the members' conference call with Gen Hayden and Ambassador Ischinger.
29. Speaking engagement at the Atlantic Council's event "NATO's Deterrence and Collective Defense" on November 12, 2013. Jason Healey spoke at a panel together with Barry Pavel, Svein Efjestad, and Stefano Stefanini on new challenges and new tools in the area of deterrence.
30. Speaking engagement at Defense One Summit on November 14, 2013. Jason Healey spoke at a panel "What are the limits and boundaries of cyber" with Peter Singer of the Brookings Institution.
31. Discussed cyber issues with the director of the DHS Office of Cybersecurity and Communications on November 21, 2013 to promote recently published NIST standards and Cybersecurity Framework. This

informal discussion supports ongoing collaboration with DHS on cyber insurance issues and potential future efforts on Cyber Situational Awareness.

Joseph Nye , former dean of the Harvard Kennedy School, and **Vicky Woodbine** of the UK Embassy to the US, provide comments at the Cyber 9/12 event on responding after cyber catastrophes.