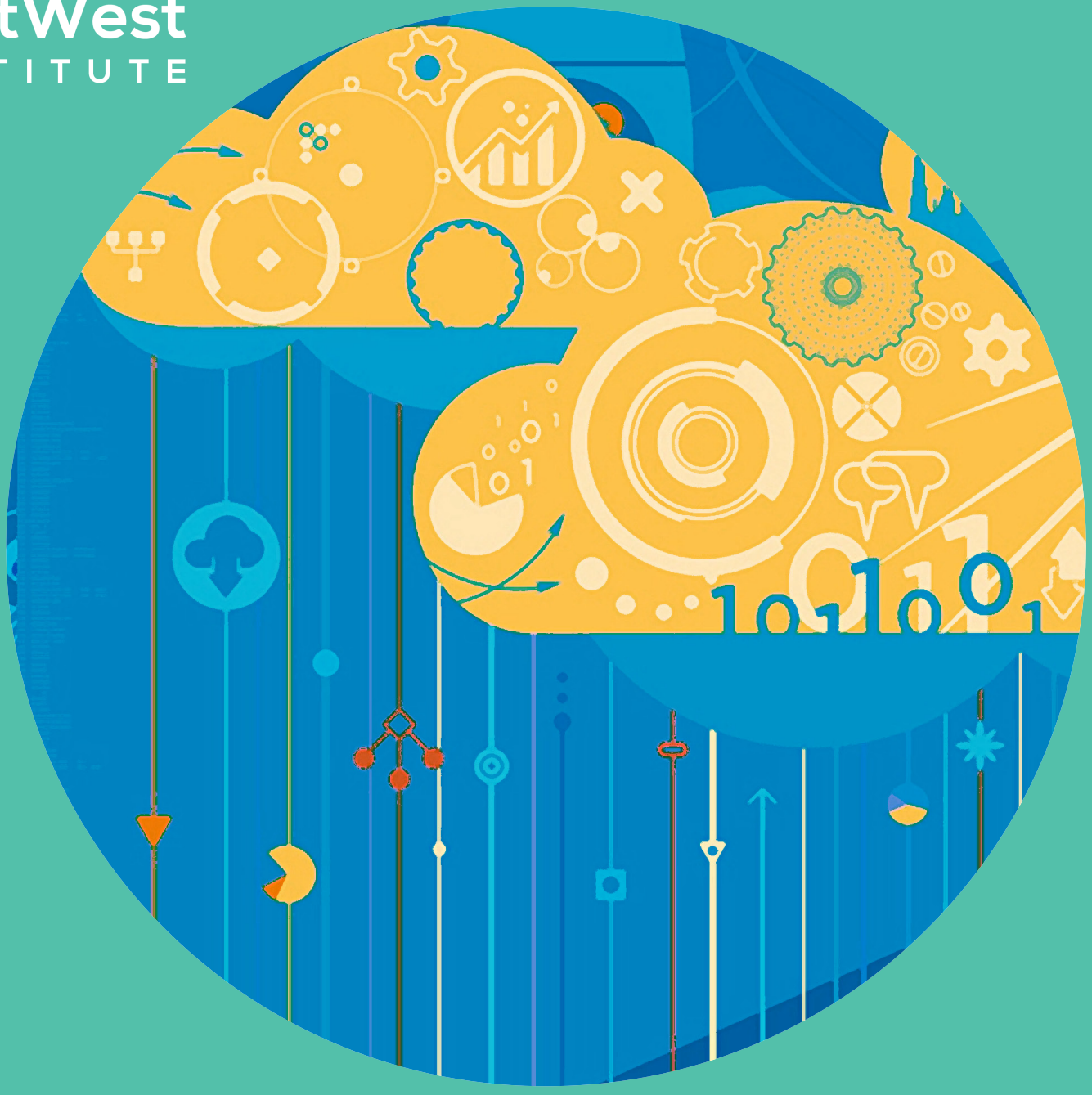
EastWest INSTITUTE



Achieving Breakthroughs

Global Cooperation in Cyberspace Initiative

San Francisco, July 2014

PROGRESS REPORT

ISSUE 1/2014

Building Trust
Delivering Solutions

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a **global go-to place for building trust, influencing policies and delivering solutions.**

–

Learn more at **www.ewi.info**

EastWest
INSTITUTE

EWInstitute
EastWestInstitute

Pathways to Improve Global Cooperation in Cyberspace

What change would make the Internet a safer and better place to work, play and live?

On the evening of June 16, 50 seasoned experts and senior policy makers from 13 countries gathered to participate in the EastWest Institute's (EWI) cyber roundtable, held in San Francisco. The opening event at the top of the historic St. Francis Hotel on Union Square, where the final conference and signing of the United Nations Charter were held nearly 70 years ago, marked an important page in EWI's history—the official launch of the Global Cooperation in Cyberspace Initiative. This three-year program aims to ensure that the economic, political, social and cultural benefits of cyberspace flow to everyone on the planet, by mitigating the negative consequences of global Internet fragmentation.

The evening began with brief remarks from Robert N. Campbell, former Vice Chairman of Deloitte, and the only board member who has participated in all four EWI cyber summits—Dallas (2010), London (2011), New Delhi (2012) and Silicon Valley (2013). EWI's Senior Vice President Bruce W. McConnell then compared the cyber initiative to a movie "produced and directed by the EastWest Institute, co-produced by EWI's sponsors, including Microsoft and Huawei Technologies," and starring the roundtable participants as the movie's actors. He stressed the importance of work done at the roundtable as it "will begin marking out pathways to greater global cooperation on behalf of the 3 billion people who are currently on the Internet, and, the next 2-plus billion who will be coming on in the next 5 to 10 years."

Strong representation from the Russian Federation, led by Ilya Rogachev, director of New Challenges and Threats at the Ministry of Foreign Affairs of the Russian Federation, confirmed once again the significance of EWI's Track 2 work that continues to build bridges between Russia and the U.S., particularly now, when official channels have been narrowed. In addition, diverse perspectives and expertise came from: the UN's International Telecommunication Union; Chinese, Japanese and Russian think tanks; Massachusetts Institute of Technology, Brown University and the National Defense University; and key non-governmental organizations, such as Mozilla and the Open Group. Additionally, Silicon Valley representatives included NXP Semiconductors, Google and The William and Flora Hewlett Foundation. Lastly, a representative from *Wired* magazine attended, agreeing to observe the meeting's Chatham House Rule.

This three-year program aims to ensure that the economic, political, social and cultural benefits of cyberspace flow to everyone on the planet, by mitigating the negative consequences of global Internet fragmentation.

Above: Working roundtable participants.

The rhythm of the next day moved between plenaries and breakthrough groups. John Hurley, EastWest board member and managing partner of Cavalry Asset Management, welcomed the participants to San Francisco. After the participants introduced themselves and answered the question, "What change would make the Internet a safer and better place to work, play and live?" the attendees heard from: Denis Chaibi, deputy head of the Political Section of the Delegation of the European Union to the United States; Karsten Geier, head of division Arms Control and Disarmament, Federal Foreign Office of Germany; Bobbie Stempfley, deputy assistant secretary for Cyber at the U.S. Department of Homeland Security who leads its cybersecurity work with critical infrastructure; Professor Zhang Xinhua, director at the Shanghai Academy of Social Sciences; and Paul Nicholas from Microsoft and Andy Purdy from Huawei Technologies USA.

After the morning plenary, the participants broke into breakthrough groups to discuss concrete steps on how to tackle problems represented by EWI's eight work streams. During this first session the experts discussed:

- **"Enhancing Global Access to Secure Products and Services,"** fighting against so-called "localization" carried out in the name of security, but which can actually reduce security.
- **"Managing Barriers to Information Flows for Innovation and Education,"** advocating the availability of Internet content to young people and businesses around the world, while respecting the legitimate need to manage content for domestic stability.
- **"Exploring Surveillance, Privacy and Big Data,"** seeking transparency and accountability in the collection and use of information about individuals by governments and companies.
- **"Modernizing International Procedures against Cyber-Enabled Crimes,"** working to update 19th century cooperation procedures to fight 21st century crime.

Experts reconvened for the working lunch on governing and managing the Internet. Ambassador Dirk Brengelmann has called 2014 the "year of Internet governance," and that certainly seems to be accurate. From the innovative "NetMundial" meeting in Sao Paolo, to the upcoming Group of Governmental Experts in New York, to the ITU Plenipotentiary in Busan in October, the topics of roles, responsibilities and structures and process-

es to govern and manage the Internet are on the front burner. One of the most impressive efforts on this front is the Global Commission on Internet Governance, chaired by Carl Bildt, Sweden's Minister of Foreign Affairs. The group was announced in January, and just conducted its first in-person meeting.

EWI Distinguished Fellow and former Deputy National Security Adviser of India Latha Reddy, who is also a member of the Bildt Commission, participated in that first meeting and provided brief remarks on Internet governance. She emphasized that without sound governance the problems discussed during the breakthrough groups will only continue to get more and more intractable. After Reddy's remarks, Michele Markoff, the deputy coordinator for Cyber Issues at the U.S. State Department, pointed out the drawbacks of a top-down approach to governing the Internet. Markoff's remarks were followed by Karsten Geier, head of division Arms Control and Disarmament: Communication and New Challenges at the German Federal Foreign Office, who provided the German perspective on this issue, and by Microsoft's Angela McKay, who emphasized the importance of including the private sector in a multi-stakeholder approach of governing cyberspace.

The afternoon breakthrough sessions focused on four additional topics:

- **"Strengthening Critical Infrastructure Resilience and Preparedness,"** making critical infrastructure more prepared and resilient when its defenses fail to defeat successful cyber attacks.
- **"Increasing ICT Product and Service Security,"** working to get stronger products built and to solve supply chain issues.
- **"Promoting Measures of Restraint in Cyber Armaments,"** tackling the problem of the growing arsenals of cyber weapons and what can be done to take targets off the table.
- **"Governing and Managing the Internet,"** a discussion focused on the advantages and disadvantages of existing models and institutions.

Apparent throughout the sessions, was a will to compromise and move toward significantly innovative solutions, despite strongly held views on the impacts of the next 2 billion Internet users, the dangers of "hegemonic" U.S. policies, and the future of sovereignty of states, companies and individuals.

All breakthrough groups achieved rough consensus on clear problem statements, and many developed draft recommendations. Such successful work will continue through two online meetings per group, scheduled to take place between now and early December. EWI, along with the German Foreign Office, will co-host the fifth annual Global Cyberspace Cooperation Summit in Berlin on December 3-5. At this forthcoming summit, cyber experts will meet, build on their progress and start mobilizing support in government and industry for change.

German Foreign Office Representative Karsten Geier announced Germany's decision to make the EWI summit an official part of its G7 Presidency, adding important visibility and gravitas to the proceedings. The summit will bring together more than 300 experts from government, including minister-level participants, the private sector, academia and civil society. The Berlin meeting will include a youth panel; participants from the Middle East, Africa, and Latin America and the hacker community.

H. Avni Aksoy from the Turkish Ministry of Foreign Affairs helped conclude the roundtable by observing, "During the Cold War, people were talking not with each other but at each other; here people talk with each other." Summary remarks by stalwart EWI cyber supporter and President's Advisory Group member Harry Raduege and former White House Cyber Director Sameer Bhalotra set a strong tone for the meeting where "minutes were kept and hours not lost."

We are excited about this highly successful first step in EWI's new cyber cooperation initiative and look forward to strong progress and growth in the months ahead. We welcome your feedback and participation. On to Berlin!

Bruce W. McConnell
Senior Vice President
EastWest Institute

EWI, along with the German Foreign Office, will co-host the fifth annual Global Cyberspace Cooperation Summit in Berlin on December 3-5.

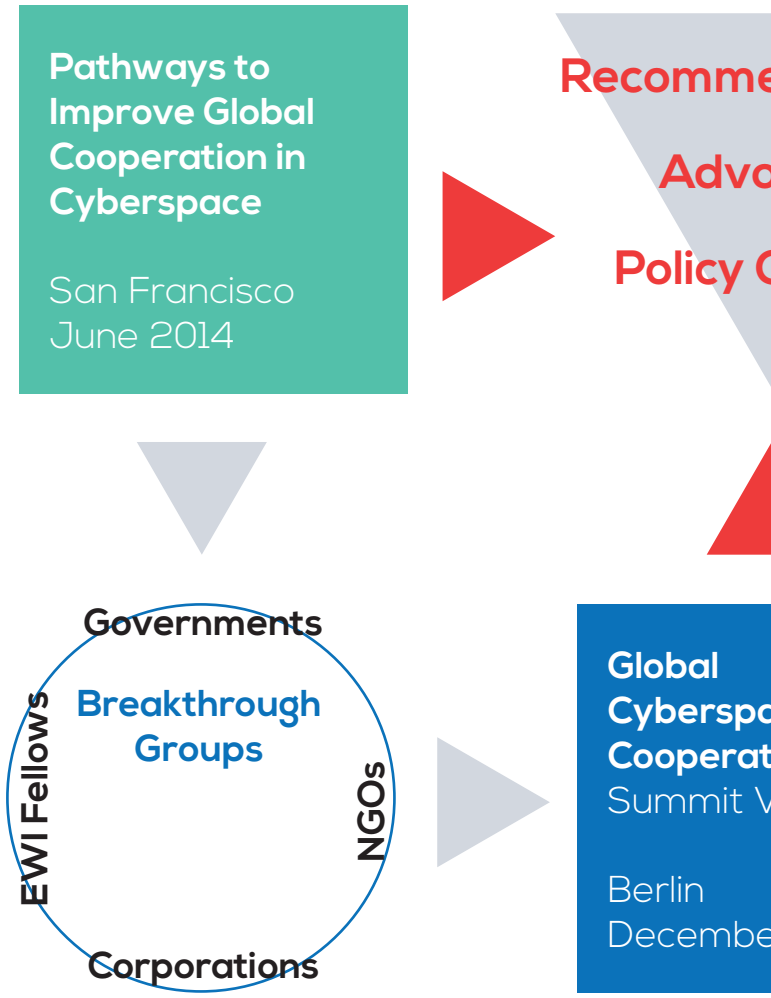
The Challenge

Economic growth and international security are increasingly endangered by national policies governing the secure flow of information and the handling of data. This development is being driven by three influences:

- **Political and Economic Concerns.** Trade issues, concerns about inappropriate or illegal Internet content, and anger about surveillance and privacy create domestic political pressure for the "localization" of products, services and data.
- **Security Concerns.** The digitization and interconnection of society, and in particular critical infrastructures, increase the risk of accidental or deliberate cyber disruptions, while international cyber criminals go unpunished and a cyber arms race threatens stability.
- **Weak Governance.** National and international Internet governance institutions are slow, weak, isolated, or non-existent.

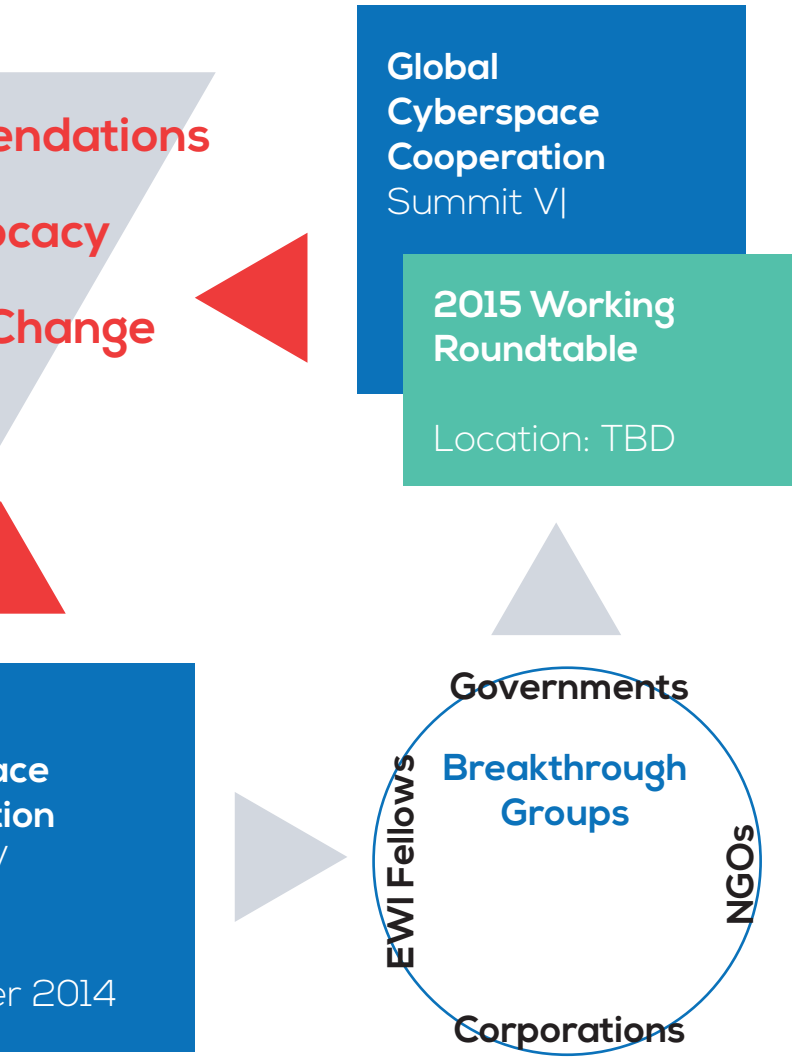
If these three influences are not successfully managed, trust in the Internet will erode and a militarized, fragmented "Splinternet" will emerge to undermine global economic growth and fuel dangerous regional and international instability. Cyberspace will cease to be the premier global arena for information exchange and dialogue. Moreover, these interrelated influences cannot be managed separately. Because the network connects everywhere, true cyber security and stability require the participation of all key governments, including the developing world. Private sector operators and suppliers, national and international non-governmental organizations, and the netizens themselves must also participate in shaping a common future.

Progress is urgently needed in the near term—every month that passes without action raises the costs to society of the current trends, and of turning those trends around. Without effective action, the future safety and livelihoods of literally billions of young, new Internet users will be damaged, leading to unrest in already fragile states.



The Work Program

The Global Cooperation in Cyberspace Initiative uses EastWest's proven process —Convene, Reframe, Mobilize—to help achieve the three objectives that will mitigate the impact of the Splinternet. This work takes place through working groups (which we call **breakthrough groups**) that have met and will continue to meet at least three times in 2014, either in person or online. These interrelated activities capitalize on EastWest's ability to help top corporate and national leaders around the world see and shape the strategic impact of issues. EastWest is utilizing its global network of technology/policy experts and senior officials responsible for cyberspace in governments and private organizations. Participants in the work include:



The Opportunity

The Splinternet is an Internet whose capacity and effectiveness are weakened by barriers to efficient information transfer, threats to personal and public security, and unresolved conflicts around norms. EastWest is helping to create institutions, processes, and policies that reduce the pressures driving fragmentation and minimize its negative consequences. The Global Cooperation in Cyberspace Initiative convenes and mobilizes government and private stakeholders around **three objectives** that match the three influences driving fragmentation:

1. **Economic and Political Development:** Increase the global availability of secure ICT products and services, manage barriers to information flows for innovation and education, and explore cyber surveillance, privacy and big data.
2. **Digital Security and Stability:** Work to mitigate cyber risks to critical infrastructure, modernize mutual law enforcement assistance in cyber-enabled crime, and promote measures of restraint in cyber weapons development and deployment.
3. **Sound Governance and Management:** Facilitate the design and testing of transparent, accountable, orderly, inclusive and agile management and governance structures that increase predictability and trustworthiness for the Internet.

The work needed to achieve a secure and stable cyber environment aligns with EastWest's mission. EastWest takes on seemingly intractable problems that, left unsolved, would result in serious conflict among and within nations on a regional or global scale. Over the past five years, EastWest's cyber collaboration has integrated public and private leadership to address several serious challenges in cyberspace. For example, EastWest has worked successfully to catalyze international arrangements that are improving communications security, reducing spam and building bilateral confidence and trust among China, India, Russia, and the United States.

- Government: ICT security and policy leaders in key governments, including China, Germany, India, the European Union, Russia, the United Kingdom, and the United States.
- Corporate: Public policy, law, security, and business executives from a geographically diverse set of international companies who provide and use cyberspace to serve their customers.
- NGOs: Selected cyber/Internet policy and advocacy groups to complement EastWest's capabilities.
- EastWest Fellows: Volunteer subject matter experts who serve as Fellows for the Institute.

Agenda

MONDAY, JUNE 16, 2014

18:00-20:00 **WELCOME RECEPTION**

TUESDAY, JUNE 17, 2014

08:00-09:35 **PLENARY SESSION I: INTRODUCTION AND OVERVIEW**

Welcome: **John Hurley**, Managing Partner, Cavalry Asset Management; Member, Board of Directors, EastWest Institute

Chair: **Bruce W. McConnell**, Senior Vice President, EastWest Institute; Former Deputy Under Secretary for Cybersecurity, U.S. Department of Homeland Security

Remarks: **Karsten Geier**, Head of Division Arms Control and Disarmament: Communication and New Challenges, Federal Foreign Office of Germany
Denis Chaibi, Deputy Head, Political Section, Delegation of the European Union to the United States
Roberta "Bobbie" Stempfley, Deputy Assistant Secretary for Cybersecurity Strategy and Emergency Communications, Office of Cybersecurity and Communications, U.S. Department of Homeland Security
Zhang Xinhua, Professor and Director, Center for Policy and Strategic Studies, Shanghai Academy of Social Sciences

Paul Nicholas, Senior Director, Global Security Strategy and Diplomacy, Microsoft
Andy Purdy, Chief Cyber Security Officer, Huawei Technologies USA

09:35-09:55 **NETWORKING BREAK**

09:55-11:45 **BREAKTHROUGH GROUP SESSION I**

Enhancing Global Access to Secure Products and Services

Leaders: **Greg Austin**, Professorial Fellow and Director, Policy Innovation Unit, EastWest Institute
Franz-Stefan Gady, Senior Fellow, EastWest Institute
John Savage, An Wang Professor of Computer Science, Brown University

Managing Barriers to Information Flows for Innovation and Education

Leaders: **Stuart Goldman**, Senior Fellow, EastWest Institute; Fellow (ret.), Bell Labs
Roger Hurwitz, Research Scientist, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology

Exploring Surveillance, Privacy and Big Data

Leaders: **Kamlesh Bajaj**, Chief Executive Officer, Data Security Council of India (DSCI)
Chris Riley, Senior Policy Engineer, Mozilla
Jürgen Schnappertz, Senior Advisor on International Security Policy, Policy Planning Staff, Federal Foreign Office of Germany

Modernizing International Procedures against Cyber-Enabled Crimes

Leader: **Merritt R. Baer**, Fellow, EastWest Institute

11:45-12:55 **WORKING LUNCHEON: GOVERNING AND MANAGING CYBERSPACE**

Chair: **Bruce W. McConnell**, Senior Vice President, EastWest Institute; Former Deputy Under Secretary for Cybersecurity, U.S. Department of Homeland Security

Remarks: **Latha Reddy**, Distinguished Fellow, EastWest Institute; Former Deputy National Security Advisor of India
Michele Markoff, Deputy Coordinator for Cyber Issues, Office of the Secretary of State, U.S. Department of State
Karsten Geier, Head of Division Arms Control and Disarmament: Communication and New Challenges, Federal Foreign Office of Germany
Angela McKay, Director, Cybersecurity Policy and Strategy, Microsoft

13:00-14:45 **BREAKTHROUGH GROUP SESSION II**

Strengthening Critical Infrastructure Resilience and Preparedness

Leaders: **Merritt R. Baer**, Fellow, EastWest Institute
Mark Bowler, Technical Council Chair, Network Centric Operations Industry Consortium (NCOIC); Senior Systems Engineer, Advanced Networks and Space Systems, Phantom Works, The Boeing Company

Increasing ICT Product and Service Security

Leaders: **Stuart Goldman**, Senior Fellow, EastWest Institute; Fellow (ret.), Bell Labs
Andy Purdy, Chief Cyber Security Officer, Huawei Technologies USA

Promoting Measures of Restraint in Cyber Armaments

Leaders: **Greg Austin**, Professorial Fellow and Director, Policy Innovation Unit, EastWest Institute
Franz-Stefan Gady, Senior Fellow, EastWest Institute
Roger Hurwitz, Research Scientist, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology

Governing and Managing the Internet

Leaders: **Latha Reddy**, Distinguished Fellow, EastWest Institute; Former Deputy National Security Advisor of India
John Savage, An Wang Professor of Computer Science, Brown University

14:45-15:05 **NETWORKING BREAK**

15:05-17:00 **PLENARY SESSION II: NEXT STEPS AND RECOMMENDATIONS**

Chair: **Bruce W. McConnell**, Senior Vice President, EastWest Institute; Former Deputy Under Secretary for Cybersecurity, U.S. Department of Homeland Security

Remarks: **Sameer Bhalotra**, Chief Operating Officer, Impermium; Former Senior Director for Cybersecurity, The White House
Harry D. Raduege, Jr., Chairman, Center for Cyber Innovation, Deloitte; Member, President's Advisory Group, EastWest Institute
Karsten Geier, Head of Division Arms Control and Disarmament: Communication and New Challenges, Federal Foreign Office of Germany

Participants

Above, from left: Michele Markoff and Zhang Xinhua; Ilya Rogachev; Latha Reddy; Bruce W. McConnell and Karsten Geier.

H. Avni Aksoy, Ambassador, Embassy of Turkey to Kenya

Margaret Anderson, Senior Advisor, EastWest Institute

Stuart Anderson, Fellow, Open WhisperSystems

Greg Austin, Professorial Fellow and Director, Policy Innovation Unit, EastWest Institute

Merritt R. Baer, Fellow, EastWest Institute

Kamlesh Bajaj, Chief Executive Officer, Data Security Council of India (DSCI)

Gary Belvin, Software Engineer, Security Team, Google

Sameer Bhalotra, Chief Operating Officer, Impermium; Former Senior Director for Cybersecurity, The White House

Mark Bowler, Technical Council Chair, Network Centric Operations Industry Consortium (NCOIC); Senior Systems Engineer, Advanced Networks and Space Systems, Phantom Works, The Boeing Company

Robert N. Campbell, Founder and CEO, Campbell Global Services LLC; Member, Board of Directors, EastWest Institute

Denis Chaibi, Deputy Head, Political Section, Delegation of the European Union to the United States

Gilliam E. Duvall, Engr., Senior Research Fellow and Chair, Cyber Integration Academic Department, The National Defense University - iCollege

Franz-Stefan Gady, Senior Fellow, EastWest Institute

Megan Garcia, Program Officer, Cyber Initiative, The William and Flora Hewlett Foundation

Karsten Geier, Head of Division Arms Control and Disarmament: Communication and New Challenges, Federal Foreign Office of Germany

Stuart Goldman, Senior Fellow, EastWest Institute; Fellow (ret.), Bell Labs

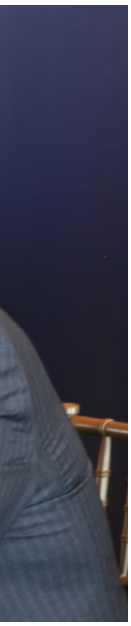
Jonah Force Hill, Consultant, Monitor 360

John Hurley, Managing Partner, Cavalry Asset Management; Member, Board of Directors, EastWest Institute

Roger Hurwitz, Research Scientist, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology

Sally Long, Director, The Open Group Trusted Technology Forum

Preetam Maloor, Strategy and Policy Advisor, International Telecommunication Union (ITU)



Michele Markoff, Deputy Coordinator for Cyber Issues, Office of the Secretary of State, U.S. Department of State

Bruce W. McConnell, Senior Vice President, EastWest Institute; Former Deputy Under Secretary for Cybersecurity, U.S. Department of Homeland Security

Angela McKay, Director, Cybersecurity Policy and Strategy, Microsoft

Viktor Minin, Chairman of the Board, Association of Chief Information Security Officer (ACISO)

Sami Nassar, Vice President and General Manager CyberSecurity Solutions, NXP Semiconductors

Paul Nicholas, Senior Director, Global Security Strategy and Diplomacy, Microsoft

Yoko Nitta, Principle Researcher, Japan Safe and Security Crisis Management

Michael O'Reirdan, Senior Fellow, EastWest Institute

Andy Purdy, Chief Cyber Security Officer, Huawei Technologies USA

Harry D. Raduege, Jr., Chairman, Center for Cyber Innovation, Deloitte; Member, President's Advisory Group, EastWest Institute

Latha Reddy, Distinguished Fellow, EastWest Institute; Former Deputy National Security Advisor of India

Chris Riley, Senior Policy Engineer, Mozilla

Ilya Rogachev, Director, Department on New Challenges and Threats, Ministry of Foreign Affairs of the Russian Federation

Leafan E. Rosen, Director of Research, Drones and Aerial Robotics Conference

John Savage, An Wang Professor of Computer Science, Brown University

Jürgen Schnappertz, Senior Advisor on International Security Policy, Policy Planning Staff, Federal Foreign Office of Germany

Igor Shaktar ool, Vice Consul, Consulate General of Russia in San Francisco

Nadezhda Sokolova, Attaché, International Information Security Division, Ministry of Foreign Affairs of the Russian Federation

Roberta "Bobbie" Stempfley, Deputy Assistant Secretary for Cybersecurity Strategy and Emergency Communications, Office of Cybersecurity and Communications, U.S. Department of Homeland Security

Kevin Sullivan, Principal Security Strategist, Microsoft

Hugo von Meijenfeldt, Consul General, Consulate General of the Netherlands in San Francisco

Rutger Vrijen, Vice President, Strategy, NXP Semiconductors

Tim Wierzbicki, Chief Development Officer and Vice President, EastWest Institute

Kim Zetter, Senior Reporter, *Wired*

Zhang Xinhua, Professor and Director, Center for Policy and Strategic Studies, Shanghai Academy of Social Sciences

Breakthrough Groups

EWI's breakthrough groups use a structured process to define difficult problems and arrive at solutions and action plans. The documents below reflect **work in progress** begun in San Francisco. Each group will meet twice online before the Berlin summit, and will continue its work over the next three years.

Enhancing Global Access to Secure Products and Services

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

What measures can stakeholders take to ensure acceptable levels of security by adopting domestic and international legal and technical standards, as well as best practices in order to minimize requirements of localization of information or technology products and services. (Hierarchy of needs)

2. Identify the stakes for each stakeholder.

- Stakeholders: national security elites; politicians; users; civil society; NGOs; academia; international organizations; governments; digital have-nots; private-sector providers and consumers; and standards organizations.
- Countries: loss of confidential government data.
- Corporations: opportunity costs, loss of IP.
- Private sector: privacy, employment opportunities.

3. Analyze alternative approaches and solutions.

- Identify preexisting and future rules of the road and how they can be supplanted (and reevaluated).
- Increase awareness of existing best practices and standards.
- Raise the level of education of those organizations responsible for the problematic governance issues that pre-date the Internet.
- Different approaches to ISP products.
- Will the market provide the answer?
- Measures to advance consistency and scale (applications and standards).
- Discourage local standards (may create barriers to innovation).
- Stakeholder expansion and re-articulation of goals.

4. Devise a win-win set of recommendations.

- Cooperation, more so than competition, is the better method to protect valuable assets.
- Right arguments for the right people to bring them on board.
- Research, education and application of best practices via a mild form of domestic regulation constitute the best path forward.

WORK IN P

II: Creating the Action Plan

1. Identify concrete next steps.

- Form a multinational and representative group with relevant stakeholders.
- Identify Rules of the Road (EU directive, etc.).
- Identify 3-4 examples of countries turning to localization.
- Identify standards and best practices and principals.
- Identify gaps, measures and scales to reach consistency and engage with key stakeholders.
- Engage with key stakeholders and formulate recommendations.
- Feedback loop at all levels (rules of the road to gaps).
- Assessing the maturity of products (maturity models).
- Legibility of certification processes.

2. Identify and secure commitments for action.

3. Establish measures of success.

Managing Barriers to Information Flows for Innovation and Education

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

There are barriers to sharing information for education and innovations. Information and communication technologies bring immense economic and social benefits. They can also be used for purposes that are inconsistent with international peace and security. There has been a notable increase in risk in recent years as ICTs are used for crime and the conduct of disruptive activities.

Concerns about Internet content are causing government entities to block or filter access to such content and the websites it appears on. While states have the obligation for public safety, such concerns need to be balanced against the Internet's potential for economic growth and prosperity, for the flourishing of imagination, for social interaction among people from different countries, and for people's right of freedom of expression as stated in the United Nations Declaration of Human Rights. Exercise of this right carries with it special duties and responsibilities and may be subject to certain restrictions as provided by law and as necessary to a) respect for the rights and reputation of others, b) protection of national security or public order, or of public health or morals.

2. Identify the stakes for each stakeholder.

- Governments with stakes of national security, public safety, education of population, economic development, democratic formation of public opinion.
- Schools with stakes in a) education, b) curriculum development, c) access to scientific information and to research and educational material, d) special needs populations.
- Industry with stakes in a) local and international collaborations, b) free flow and use of data for economic purposes across borders, c) skilled workforce, d) protection of intellectual property and proprietary information, e) utilization of the Internet as stable and adaptive production and marketing environments.
- Individuals have stakes in a) diverse and reliable information; b) privacy; c) public safety and morality.

3. Analyze alternative approaches and solutions.

- Innovation barriers.
- Education barriers.

4. Devise a win-win set of recommendations.

II: Creating the Action Plan

1. Identify concrete next steps.

2. Identify and secure commitments for action.

3. Establish measures of success.

Issues For Further Discussion:

- Reaction of governments to the real problem.
- Freedom and legal limitations.

PROGRESS

Exploring Surveillance, Privacy and Big Data

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

Creating an effective balance of security and privacy in the use of "personal data" in a big data world, including government surveillance (whether mass surveillance, surveillance by proxy, or targeted surveillance) and corporate practices; and promote transparency and openness in the design and implementation of that balance.

2. Identify the stakes for each stakeholder.

- Governments: Security, rights, trust of their states and citizens; economic interests (IP, trade); diplomatic relations.
- Intergovernmental institutions: Cooperation, stability; global economic growth and development.
- Private sector corporations: Trust, transparency with users and governments; predictability and rule of law; innovation; confidence in investments and protection of intellectual property.
- Citizens of the world: Universal human rights; security and stability; transparency on the use of data by governments and corporations.
- Internet engineers and academia: Innovation, growth, health and effective operation of the global network.
- Privacy advocates: Trust, transparency and universal rights.

3. Analyze alternative approaches and solutions.

- Standards development: – e.g. IETF; also intergovernmental approaches.
- Technological solutions: Development of new tools for protections of data; encouraging greater use of existing solutions; emphasis on global protections (e.g. Heartbleed / SSL). Explore shared responsibility over infrastructure and accountability.
- Take advantage of expertise in independent technical communities: Hackers, data scientists and other experts who are often left out of political conversations.
- Evaluation/progress of national policy solutions: (including potential concrete parliamentary actions) to strategy, including oversight and limits, on surveillance practices (in every country in the world).
- Technical: Literacy challenges; resource challenges; awareness challenges.
- Exploration of ways to de-emphasize data.
- Increase education of policymakers across governments.

WORKIN

Above, from left: Paul Nicholas; Roberta "Bobbie" Stempfley.

- Improve transparency in use of data; create incentives to minimize use.
- Promote competition to prevent abuse of market power of big companies and to save market chances of small companies.

4. Devise a win-win set of recommendations.

- (Technology) Work to reduce/minimize indiscriminate use of data through improved technical and procedural safeguards, and effective oversight.
- (Policy) Starting point: Adopt a broad, inclusive, consultative process / structure for discussion that reflects all stakes and stakeholders.
- (Combined) Study new ways (including technologies and processes) of engaging in necessary corporate and government capabilities that minimize harm to rights.

II: Creating the Action Plan

1. Identify concrete next steps.

- Work to improve literacy and education on technology and practices around (big) data (among policymakers).
- Expand on the problem and detail the "win-win" recommendations further.
- Develop norms for government and for private sector practices building on expanded understanding of problems and recommendations.
- Foster (apolitical) collaboration especially within the technology industry and civil society to develop recommendations and frameworks, and to be effective contributors to change.

2. Identify and secure commitments for action.

3. Establish measures of success.

Issues For Further Discussion:

- Trickle-down of capabilities to smaller actors (including cyber criminals) and development of safeguards.
- Government surveillance practices—necessity, substantive limitations and mechanisms.
- Context and maintaining necessary flexibility (e.g. emergency scenarios).

PROGRESS

Modernizing International Procedures against Cyber-Enabled Crimes

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

Stages in the law enforcement process:

- Laws and norms (i.e. old style crimes perpetrated in new cyberspace formats);
- Evidence perspective (forensics, industry cooperation);
- Enforcement (sentences, consequences for actions); and
- International agreements for law enforcement as part of the solution set.

Questions being raised:

- How do we define limits/boundaries of jurisdiction in cyberspace? The Budapest Convention is not adequate (i.e. drafted by a few countries, but not globally scalable to carry out the procedures stated).
- How do we define the acts that constitute cyber crime?
- Should the scope be limited? Such as, only crimes for profit or use of the Internet to promote human trafficking?

2. Identify the stakes for each stakeholder.

- Do all countries have a voice in the crime discussion?
- Individual users of the Internet should be stakeholders. Who should speak for them? NGOs? Who do they go to?
- Is there a method to gather data on the extent of cybercrime?
- The needs of national and international law enforcement are not always shared by industry players.

3. Analyze alternative approaches and solutions.

- Train police forces in best practices.
- Increase cooperation to encourage multilateral agreements.
- Organize face to face meetings.
- Create joint investigation teams to ease procedural matters.
- What is the responsibility of industry to turn over forensics evidence?
- Think of cyber crime in terms of a public health model—as a way to describe the environment and a way to organize the cyber crime environment.

4. Devise a win-win set of recommendations.

- Establish a Cyber Interpol.
- Create preventive measures:
  - » Education
  - » Minimum cyber hygiene to reduce the basic consumer threats and make the high target-oriented crimes more visible.
- Better align legal consequences (sentencing and arrest) to the proportion of the crime.
- Create a non-anonymous environment for more secure interactions (i.e. e-voting).

WORKIN

II: Creating the Action Plan

1. Identify concrete next steps.

2. Identify and secure commitments for action.

a) Private sector:

- Create a set of simple recommendations to limit users' probability of being exposed to criminal activity online (awareness, basic rules from ISPs).
- Find technological ways to limit exposure to cyber crime.
- Encourage industry to have proactive conversations on the potential for criminals to use new technologies.

b) States:

- Create an atmosphere to encourage the sharing of information on cyber crime.
- Can the EU's approach to cyber crime be looked at as a good example and as a first step in cooperation?

3. Establish measures of success.

Promoting Measures of Restraint in Cyber Armaments

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

Mission: Promote measures of restraint in the use of cyber weapons against civil nuclear facilities, submarine cables and other Internet infrastructure and financial exchanges and clearinghouses. Explore potential implantation regimes.

- Problem of generally agreed definition of cyber armament, cyber war, etc.
- Focus on behavior rather than capabilities.
- Lack of predictability of state behavior in cyberspace (White Papers on strategies and intentions).
- Enhance stability of international community to combat malicious actors with intense cooperative measures.
- What are inherently destabilizing acts in cyberspace?
- No one is going to engage in self-restraint. What constitutes self-restraint?
- 1972 U.S.-Soviet Incidents at Sea Agreement (10 concrete measures).
- Unwanted escalation of crisis in cyberspace.
- Lack of state-to-state signaling mechanisms in cyberspace, which leads to miscalculations/misconception by states.
- Non-state actors out of scope of state to state regulations/constraints in cyberspace (UN Group of Governmental Experts agreed that humanitarian law applies to cyberspace. States have responsibility to reign in non-state actors operating from their territory).
- In the absence of wider agreement on issues, how can we reduce/dissuade malicious actors from engaging in attacks?
- Confidence building measures in cyberspace have loopholes.
- Lack of international agreements not to attack specific critical information infrastructure.
- Question of when international norms for conducting war apply to cyberspace (e.g. mass disruption in critical infrastructure should never be permissible).
- Lack of agreement as to what constitutes the threshold of the use of force in war in the non-cyber world (in the eye of the beholder).

States are concerned about the security and stability of their critical infrastructures. Unlike non-cyber weaponry, cyber capabilities are usable across the spectrum of force. There are classes of disruptive effects or critical civilian targets that should be off-limits. International humanitarian law applies only to situations in times of armed conflict. What should be the peacetime rules?

2. Identify the stakes for each stakeholder.

- Critical Infrastructure
- CERT
- Obligation to assist victims

3. Analyze alternative approaches and solutions.

4. Devise a win-win set of recommendations.

II: Creating the Action Plan

1. Identify concrete next steps.

2. Identify and secure commitments for action.

3. Establish measures of success.

PROGRESS

Strengthening Critical Infrastructure Resilience and Preparedness

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

- Critical Infrastructure (CI): How many and do they match across nations? Sixteen in the U.S., 13 in Japan; some nations have no defined list of critical infrastructures.
- Public / Private ownership ratio of CI varies from nation to nation; one size does not fit all. Is there a successful model that can be shared?
- Privately owned CI must follow government rules and regulations.
- Vast number of disasters or emergency situations that can impact CI.
- Piecemeal systems provide some benefit.
- Lack of understanding can be lead to vulnerability.
- Tension between interconnection and susceptibility to attacks.
- Internet of things
- Patchwork of private and public actors provides some measure of resilience.

Summary Statement: Increasing interconnection of critical infrastructure increases attack surfaces and the potential after effects and effectiveness of attacks; improved P&R minimizes effects and impacts. Also improves resilience against natural disasters.

Short version: Continuity of operations and life after both man-made and natural adverse events (cyber attacks, earthquakes, etc.).

2. Identify the stakes for each stakeholder.

- Private sector, public sector utilities
- Local and national government
- NGO and first responder
- People (civilians).
- Standards Organizations
- Education / academia
- Technologists, innovators
- Critical Infrastructure CERTS

3. Analyze alternative approaches and solutions.

- Require information-sharing; education is critical.
- Think about infrastructure in terms of lifecycle. Classes of threats.
  - » How do we add preparedness and resilience to lifecycle?
  - » Resilience can be very architecture dependent, must be designed-in in most cases
- Relationship to CERTs?
- Trust and access control is essential.
- Expanding enhance skill capability of CERTs and young professionals and CI workers.

WORK IN P

Above, from left: Leafan E. Rosen; Harry D. Raduege, Jr.

- Trust and education is closely linked.
- Maintaining skills for preparedness.

4. Devise a win-win set of recommendations.

II: Creating the Action Plan

1. Identify concrete next steps.

- Identify the requirements for preparedness and resilience.
  - » Will vary across nations depending on current maturity and level of interconnectedness and lifecycle.
- Agree on method and criteria for measuring maturity.
- Partition technical and social influences / approaches?
- Survey and map critical infrastructure across varying nations.

2. Identify and secure commitments for action.

a) States:

- Improved trust mechanisms.
- Intra-government coordination.
- International bodies to coordinate better, harmonization of policy and regulations.
- Economic incentives.
- Pursuit of bad actors.
- Fostering local preparedness activities.
- Encourage private sector investment and diversity of capabilities.
- Strategic reserve: how to apply to critical infrastructure.

b) NGOs:

- Provide neutral area for meeting and discussion.

3. Establish measures of success.

- Sharing best practices.
- International standards.
- Stakeholder diversity and level of involvement.
- Measure resiliency via exercises and tests.

PROGRESS

Increasing ICT Product and Service Security

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

The security of ICT products and services has not kept up with their worldwide spread and availability, as well as society's increased dependence on them. This situation carries untenable risk to public safety, national security, and economic viability.

- Product security has not kept up with product offerings.
- As a result there is no assurance that systems are designed to operate in a secure manner.
- Systems may not have been designed to operate in a secure manner.
- Scale, complexity of integration.
- The current Internet is primarily a free system. Would other business models produce more secure results?
- Need to consider global nature of supply chain and the transient nature of the security properties of the final product.
- Four major types of assurances that standards/best practices and certification/accreditation/SLAs need to be taken into account:
  - » Functional assurance of the product: the product does exactly what it is supposed to do;
  - » Product security levels of assurance: the product meets certain security assurance levels based on the requirements of that environment and the acceptable level of risk for that environment;
  - » Product integrity and supply chain assurance: the technology providers, component suppliers and integrators who are building these products must follow best practices and meet certain assurances in the processes they use for design, development, manufacture and delivery of ICT products (both in-house and in the supply chain) in order to mitigate risks associated with vulnerabilities, tainted and counterfeit products;
  - » Operational assurance: operational and security standards as well as best practices that must be in place and followed during operation.

2. Identify the stakes for each stakeholder.

- Component suppliers, product developers, manufacturers, intermediates (ISPs, integrators), end users/consumer.
- Governments (export of technology, trade practices, import, regulator).
- Consultant (provide expert risk analysis, how to meet security requirements).
- Standards bodies.
- Companies.
- Venture capitalists.
- Media (Explain security risks).

3. Analyze alternative approaches and solutions.

- Some services require higher levels of security.
- Identify and leverage standards, best practices, and identify gaps.
- Need different standardization levels of security. Services are interconnected. Third party accreditation / certification and independent product evaluation.
- How can competition be leveraged to increase security? (A demand side strategy).
  - » Insurance, accreditation and fraud calculations.
  - » What incentives do users have to choose secure products? Should they carry more risk?
- Understand the market incentives. How did we get here? No security requirements in purchase or SLA contracts. Need agreement on how to conduct global supply chain audits.
- Need for monetization.
- Consider privacy policy requirements as inspiration for security policy disclosure requirements.
- Education – increase supply of skills. Increase legal learning opportunities.

WORKING

- Create connections between industry security alliances.
- Create report or a set of principles that governments could agree on.

4. Devise a win-win set of recommendations.

- Develop recommendations for everything in section 3?
- What could EWI do?
  - » Reframe an issue. Increase global awareness. Who should be at the table?
- Create new incentives.

II: Creating the Action Plan

1. Identify concrete next steps.

- Find existing bodies in this space.
  - » IEEE, ISO, IETF, Open Group, ISF, ITU, NIST, ISCCC, FIDO, Common Criteria.
- Form a group of the right stakeholders (e.g. EU).
- Provide examples of problems with the way things are occurring now.
- Identify standards, best practices, accreditation programs.
- Analyze the incentives and gaps. Identify benefit or an enforcement of better security.
- Identify possible recommendations and actions.
- Stakeholder engagement about the options.
- Develop a set of principles that we follow, possibly beginning with something like the following:
  - » Don't invent new standards/accreditation programs. Where they exist and are applicable, then list them as options for improving cybersecurity and mitigating threat risks. (The cybersecurity issues are too urgent not to recommend something that already exists, even if it may not be perfect—standards are meant to evolve: gaps will surface as threats increase and change.)
- As we develop principles write them down and get agreement.
- If we get agreement on the four areas mentioned above then it might be useful to identify a set of standards and accreditation programs that we know exist and apply to each of the four areas referenced above - the group's role could then be to get feedback from industry subject matter experts and governments and make sure it is accurate and complete. (The problem could be that we end up with a very large compendium of standards with no calibration—much as arguably happened in the NIST compendium exercise with the Framework, which they eventually abandoned - in fact, that could be a good reference for us if they would allow us to use it.) For example,
  - » Functional assurance of the product: TBD—the most common approach for this category is consumer/supplier development contracts (requirements, acceptance criteria, testing, installation etc.) and SLAs.
  - » Product security levels of assurance: Common Criteria*, FIPS-140, ...
  - » Product integrity and supply chain assurance: O-TTPS*, ISO 27036*, NIST SP 800-161, ...
  - » Operational assurances: SP 800-82 (Industrial Control Systems), ...

2. Identify and secure commitments for action.

3. Establish measures of success.

- Key stakeholders signing off.

Issues For Further Discussion:

- May be a precursor problem: market failure, or regulatory failure, education.
- Legacy systems.

PROGRESS


Andy

Governing and Managing the Internet

I: Identifying the Problem and Its Solutions

1. State the problem to be addressed.

The Internet provides a new medium for communication, computation and storage that is insufficiently secure and robust. It expands opportunities for crime, fraud, theft, and abuse. Internet governance mechanisms to deal with these issues are slow, weak, isolated or non-existent and need to be improved.

The problem with existing governance models is their legitimacy, both culturally and politically. There is also an accountability problem.

2. Identify the stakes for each stakeholder.

- Private sector: Growing risks to all the economic benefits of the Internet including innovation and global growth.
- Governments: National security, increased costs of defense, international relations, conflict risks, public order and radicalization.
- Civil society and users: lack of trust, privacy, freedom of expression, and human rights.
- Internet technical community, academia.
- International and intergovernmental organizations.

3. Analyze alternative approaches and solutions.

Multi-stakeholder model (MSM) is advocated by Western nations. Multilateral and intergovernmental mechanisms are proposed by some states.

4. Devise a win-win set of recommendations.

Separate governance issues from those that primarily concern the technical management of the Internet from those that concern international public policy issues.

Bring more clarity in decision-making and handling disputes in the multi-stakeholder model.

- Improve understanding of roles and responsibilities.
- Create mechanisms for determining roles and responsibilities.

Improved mechanisms are a way to increase legitimacy by supporting redress of grievances and respecting all viewpoints.

II: Creating the Action Plan

1. Identify concrete next steps.

Explore strengths and weaknesses of existing and emerging models of governance, including multi-stakeholder and multilateral fora, and intergovernmental organizations.

2. Identify and secure commitments for action.

3. Establish measures of success.

Success will be measured by the continually, smooth functioning, open, secure and trustworthy Internet, and the harmonious resolution of governance issues.

WORK IN PROGRESS

Clockwise from left: Jürgen Schnappertz, Nadezhda Sokolova and Kamlesh Bajaj; John Savage; Andy Purdy; Robert N. Campbell; John Hurley; Yoko Nitta.

EastWest Institute Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC

H.E. Dr. Armen Sarkissian (Armenia)
Vice-Chairman
EastWest Institute
President
Eurasia House International
Ambassador Extraordinary and Plenipotentiary
Embassy of the Republic of Armenia to the United Kingdom
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder and CEO
EastWest Institute

R. William Ide III (U.S.)
Counsel and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
McKenna Long and Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Former Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Hamid Ansari (U.S.)
President and Co-Founder
Prodea Systems, Inc.

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
Compass-EOS

Kim Campbell (Canada)
Founding Principal
Peter Lougheed Leadership College at the University of Alberta
Former Prime Minister of Canada

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Co-Founder and Managing Principal
The Chertoff Group

David Cohen (Israel)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Hu Yuandong (China)
Chief Representative
UNIDO ITPO-China

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference
Global Head of Governmental Affairs
Allianz SE

Ralph Isham (U.S.)
Managing Director
GH Venture Partners LLC

Anurag Jain (India)
Chairman
Laurus Edutech Pvt. Ltd.

Gen. (ret) James L. Jones (U.S.)
Former U.S. National Security Advisor
Former Supreme Allied Commander Europe
Former Commandant of the Marine Corps

Haifa Al Kaylani (Lebanon/Jordan)
Founder and Chairperson
Arab International Women's Forum

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

Gen. (ret) T. Michael Moseley (U.S.)
President and CEO
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)
Former Permanent Representative
Permanent Mission of Japan to the United Nations

Ronald P. O'Hanley (U.S.)
Former President, Asset Management
Fidelity Investments

Amb. Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab Emirates in Washington D.C.

Admiral (ret) William A. Owens (U.S.)
Chairman
AEA Holdings Asia
Former Vice Chairman
U.S. Joint Chiefs of Staff

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Louise Richardson (U.K.)
Principal
University of St. Andrews

John Rogers (U.S.)
Managing Director
Goldman Sachs & Co.

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
Chairman
Asurion

Amb. Pierre Vimont (France)
Executive Secretary General
European External Action Service (EEAS)
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Management, LLC

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.

CHAIRMEN EMERITI

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs of Germany

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Former Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, the OSCE and the United Nations in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest INSTITUTE

Global Cyberspace Cooperation Summit V

CO-HOSTED BY

Federal Republic of Germany
Foreign Office

December 3-5

Berlin
Germany

cybersummit.info
#cybersummit2014

EastWest INSTITUTE

SAN FRANCISCO 2014

June 16 - 17

Partner:

IEEE

IEEE COMMUNICATIONS SOCIETY

Pathways to Improve Global Cooperation in Cyberspace

Working Roundtable

Sponsors:

Federal Foreign Office of Germany

Huawei Technologies

Microsoft

ZEIT-Stiftung Ebelin und Gerd Bucerius

www.ewi.info

–

EWInstitute

EastWestInstitute

–

#cybersummit2014