Global Cooperation in Cyberspace Initiative

2014-2015 Action Agenda

Copyright © 2015 EastWest Institute
Illustrations by Dragan Stojanovski

The views expressed in this publication do not necessarily reflect the position of the EastWest Institute, its Board of Directors or staff.

—

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.

—

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

—

communications@ewi.info
www.ewi.info

Chairman's Letter

Cyberspace has become the most essential infrastructure to the conduct of global business and government. These institutions thrive on predictability and continuity. As a steady stream of virulent cyber attacks demonstrates, however, the global digital environment is becoming an increasingly unpredictable and unstable space, where risks are extremely difficult to evaluate and manage.

The EastWest Institute (EWI) has been in the vanguard working internationally to improve the safety and security of cyberspace. Our fifth Global Cyberspace Cooperation Summit, concluded in Berlin in December 2014 and co-hosted by the German Foreign Office, capped the first year of our expanded cyber cooperation initiative that addresses the interdependent risks and threats that complicate operations in cyberspace today.

At the summit, over 250 participants from 42 countries heard Dr. Thomas de Maizière, federal minister of the interior of Germany, advocate for a shared Internet, where freedom, trust and security can thrive side by side. De Maizière spoke optimistically about the potential for a safe and secure Internet that abides by rules and regulations. "The Internet cannot be viewed as a separate entity. The same laws must apply in both the analog and digital worlds." He added, "Trust is the new currency of the Internet, but the price has not yet been set. All of us globally must work toward that, and that is why we are here."

EWI's cyberspace work moves forward with that exact sentiment. As Bruce McConnell, EWI's senior vice president and leader of the cooperation initiative, told summit participants, "We are here to work toward making the Internet a vehicle for a safer, more peaceful, more secure, more open world—where the creative human spirit can thrive."

Cyber-enabled crime, insecure technology, murky supply chains, state-sponsored censorship, the balance between individual online privacy with security and convenience, and the proliferation of cyber weapons—these issues must be addressed by cooperative action by governments, businesses, and civil society from around the world. **EWI is the premier global convener of ongoing work to reframe and resolve these issues creatively and effectively**.

This action agenda highlights EWI's 2014 cyber work and provides a road map for 2015. We welcome your feedback and participation. Onward to a safer and more secure cyberspace!

Ross Perot, Jr.
Chairman of the Board
EastWest Institute

Global Cooperation in Cyberspace: An Overview

"It was John Mroz's deep belief that building trust and avoiding conflict in cyberspace was possible. We are all working toward that today and moving forward in his memory."

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

For three and a half decades, the East-West Institute has been working to reduce international conflict by building trust where it is in deficit. We address daunting challenges facing the world by convening leaders from governments, businesses and civil society, developing new, actionable solutions and mobilizing our network for action.

These challenges are ever more apparent in cyberspace, where existing national and international organizations, national authorities, laws, norms, and the technology itself are inadequate to address the rapidly evolving threats and increasing risks.

EWI began its cyber work in 2009 as the pioneer organization that initiated a global dialogue on cyberspace security, diplomacy and deterrence. Since then, EWI has convened a global network of technology and policy experts, senior officials responsible for cyberspace in governments and leaders of businesses, and civil society to make concrete progress toward creating new institutions, processes and policies that will improve the safety and security of cyberspace.

In 2013, EWI expanded the scope of the Global Cyberspace Cooperation Initiative to utilize its **proven trust-building process—Convene, Reframe, Mobilize**—to address three objectives: economic and social progress, digital security and stability, and sound governance.[1] EWI's past successes have helped **shorten repair times for damaged undersea cables**, **reduce spam** on a global basis, and **build bilateral confidence and trust between East and West** to improve crisis response and combat malicious hackers.

In 2015, we will continue to work with governments, business and civil society to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion.

1 We **convene** discreet conversations among representatives of institutions and nations who would not otherwise meet. There we help **reframe** difficult questions and devise new, win-win approaches. We then **mobilize** support for the results of this work to make change happen, working through our extensive networks of key individuals in capitals and corporate headquarters around the world.

"The privacy of digital identities and the technology to protect it, will determine if cyberspace will continue to be an opportunity for businesses and services to thrive, or a threat to our infrastructure and economy. Through events like the Global Cyberspace Cooperation Summit in Berlin, EWI is well positioned to bring awareness of the problem and the solutions that could be applied, drawing experiences from best security and technology practices in government and industry."

Ruediger Stroh
Executive Vice President and General Manager, Security & Connectivity, NXP Semiconductors

Introduction

Cyberspace—the global system of electronically interconnected people, information, processes, and technology—is a principal stage upon which modern life appears and is acted out. For 3.5 billion "netizens" and the critical sectors they depend on—finance, business, culture, politics, entertainment, medicine—the world cannot function in the 21st century outside of cyberspace.

Since its earliest days, cyberspace has been unruly and unpredictable, a frontier where the future is recreated daily. Its fluidity and ambiguity have fed innovation and collaboration, lowering costs all along the value chain and increasing productivity. Yet with these growing benefits has come increasing malice. Cyberspace can be at times a rather dangerous place for ordinary people and businesses to conduct their daily affairs, risking its peaceful uses and our collective progress.

Cyberspace is no great respecter of boundaries, whether political, legal, organizational, or geographic. Accordingly, cooperation is essential to successfully address existing and emerging conflicts—both in cyberspace and, increasingly, across all areas of human endeavor.

In 2014, building on a strong foundation of work on traditional cybersecurity issues, we rebranded and expanded the scope of the Global Cooperation in Cyberspace Initiative to reflect the increasingly interdependent set of issues that are at the core of conflict in and around cyberspace.

The strategic objective of the initiative is to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion. EWI has identified three objectives for the initiative, to be pursued over the three-year period 2014-2016:

- Enhance the beneficial economic, political and social impacts of the global growth in Internet use.
- Increase the security and stability of cyberspace and its technologies.
- Strengthen the institutional framework that governs the Internet.

"In a world where every individual is increasingly dependent on information technology, it is important that governments reach agreements on cybersecurity norms of behavior and that the activities of governments and businesses be scoped appropriately."

Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft

"We believe that we need to work better at seeing the interdependence of international security, national security and economic security. We need to rethink these silos. These functions can no longer afford to be evaluated independently."

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

"There is a need to limit mass surveillance by governments through appropriate mechanisms like rules of the road or treaties."

Kamlesh Bajaj
CEO, Data Security Council of India (DSCI)

2014: A Successful Year

Now in its sixth year, EastWest's initiative to prevent conflict in cyberspace registered new milestones in policy mobilization. In 2014, leading corporations and governments partnered with EastWest as it continued to push for policy breakthroughs that will help build confidence in cooperative approaches to cyberspace governance.

EastWest has mobilized a global network of policymakers and specialists, all serving voluntarily, to advocate for such breakthroughs. In 2014 alone we contributed to major policy deliberations in Garmisch, Munich, Qatar and São Paulo. Our network includes a broad range of partner organizations (including Fudan University, the Institute for Information Security at Moscow State University, the Institute of Electrical and Electronics Engineers, the Internet Society of China, and ZEIT-Stiftung Ebelin und Gerd Bucerius) and a small network of highly qualified fellows and longtime collaborators from Australia, Austria, Germany, India, Ukraine and the U.S. The initiative depends for its success on the active engagement of EWI's directors, several of whom are leaders in the ICT industry or policy. For example, EWI board member and former U.S. Secretary of Homeland Security Michael Chertoff and Distinguished EWI Fellow and former Indian Deputy National Security Advisor Latha Reddy are serving on the Global Commission on Internet Governance organized by Carl Bildt, former foreign minister and prime minister of Sweden.

EWI and its fellows also published key findings and recommendations, which we have advocated for in capitals and corporate headquarters around the world. In *Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies,*[2] Fellows Greg Austin and Sandro Gaycken argue that much stronger security built into products and services will do more to reduce attacks than continuing to rely on add-on defensive measures. In *A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets,*[3] introduced by Nobel Peace Laureate Mohamed ElBaradei and

2 *Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies* (http://www.ewi.info/idea/resetting-system#sthash.qu0m0eKJ.dpuf)

3 *A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets* (http://www.ewi.info/idea/measure-restraint-cyberspace#sthash.cRrILH9C.dpuf)

EWI Policy Report

A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets

This report urges all parties to commit to taking civilian nuclear facilities off limits for cyber attacks. As a first step, it proposed that the Nuclear Security Summit in The Hague should open a debate "with the purpose of promoting early agreement that use of technological attacks (including cyber means) against the safe operation of civilian nuclear assets in peacetime should be prohibited by a legally binding multilateral instrument." The paper also recommends the establishment of a multilateral response center for nuclear information security incidents of high severity.

In the preface, Nobel Peace Laureate and Former Director General of the International Atomic Energy Agency Mohamed ElBaradei states: "The EastWest Institute takes a refreshingly direct approach, drawing on the successful experiences of global arms control negotiations in non-cyber arenas."

According to EWI Senior Vice President Bruce McConnell, "Given the potential risks to humanity and the planet, nations should refrain from attacking civilian nuclear assets using cyber weapons. It's a concrete step to advance peace in cyberspace."

released at the 2014 Munich Security Conference, EWI urges all parties to commit themselves to making civilian nuclear facilities off limits for cyber attacks.

These reports and activities go hand in hand with the work of seven collaborative breakthrough groups, whose participants—decision-makers from key sectors from around the world—work in person and virtually to address specific issues. Each breakthrough group is working to develop actionable recommendations for industry and government that, if implemented, will have significant impact in making cyberspace and the real world safer, more stable and more secure.

To support the work of the breakthrough groups in 2014, EWI hosted two in-person meetings, a roundtable in San Francisco in June and a summit in Berlin in December. In addition, from July through November, each of the seven breakthrough groups convened twice by phone and collaborated via email. These discussions built on the work accomplished in San Francisco and set the stage for the Berlin summit.

2015: Reducing Cyber Conflict, Crime and Disruption

In 2015, the initiative will continue to develop and advocate for recommended changes in national and corporate policies and procedures relevant to creating a safer and more secure cyberspace. The principal means of developing recommendations is the breakthrough groups.

The scope of the 2015 breakthrough group work is laid out in the table on pages 8 and 9. Throughout the year, EWI will convene the groups through in-person events and online meetings. As recommendations mature, EWI will lead the preparation of reports detailing and supporting the conclusions. EWI will also lead the mobilization for advocacy of the recommendations in capitals and corporate headquarters worldwide.

Furthermore, EWI will develop additional recommendations in areas where it believes improved clarity or emphasis would advance the use of known techniques that could make a great difference in emerging security or stability issues. For example, in the exponentially growing domain of cloud services, many providers are still relying on authentication mechanisms based on username and password. This approach is increasingly compromised by widely available attack tools and is resulting in major damages to corporations and governments. EWI will recommend approaches that would help to overcome this weakness.

Finally, EWI will use its annual Global Cyberspace Cooperation Summit to highlight and build momentum for the recommendations. Building on the work of previous summits, this sixth summit will convene government and corporate leaders, along with civil society and EWI's own fellows to address these and other issues threatening the future of cyberspace and its ability to deliver benefits to citizens around the world.

"Cyber crime laws are useless if they are not internationally enforced."

Marina Kaljurand
Undersecretary and Legal Adviser, Cyber Security, Ministry of Foreign Affairs of Estonia

EWI Discussion Paper

Exploring Multi-Stakeholder Internet Governance

Internet governance is now an active topic of international discussion. Interest has been fueled by media attention to cyber crime, global surveillance, commercial espionage, cyber attacks and threats to critical national infrastructures. Many nations have decided that they need more control over Internet-based technologies and the policies that support them. Others, emphasizing the positive aspects of these technologies, argue that traditional systems of Internet governance, which they label "multi-stakeholder" and which they associate with the success of the Internet, must continue to prevail. In February 2015, EWI published the report *Exploring Multi-Stakeholder Internet Governance*. This paper introduces multi-stakeholder Internet governance, examines its strengths and weaknesses, and proposes steps to improve it.

Written by EWI Professorial Fellow and Brown University An Wang Professor of Computer Science John E. Savage, and EWI Senior Vice President Bruce McConnell, the report supports the work of the initiative's breakthrough group on Governing and Managing the Internet. EWI is now presenting the findings and recommendations to government officials and private sector stakeholders.

Breakthrough Groups - Areas of Work

Breakthrough Group	Context, Premise and Scope of Work
Increasing the Global Availability of Secure ICT Products and Services	The availability of secure information and communications technology (ICT) products and services has tended to lag ICTs' worldwide spread and society's increased dependence on them. This situation creates risks to public safety, national security, privacy and economic viability. This breakthrough group explored approaches to increase that availability, including by enhancing the security of ICT supply chains, promoting the adoption of highly secure computing, and evaluating the security benefits and costs of relying on local sources of supply compared with taking advantage of the global marketplace.
Managing Objectionable Electronic Content Across National Borders	The interconnection of ICTs brings immense economic and social benefits. ICTs can also be used for purposes that are inconsistent with 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. Security concerns about Internet content are causing government entities to block or filter access to locally objectionable content and the websites it appears on. This is creating or exacerbating barriers to the global sharing of information for education and innovation. While states have the obligation for public safety, such concerns need to be balanced with 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 respect for the rights and reputation of others, and the protection of national security, public order, or of public health or morals.
Increasing Transparency and Account-ability in Personal Data Collection	Recent revelations about the extent of the collection of personal data are generating concerns about privacy and disrupting longstanding partnerships. While governments and companies will continue to rely on personal data to provide security and business benefits, this breakthrough group focused on approaches and frameworks that enhance privacy by limiting the uses of such data and create transparency into what is collected and how it is used.
Strengthen-ing Critical Infrastructure Resilience and Prepared-ness	The increasing digitization and interconnection of society, and in particular critical infrastructures, increase the risk of accidental or deliberate cyber disruptions. While many groups are working hard to improve the security of systems that critical infrastructure depends on, less is being done in the areas of critical infrastructure preparedness and resilience, especially in the areas of contagion risk for interconnected systems, emergency communications, submarine cable incident response and regional CERT-CERT cooperation. This breakthrough group found ways to promote preparedness and resilience to cyber threats and address these challenges.
Modernizing International Procedures against Cy-ber-enabled Crimes	Global losses from cyber-enabled crimes likely exceed $400 billion annually. While organizations and enterprises continue to invest in protective technologies and techniques, progress on finding, prosecuting and punishing cyber criminals is slow. The cross-border nature of these crimes, the differing roles of governments and private sector service providers, and variations in national capacities, laws and procedures are among the factors that make progress difficult. In particular, better cooperation is essential between law enforcement and the private sector on a global basis.
Promoting Measures of Restraint in Cyber Armaments	The cyber arms race among major powers has a destabilizing effect on the international order. The United Nations Group of Governmental Experts (GGE) and others are examining how international humanitarian law applies in cyberspace. This breakthrough group is taking a bottom-up approach and exploring implementation of measures of restraint in the use of cyber weapons against civil nuclear facilities, submarine cables and other Internet infrastructure, and financial exchanges and clearinghouses.
Governing and Managing the Internet	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. Governance mechanisms to deal with such a broad range of issues are often slow, weak or isolated, and need to be improved. In addition, existing governance models encounter questions regarding their legitimacy, culturally and politically, in part because of concerns about their composition and degree of accountability. This breakthrough group analyzes emerging approaches for improving potential effectiveness and proposes models that demonstrate agility, transparency, predictability, inclusivity and accountability.

2014 Accomplishments	2015 Goals
Developed draft, baseline international assurance and integrity standards that will enable customers to demand more secure ICT products and services, regardless of where they are manufactured. To seed the discussion, the group received a report from Huawei Technologies entitled "Cyber Security Perspectives – 100 Requirements When Considering End-To-End Cyber Security With Your Technology Vendors."	Refine and promote international assurance and integrity standards that will enable customers to demand more secure ICT products and services, regardless of where they are manufactured.
Focused on creating transparent and precise criteria for the private sector to evaluate governmental requests for takedowns, filtering and blocking; and on encouraging states to empower and educate users about objectionable content while increasing access to information for innovation and education.	Develop transparent and precise criteria for the private sector to evaluate governmental requests for takedowns, filtering and blocking. Encourage states to empower and educate users about objectionable content while increasing citizen access to information for innovation and education.
Emphasized on the need for transparency about data collection and use before and after collection; and on promoting technical solutions that enhance accountability.	Develop norms regarding transparency about data collection and use. Identify and publicize technical solutions that enhance accountability.
Developed the idea of international "resilience exercises" that highlight cross-border interdependencies among the most critical functions of national infrastructures.	Create plan for international "resilience exercises" that highlight cross-border interdependencies among the most critical functions of national infrastructures.
Identified measures to improve cooperation between law enforcement and the private sector on cyber-enabled crimes.	Promote best practices and transparency regarding corporate policies for providing data to law enforcement. Evaluate the effects of filtering and blocking as a means of reducing the flow of illegal content.
In January 2014, EWI released a publication at the Munich Security Conference, *A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets*. The report urges all parties to commit to taking civilian nuclear facilities off limits for cyber attacks and recommends the establishment of a multilateral response center for nuclear information security incidents of high severity. The group refined its approach to include identifying assets that should not be attacked and levels of damage that should be deemed unacceptable, with attention to measures that would help limit escalation. To support the discussion, the group received a report from Microsoft, "International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World."	Identify national assets that should not be attacked and levels of damage that should be deemed unacceptable, with attention to measures that would help limit escalation.
Identified the major points of disagreement among states regarding the appropriate limits of sovereignty and the roles of the private sector, academia and civil society. To stimulate the discussion, EWI released a study on *Exploring Multi-Stakeholder Internet Governance*. This paper introduces multi-stakeholder Internet governance, examines its strengths and weaknesses, and proposes steps to improve it.	Develop middle-ground approaches that balance sovereignty and multi-stakeholder involvement.


Global Cooperation in Cyberspa
#cyb summ 2014 • erlin 2014

2014 Events

San Francisco
June 2014

The EastWest Institute hosted a working roundtable on Pathways to Improve Global Cooperation in Cyberspace in San Francisco in June 2014.

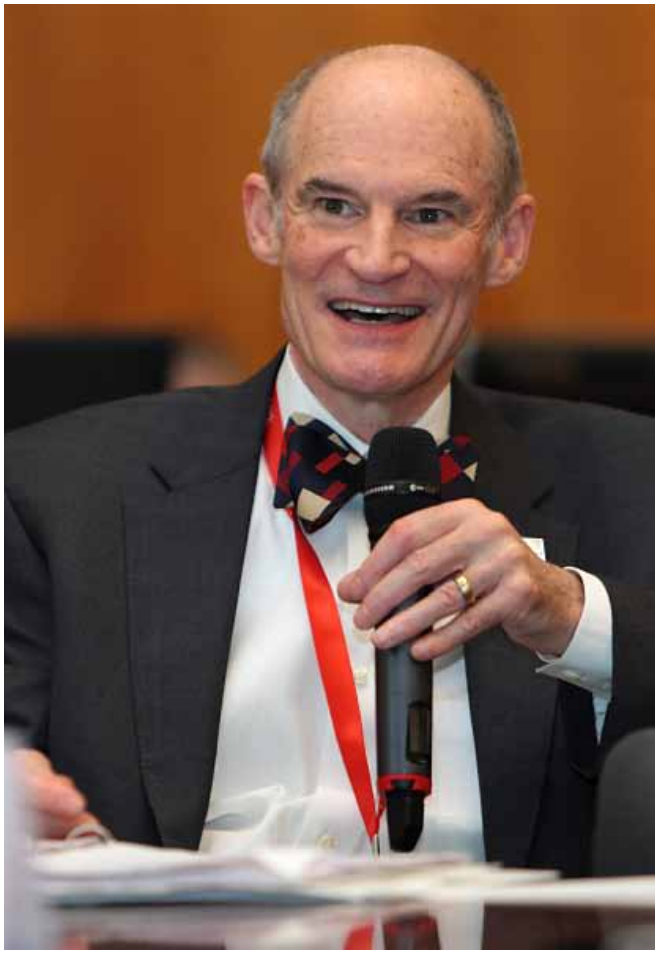
The roundtable brought together 50 seasoned experts and senior policymakers from 13 countries to work on key issues. Strong representation from Russia confirmed once again the significance of EWI's Track 2 work to build bridges between Russia and the U.S., particularly now, when official channels are narrowed. Other countries strongly represented included China, Germany, India and the U.S.

Diverse perspectives and expertise also came from: the UN's International Telecommunication Union (ITU); Chinese, Japanese and Russian think tanks; the Massachusetts Institute of Technology (MIT), Brown University and the National Defense University; the William and Flora Hewlett Foundation; and key non-governmental organizations, such as Mozilla and The Open Group. Additionally, private sector representatives included supporters Microsoft, Huawei Technologies and NXP Semiconductors.

Participants separated into breakthrough groups to discuss concrete next steps. All breakthrough groups successfully identified and agreed on key obstacles and possible solutions to the challenges targeted by EWI's initiative. This work is continuing over the next two years.

"EWI continues to build on the successes of the four previous summits, and through these convenings governments, the private sector and civil society are moving closer to solutions."

Ambassador Dr. Norbert Riedel
Commissioner for International Cyber Policy, Federal Foreign Office of Germany



Clockwise from above: Global Cyberspace Cooperation Summit V in Berlin, Bruce McConnell, Working Roundtable in San Francisco

Berlin
December 2014

The **German Foreign Office and EWI** co-hosted the Global Cyberspace Cooperation Summit V in Berlin, Germany, on December 3-5, 2014.

The summit took place at the Foreign Office Conference Center and continued the success of the first four summits in Dallas (2010), London (2011), New Delhi (2012) and Silicon Valley (2013), as well as the working roundtable in San Francisco.

The institute's annual cyber summits provide a crucial forum for building international, private-public actions to foster international cooperation in cyberspace. The three-day summit welcomed over **250 participants from 42 countries**, including China, the EU, Germany, India, Russia and the U.S. as well as Estonia, France, Japan, Jordan and Ukraine. The Berlin summit brought together leading global experts from the fields of business, government, policy, technology and civil society to pursue EWI's seven breakthrough groups (as shown on pages 8 and 9):

- Increasing the Global Availability of Secure ICT Products and Services
- Managing Objectionable Electronic Content Across National Borders
- Increasing Transparency and Accountability in Personal Data Collection
- Strengthening Critical Infrastructure Resilience and Preparedness
- Modernizing International Procedures against Cyber-enabled Crimes
- Promoting Measures of Restraint in Cyber Armaments
- Governing and Managing the Internet

The summit experience was enriched by the **participation of EWI supporters** Microsoft; Huawei Technologies; NXP Semiconductors; CenturyLink; Hewlett-Packard; ZEIT-Stiftung Ebelin und Gerd Bucerius; PricewaterhouseCoopers; Goldman Sachs; Senatsverwaltung für Justiz und Verbraucherschutz Berlin; the Observer Research Foundation; and Oxford Analytica. These organizations provided wide support during the summit, including two receptions: one hosted by Microsoft

"China is committed to working together for cyberspace security."

Fu Cong
Coordinator for Cyber Affairs, Ministry of Foreign Affairs of China

From top left to bottom right: Dr. Thomas de Maizière; Latha Reddy; Akira Kono; Christopher Painter; Marina Kaljurand; Dr. Markus Ederer; Katherine Getao; Ilya Rogachev; Scott Charney; Fu Cong; Rt Hon Baroness Neville-Jones DCMG; John Suffolk; Phil Venables; Joanna Świątkowska; Sizwe Snail ka Mtuze; Samir Saran













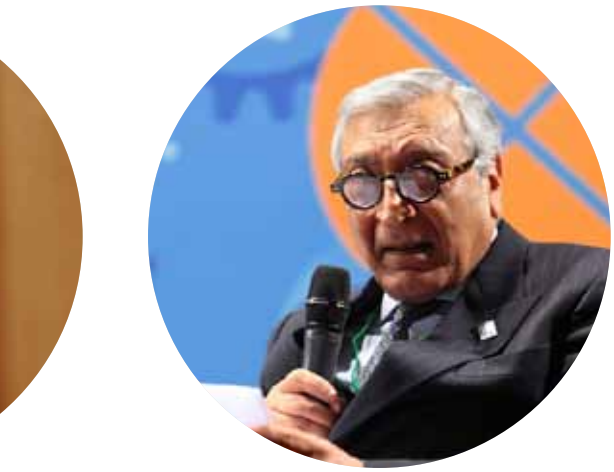












and another by Berlin Senator for Justice and Consumer Protection Thomas Heilmann. In addition, **Microsoft** used the occasion of the summit to release its thought leadership paper, "International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World."[4] **Huawei Technologies** released its own white paper, "Cyber Security Perspectives – 100 Requirements When Considering End-To-End Cyber Security With Your Technology Vendors."[5]

In opening keynote addresses, both Federal Minister of the Interior of Germany **Dr. Thomas de Maizière** and State Secretary of the Federal Foreign Office of Germany **Dr. Markus Ederer** outlined the state of cyber affairs as it stands today.

De Maizière outlined the vulnerability of data and information structures. Highlighting the Home Depot credit card breach in the U.S. earlier in the year, he noted that "As long as it only hits us in the pocketbook, we can probably get over it. But if vital services are affected, that's when things really get serious."

He continued, "We have reached a watershed in our international cooperation concerning the Internet" and called on all participants to, in light of political and cultural debates, find out if a common denominator is possible. After outlining beliefs from both sides of the aisle, de Maizière stated, "In principle, the Internet is not a separate world. So in principle, the same things must apply on the Internet as in the analog world. The same access, the same methods, the same judgements, the same understanding of the state and of fundamental rights."

He pointed to responsibility, trust and security as three main guidelines, stating, "We must use the same methods and assessments we use elsewhere in relations between government and citizens."

On the second day, **Ederer** touched on five points of cyberspace: opportunities, challenges, trust, rules and shared interests. Speaking about cyberspace cooperation, he

4 "International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World" (http://aka.ms/cybernorms)

5 "Cyber Security Perspectives – 100 Requirements When Considering End-To-End Cyber Security With Your Technology Vendors" (http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm#.VNvM8fnF9qW)

"To preserve and develop the global Internet, we have to build and rebuild trust."

Dr. Markus Ederer
State Secretary of the Federal Foreign Office of Germany

From top left to bottom right: Admiral (ret.) William A. Owens; Rebecca MacKinnon; John Hurley; Kamlesh Bajaj; Carlos Perez; Ambassador Dr. Norbert Riedel; Sascha Suhrke; Ambassador Kanwal Sibal; Karsten Geier; Angela McKay; Peter Swire; Ruediger Stroh; Robert N. Campbell; Andrzej Kawalec; Merritt R. Baer; Alexander Seger

"Trust is the new currency of the Internet, but the price hasn't been set yet. All of us globally must work toward that, and this is why we are here."

Dr. Thomas de Maizière
Federal Minister of the Interior of Germany

observed that "The Internet brought politics closer to the people, made politics more transparent, more responsive, and in a way more democratic." He urged participants to be as inclusive and interactive in their discussions as possible, and to use the opportunity to exchange views between government, industry and civil society representatives to "build the trust that is so urgently needed." Ederer also stated that "Cybersecurity is a common concern. It should be pursued regardless of political differences, in the interest of global stability" and argued "We need to balance freedom and security. That balance needs to be well thought through and made subject of a political discourse, nationally and internationally. And the instruments of security need to be proportional to the costs they impose on our privacy."

Ederer concluded that "The EastWest Institute's 2014 Cyberspace Cooperation Summit here at the Federal Foreign Office in Berlin promises to be an important milestone in a multi-annual process, assuring participants "You all are doing a tremendously important job!"

Plenary panel sessions included:

Overview of International Cyberspace Cooperation: Governments, companies and civil society depend on a safe and reliable cyber environment. Yet, no single set of actors can ensure the safety, security and reliability of cyberspace. Panelists discussed current cooperation and ways to improve it.

Exploring Surveillance, Privacy and Big Data: Revelations about data collection by governments and companies are generating concern and disrupting longstanding partnerships. Panelists discussed approaches to enhance privacy by limiting the collection and use of personal data by governments and companies.

Promoting Measures of Restraint in Cyber Armaments: The cyber arms race among major powers has a destabilizing effect on the international order. The United Nations Group of Governmental Experts and others are examining how international humanitarian law applies in cyberspace. Panelists discussed potential implementation regimes where restraint in the use of cyber weapons applies to civil facilities and infrastructure.

From top to bottom: Andrey Kulpin; Roberta "Bobbie" Stempfley; Gib Godwin; Sandro Gaycken

Breakthrough Group Reports and Observations: Leaders of breakthrough groups reported on the results of the sessions, concentrating on proposed next steps to address critical issues in cyberspace. This was followed by reflections from a distinguished panel.

Next Steps and Way Ahead: The panel featured senior stakeholder reflections on the work of the summit and identified the emerging policy and management issues requiring attention.

For the second time in EWI's cyber summit history, there was a **Young Cyber Leaders Respond** panel where young leaders from academia and the nonprofit sector shared their reflections on the future of cyberspace. As one member of the panel asserted refreshingly, "We do not operate from a Cold War paradigm mindset."

Special Interest Sections

Four special interest sections provided informal, interactive discussions and updates on key international cyberspace developments.

- **Whistleblower Procedures** examined the meaning of "correct" procedures for a situation where someone reveals sensitive information.
- **Transatlantic Partnership** worked toward reaffirming the transatlantic partnership by helping to identify a joint agenda on cyber issues.
- **Industry 4.0**—the "fourth industrial revolution"—explored the ongoing trend of informatization and industrialization merging to create companies, industries and economies that are high tech and highly efficient.
- **Governing and Managing the Internet** presented the continuous work in various international venues, including NETmundial and the Global Commission on Internet Governance.

"Small steps can have a large impact in cyberspace, and so we must be bold and take action in this critical time."

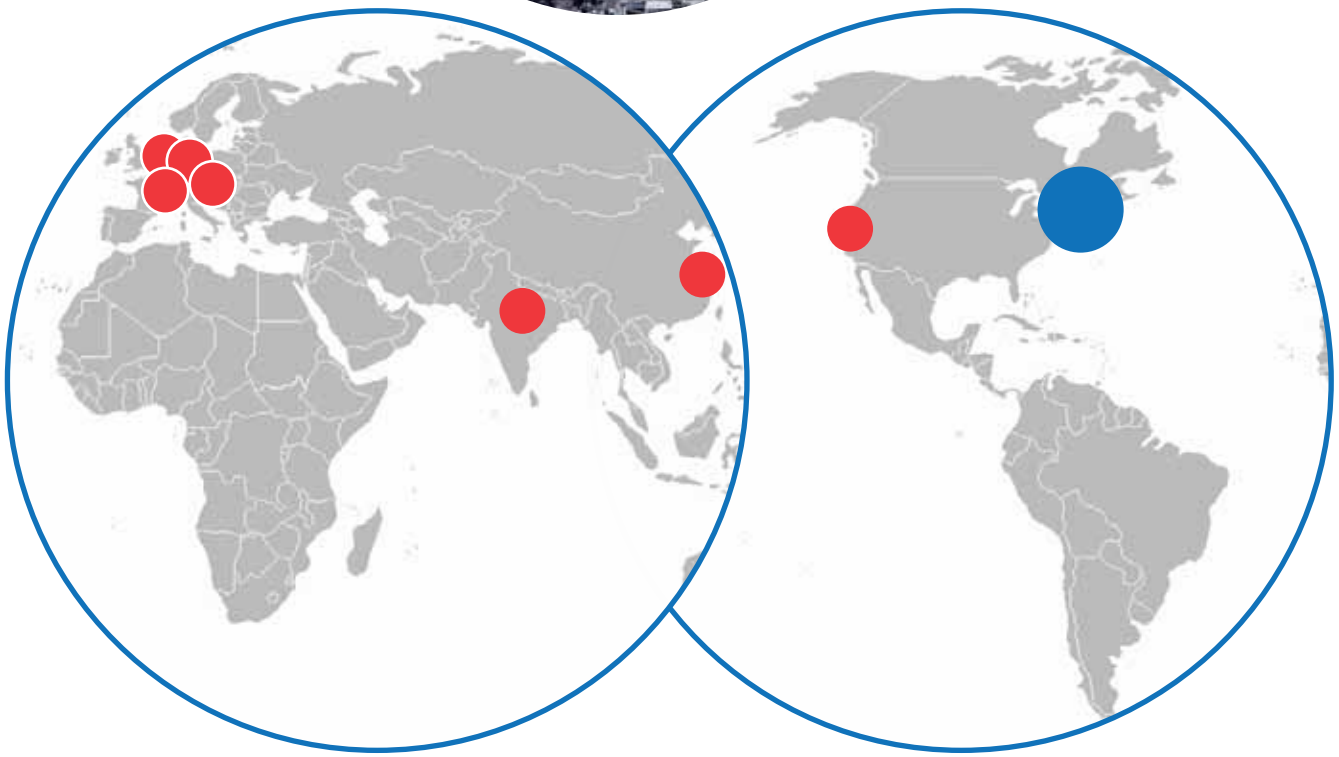
John Suffolk
Senior Vice President and Global Cyber Security Officer, Huawei Technologies Co., Ltd.

From top to bottom: Lt. General (ret.) Harry D. Raduege, Jr.; Michael O'Reirdan; Sameer Bhalotra; Andy Purdy

2015 Events

Global Cyberspace Cooperation Summit VI

New York
September 9-10



Breakthrough Events

The Hague
April 16

Garmisch
April 20

Silicon Valley
May 28

Strasbourg
June 18

New Delhi
October 14

Shanghai
Late October

Munich
February 2016

How You Can Participate

Join a High-Level Community of Cyberspace Cooperation Leaders and Make Change Happen

The EastWest Institute welcomes select corporations and other organizations to join the Global Cooperation in Cyberspace Initiative, where they can influence the global conversation and shape actionable recommendations at the leading edge of this rapidly changing field.

We offer a range of benefits to our partners in the cyberspace community—policy-influencing, international networking occasions and opportunities to showcase thought leadership.

Who Can Benefit

- Companies responsible for the creation, operation and expansion of the Internet—manufacturing, logistics, finance and critical infrastructure organizations—are invited to sponsor our work. Benefits to your company include:
  - » Sitting at the table with policy and business decision-makers shaping the global future of the Internet.
  - » Gaining up-to-the minute market and policy intelligence.
  - » Taking advantage of high-level networking and new business opportunities.
  - » Raising your company's profile and enhancing its reputation.
    - › The annual summit and ongoing breakthrough group dialogues enable you to showcase your thought leadership with speaking platforms and white papers.
- Key civil society organizations and academics can offer their thought leadership and broaden their networks and perspectives.

Why EastWest

While other organizations contribute to the field through publication and research, EWI advances thought leadership into action. To increase security and stability in cyberspace, perspectives from government, corporations and civil society beyond the West, including China, India, Russia, East Asia and the Middle East, must come to the table. EWI is uniquely effective because we do not take the position of any government or company. Instead, we develop and advocate for practical measures that reflect the knowledge of engaged experts from the world's major cyber powers.

Learn More

EastWest Senior Vice President Bruce McConnell is available to answer your questions at +1 212 824 4138 or bwm@ewi.info.

Upon request, current sponsors and other participants will provide their perspective on how they have benefitted.

EastWest maintains offices in New York, Moscow, Brussels and Washington. Our board of directors and network of engaged fellows and experts spans over 50 countries, including China, Japan, Korea, India, Pakistan and much of the Middle East and the EU.

"We are here to help make the Internet a vehicle for a safer, more peaceful, more secure, more open world—where the creative human spirit can thrive."

Bruce McConnell
Senior Vice President, EastWest Institute

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

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

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)
Chairman of the Board
Kurt Group

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

Karen Linehan Mroz (U.S.)
President
Roscommon Group Associates

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

Admiral (ret) William A. Owens (U.S.)
Chairman
Red Bison Advisory Group LLC
Chairman of the Board of Directors
CenturyLink

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
JSC Freight One (PGK)
Non-Executive Director
Vandex Company

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-FOUNDERS

John Edwin Mroz* (U.S.)
Former President and CEO
EastWest Institute

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

Supporters

Microsoft
Huawei Technologies
NXP Semiconductors
CenturyLink
Hewlett-Packard
ZEIT-Stiftung Ebelin und Gerd Bucerius
PricewaterhouseCoopers
Goldman Sachs
Senatsverwaltung für Justiz und Verbraucherschutz Berlin
Observer Research Foundation
Oxford Analytica

2014 Summit Co-hosted by

Federal Republic of Germany
Foreign Office

Partner

IEEE

IEEE COMMUNICATIONS SOCIETY

Media Partners

SCIENTIFIC AMERICAN™

NEWEUROPE

The European
DAS DEBATTEN-MAGAZIN

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