EastWest INSTITUTE

Global Cooperation in Cyberspace Initiative

2016-2017 Action Agenda

—

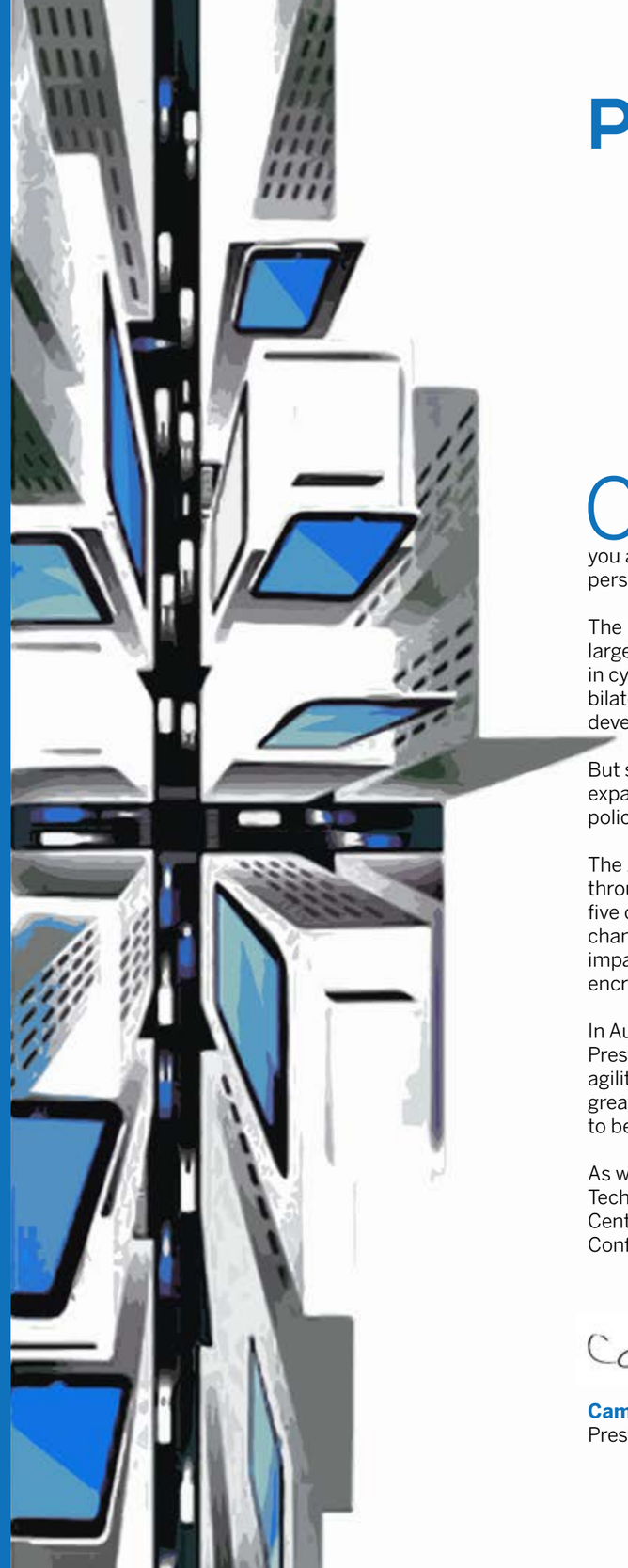
The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow, Washington, D.C. and San Francisco.

—

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

—

communications@eastwest.ngo
www.eastwest.ngo



President's Letter

Security and stability in cyberspace require unconventional approaches that transcend conventional bilateral and regional methods and that directly engage the private sector in developing security policy.

Cyberspace is an essential infrastructure for business and government worldwide. Vicious cyber attacks are now a daily occurrence, making the global digital environment increasingly unpredictable and unstable. Whether you are responsible for governance, business, or simply monitoring your own personal information, cyber risk is extremely difficult to evaluate and manage.

The EastWest Institute's Global Cooperation in Cyberspace Initiative is now its largest program. This growth has come in part because security and stability in cyberspace require unconventional approaches that transcend conventional bilateral and regional methods and that directly engage the private sector in developing security policy.

But size is not necessarily an indicator of relevance. The terrain of cyber risk is expanding and changing so rapidly that issues can appear and disappear before policy can respond.

The *2014-2015 Action Agenda* laid out seven areas of work to be conducted through our volunteer breakthrough groups. Their diligent efforts have moved five of them forward to a point where policy development will be replaced by change advocacy. This success enables us to focus in on new areas, including the impacts of the coming "Internet of Everything," and of the ubiquitous availability of encryption.

In August 2015, as I began my tenure as the EastWest Institute's second CEO and President in its 35-year history, I have challenged all our programs to increase their agility by looking further into the future. In the words of the Canadian ice hockey great Wayne Gretzky, I've asked the programs to "skate to where the puck is going to be." Our cyber program has fully embraced the challenge.

As we move into 2016-2017, we thank our 2015 supporters—Microsoft, Huawei Technologies, Palo Alto Networks, NXP Semiconductors, Qihoo 360, Unisys, CenturyLink, The William and Flora Hewlett Foundation and the Munich Security Conference—without whom this important work would not be possible.

Cameron Munter
President and CEO, EastWest Institute

Global Cooperation in Cyberspace: An Overview

For 35 years the EastWest Institute (EWI) has worked to prevent dangerous international conflict by building trust. Conflict is looming in cyberspace, where existing national and international institutions, laws, norms and the technology itself appear inadequate to address rapidly increasing risks.

Whether the venue is a quiet strategy discussion with a senior official at one of a dozen global cyber powers, or a convocation of international experts focused on a specific technology-policy gap, EWI helps drive solutions.

Since 2009, EWI has conducted a global dialogue on cyberspace security, diplomacy and deterrence. Our global network of technology and policy experts, senior government cyber officials, and business and civil society leaders envisions and works to create new institutions, processes and policies to improve the safety and security of cyberspace.

The foundation of EastWest's success is our proven trust-building process—Convene, Reframe, Mobilize. We **convene** discreet conversations across governments and private institutions who might otherwise not meet. We help them **reframe** difficult questions and devise win-win approaches. We then **mobilize** support for the results to make change happen, working through our extensive networks of key individuals in capitals and corporate headquarters around the world. Whether the venue is a quiet strategy discussion with a senior official at one of a dozen global cyber powers, or a convocation of international experts focused on a specific technology-policy gap, EWI helps drive solutions.

The Uneasy Cyber Environment

Three developments raise the stakes in our work for cyberspace security and stability.

First, because of long overdue recognition of the enormous value that is at risk in the digital world, the topic of cybersecurity has moved from the back office to boardrooms and prime ministers' offices worldwide. This shift increases demand for credible and clear articulation of the way forward through a morass that combines geopolitical hype, geek-speak, unverifiable claims, and the Wild West. Many boards are becoming educated about their cyber risk exposure and how to manage it. EWI is responding by speaking about cyber in language familiar to senior management.[1]
But even with this new awareness, senior management's responses for the most part conjure the image of people building smarter and safer cabanas on a beach that will soon experience a cybersecurity tsunami—the Internet of Everything.

This is the second development. As Harvard's Michael Porter has observed, "smart, connected devices" create new strategic choices around how to use, manage and protect the extensive, sensitive data these devices generate. These devices challenge traditional roles and relationships within and across industries and governments.[2] As information ("big data") becomes ubiquitous, the nature of channels and constituents will morph in ways we do not fully understand. Smart, connected devices are also changing the impact of the Internet. The introduction of connected intelligence into the objects of everyday life—drones, cars, chopsticks that sense what you are eating—introduces an unmatched set of security threats, vulnerabilities and potential consequences. The risks go well beyond personal safety, to the destabilization of traditional security alliances through unattributable attacks and miscalculations, and, potentially lead to greater constraints on individual freedom. EWI is responding by identifying new areas of security risk engendered by the exploding connection of smart devices in everyday life.

The third development is geopolitical. The longstanding struggle between the network's democratizing political influence and its potential as a tool to manage behavior from the center is now being joined in earnest. On the freedom side, increased transparency, individual empowerment, and support for collaboration across boundaries continue to challenge industrial age and post-war organizational paradigms at all levels.
On the control side, the collection and use of data to understand deeply how and where citizens and consumers spend their time, what and who they care about, and how they make decisions, is de-bunking the Western belief that economic democracy leads inevitably to political freedom. This tension is heightened by growing concern in the West, particularly Europe, about terrorist use of the Internet for education, recruitment and operational planning. The Internet has thus become a proxy, and a catalyst, for a larger global conversation and disagreement around political, cultural and social values. EWI is responding with continuing work to maintain efficient information and technology flows across borders, consistent with local values.

The 2016-2017 Agenda

The Global Cooperation in Cyberspace Initiative anticipates future security risks, defines the outlines of potential conflict, and brings together the people who can do something about it. Our breakthrough groups continue to be the center of our work to develop practical approaches to tough cyberspace challenges. These international teams meet online, on the phone, and in person to develop recommendations that we then advocate for adoption in the capitals and headquarters of the world's major cyber powers, both government and corporate.

In the months ahead, we will make measurable progress towards three goals:

- Enhance **deterrence** against malicious cyber activities.
- Improve the **security** of Internet products and services.
- Maintain efficient information and technology **flows** across borders consistent with local values.

Six breakthrough groups will carry over or complete work they began in 2014-2015, with a view that each group will help advance one or more of these goals. In addition, we are turning our focus to two new challenges where the international aspects are underappreciated. First, we have redirected our work on transparency and surveillance to focus it on the spread of what former U.S. Secretary of Homeland Security Michael Chertoff has called "ubiquitous encryption,"[3] a development that is a boon to companies and individuals that want to keep their information

"The need for cooperation increases with each new breach and with each new app that millions have come to depend on. As with so many hard global issues, we are all in this together."

Bruce W. McConnell
Global Vice President, EastWest Institute

1 See: Cybersecurity Risks and Rewards: How Much Should CEOs Worry about Cybersecurity? What Should CEOs Do to Minimize Risk? (https://cybersummit.info/sites/cybersummit.info/files/CIRP_Cybersecurity%20Risks%20and%20Rewards_SummitVI.pdf), September 2015, EastWest Institute; and, Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, co-authored by Palo Alto Networks (www.paloaltonetworks.com) and available at www.securityroundtable.org.

2 See: How Smart, Connected Products Are Transforming Competition (https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition/ar/1), Michael E. Porter and James E. Heppelmann, Harvard Business Review, November 2014; and, Cars—Hardware or Software?, (http://www.marketplace.org/topics/business/final-note/cars-hardware-or-software) Kai Ryssdal, Marketplace, May 21, 2015, 16:00.

3 See: Why the Fear over Ubiquitous Data Encryption Is Overblown (https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html). Chertoff, M., Lynn, W., & McConnell, M., The Washington Post, July 28, 2015.

private, and a headache for law enforcement and intelligence around the world. The U.S. will debate the issue well into 2016 with a policy decision unlikely before the arrival of a new president. Similar debates are occurring in Europe and Asia. But the problem cannot be resolved by any single nation or group of nations. Working through our networks, EWI will develop and deliver an international perspective to those debates. We will also begin exploring new areas of security risk engendered by the exploding connection of smart devices in everyday life.

More information about these breakthrough groups, topics, and plans is contained in the table on pages 8-9.

In-person convening is core to EWI's mission success. In 2016 we will work with partner organizations to co-host working sessions on: the geopolitics of cybersecurity cooperation at the Munich Security Conference; security as a non-tariff trade barrier with the World Trade Organization and the International Telecommunication Union; cooperation against cyber-enabled crime with the Russian International Affairs Council; and, international encryption policy with a variety of partners in Europe. We will also conduct a mid-year strategic review at The William and Flora Hewlett Foundation in Palo Alto.

We intend to forego hosting a major EWI cyber summit in 2016, in favor of smaller, more focused meetings. We find these co-hosted meetings to be more productive for policy development and advocacy. However, there is still value, for networking and cross-pollination, of a larger meeting, which we will do in spring 2017.

Finally, to better align with ongoing global shifts in influence and power, EWI is expanding the range of its cyberspace initiative by establishing a center in San Francisco.

We continue to position EWI as a global leader in international cyberspace cooperation in the context of extremely rapid change in the global policy and technology environment.

"To what extent does the Internet pose a threat to the legitimacy and the capability of the state?"

Cameron Munter
President and CEO, EastWest Institute

2015: Reports and Successes

Read all our reports at:
www.eastwest.ngo/issues/cyberspace

In 2015, EWI followed the methods of work that have led to such past successes as shortened repair times for undersea cables, a global reduction in spam, and agreements between the U.S. and Russia and China to build bilateral confidence and trust, improve crisis response and combat malicious hackers. We benefitted from excellent cooperation from governments, companies, nonprofits and individuals around the world. These experts and officials participated in our breakthrough groups and summit and provided informal advice and perspectives throughout the year.

EWI convened its sixth successful Global Cyberspace Cooperation Summit in New York in September—200 people, 36 countries—representing governments, companies, academia and civil society. We also co-hosted four smaller meetings focused on specific topics or players (including crime and Russia) with partners ranging from the government of the Netherlands to The William and Flora Hewlett Foundation. And we delivered our message speaking in front of nearly 10,000 cyber leaders at a dozen conferences.

After the summit we reported results from three of the breakthrough groups, recommending that governments and companies take specific actions in the areas of:

- Increasing the Global Availability and Use of Secure ICT Products and Services
- Promoting Measures of Restraint in Cyber Armaments
- Modernizing International Procedures against Cyber-enabled Crimes

We continued to talk quietly with governments to build increased trust and understanding, in the long tradition of EWI. For example, the Obama-Xi agreements of September 2015 reflect a better appreciation among the parties of each other's viewpoints and perspectives. They create an umbrella for real cooperation in responding to cyber attacks coming from servers located in the U.S. or China and directed at the other party.

Five Ways to Increase the Security of Cyber Products and Services

The availability of secure information and communications technology (ICT) products and services has tended to lag behind ICTs' worldwide spread and society's increased dependence on them. This situation creates risks to public safety, national security, privacy and economic viability.

This report, stemming from the Breakthrough Group on Increasing the Global Availability and Use of Secure ICT Products and Services, analyzes feedback received from the group's 2015 request for input on preferences and principles that are important to both suppliers and buyers in the ICT community. The report acts as a summary of findings thus far, and will be built on in 2016 to provide practical guideposts for evaluating and enhancing the security of ICT products and services. These guideposts will then be used to seek international support by private organizations and governments for these principles and the transparent use of such standards and best practices.

This breakthrough group, headed by leaders within the ICT community, continues to explore 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.

Learn more at www.cybersummit.info/2015/breakthroughs/increasing-global-availability-and-use-secure-ict-products-and-services#5ways.

Promoting International Cyber Norms: A New Advocacy Forum

The proliferation of cyber weapons is on the rise and threatens the stability of international order, particularly when critical infrastructure may become a target. Civilians are at risk due to lack of agreements on restraint during cyber conflicts and the uncertainties surrounding the extension of international law in cyberspace.

This report examines the roles of non-governmental actors within the realm of cyber norms, an area dominated by business and government definitions. It argues that "governments have long recognized the need to partner with business and civil society in framing new approaches to international norms and normative behavior in cyberspace…The international community now has a unique opportunity to ramp up its efforts." To this end, it advocates for the creation of a forum that would integrate private, public and nonprofit sector ideas.

Written by EWI Professorial Fellow Greg Austin and EWI Global Vice President Bruce McConnell, this report supports the work of EWI's Breakthrough Group on Promoting Measures of Restraint in Cyber Armaments.

Learn more at www.eastwest.ngo/idea/slowing-cyber-arms-race.

Convicting More Cyber Criminals

The EWI Breakthrough Group on Modernizing International Procedures against Cyber-enabled Crimes is working to combat crime and criminals in cyberspace by improving cooperation among law enforcement agencies and with the private sector on a global basis. In 2015, the group focused on increasing the transparency of corporate policies responding to information requests from law enforcement, and promoting a standard format for international information requests under mutual legal assistance procedures.

The report, *Convicting More Cyber Criminals: Faster, Better Responses to International Law Enforcement Assistance Requests in Connection with Cyber-enabled Crimes through Corporate Transparency Notices and Online Tool for Authoring Assistance Requests*, provides a guideline form for those law enforcement officials seeking access to records from the private sector. It advocates that private companies in possession of relevant data to an ongoing criminal investigation should post a policy based on the Model Corporate Transparency Notice.

The report also outlines the United Nations Office on Drugs and Crime's (UNODC) "Mutual Legal Assistance Request Writer Tool" as the most advanced authoring tool today and recommends ways in which it can be improved, including to encourage states to actively participate in the tool's development and to make the tool public so that companies and civil society may also provide useful feedback.

Learn more at www.eastwest.ngo/idea/convicting-more-cyber-criminals.

Breakthrough Groups: Areas of Work

	Breakthrough Group	Context, Premise, Scope	2015 Accomplishments	2016-2017 Goals
New Work 2016-2017	**Ubiquitous Encryption and Lawful Government Access**	As strong encryption becomes the norm for data in motion and at rest, data owners are more secure, but law enforcement organizations can face difficulty in lawful access to plaintext to combat crime and conduct investigations. Solutions must balance overall security and economic effects on a global basis.	Convened public and private discussions involving key government and industry representatives. Secured buy-in to contribute an international perspective to national debates.	Conduct an international workshop on approaches to balancing the security impacts of encryption, develop recommendations, and advocate for action in capitals and corporate headquarters.
	Anticipating Security Risks from Smart, Connected Devices	The introduction of connected intelligence into the objects of everyday life—drones, cars, chopsticks—introduces an unprecedented set of security threats, vulnerabilities, and potential consequences. These risks affect personal safety, warfighting norms, and individual freedom.	Identified the issue and began informal discussions.	Anticipate emerging international security impacts of the rapid spread of smart, connected devices. Identify a small number of technologies that could be suitable for commercial and political risk-reduction measures.
	Strengthening Critical Infrastructure Resilience and Preparedness	The growing digitization and interconnection of critical infrastructures increases the risk of accidental or deliberate cyber disruptions. An action-oriented, interactive, community-based platform will enable critical infrastructure owners and operators to share stories and good practices worldwide.	Developed a concept, work plan and expanded stakeholder population to create and populate a platform for international sharing about cyber risk to critical infrastructure and good practices to mitigating risk.	Launch the platform. Recruit members from critical infrastructure owners and operators worldwide who will share stories and good practices.
Work Moving to Advocacy in 2016	**Increasing the Global Availability and Use of Secure ICT Products and Services**	Governments and enterprises are demanding that ICT products and services have sufficient integrity to support critical business and mission functions. The ICT marketplace thrives on technological innovation that leverages resources globally. These forces can be synergistic if approached holistically and objectively.	Published principles for governments, ICT providers and suppliers, including: open, fair markets; objective, transparent procurement requirements based on international security standards; and commitments not to undermine the security of products and services.	Create guidance based on standards, practices and risk management approaches to enable ICT buyers to evaluate and acquire secure ICT products and services objectively, confidently and consistent with their risk management profiles.
	Promoting Measures of Restraint in Cyber Armaments	The cyber arms race is destabilizing to international order. A standing forum involving the private sector and civil society could develop and advocate norms. A "mutual cyber assistance request" protocol would enhance state-to-state cooperation and trust in cyber incident response.	Recommended the creation of a non-governmental forum to develop and promote the adoption of emerging consensus norms of state behavior in cyberspace, initially focused on peacetime.	Collaborate to make such a forum into a reality. Develop and advocate for a model "mutual cyber assistance request" protocol.
	Governing and Managing the Internet	Existing governance models for Internet policy and operations are under challenge as the demography of cyberspace changes. New models can be developed that demonstrate greater legitimacy, requiring effectiveness, transparency, and constituent alignment.	Developed middle-ground proposals that recognize both the importance of the multi-stakeholder influence model and the unique responsibility and accountability of states.	Circulate and socialize middle ground approaches and advocate for them in appropriate international and multi-stakeholder forums.
	Modernizing International Procedures against Cyber-enabled Crimes	Annual losses from cyber-enabled crime exceed $375 billion. Cross-border legal cooperation is slow, including between law enforcement and corporations. Increased transparency of corporate response policies and a standard format for mutual legal assistance requests will help speed investigations and increase convictions.	Published a "Model Corporate Transparency Notice" to improve the effectiveness of law enforcement-corporate communications. Supported work by the United Nations Office on Drugs and Crime (UNODC) to increase efficiency in writing mutual legal assistance requests.	Convince key Internet companies to post transparency notices that help assist law enforcement connect effectively with the company. Encourage governments to work with the UNODC to refine and promote its automated request-writing assistance tool. Encourage UNODC to make the tool public.
	Managing Objectionable Electronic Content Across National Borders	Security concerns are causing government entities to block or filter access to locally objectionable content. Improved cooperation between private sector Internet platforms and law enforcement officials will better enable local laws and customs to be respected while maintaining information flows.	Identified the Internet & Jurisdiction Project as the premier effort to broker cross-jurisdiction information takedown requests where the content is illegal in one jurisdiction and not in the other.	Continue to collaborate with and advocate for the Internet & Jurisdiction Project.

2015 Events

"In the future, ensuring that data can be used correctly and properly will be a very important issue."

Yao Li
Engineer, National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)

From top left to bottom right: Katherine Getao; Joseph S. Nye, Jr.; Robert Shlegel; Ryuichi Hirano; Udo Helmbrecht; Frédérick Douzet; Astrid Stuth Cevallos; Dr. Chris C. Demchak; Christopher Painter; Yao Li; Thomas Fitschen; Kamlesh Bajaj; Scott Charney; Sorin Ducaru

Palo Alto, May 2015

Breakthrough group leaders met to discuss their progress with fellow cyber experts from business, government and academia at a working roundtable in Palo Alto, hosted by the EastWest Institute and The William and Flora Hewlett Foundation.

Thirty-six participants from ten countries compared perspectives to refine the initiative's existing work program and explore additional areas for action. Contributions from government organizations and think tanks from China, Russia, Europe and India allowed for a global consideration of the tasks at hand. At the heart of Silicon Valley, the roundtable also brought opportunities for private-public partnerships. Initiative supporters—Microsoft, Huawei Technologies, Palo Alto Networks, NXP Semiconductors, Unisys and The Open Group—exhibited their continued leadership in developing the ideas for a safer, more secure Internet, as well as building momentum behind them.

The frank discussions ensured that the breakthrough groups can not only maneuver within a fraught international atmosphere, but helped expand what can be accomplished. Past work was strengthened and goals were set for the sixth Global Cyberspace Cooperation Summit.

New York, September 2015

The EastWest Institute hosted its sixth Global Cyberspace Cooperation Summit in New York City on September 9-10.

The summit provided a forum for global leaders to frame obstacles and forge progress towards a cyberspace shaped and secured for an increasingly connected world. In keynote speeches, plenary panel discussions and breakthrough group meetings, 200 participants from 36 countries represented the growing concerns of business, government, technology and civil society over the future of cyberspace.

"It's so easy for citizens to lose trust in their governments and corporations as a result of negative cyber incidents; that is the biggest risk that governments must address in this realm."

Katherine Getao
ICT Secretary, Ministry of Information, Communications and Technology of Kenya

"The world needs a better way to manage cybersecurity risks. The answer lies in globally accepted cybersecurity norms of behavior for nation states, vendor transparency and increased user control."

Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation

"None of us, alone, can be better informed, smarter, stronger and better protected than all of us, together, as an Alliance."

Sorin Ducaru
Assistant Secretary General, Emerging Security Challenges, NATO

"How do we create a safe space where the Internet touches things that could affect the health and safety of civilians?"

Davis Hake
Director of Cybersecurity Strategy, Palo Alto Networks

"We've been arguing the encryption debate too much on the basis of 'anecdata.'"

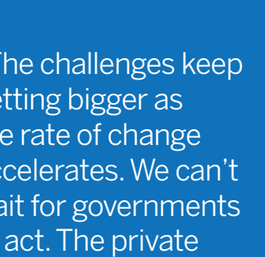
Susan Landau
Professor, Cybersecurity Policy, Worcester Polytechnic Institute; Visiting Professor, Computer Science, University College London

"We tend to lose sight of the enormous interconnectedness and positive developments that cyberspace has brought to our lives."

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

"The challenges keep getting bigger as the rate of change accelerates. We can't wait for governments to act. The private sector must."

Admiral (ret.) William A. Owens
Chairman, Red Bison Advisory Group LLC; Chairman, Board of Directors, CenturyLink; Member, Board of Directors, EastWest Institute



Microsoft's Corporate Vice President Scott Charney stated that it was timely to apply conceptual frameworks to foster a more substantive norms debate. He described three "buckets of norms"—offensive, defensive and industry—and highlighted areas where the different stakeholders anchoring these norms could converge. From the private sector perspective, norms are critical for business continuity, by safeguarding the global information and communications technology (ICT) supply chain and ecosystem. He reiterated that "We have to think about the right fora for each category of norms, and be clear about the outcomes we want from those norms."

Concerned about the inability of states to combat criminal uses of the Internet, Russian State Duma Member Robert Shlegel urged the creation of credible international legal mechanisms in cyberspace. The currently championed multi-stakeholder model of Internet governance is vague and powerless, he mused, "an imitation of Internet governance rather than an effective solution." Without more concrete developments, he warned that states may take a more defensive stance in cyberspace, ultimately turning the Internet into "a network of walls."

Retired Admiral William Owens, Chairman of the Board of CenturyLink, stressed that it was incumbent on leaders in the global ICT industry to address cybersecurity challenges indigenously ahead of the curve. The accelerating rate of technological change, industry's provision of secure ICT to enterprises, and the ensuing burden of liability, were key considerations that should motivate industry "self-protection." Drawing on examples in the nuclear industry, he proposed giving thought to the application of solutions and frameworks for self-regulation "to address the new world that demands industry gets involved to handle its own problems."

The summit thrived on the support and leadership provided by the initiative's supporters—Microsoft, Huawei Technologies, Palo Alto Networks, NXP Semiconductors, Qihoo 360, Unisys, CenturyLink and The William and Flora Hewlett Foundation—as well as by its partners—the IEEE Communications Society, the Munich Security Conference, The Open Group and the University of New South Wales.

Summit participants convened to further the work of six EWI breakthrough groups:

- Increasing the Global Availability and Use of Secure ICT Products and Services
- Managing Objectionable Electronic Content Across National Borders
- 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

"One big challenge in cyberspace discussions is the failure to take action on agreed common interests and principles. The EastWest Institute provides a premier platform to come together and drive change."

Donald (Andy) Purdy
Chief Security Officer, Huawei Technologies USA

From top left to bottom right: Davis Hake; Sadie Creese; Fred Teng; Susan Landau; Matt Bross; Robert Anderson, Jr.; Andy Purdy; Sally Long; Latha Reddy; Bertrand de La Chapelle; Admiral (ret.) William A. Owens; Robert N. Campbell; Gib Godwin; Joanna Świątkowska

2015 Side Meetings

Global Conference on CyberSpace (GCCS)
The Hague, April 16-17
Promoting Measures of Restraint in Cyber Armaments

Ninth International Forum, "State, Civil Society and Business Partnership on International Information Security"
Garmisch, April 20-23
Governing and Managing the Internet

Octopus Conference
Strasbourg, June 17-19
Modernizing International Procedures against Cyber-enabled Crimes

From top left to bottom right: Anthony Moyegun; Suzanne E. Spaulding; Greg Austin; Zhang Xinhua; Michael O'Reirdan; Tom Patterson; Angela McKay; Lt. General (ret.) Harry D. Raduege, Jr.; John E. Savage; Samir Saran; Ilya Rogachev; Sami Nassar; Karen Linehan Mroz

Plenary panel sessions included:

Is Cooperation Possible in Cyberspace?

As our dependence on cyberspace deepens, so does the tension between the approaches of nations to secure it. How is cooperation possible in this environment? Representatives of major cyber powers—France, Germany, Japan, Russia, and the U.S.—discussed what can be done in concert to calm the waters and help cyberspace reach its potential.

Global Encryption—Will It Make Us Safer?

Many cloud service providers and device manufacturers are enabling the encryption of user data to protect themselves and their users. This development raises concerns with law enforcement and intelligence officials regarding their ability to prevent and respond to security threats. The panel examined the trade-off between information security and legitimate government access.

The Internet and the State

The interplay between state sovereignty, national and international law, and the boundary-crossing nature of the Internet challenges the state's autonomy within national borders. Meanwhile, Internet governance conversations seek an elusive middle ground between multi-lateral and multi-stakeholder models. The panel examined the limits of the state and explored other models for effectiveness, accountability and alignment with constituent values.

Young Cyber Leaders Look Ahead

Young professionals working on critical cyberspace issues shared their reflections on the summit and its relevance to the most pressing problems facing cyberspace today and in the future.

Privacy in the Age of Surveillance

The unexpected scope of personal data collection by governments and companies is fracturing longstanding partnerships among international players. This panel focused on ways to enhance individual privacy while recognizing the continued need of governments and corporations to collect and use personal data.

Breakthrough Group Outcomes and Next Steps

Breakthrough group representatives reported on the results from summit sessions and work done throughout the year, focusing on proposed next steps. A distinguished panel then shared its reflections. Further information on the 2016-2017 work plan can be found on pages 8-9.

Finally, two special interest groups convened:

Two-Factor Authentication examined progress and methods to widen the usage of this security practice.

Government Access to Plaintext Information examined tradeoffs associated with mechanisms to provide authorized government agencies with access to the plaintext version of encrypted information.

"As a global technology provider, we have a focus on the cross-border components of critical infrastructure – that's EWI's sweet spot."

Tom Patterson
Vice President and General Manager, Global Security Solutions, Unisys

"Privacy protection is essential for the trust that is the coin of the realm."

Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security

"Every day we see an increase in critical services and data moving to the cloud and it is crucial that we protect this information. Secure element ICs revolutionized security for banking cards, ePassports and mobile payment. Today, through the FIDO U2F authentication protocol, these secure elements bring a new level of privacy and security to enterprise networks and consumer cloud services."

Sami Nassar
Vice President and General Manager, Cyber Security Solutions, NXP Semiconductors

"Agreeing on a set of rules of conduct of states in cyberspace becomes more and more important."

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

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.

How Can You 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:**

Key civil society organizations and academics can offer their thought leadership and broaden their networks and perspectives.

Sitting at the table with the policy and business decision-makers shaping the global future of the Internet.

Taking advantage of high-level networking and new business opportunities.

Raising your company's profile and enhancing its reputation and brand recognition.

Gaining up-to-the minute market and policy intelligence.

The summit and ongoing breakthrough group dialogues enable you to showcase your thought leadership with speaking platforms and white papers.

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 Global Vice President Bruce McConnell is available to answer your questions at +1 212 824 4138 or bwm@eastwest.ngo.

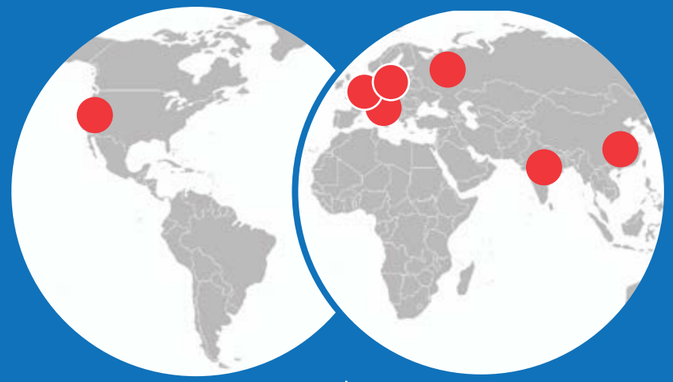
–

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

–

EastWest maintains offices in New York, Moscow, Brussels, Washington and San Francisco. 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.

2016 Events



- Cybersecurity Roundtable, Munich Security Conference — **Munich** February 2016
- International Encryption Policy Workshop — **The Hague** May 2016
- High-Level Dialogue on Cyberspace Cooperation Co-hosted by the Russian International Affairs Council — **Moscow** May 2016
- Global Cooperation in Cyberspace Progress Roundtable — **Palo Alto** June 2016
- Security as a Non-Tariff Trade Barrier Roundtable Co-hosted by the International Telecommunication Union and the World Trade Organization — **Geneva** September 2016
- Workshop on Security Risks of the Internet of Everything — **United States** Fall 2016
- Trilateral Cybersecurity Track 2 — **Asia** Fall 2016

EWI Board of Directors

OFFICE OF THE CHAIRMAN

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
Dentons US LLP

Cameron Munter (U.S.)
CEO and President
EastWest Institute
Former Ambassador
Embassy of the United States to Pakistan

CO-FOUNDERS

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

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

MEMBERS

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

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

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

Michael Chertoff (U.S.)
Executive Chairman and Co-Founder
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.)
Founder and Managing Director
GH Venture Partners LLC

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)
Professor
The Institute for Peace Science at Hiroshima University
Former Permanent Representative
Permanent Mission of Japan to the United Nations

Ronald P. O'Hanley (U.S.)
President & CEO
State Street Global Advisors

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

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)
Former 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

CHAIRMEN EMERITI

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

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

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

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.

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Former Senior Executive Vice President
Central National-Gottesman 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 Cooperation in Cyberspace Initiative

SUPPORTERS

Microsoft
Huawei Technologies
Palo Alto Networks
NXP Semiconductors
Qihoo 360
Unisys
CenturyLink
The William and Flora Hewlett Foundation

PARTNERS

IEEE Communications Society
Internet & Jurisdiction Project
Munich Security Conference
The Open Group
The University of New South Wales

Building Trust Delivering Solutions

The EastWest Institute works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability. We forge new connections and build trust among global leaders and influencers, help create practical new ideas, and take action through our network of global decision-makers. Independent and nonprofit since our founding in 1980, we have offices in New York, Brussels, Moscow, Washington, D.C. and San Francisco. Learn more at **www.eastwest.ngo**.

EWInstitute EastWestInstitute