EastWest INSTITUTE

Global Cyberspace Cooperation Summit VI

New York 2015

September 9 – 10, 2015

Agenda

The EastWest Institute is proudly hosting the 2015 Global Cyberspace Cooperation Summit in New York City.

EWI's Global Cooperation in Cyberspace Initiative is convening policymakers, business leaders, technical experts and civil society with the objective to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion.

This invitation-only meeting of international actors aims to coordinate and consolidate the initiative's progress, showcase results and promote collective action. The annual cyber summits provide a crucial forum for building international, private-public action to foster international cooperation in cyberspace. Breakthrough groups, aligned with the initiative's objectives of economic and political development, digital security and stability, and sound governance and management, carry the program forward.

Global Cyberspace Cooperation Summit VI
New York 2015
September 9-10, 2015

The Westin New York at Times Square
270 West 43rd Street
New York, NY 10036
USA

September 9, 2015

08:00-09:00   Registration

09:00-09:15   Welcome

09:15-09:35   Keynote Address

09:35-09:55   Breakthrough Group Progress Update

09:55-11:25   Plenary Panel I: Is Cooperation Possible in Cyberspace?

As the scope and depth of our dependence on cyberspace increase, so do the risks posed to the confidentiality, integrity and availability of electronic information and services. Nations and corporations strive to protect their most critical information assets in the face of actual and potential criminal, terrorist and military attacks from every side. How is cooperation possible in this increasingly tense environment? Representatives of major cyber powers – public and private – will discuss what they can do in concert to calm the waters and help cyberspace realize its full potential for economic and social benefit.

11:25-11:50   Networking Break

11:50-12:50   Keynote Conversation

12:50-14:00   Lunch

14:00-15:30   Breakthrough and Special Interest Groups - Session I

Promoting Measures of Restraint in Cyber Armaments

The cyber arms race among major powers has a destabilizing effect on 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 developing recommendations that would stimulate the creation of a standing forum involving private sector and civil society for norms research and advocacy. It is examining areas of emerging consensus on norms of state behavior across governments and intergovernmental organizations. Finally, it is developing a "mutual cyber assistance request" protocol to enhance state-to-state cooperation on cyber incidents, as a confidence building measure.

Modernizing International Procedures against Cyber-enabled Crimes

Global losses from cyber-enabled crimes likely exceed $400 billion annually. Progress on identifying, prosecuting and punishing cyber criminals across borders is slow. In particular, better cooperation is essential between law enforcement and the private sector on a global basis. This group is focusing on: (i) increasing the transparency of corporate response policies; (ii) developing a standard format for information requests under mutual legal assistance procedures. This session will review progress on these initiatives and plan for future success.

Strengthening Critical Infrastructure Resilience and Preparedness

The growing digitization and interconnection of society, and in particular critical infrastructures, increase the risk of accidental or deliberate cyber disruptions. This group is focused on the development of an action-oriented, interactive, community-based platform where critical infrastructure owners and operators can share stories related to cyber incidents. The platform will serve as an awareness and education resource. This session will present and refine the concept, provide feedback and roll out the work program.

Two-Factor Authentication

While most would agree it is time to "kill the password dead," adoption of two-factor authentication is slow. How can EWI help accelerate this improvement? This session will review the work of the FIDO (Fast IDentity Online) Alliance and explore alternatives for accelerating progress on a global scale.

15:30-16:00   Networking Break

16:00-17:30   Breakthrough and Special Interest Groups - Session II

Increasing the Global Availability and Use of Secure ICT Products and Services

Governments and enterprises globally are increasingly concerned about the availability of ICT products and services that have sufficient integrity to support critical business and mission functions. One major challenge derives from the nature of the ICT marketplace, which thrives on technological innovation and development that leverages resources from all over the world. This group's objective is to enable the availability and use of more secure ICT

products and services. For providers in the ICT supply chain, the group promotes the use of recognized and proven international standards and best practices that improve product and service integrity. For buyers of ICT, the group fosters procurement practices founded on those same standards and best practices. It also works to prevent and, where necessary, break down trade barriers so that buyers can identify and utilize trusted providers regardless of their locale. The session will present the results of a survey of ICT vendors and buyers and discuss the action plan going forward.

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.

Managing Objectionable Electronic Content Across National Borders

Security concerns about Internet content are causing government entities to block or filter access to locally objectionable content and the websites it appears on. 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. This session will explore ways of increasing cooperation between private sector Internet platforms and law enforcement officials to better enable local laws and customs to be respected.

Government Access to Plaintext Information

This session will explore the tradeoffs associated with mechanisms to provide authorized government agencies with access to the plaintext version of encrypted information. It will examine the context in which decisions about such mechanisms would be made and identify and characterize possible mechanisms and means of obtaining information sought by the government for law enforcement or intelligence investigations. It will discuss ways to characterize risks so that they could be weighed against the potential law enforcement or intelligence benefits.

17:30-18:30   Reception

September 10, 2015

08:30-09:00	Registration
09:00-09:10	**Welcome and Report Back from Day I**
09:10-09:30	**Keynote Address**
09:30-10:40	**Plenary Panel II: 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 significant concerns among law enforcement and intelligence officials that the spread of strong encryption will reduce their ability to anticipate, prevent or investigate serious crimes, terrorist activities and military threats. The panel will examine the tradeoffs between information security and legitimate government access.

10:40-11:10	Networking Break
11:10-12:20	**Plenary Panel III: 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 will examine the limits of the state and will explore other models that are effective, accountable and aligned with constituent values.

12:20-12:40	**Keynote Address**
12:40-13:40	Lunch

13:40-14:00   **Keynote Address**

14:00-14:50   **Plenary Panel IV: Young Cyber Leaders Look Ahead**

This panel will feature young professionals working on critical cyberspace issues. Panelists will share their reflections on the summit and its relevance to the most pressing problems facing cyberspace today and in the future.

14:50-15:20   Networking Break

15:20-15:40   **Keynote Address**

15:40-16:25   **Plenary Panel V: 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 will focus on ways to enhance individual privacy while recognizing the continued need of governments and corporations to collect and use personal data.

16:25-17:45   **Plenary Panel VI: Breakthrough Group Outcomes and Next Steps**

Breakthrough group representatives will report on the results from summit sessions and work done throughout the year, focusing on proposed next steps. They will be followed by reflections from a distinguished panel.

SUPPORTERS

Microsoft
Huawei Technologies
Palo Alto Networks
NXP Semiconductors
Qihoo 360
Unisys
CenturyLink

PARTNERS

IEEE Communications Society
Munich Security Conference
The Open Group

EastWest
INSTITUTE

New York

Brussels

Moscow

Washington, D.C.

ewi.info
@EWInstitute
#EWIcyber