Global Cooperation in Cyberspace Initiative
June 2015 Update

The strategic objective of the Global Cooperation in Cyberspace Initiative is to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion. The EastWest Institute (EWI) is working over a three year period, 2014-2016, to: 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; and strengthen the institutional framework that governs the Internet.

May 28 Roundtable

On May 28 in Palo Alto, hosted by the William and Flora Hewlett Foundation, 36 global cyber cooperation leaders from 10 countries met to discuss the initiative's work streams and examine gaps and synergies among them. As summarized below, the initiative's priorities and work programs have been updated in preparation for the **Global Cyberspace Cooperation Summit VI** in **New York, September 9-10, 2015**.

Breakthrough Group Progress and Near-Term Plans

The Global Cooperation in Cyberspace Initiative uses EWI's proven process—Convene, Reframe, Mobilize—to achieve its objectives. This work is taking place through working groups—called breakthrough groups—that convene in person and online. As a result of the Palo Alto meeting, near-term plans for the seven existing breakthrough groups include:

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

- Seek broad feedback on draft principles and approaches that buyers, including governments, can use to communicate security preferences to ICT product and service vendors.
- ***At the Summit:*** present refined principles and approaches.
- Issue a draft guidance document by the end of 2015.

Modernizing International Procedures against Cyber-enabled Crimes

- ***At the Summit:*** Present best practices for corporations' responses to requests for assistance from foreign law enforcement officials investigating cyber-enabled crimes.
- ***At the Summit:*** Present a draft uniform format for assistance requests made under Mutual Law Enforcement Assistance Treaty (MLAT) auspices.
- Develop model protocols, including single points of contact, for mutual assistance.

For more information and to participate: www.ewi.info/cyber or email us at cyber@ewi.info.

Promoting Measures of Restraint in Cyber Armaments

- ***At the Summit:*** Present a summary of emerging consensus norms for state behavior in cyberspace under development by governmental and multi-stakeholder groups.
- ***At the Summit:*** Propose a non-governmental structure for the regular review and advocacy of such norms.
- Develop a standard protocol for state-to-state requests for post-incident assistance.
- Continue work to identify key elements of critical information infrastructure that should be off-limits for state-on-state cyber attacks.
- Examine deterrent effects of such norms on non-state actors.

Governing and Managing the Internet

- ***At the Summit:*** Propose a middle-road model and structure for governance that incorporates multi-stakeholder and multi-lateral elements.
- Continue to elaborate and refine the proposed approach.

Strengthening Critical Infrastructure Resilience and Preparedness

- ***At the Summit:*** Promote the usefulness of exercises with C-level participants that explore cross-border impacts of cyber attacks on critical information infrastructure.
- Continue work to develop cross-border exercise scenarios.

Managing Objectionable Electronic Content Across National Borders

- ***At the Summit:*** Announce a formal partnership with the Internet Jurisdiction Project regarding the development and promotion of protocols for requesting and responding to transnational requests for content takedown and domain seizure.
- Continue work to examine the economic technological and political consequences of content filtering and blocking.

Increasing Transparency and Accountability in Personal Data Collection

- Develop a compendium of national laws on data collection, retention and use.
- Examine the impact of private sector collection activities on individual privacy.

New Work Areas

Two additional topics were added to the initiative at the May 28 Roundtable:

Promoting Two-factor Authentication

- Publish and distribute a C-level primer on two-factor authentication and its importance in increasing security.

Managing the Spread of Encryption

- ***At the Summit:*** Explore the tradeoffs between widespread private use of strong encryption and the ability of domestic and national security authorities to perform their missions.

For more information and to participate: www.ewi.info/cyber or email us at cyber@ewi.info.