EastWest
INSTITUTE

Global Cyberspace Cooperation Summit V

December 3-5, 2014
German Foreign Office Conference Center
Berlin, Germany

DRAFT AGENDA

As of November 7, 2014

DECEMBER 3, 2014

12:30-13:30 REGISTRATION

13:30-14:10 SPECIAL REMARKS

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

Representative, United States TBD

14:15-15:45 BREAKTHROUGH GROUPS

In these interactive sessions, participants will develop recommended solutions to specific problems in cyberspace that are of high consequence but remain unsolved.

Breakthrough Group I: Exploring Surveillance, Privacy and Big Data

Recent revelations about the extent of surveillance have generated anger and are consequently disrupting longstanding partnerships. While governments and companies will continue to rely on personal data to provide security and business benefits, this breakthrough group will focus 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.

Breakthrough Group II: Strengthening Critical Infrastructure Resilience and Preparedness

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 will find ways to promote preparedness and resilience to cyber threats and address these challenges.

Breakthrough Group III: Governing and Managing the Internet

National and international Internet governance institutions are slow, weak, isolated or non-existent. Indeed, much of the work of this initiative would be unnecessary if strong Internet governance institutions existed. A variety of groups are already discussing potential approaches to improve Internet governance. This breakthrough group will analyze emerging approaches for their potential effectiveness and propose models that demonstrate agility, transparency, predictability, inclusivity and accountability.

15:45-16:15 NETWORKING BREAK

16:15-17:45 BREAKTHROUGH GROUPS

Breakthrough Group IV: Increasing the Global Availability of Secure ICT Products and Services

The availability of secure ICT products and services has not kept up with the worldwide spread of ICTs, or with society's increased dependence on them. As a result, there is little trust among users that their systems are designed and built to operate in a secure manner. This situation is untenable. This breakthrough group will explore approaches to increase the availability of secure ICT products and services, 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.

Breakthrough Group V: Modernizing International Procedures against Cyber-Enabled Crimes

Attempts to reduce the spiraling global cost of cyber-enabled crime are hampered in part by the antiquated and cumbersome procedures governing cooperation among law enforcement officials internationally. This breakthrough group will identify ways to bring 21st century techniques and tools to enhance such cooperation in the prosecution and investigation of cyber-enabled crimes.

Breakthrough Group VI: 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 will take a bottom-up approach and explore 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. The group will also develop and propose potential implementation regimes and take on other matters of potential use to the GGE.

Breakthrough Group VII: Managing Barriers to Information Flows for Innovation and Education

Concerns about Internet content that is locally inappropriate and/or illegal are causing government entities to block or filter access to such content and the websites it appears on. This approach is harmful for countries and their citizens because it limits the potential for economic growth and prosperity, restricts the flourishing of imagination, limits social interaction among people from different countries and violates people's right of freedom of expression as stated in the United Nations Declaration of Human Rights. While concerns about domestic security and stability are often valid, excessive control over content is counterproductive. This breakthrough group will seek to recognize domestic concerns while promoting the benefits of the broadest possible access to information, in particular information that will encourage and promote innovation and education.

DECEMBER 4, 2014

09:00-10:00 REGISTRATION

10:00-10:15 WELCOME REMARKS

10:15-10:35 WELCOMING KEYNOTE ADDRESS

10:40-11:00 KEYNOTE ADDRESS

11:00-11:30 NETWORKING BREAK

11:30-12:10 PLENARY PANEL I: 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 will discuss current cooperation in cyberspace and ways to improve it.

12:15-13:00 **PLENARY PANEL II: EXPLORING SURVEILLANCE, PRIVACY AND BIG DATA**

Revelations about data collection by governments and companies are generating concern and disrupting longstanding partnerships. Panelists will discuss approaches to enhancing privacy by limiting the collection and use of personal data by governments and companies.

13:00-14:15 LUNCH BUFFET

14:30-15:10 **PLENARY PANEL III: 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 will discuss potential implementation regimes where restraint in the use of cyber weapons applies to civil facilities and infrastructure.

15:15-16:30 **BREAKTHROUGH GROUPS**

Breakthrough Group I: Exploring Surveillance, Privacy and Big Data

Recent revelations about the extent of surveillance have generated anger and are consequently disrupting longstanding partnerships. While governments and companies will continue to rely on personal data to provide security and business benefits, this breakthrough group will focus 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.

Breakthrough Group II: Strengthening Critical Infrastructure Resilience and Preparedness

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 will find ways to promote preparedness and resilience to cyber threats and address these challenges.

Breakthrough Group III: Governing and Managing the Internet

National and international Internet governance institutions are slow, weak, isolated or non-existent. Indeed, much of the work of this initiative would be unnecessary if strong Internet governance institutions existed. A variety of groups are already discussing potential approaches to improve Internet governance. This breakthrough group will analyze emerging approaches for their potential effectiveness and propose models that demonstrate agility, transparency, predictability, inclusivity and accountability.

16:30-16:50 NETWORKING BREAK

16:50-18:00 BREAKTHROUGH GROUPS

Breakthrough Group IV: Increasing the Global Availability of Secure ICT Products and Services

The availability of secure ICT products and services has not kept up with the worldwide spread of ICTs, or with society's increased dependence on them. As a result, there is little trust among users that their systems are designed and built to operate in a secure manner. This situation is untenable. This breakthrough group will explore approaches to increase the availability of secure ICT products and services, 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.

Breakthrough Group V: Modernizing International Procedures against Cyber-Enabled Crimes

Attempts to reduce the spiraling global cost of cyber-enabled crime are hampered in part by the antiquated and cumbersome procedures governing cooperation among law enforcement officials internationally. This breakthrough group will identify ways to bring 21st century techniques and tools to enhance such cooperation in the prosecution and investigation of cyber-enabled crimes.

Breakthrough Group VI: 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 will take a bottom-up approach and explore 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. The working group will also develop and propose potential implementation regimes and take on other matters of potential use to the GGE.

Breakthrough Group VII: Managing Barriers to Information Flows for Innovation and Education

Concerns about Internet content that is locally inappropriate and/or illegal are causing government entities to block or filter access to such content and the websites it appears on. This approach is harmful for countries and their citizens because it limits the potential for economic growth and prosperity, restricts the flourishing of imagination, limits social interaction among people from different countries and violates people's right of freedom of expression as stated in the United Nations Declaration of Human Rights. While concerns about domestic security and stability are often valid, excessive control over content is counterproductive. This breakthrough group will seek to recognize domestic concerns while promoting the benefits of the broadest possible access to information, in particular information that will encourage and promote innovation and education.

18:30-20:00 COCKTAIL RECEPTION hosted by Berlin Senator of Justice Thomas Heilmann
Venue: Basecamp, Mittelstraße 51-53, 10117 Berlin

<u>DECEMBER 5, 2014</u>

09:00-09:30 REGISTRATION

09:30-10:30 SPECIAL INTEREST SECTIONS

- Group 1 - Whistleblower Procedures
- Group 2 - Transatlantic Partnership
- Group 3 - Industry 4.0
- Group 4 - Governing and Managing the Internet

10:30-11:00 NETWORKING BREAK

11:00-12:30 PLENARY PANEL IV: BREAKTHROUGH GROUP REPORTS AND OBSERVATIONS

Representatives of breakthrough groups will report on the results of the sessions, concentrating on proposed next steps to address critical issues in cyberspace. This will be followed by reflections from a distinguished panel.

12:30-12:50 KEYNOTE ADDRESS

12:50-13:50 LUNCH BUFFET

14:00-15:00 PLENARY PANEL V: YOUNG CYBER LEADERS RESPOND

The panel will feature young leaders and their perspectives on cyberspace issues requiring global cooperation. These panelists will report their impressions of the summit and thoughts on the way forward.

15:00-16:00 PLENARY PANEL VI: NEXT STEPS AND WAY AHEAD

The panel will feature senior stakeholder reflections on the work of the summit in enhancing international cooperation in cyberspace. In addition, the panelists will look to the future and identify the emerging policy and management issues requiring attention.