Global Cyberspace Cooperation Summit VII

March 14–16, 2017
University of California, Berkeley

Draft Agenda
As of February 7, 2017

EastWest INSTITUTE

cybersummit.info

March 14, 2017

University of California, Berkeley
Clark Kerr Campus Conference Center

Pre-Summit Workshops

The first day of the Global Cyberspace Cooperation Summit will focus on four topic areas identified in consultation with the EastWest Institute's key stakeholders and partners.

In these interactive sessions, participants from around the world will develop recommended solutions to specific high consequence problems in cyberspace that remain unsolved. Outcomes and priorities identified during the first day will feed the breakthrough group sessions on March 15.

The success of the summit will be measured by the policy breakthroughs made in these interactive working sessions over all three days and by the effectiveness of the follow-on activities of the associated breakthrough groups.

08:00-09:00 REGISTRATION

09:00-10:30 **BREAKTHROUGH GROUPS—SESSION I**

Ubiquitous Encryption and Lawful Government Access

The national debate on encryption has produced a fault line between law enforcement and industry, the latter supported by privacy and civil liberties advocates. Recognizing that no national solution in itself will be adequate, this session will explore middle ground proposals that reflect the international availability of encryption.

Resilient Cities and the Internet of Things

The introduction of connected intelligence into industrial settings and its integration into so-called "smart cities," create an unprecedented set of security risks to everyday life. This breakthrough group aims at testing two novel ideas as a means to tackle cybersecurity in resilient cities and the Internet of Things (IoT): that the proliferation of smart, interconnected devices provides an opportunity rather than a threat to cybersecurity; and that the way security is managed will necessarily shift to the network level, as the sheer number of interconnected devices makes it nearly impossible to maintain the security of endpoints. This session will chart ways to increase the cyber resilience of "smart" urban environments on a global basis, looking at ways to improve readiness, responsiveness and reinvention.

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

In September 2016, this breakthrough group published *Purchasing Secure ICT Products and Services: A Buyers Guide*, which outlines questions that ICT consumers can ask their suppliers to understand how to manage security risks, including supply chain risk, introduced into enterprises by commercial technology. This session will solicit feedback on the Guide and explore ways to address the need for security standards in the procurement of ICT products and services.

10:30-11:00 NETWORKING BREAK

11:00-12:30 **BREAKTHROUGH GROUPS—SESSION II**

Ubiquitous Encryption and Lawful Government Access *(continued)*

Resilient Cities and the Internet of Things *(continued)*

Increasing the Global Availability and Use of Secure ICT Products and Services *(continued)*

12:30-13:30 LUNCH

13:30-15:00 **BREAKTHROUGH GROUPS—SESSION III**

Ubiquitous Encryption and Lawful Government Access

The national debate on encryption has produced a fault line between law enforcement and industry, the latter supported by privacy and civil liberties advocates. Recognizing that no national solution in itself will be adequate, this session will explore middle ground proposals that reflect the international availability of encryption.

Resilient Cities and the Internet of Things

The introduction of connected intelligence into industrial settings and its integration into so-called "smart cities," create an unprecedented set of security risks to everyday life. This breakthrough group aims at testing two novel ideas as a means to tackle cybersecurity in resilient cities and the Internet of Things (IoT): that the proliferation of smart, interconnected devices provides an opportunity rather than a threat to cybersecurity; and that the way security is managed will necessarily shift to the network level, as the sheer number of interconnected devices makes it nearly impossible to maintain the security of endpoints. This session will chart ways to increase the cyber resilience of "smart" urban environments on a global basis, looking at ways to improve readiness, responsiveness and reinvention.

Systemic Risk and Cyber Insurance

Little work exists to understand systemic cyber risk to enterprises and how it can be measured and managed. Insurers and reinsurers are struggling to model risk and price policies in the face of large-scale risk to general business continuity and the potential for cascading failures. This breakthrough group will examine systemic risk beyond financial systems, its impact on general business continuity, and the implications for the insurance industry. It will develop and disseminate approaches to mitigating risk and improving loss prevention across key industries worldwide.

15:00-15:30 NETWORKING BREAK

15:30-17:00 **BREAKTHROUGH GROUPS—SESSION IV**

Ubiquitous Encryption and Lawful Government Access *(continued)*

Resilient Cities and the Internet of Things *(continued)*

Systemic Risk and Cyber Insurance *(continued)*

17:00-18:30 COCKTAIL RECEPTION

March 15, 2017

University of California, Berkeley
Clark Kerr Campus Conference Center

08:00-09:00	REGISTRATION
09:00-09:15	**WELCOME REMARKS**
09:15-09:35	**WELCOMING KEYNOTE ADDRESS**
09:35-09:50	**GLOBAL COOPERATION IN CYBERSPACE INITIATIVE: PROGRESS REPORT**
09:50-10:10	**KEYNOTE ADDRESS**
10:10-11:10	**PLENARY PANEL I: THE STATE OF CYBER 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. Given the increasing dependence on cyberspace, including through use of cloud-based software, the proliferation of smart devices through the Internet of Things, and digitized infrastructure, there is a greater need than ever for multi-party industry cooperation in order to understand the nature of these developments and create new norms of governance and policies to deal with the associated risks and security challenges. Panelists will discuss current cooperation in cyberspace, highlighting areas of progress and current obstacles, and possible ways to improve going forward.
11:10-11:30	NETWORKING BREAK
11:30-11:50	**KEYNOTE ADDRESS**
11:50-13:00	**PLENARY PANEL II: GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE**
	To be formally launched in February 2017, the Global Commission on the Stability of Cyberspace (GCSC) brings together stakeholders from the international security and cyberspace communities to develop proposals for norms and policies to guide responsible state and non-state behavior in cyberspace. Commission members will provide an early insight into its priorities and direction.
13:00-14:00	LUNCH
14:00-15:30	**BREAKTHROUGH GROUPS—SESSION I**
	Ubiquitous Encryption and Lawful Government Access
	The national debate on encryption has produced a fault line between law enforcement and industry, the latter supported by privacy and civil liberties advocates. Recognizing that no national solution in itself will be adequate, this session will explore middle ground proposals that reflect the international availability of encryption.

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

In September 2016, this breakthrough group published *Purchasing Secure ICT Products and Services: A Buyers Guide*, which outlines questions that ICT consumers can ask their suppliers to understand how to manage security risks, including supply chain risk, introduced into enterprises by commercial technology. This session will solicit feedback on the Guide and explore ways to address the need for security standards in the procurement of ICT products and services.

Promoting Norms of Responsible Behavior in Cyberspace

Global security and prosperity depend on a secure and stable cyberspace. A myriad of factors threaten equilibrium including: cyberspace's continued militarization, growing activism by non-state actors, sector based risks that require specialized knowledge, and persistent asymmetries in capability. This session will discuss multi-party norms-building processes, as well as the particular challenges that remain in bridging normative divides.

15:30-16:00 NETWORKING BREAK

16:00-17:30 BREAKTHROUGH GROUPS—SESSION II

Resilient Cities and the Internet of Things

The introduction of connected intelligence into industrial settings and its integration into so-called “smart cities,” create an unprecedented set of security risks to everyday life. This breakthrough group aims at testing two novel ideas as a means to tackle cybersecurity in resilient cities and the Internet of Things (IoT): that the proliferation of smart, interconnected devices provides an opportunity rather than a threat to cybersecurity; and that the way security is managed will necessarily shift to the network level, as the sheer number of interconnected devices makes it nearly impossible to maintain the security of endpoints. This session will chart ways to increase the cyber resilience of “smart” urban environments on a global basis, looking at ways to improve readiness, responsiveness and reinvention.

Systemic Risk and Cyber Insurance

Little work exists to understand systemic cyber risk to enterprises and how it can be measured and managed. Insurers and reinsurers are struggling to model risk and price policies in the face of large-scale risk to general business continuity and the potential for cascading failures. This breakthrough group will examine systemic risk beyond financial systems, its impact on general business continuity, and the implications for the insurance industry. It will develop and disseminate approaches to mitigating risk and improving loss prevention across key industries worldwide.

Election Systems Security

Following a contentious election in the United States which featured discussions of the cybersecurity of voting machines and political data, this session will discuss the cybersecurity threats to electoral processes, and how countries and companies might work together to address them.

17:30-19:00 COCKTAIL RECEPTION

March 16, 2017

University of California, Berkeley
Clark Kerr Campus Conference Center

08:00-09:00	REGISTRATION
09:00-09:45	**PLENARY PANEL III: INSIGHTS FROM YOUNG LEADERS** 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.
09:45-10:40	**PLENARY PANEL IV: REPORT BACK FROM BREAKTHROUGH GROUP SESSIONS & NEXT STEPS – PART I** Breakthrough group representatives will report on the results from summit sessions earlier in the week and work done throughout the year, focusing on proposed next steps. They will be followed by reflections from a distinguished panel and an opportunity for questions from the audience.
10:40-11:05	NETWORKING BREAK
11:05-12:00	**PLENARY PANEL IV: REPORT BACK FROM BREAKTHROUGH GROUP SESSIONS & NEXT STEPS – PART II** Breakthrough group representatives will report on the results from summit sessions earlier in the week and work done throughout the year, focusing on proposed next steps. They will be followed by reflections from a distinguished panel and an opportunity for questions from the audience.
12:00-12:40	**PLENARY PANEL V: TECH+PEOPLE: SECURING THE FUTURE CONNECTION** Industry executives will discuss developments in technology and security, and the implications for people, processes, and business models in the next five years.
12:40-13:00	**KEYNOTE ADDRESS**
13:00-14:00	LUNCH

Global Cooperation in Cyberspace: Building Trust, Delivering Solutions.

Global Cyberspace Cooperation Summit VII

March 14-16, 2017
University of California, Berkeley

cybersummit.info

EastWest INSTITUTE