Global Cyberspace Cooperation Summit VII

March 14-16, 2017
University of California,
Berkeley

Draft Agenda
As of March 3, 2017

EastWest
INSTITUTE

In partnership with the
Center for Long-Term Cybersecurity
University of California, Berkeley

cybersummit.info

March 14, 2017: Pre-Summit Workshops

University of California, Berkeley
Clark Kerr Campus Conference Center

The first day of the Global Cyberspace Cooperation Summit will focus on five 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.

DAY OVERVIEW:

08:00-09:00 Registration

09:00-10:30 Session I
Ubiquitous Encryption and
Lawful Government Access
Resilient Cities and the Internet of Things
Increasing the Global Availability and Use
of Secure ICT Products and Services

10:30-11:00 Networking Break

11:00-12:30 Session II
Ubiquitous Encryption and
Lawful Government Access
Resilient Cities and the Internet of Things
Increasing the Global Availability and Use
of Secure ICT Products and Services
International Stability and Cyber Capacity
Building

12:30 – 13:30 Lunch and Poster Sessions

13:30-15:00 Session III
Ubiquitous Encryption and
Lawful Government Access
Resilient Cities and the Internet of Things
Systemic Risk and Cyber Insurance
Promoting Norms of Responsible Behavior in
Cyberspace

15:00-15:30 Networking Break

15:30-17:00 Session IV
Ubiquitous Encryption and
Lawful Government Access
Resilient Cities and the Internet of Things
Systemic Risk and Cyber Insurance

17:00-18:30 Cocktail Reception

Breakthrough Groups

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.

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.

The government of the Netherlands, the EastWest Institute, and The Hague Centre for Strategic Studies formally launched the Global Commission on the Stability of Cyberspace at the Munich Security Conference in February 2017. The Commission 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.

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.

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.

08:00-09:00 REGISTRATION

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

Ubiquitous Encryption and Lawful Government Access
Workshop I: Emerging National Policies: the United States and India

This workshop focuses on the state of encryption in the United States and India with the purpose to better understand where the two states stand on encryption policy today, how they got there and where they are likely to go moving forward. The workshop will identify particular challenges and scenarios relevant to government access to encrypted data and discuss possible solutions to overcome impediments currently faced by agencies tasked to protect national security and public safety reducing negative effects on privacy and security.

Resilient Cities and the Internet of Things
Workshop I: Cyber Resilience and the Modern City

Cities across the globe are striving to increase their resilience to a wide range of social, economic and physical challenges. As cities build and implement resilience strategies, there is a growing recognition that many of their solutions rely on cyber. As a result, understanding and building city capabilities for cyber resilience is emerging as a key area of focus. This workshop brings together thought leaders from cities, technology, government, and civil society to explore the challenges, opportunities, and nascent frameworks for incorporating cyber resilience into city strategies and operations.

Increasing the Global Availability and Use of Secure ICT Products and Services
Workshop I: Cross-Organization Collaboration to Increase the Availability of Secure ICT

Various organizations have come up with guidelines, principles and standards to increase the security of information and communications technology (ICT) and emphasize the need to address supply chain risk. The EWI ICT Buyers Guide lays out principles and maps the concept of supply chain risk to existing international standards to enable ICT buyers to make security-informed procurement decisions. This workshop will review the core ideas of the ICT Buyers Guide and identify new opportunities for cross-organization collaboration to harness the efforts undertaken by an increasing number of national and international organizations to address supply chain risk in a principled manner. It aims at identifying strategic collaboration to further the development of frameworks concerned with ICT security and supply chain risk.

10:30-11:00 NETWORKING BREAK

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

Ubiquitous Encryption and Lawful Government Access
Workshop II: Emerging National Policies: Europe and a Comparative Look

Recent reports from the press observe that encryption is a factor in criminal investigations for all kinds of data and applications. European law enforcement agencies identified the lack of sufficient technical capacity to decrypt protected data as a serious barrier to accessing critical evidence in investigations. This workshop will provide a European perspective and will discuss how the legitimate interest of government access can be balanced with the rights of individuals to security and privacy, and the need for network security by ICT services and commercial users. It will also present the preliminary results of EWI research comparing encryption policies in major democracies worldwide.

Resilient Cities and the Internet of Things
Workshop II: Safer Cities: Creating the Cyber/Privacy Interlock

Security without privacy is not secure, and privacy without security is not private, but when cities architect in advanced security that protects citizen privacy by design, we can begin to build safe cities that will truly protect citizens globally. Well-intentioned and highly funded cities are already finding their infrastructure hacked and citizen privacy sacrificed. This workshop will leverage critical infrastructure protection to make cities safer, and discuss relevant resources and tools to that end. The goal is to identify best practices and paths and to start developing an open source blueprint for safer cities that optimally protect citizens' security and privacy.

Increasing the Global Availability and Use of Secure ICT Products and Services
Workshop II: International Trade and Cybersecurity

The ICT Buyers Guide is at a critical stage as EWI is pushing forward the broader adoption of the guide. EWI focuses on two approaches: (a) make ICT buyers aware of the guide and showcase ways to implement it into their existing processes; (b) enhance cybersecurity as an ICT trade issue in the appropriate international fora. In that context, this will explore how international trade frameworks, initiatives, and agreements can help drive adoption and increase the availability of secure ICT

International Stability and Cyber Capacity Building

Cyber capacity building has become part of the UN Group of Governmental Experts' discussions. The session introduces cyber capacity building as a topic for further research and discussion. It will focus on recent initiatives and the GGE's work in this area and identify the main challenges facing the international community.

12:30-13:30 LUNCH AND POSTER SESSIONS

Faculty, researchers and students of Bay Area universities and research institutions will present their ongoing and completed cybersecurity research.

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

Ubiquitous Encryption and Lawful Government Access
Workshop III: Alternative Views and Pathways in the "Going Dark" Debate

Due to the growth of default-enabled encryption schemes, law enforcement is increasingly confronted with encrypted data it lacks the ability to access, leaving cases unsolved with locked smartphones that might hold answers. Yet, new surveillance capabilities and new technologies, like the emerging Internet of Things, may drastically add more sources of unencrypted data. This workshop will consider alternative views and potential pathways in the "Going Dark" debate and discuss whether all communications data will be encrypted or otherwise be beyond the reach of law enforcement in the future, and discuss different trajectories the encryption debate may take us.

Resilient Cities and the Internet of Things
Workshop III: Improving Security through Partnership across the IoT Ecosystem

As the world’s digital infrastructure becomes increasingly interconnected, it becomes clear that cybersecurity is a fundamentally distributed challenge that companies and countries simply cannot address alone. This workshop will discuss the critical role of technology and process integration across the ecosystem in enhancing the security of the Internet of Things. With an emphasis on enterprise-level and smart city application for IoT, the discussion will bring together cybersecurity companies, service providers, and system integrators to discuss how their cross-industry partnerships are essential to securing the complex and highly distributed IoT landscape.

Systemic Risk and Cyber Insurance
Workshop I: Understanding Systemic Cyber Risk

Growing societal dependence on technology has created some questions around whether systemic cyber risk can be defined, measured, and managed. In 2016, the World Economic Forum (WEF) took initial steps towards addressing this challenge in their white paper, *Understanding Systemic Cyber Risk*, which highlighted that “large-scale cyber attacks” are a “high impact/high likelihood” risk. This workshop will begin to develop a conceptual framing for what constitutes systemic cyber risk and will use the WEF report as a baseline, to open up and deepen the discussion.

Promoting Norms of Responsible Behavior in Cyberspace

The government of the Netherlands, the EastWest Institute, and The Hague Centre for Strategic Studies formally launched the Global Commission on the Stability of Cyberspace at the Munich Security Conference in February 2017. The Commission 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. This session will discuss the universalization of emerging cyber norms and the role of multi-party norms-building processes. In particular, Commissioners will solicit feedback from experts regarding the elaboration of cyber norms.

15:00-15:30 NETWORKING BREAK

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

Ubiquitous Encryption and Lawful Government Access
Workshop IV: Government Hacking: Law, Policy, and the Future

Government hacking is one proposed alternative to mandating exceptional access for law enforcement. In the United States, law enforcement has used exploits to investigate suspects for over a decade, most recently in the so-called "Playpen" cases. However, regulation of this law enforcement technique is slow to catch up to practice. Recent changes to federal criminal procedure rules now expressly authorize the issuance of a "warrant to hack" in certain circumstances. This workshop reviews the present state of the law and explores technical and policy debates with regard to government hacking and discusses the feasibility of government hacking as a middle ground solution to the encryption debate.

Resilient Cities and the Internet of Things

Workshop IV: Security as an IoT Market Differentiator: The Role of Venture Capitalists in Incentivizing Better Security across the IoT Ecosystem

Much of the current global policy discussion around the Internet of Things has been focused on finding incentives that promote better security. This workshop will bring together key thought leaders from the venture capital and technology start up community to discuss the role of one powerful and well-established incentive—investment capital—in driving higher levels of the security across the IoT ecosystem. It will discuss the emerging global trends in IoT investment, the role for security to be a market differentiating factor in the future, and how thoughtful government policy can shape this landscape.

Systemic Risk and Cyber Insurance

Workshop II: Underwriting Systemic Cyber Risk

The insurance industry helps firms mitigate and transfer emerging risk. Through the underwriting process, market incentives can identify best practices across industries and drive behavioral change and loss prevention. However, systemic cyber risk presents a unique challenge for the insurance industry. This workshop will examine how the insurance industry currently addresses the underwriting in the context of systemic cyber risk, how a prolonged service failure for myriad companies would impact business and in turn the insurance industry and how the adoption of new technologies or the retention of legacy systems affects systemic risk. In addition, it will examine the interplay of industry with government to determine whether a regulatory mechanism can be used to protect against a systemic event challenging financial stability within the insurance industry.

17:00-18:30 COCKTAIL RECEPTION

March 15, 2017

University of California, Berkeley
Clark Kerr Campus Conference Center

08:00-09:00	REGISTRATION
09:00-09:10	**WELCOME REMARKS**
09:10-09:25	**WELCOMING KEYNOTE ADDRESS**
09:25-09:40	**GLOBAL COOPERATION IN CYBERSPACE INITIATIVE: PROGRESS REPORT**
09:40-10:00	**KEYNOTE ADDRESS**
10:00-11:20	**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.
11:20-11:40	NETWORKING BREAK
11:40-12:10	**KEYNOTE CONVERSATION**
12:10-13:00	**PLENARY PANEL II: GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE**
	The government of the Netherlands, the EastWest Institute, and The Hague Centre for Strategic Studies formally launched the Global Commission on the Stability of Cyberspace at the Munich Security Conference in February 2017. The Commission 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. During this panel discussion, Commission members will provide early insights 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. With the participation of members of the Global Commission on the Stability of Cyberspace, this session will discuss emerging norms and multi-party norms-building processes.

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

09:00-09:15 PROGRESS REPORT FROM WEDNESDAY MARCH 15

09:15-10:00 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.

10:00-10:40 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.

10:40-11:00 NETWORKING BREAK

11:00-11:30 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.

11:30-11:45 KEYNOTE ADDRESS

11:45-12:35 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.

12:35-13:00 KEYNOTE CONVERSATION

13:00-14:00 LUNCH

Global Cooperation in Cyberspace Initiative

Supporters:

Microsoft
Huawei Technologies
Unisys
Sonus Networks
Palo Alto Networks
Qihoo 360
NXP Semiconductors
CenturyLink
VimpelCom
The Hague Centre for Strategic Studies
William and Flora Hewlett Foundation

Partners:

IEEE Communications Society
Munich Security Conference
The Open Group
Fudan University
University of New South Wales
Webster University Cyberspace Research Institute
Center for Long-Term Cybersecurity, University of California, Berkeley

Global Cyberspace Cooperation Summit VII

March 14-16, 2017
University of California, Berkeley

cybersummit.info

EastWest
INSTITUTE