BUILDING TRUST IN CYBERSPACE

3rd WORLDWIDE CYBERSECURITY SUMMIT IN NEW DELHI

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

www.ewi.info

3RD WORLDWIDE CYBERSECURITY SUMMIT
NEW DELHI
2012

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

On the cover: “Where The Internet Lives," Google data center

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, Moscow and Washington, D.C.

For more information about the EastWest Institute or this publication, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info

www.ewi.info

SUMMIT CO-SPONSOR

IEEE

IEEE COMMUNICATIONS SOCIETY

SUMMIT PARTNERS

FICCI

NASSCOM

DSCI
PROMOTING DATA PROTECTION

SUMMIT PRIVATE SECTOR PARTNERS

TIER 1

Reliance
Industries Limited
Growth is Life

Microsoft

vodafone

HUAWEI

Goldman Sachs

KNIGHTSBRIDGE
CYBERSYSTEMS

Deloitte.

TIER 2

airtel

RELIANCE
Communications

FT
FINANCIAL
TIMES

Fidelity
INVESTMENTS

!dea

at&t

AKIN GUMP
STRAUSS HAUER & FELD LLP

STROZ FRIEDBERG

TATA COMMUNICATIONS

TIER 3

steria

FLUXONIX
Inducing Innovation

Laurus
Edutech
SKILL INDIA

MEDIA PARTNERS

technology
review
Published by MIT

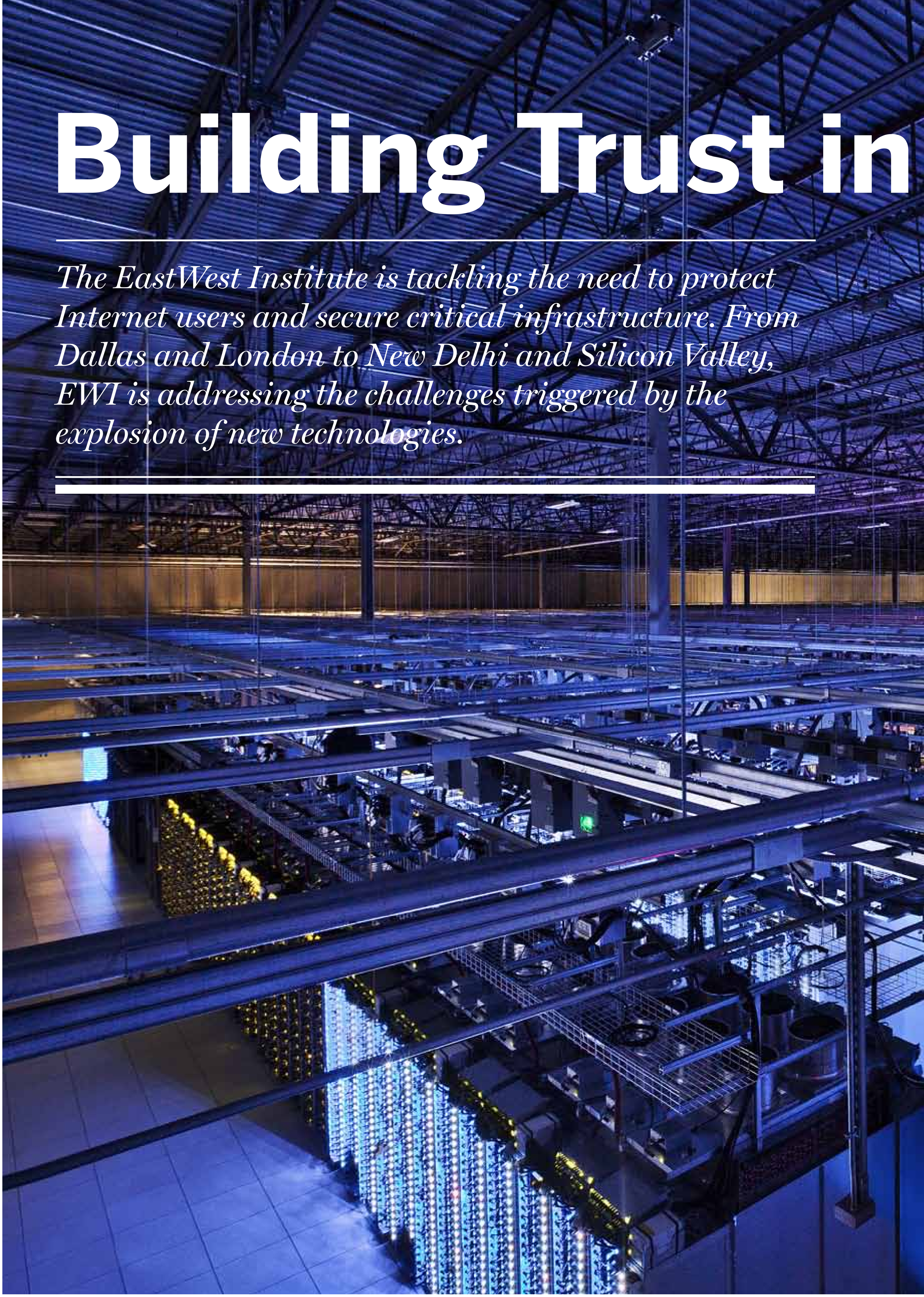
DATAQUEST

PARTNER

TeleGeography

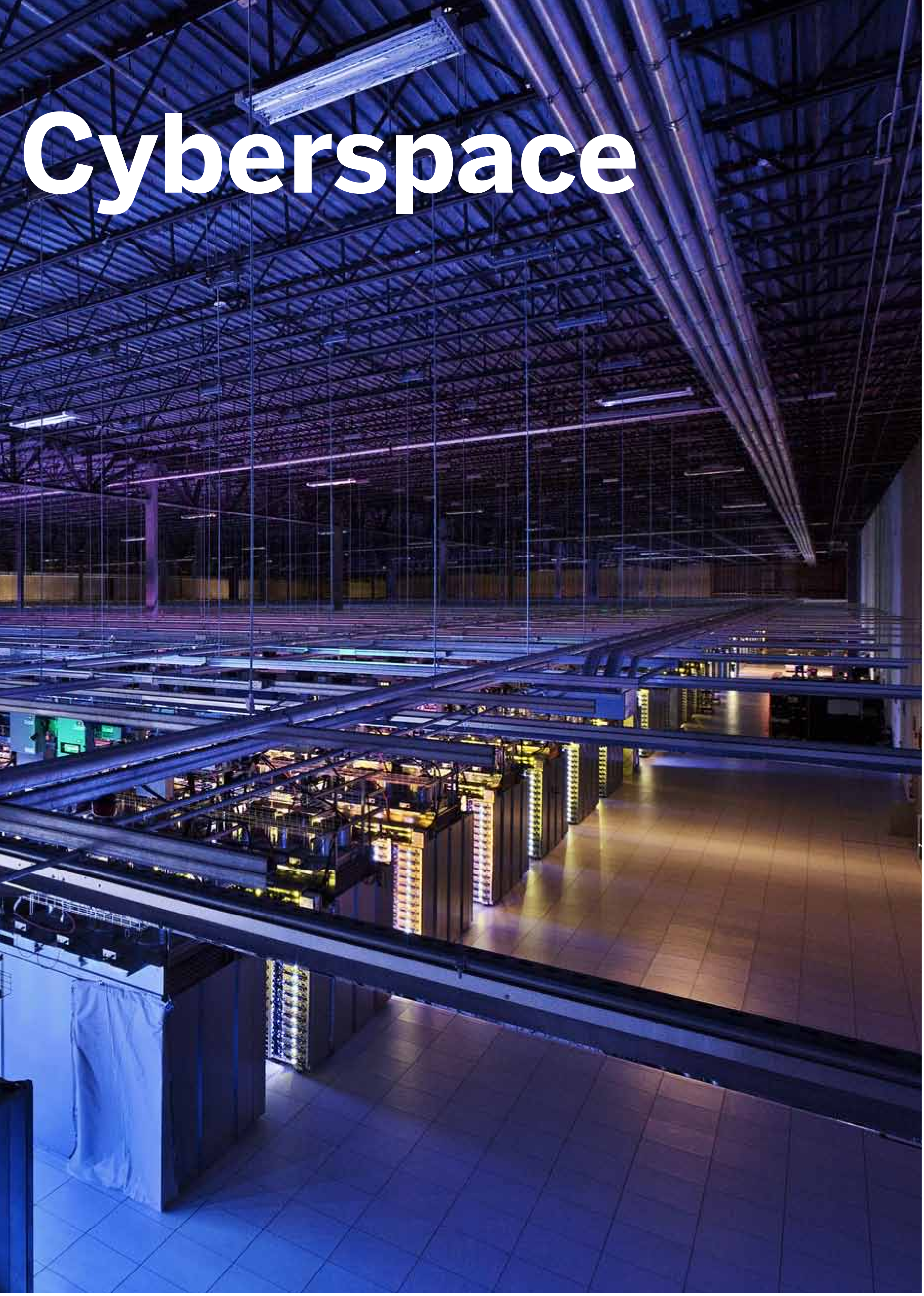
Building Trust in

The EastWest Institute is tackling the need to protect Internet users and secure critical infrastructure. From Dallas and London to New Delhi and Silicon Valley, EWI is addressing the challenges triggered by the explosion of new technologies.



Google data center

Cyberspace



SCHMIDT
WORLDWIDE CYBERSECURITY SUMMIT
WORLDWIDE CYBERSECURITY SUMMIT
WELCOME

In the span of three years, the magnitude of the cybersecurity problem has grown exponentially. Each day brings headlines of new breaches, resulting in staggering losses. Some are purely criminal in nature, while others involve far more complex schemes of cyber espionage and cyber sabotage. We live in an age when hundreds of viruses—with names like Stuxnet, Flame and Shamoon—are threatening to wreak havoc on both the private and public sectors across the globe. Most fundamentally, such actions are undermining international trust at every level.

Former U.S. Secretary of Homeland Security Michael Chertoff, a member of EWI's board of directors, summed up the cybersecurity problem this way: "What we have now learned over the last 10 or 20 years, is that you cannot assume trust. That is why we're dealing with a persistent problem of criminality, theft of intellectual property and even efforts to sabotage or damage our infrastructure using the Internet."

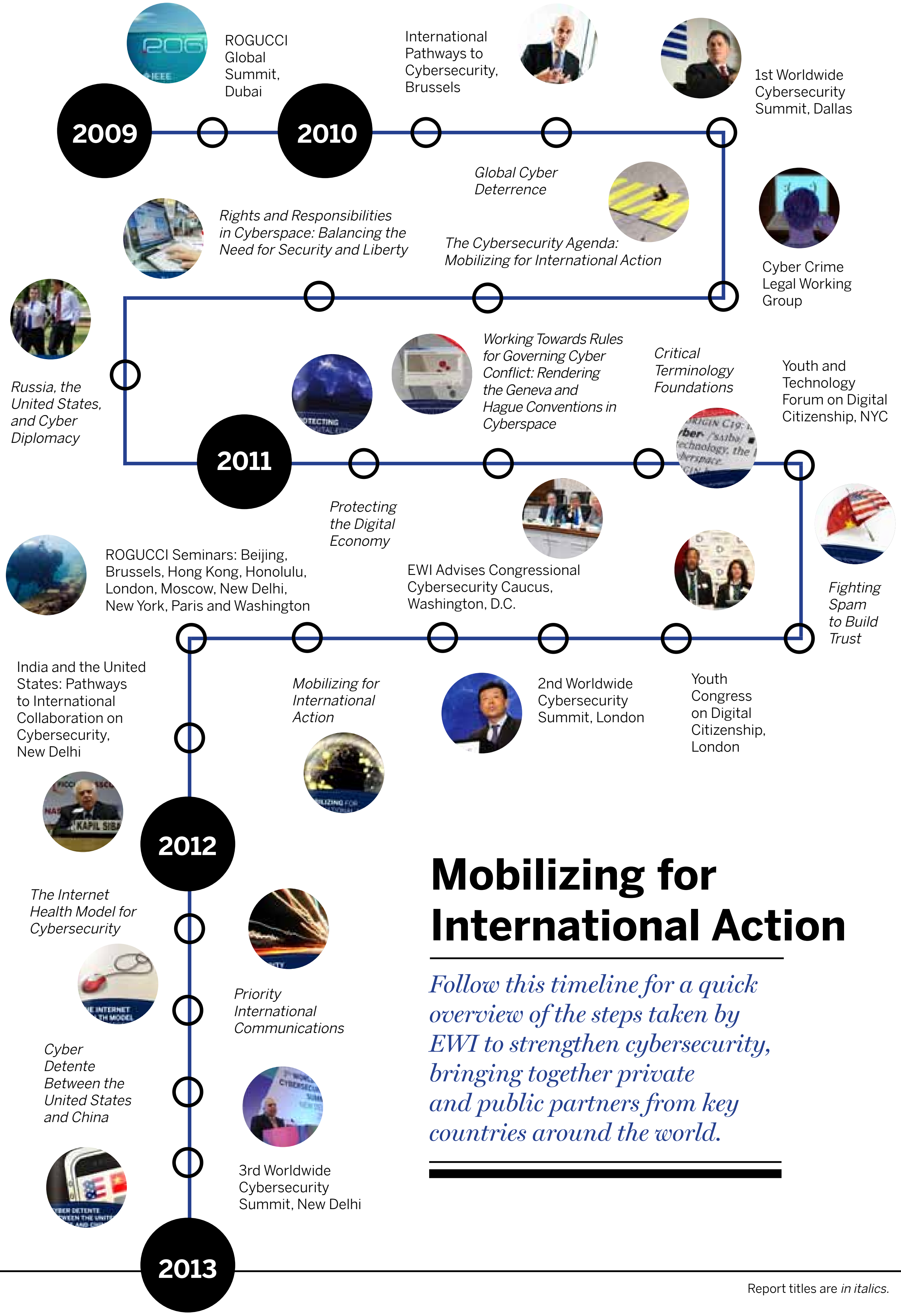
All of which underscores the point that securing cyberspace is a global challenge—one that cannot be solved by a single company or country on its own. That is why the EastWest Institute launched the Worldwide Cybersecurity Initiative, bringing together government and corporate partners to protect the world's digital infrastructure. Experts from across the globe agree that progress in cybersecurity will only be achieved through trust-building among nations and between the private and public sectors. With a 30-year history of trust-building that dates back to the Cold War era, EWI is uniquely positioned to propel that effort.

"What we have now learned over the last 10 or 20 years, is that you cannot assume trust. That is why we're dealing with a persistent problem of criminality, theft of intellectual property and even efforts to sabotage or damage our infrastructure using the Internet."

- Michael Chertoff

To do so, EWI began hosting annual Worldwide Cybersecurity Summits, kick-starting an ongoing process to propose solutions to specific problems. The first summit, "Protecting the Digital Economy," took place in 2010 in Dallas where a broad spectrum of experts from the United States, Russia, China, India and other nations discussed the limitations of current cyber legislation and identified top priorities for the EWI cybersecurity agenda. The top six issues: protecting undersea cable infrastructure; priority international-

Above, from the top:
Dallas 2010, London 2011, New Delhi 2012



2009

ROGUCCI Global Summit, Dubai

2010

International Pathways to Cybersecurity, Brussels

Global Cyber Deterrence

1st Worldwide Cybersecurity Summit, Dallas

Cyber Crime Legal Working Group

The Cybersecurity Agenda: Mobilizing for International Action

Rights and Responsibilities in Cyberspace: Balancing the Need for Security and Liberty

Russia, the United States, and Cyber Diplomacy

2011

Protecting the Digital Economy

Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace

Critical Terminology Foundations

Youth and Technology Forum on Digital Citizenship, NYC

Fighting Spam to Build Trust

Youth Congress on Digital Citizenship, London

2nd Worldwide Cybersecurity Summit, London

EWI Advises Congressional Cybersecurity Caucus, Washington, D.C.

Mobilizing for International Action

ROGUCCI Seminars: Beijing, Brussels, Hong Kong, Honolulu, London, Moscow, New Delhi, New York, Paris and Washington

India and the United States: Pathways to International Collaboration on Cybersecurity, New Delhi

2012

The Internet Health Model for Cybersecurity

Priority International Communications

Cyber Detente Between the United States and China

3rd Worldwide Cybersecurity Summit, New Delhi

2013

Mobilizing for International Action

Follow this timeline for a quick overview of the steps taken by EWI to strengthen cybersecurity, bringing together private and public partners from key countries around the world.

Report titles are *in italics*.

communications; conflict policy and rules of engagement; cybersecurity breach information sharing; ICT development/supply chain integrity; and emergency response coordination capability.

The Dallas summit launched a series of breakthrough groups—small international groups of experts committed to addressing specific cybersecurity threats. It also resulted in new Track 2 bilateral processes with experts from the United States and Russia to develop "rules of the road" for cyber conflicts, and experts from the United States and China to produce joint recommendations for fighting spam and botnets. Such processes continue throughout the year—culminating at the summits where the next practical steps are mapped out.

The London summit in 2011, "Mobilizing for International Action," built on the work of the Dallas summit, with meetings of existing breakthrough groups and informal opportunities for cross-sector collaboration. Specific recommendations were advanced for international connectivity and emegency preparedness of the financial services sector.

Experts from across the globe agree that progress in cybersecurity will only be achieved through trust-building among nations and between the private and public sectors. With a 30-year history of trust-building that dates back to the Cold War era, EWI is uniquely positioned to propel that effort.

"The Next Billion Netizens Connect" was the theme of EWI's third summit in 2012 in New Delhi, which continued this process. This location underscores India's rapid emergence as a key player on cybersecurity issues.

Three breakthrough groups were chosen for the New Delhi summit in consultation with the Indian government and private sector leaders: ICT development/supply chain integrity; the role of international companies in cloud computing and storage; and payload security. At the New Delhi summit, leading Indian and Chinese cyber experts declared their commitment to increased cooperation between their two countries, particularly between their Computer Emergency Readiness Teams (CERTs). This offered a concrete example of the kind of trust-building EWI is working to promote.

EWI has already begun planning for its fourth summit, to be held in Silicon Valley in November 2013. It will be called the 4th Worldwide Cybersecurity Trustbuilding Summit—and will bring together innovators with global leaders to address cross-border challenges. From Dallas to London to New Delhi and Silicon Valley, the search for practical solutions continues.

Above: "Where The Internet Lives," Google data center

Delivering Solutions

The chart and select examples below show the progress on EWI's cybersecurity recommendations to date. The institute considers a recommendation as having entered the implementation stage when the first "required commitments" are made and "next steps" taken. It moves to the "institutionalization" stage when private companies, governments or NGOs have integrated the recommendation into their work to achieve sustainability.

27 2010-12: **Recommendations produced**

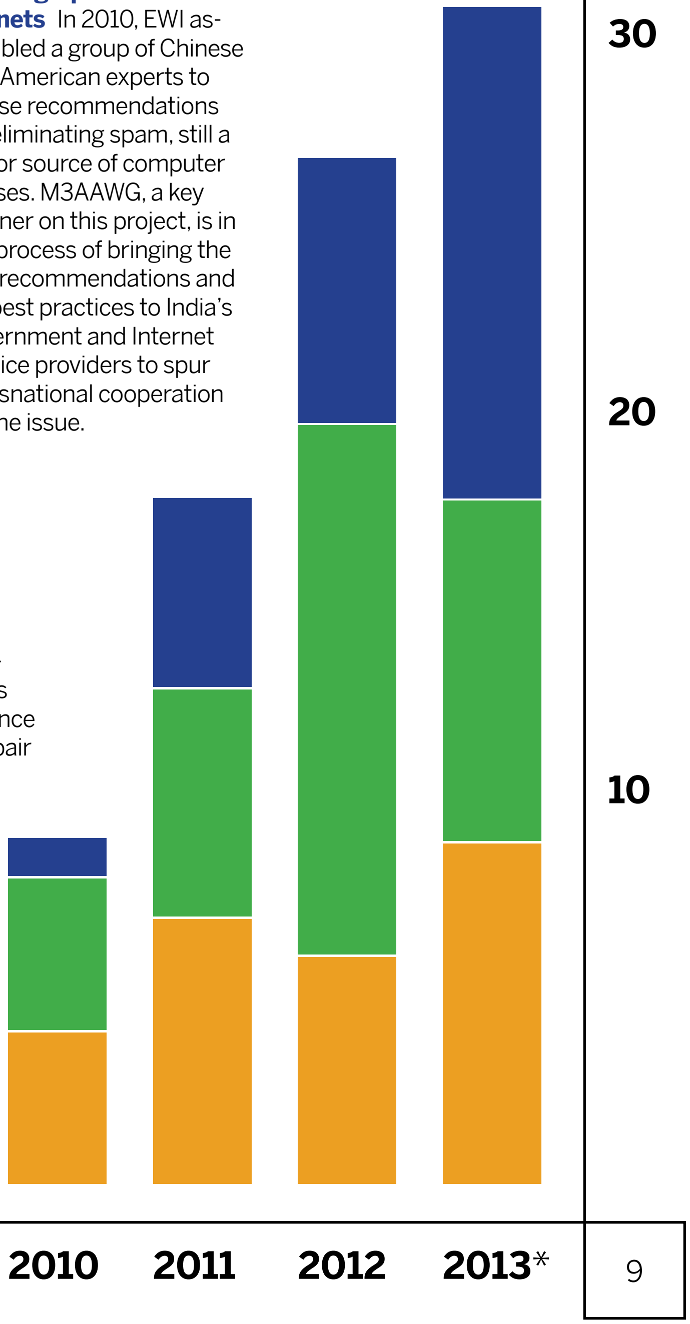
14 52% **Implemented**

7 26% **Institutionalized**

Fighting Spam and Botnets In 2010, EWI assembled a group of Chinese and American experts to devise recommendations for eliminating spam, still a major source of computer viruses. M3AAWG, a key partner on this project, is in the process of bringing the two recommendations and 46 best practices to India's government and Internet service providers to spur transnational cooperation on the issue.

Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Undersea communications cables are responsible for carrying over 99 percent of all international Internet traffic. Due in part to EWI's work in the field, India's government has committed to achieving best-in-class performance for authorizing the repair of these cables. Under new policies, repair time will be reduced from 12 weeks to a few days.

Measuring the Cybersecurity Problem
In 2013, EWI will advocate for the establishment of an independent, trusted entity to receive reports on private sector cybersecurity breaches. Once companies have committed to contributing information anonymously, this entity will be able to establish benchmarks, delivering the clearest picture yet of the cybersecurity problem.

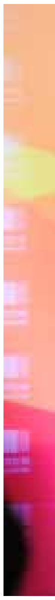


* Projection

New Delhi 2012

At the 3rd Worldwide Cybersecurity Summit in New Delhi, more than 300 participants from 22 countries heard from an impressive international line-up of cyber experts and policy strategists from both the private and public sectors.

3rd WORLDWIDE
CYBERSECURITY
SUMMIT
NEW DELHI
2012



The focus of the New Delhi summit was on areas where international cooperation is vital—and the vulnerabilities pose serious risks. EastWest Institute President John Mroz declared: “We are here for a purpose—to build trust and find solutions together.” He pointed out that the two previous annual summits in Dallas and London have led to the implementation of 52 percent of the 27 recommendations that came out of those consultations. “This is a process, not just a conference,” he added.

The conference’s location was no accident. “We are all in the room today because we recognize that India is an essential partner on cybersecurity,” said Ross Perot, Jr., chairman of the EastWest Institute.

High-ranking Indian officials—among them, Deputy National Security Advisor Latha Reddy and Secretary R. Chandrashekhar of the Department of Telecommunications—not only participated in the summit but also helped frame key issues on the agenda. In addition, the EastWest Institute partnered with the National Association of Software and Service Companies (NASSCOM), the Federation of Indian Chambers of Commerce and Industry (FICCI) and the Data Security Council of India (DSCI), which sponsored three breakthrough groups. The topics were chosen in consultation with the Indian government and private sector leaders.

"It is no longer a question of a nation protecting its own security; it’s a question of the global community protecting itself. India pledges to work with the global community.”

- Kapil Sibal

Kapil Sibal, India’s Minister for Communications and Information Technology, appealed for “a global agreement” on how to protect the key infrastructure of the digital world. Pointing out that for the first time in human history everyone is operating from the same platform, Sibal declared: “It is no longer a question of a nation protecting its own security; it’s a question of the

Above, from left:
Kapil Sibal, India's Minister for Communications and IT; EWI Chairman Ross Perot, Jr.;
EWI President and CEO John Edwin Mroz; Punit Renjen, Chairman of the Board, Deloitte LLP

global community protecting itself." He called for a new understanding about what constitutes cyber crime and how to combat it, including the idea of empowering "cyber justices" in the future who would adjudicate such cases. "India pledges to work with the global community," he added.

While there were mixed reactions to Sibal's proposals, most participants agreed that the rapid pace of technological change has triggered a corresponding leap in exposure to vulnerabilities that can be exploited by cyber criminals. But some proposed solutions have also raised fears about government intrusion that could threaten privacy and individual freedoms.

Erin Nealy Cox, Executive Managing Director at Stroz Friedberg, pointed out that companies often lack basic information on the cybersecurity problems they face. "CEOs need more metrics in this area," she said, arguing that without such information much of the spending on cybersecurity could prove ineffective.

"EWI has certainly provided leadership by serving as a catalyst for collective transnational action."

- Punit Renjen

In his concluding keynote address, Deloitte's Indian-born Chairman of the Board Punit Renjen commended EWI's decision to hold the summit in New Delhi. "India has a cyber vision that is grand and it is bold," he said, pointing to the way the Internet has lifted millions from poverty. But he also noted that most of the population still lacks connectivity, and cyber crime is already taking a heavy toll, with an estimated $6 billion in annual losses in India and $400 billion worldwide. "Right now it seems that the bad guys are winning," he said.

"This is a great, great challenge; that's why these summits are so important," Renjen continued. "EWI has certainly provided leadership by serving as a catalyst for collective transnational action."

“We like to use the term that we ‘leapfrogged’ in technology, because in a sense our whole industrial revolution has been compressed into 60 years, what other countries took 100, 200, 250 years to do. We started off with almost no industry when we became independent in 1947, except for a textile industry, which had actually been driven into the ground by the introduction of a lot of imported textiles. So we really had to start from scratch. Particularly with the IT technology, cyber technology, we did leapfrog.”

LATHA REDDY

DEPUTY NATIONAL SECURITY ADVISOR, INDIA

“I think we’re entering an age of interdependence. More and more, nations of the world are becoming dependent on each other, with economies, with security, with opportunities. An industrial age has moved into an information age, and now we’re going into an interdependence age. Not one country or one company can solve the issues of cybersecurity alone.”

HARRY D. RADUEGE, JR.

LT. GENERAL (RET.), CHAIRMAN, DELOITTE CENTER FOR CYBER INNOVATION

"Just imagine how the world and society would function if every three to five minutes, our cell phones would ring. Today, we are aware of spam whenever we open our mailbox; a good 30 to 40 percent is spam, despite the special filters that are applied. Imagine what could happen if it were to occur on the voice side: we'd all go mad."

J. SATYANARAYANA

SECRETARY, DEPARTMENT OF ELECTRONICS AND IT, MINISTRY OF COMMUNICATIONS AND IT, INDIA

"We had very good talks with Dr. Rai on how to improve cooperation between China and India's computer emergency response teams. We can help each other to stop the threats."

ZHOU YONGLIN

DIRECTOR, INTERNET SOCIETY OF CHINA

"The more you frighten people, the less people will use technology that drives the economy forward."

JOHN SUFFOLK

GLOBAL CYBER SECURITY OFFICER, HUAWEI

"Cyberspace is not a lawless space, but a space where laws do apply and where there are constraints on state behavior. That's one part of it. The second part is the practical things we can do to build better confidence, better transparency, better cooperation and, ultimately, better stability. The point here is to avoid conflict and to make sure that conflict doesn't benefit any state."

CHRISTOPHER PAINTER

COORDINATOR FOR CYBER ISSUES, U.S. DEPARTMENT OF STATE

"We have to act fast to catch up to the development of hacking technology."

TORU NAKAYA

DIRECTOR-GENERAL, INSTITUTE FOR INFORMATION AND COMMUNICATIONS POLICY (IICP), MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS, JAPAN

"I think private sector CEOs need more metrics in this area. One would agree that a CEO would not be making a sound decision if he just went on his own sense of whether he was making profits, or he felt like his return on investment was good. He's going to want to rely on solid metrics, and I think in the area of cybersecurity and risk, we ought to expect metrics as well."

ERIN NEALY COX

EXECUTIVE MANAGING DIRECTOR, STROZ FRIEDBERG

"I do believe that apart from having closed communication networks, which connect key people, it is important to be able to have a layer of priority communication in the public network."

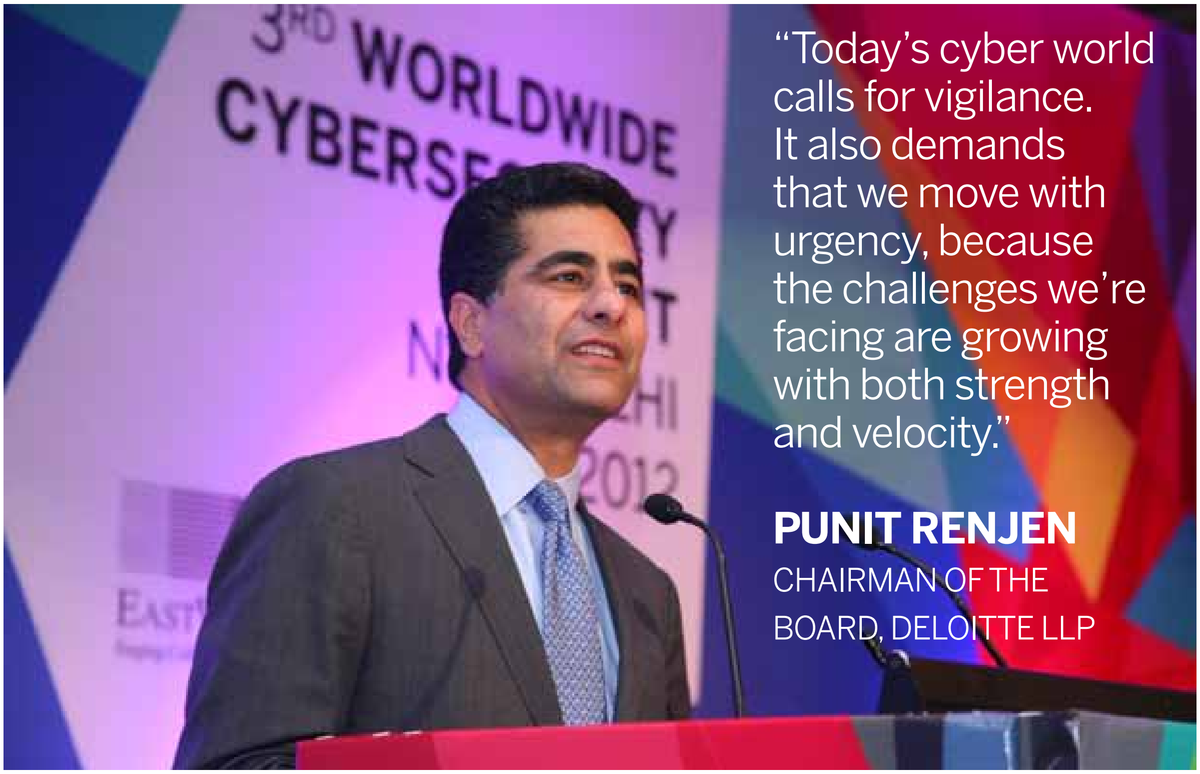
R. CHANDRASHEKHAR

SECRETARY, DEPARTMENT OF TELECOMMUNICATIONS, MINISTRY OF COMMUNICATIONS AND IT, INDIA

"Will we become a rogue nation or will we become a cybersecurity superpower is really the question."

PRADEEP GUPTA

CHAIRMAN & MANAGING DIRECTOR, CYBER MEDIA (INDIA) LTD.



"Today's cyber world calls for vigilance. It also demands that we move with urgency, because the challenges we're facing are growing with both strength and velocity."

PUNIT RENJEN

CHAIRMAN OF THE BOARD, DELOITTE LLP

“We’ve seen considerable work moving forward in botnet mitigation and in helping to understand the issues involved in undersea cables, yet we still have a lot more to do. The other outcome that I want to highlight is the commitment to coming to the table. Having these vigorous conversations helps to drive awareness and will move the ball forward.”

ANGELA MCKAY

PRINCIPAL SECURITY STRATEGIST, MICROSOFT

"They say, ‘The more you sweat in peace the less you bleed in war.’ And cybersecurity is war. The point is how often have you rehearsed and practiced your incident response to be ready for combat? You’ve got to put all three contours of preventive, detective and corrective action across the domains of people, processes and technology."

BURGESS COOPER

VICE PRESIDENT & CHIEF TECHNOLOGY SECURITY OFFICER, VODAFONE INDIA

“In order to achieve international cooperation we need to first focus on local efforts, awareness and local cooperation.”

VARTAN SARKISSIAN

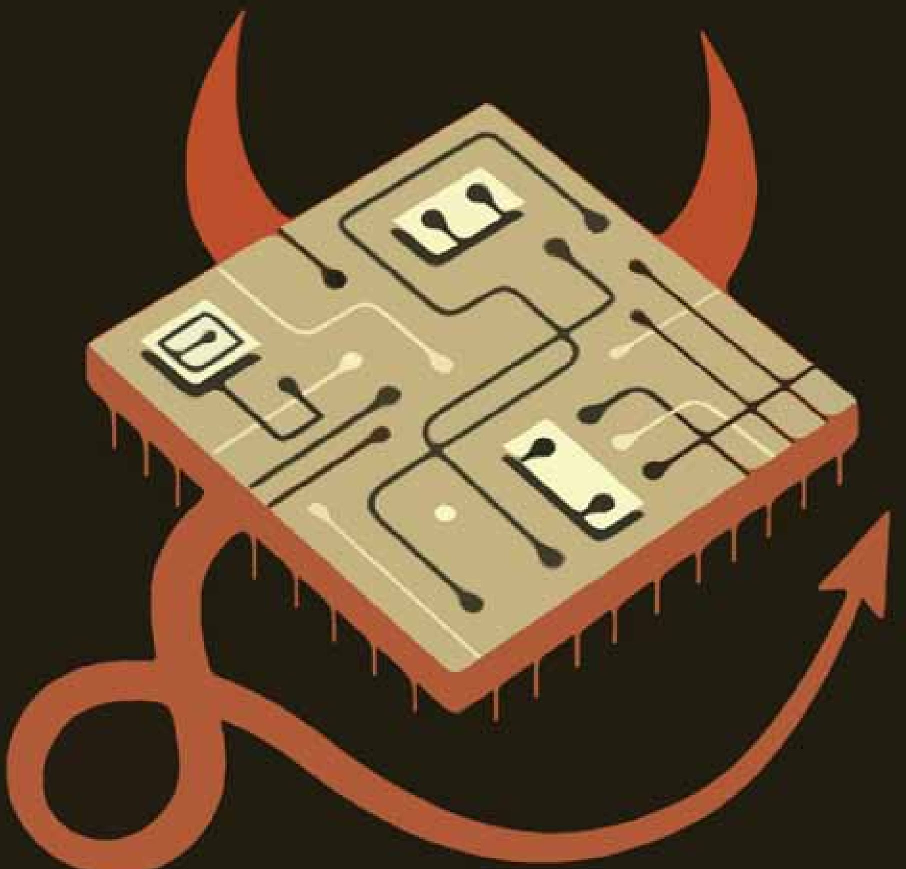
CEO, KNIGHTSBRIDGE CYBERSYSTEMS

Troubling Numbers

Every year during the summit we poll our international participants about the current situation in cyberspace and what needs to be done. Here are some of the results.

93%

THINK THAT THE CYBERSECURITY RISK IS HIGHER THAN ONE YEAR AGO



33%

FEEL PROTECTED ONLINE

41%

THINK THEIR ONLINE PRIVACY IS NOT SUFFICIENTLY PROTECTED

“We’re not looking for sudden, simple, single solutions. This has got to be incremental. I think we’ve got to avoid the seduction of that pursuit of the single but rather unattainable solution. So we need to build on existing legislation, recognizing the regional differences.”

MIKE ST. JOHN-GREEN
FORMER DEPUTY DIRECTOR, OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE, U.K.

"The second big driver for what we’re doing is how do we create a payment system which allows the government to accurately credit money or goods to people’s accounts in an unambiguously verifiable way. That’s all about making the use of public funds more efficient, more effective and more equitable."

NANDAN NILEKANI
CHAIRMAN OF THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA

“Now that we’re on this train, I don’t think it’s possible to get off. The Internet is becoming so integrated into everybody’s life that I just don’t think escape or a return to a pre-Internet age is possible.”

JOHN M. HOWELL EXECUTIVE DIRECTOR, IEEE COMMUNICATIONS SOCIETY

"At the end of the day, most of the corporate leaders dramatically underestimate the threat and they don't know what to do with that. In some cases the regulation is not there; in some cases they are basically squeezed between their budgets and balance sheets. In many cases, they think that whatever their CTOs are doing for the companies is more than enough."

ARMEN SARKISSIAN

VICE-CHAIRMAN, EASTWEST INSTITUTE;
FORMER PRIME MINISTER OF ARMENIA

"There are four aspects that are now shaping the entire cyberspace. One is connectivity; the second is mobility; the third is the social media, and the fourth is consumerization."

GULSHAN RAI

DIRECTOR GENERAL, CERT INDIA,
DEPT OF ELECTRONICS & IT, INDIA

"The challenge is to go from individual personal relationships to a process that allows for a continuous exchange of important information as opposed to exceptional exchange of information."

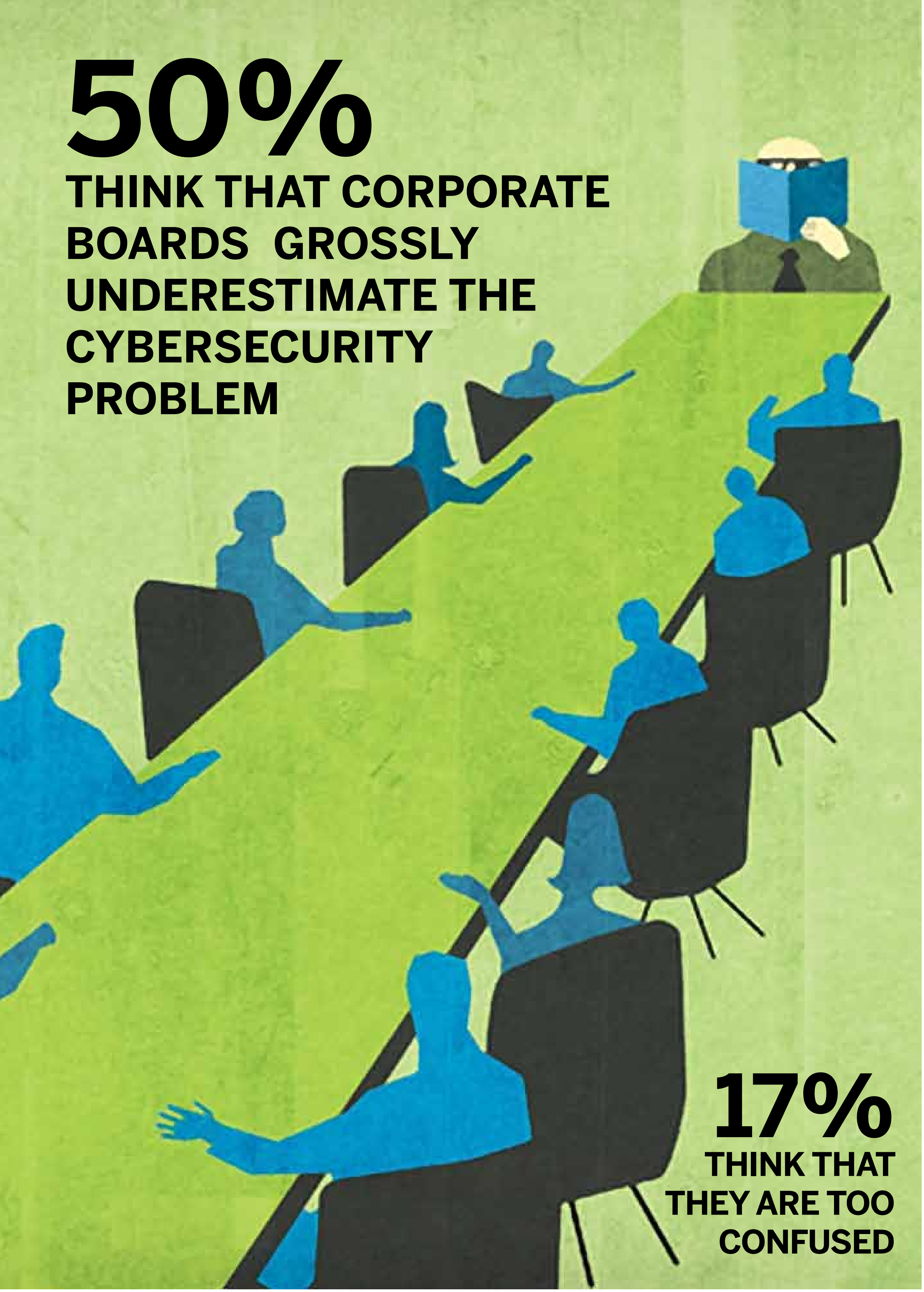
GREG SHANNON

CHIEF SCIENTIST, CERT PROGRAM,
CARNEGIE MELLON UNIVERSITY

"Insecurity in the cyber world comes in all forms and is perpetrated by all kinds of players."

MARIA LIVANOS CATTAUI

FORMER SECRETARY GENERAL, INTERNATIONAL
CHAMBER OF COMMERCE; MEMBER, BOARD OF
DIRECTORS, EASTWEST INSTITUTE

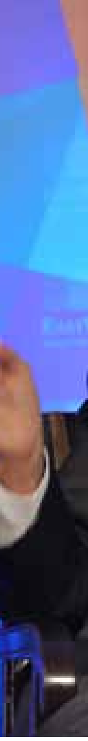


50%

THINK THAT CORPORATE BOARDS GROSSLY UNDERESTIMATE THE CYBERSECURITY PROBLEM

17%

THINK THAT THEY ARE TOO CONFUSED



62%

SAY THAT THEIR GOVERNMENTS ARE IN THE EARLY STAGES OF UNDERSTANDING THE CYBERSECURITY PROBLEM AND COMMITTING TO INTERNATIONAL COOPERATION

"If any issue consistently emerged from the cyber summit in Dallas, the summit in London and yesterday's outstanding summit activities, it's the criticality of strong international cooperation, public and private, to drive the policy changes, the business process changes and multilateral agreements to improve cybersecurity."

BOB CAMPBELL

CEO, CAMPBELL GLOBAL SERVICES; MEMBER, BOARD OF DIRECTORS, EASTWEST INSTITUTE

"This summit process has proven effective in developing innovative recommendations, seeing these recommendations implemented by major companies and governments, and then seeing their recommendations institutionalized by long-term sustainable changes."

VIJAY BHARGAVA

PRESIDENT, IEEE COMMUNICATIONS SOCIETY

"Some of the points we have reflected in our Information Technology Act could actually become a global yardstick or a point or base on which all of the international diplomacy on cybersecurity can go forward."

SUBIMAL BHATTACHARJEE

COUNTRY HEAD, GENERAL DYNAMICS

"One of our prominent speakers told me privately that his major worry is that one day we will cross a really difficult divide, and will confront a situation when people will die as a result of a cybersecurity attack. That could be a game changer of the worst type."

JOHN EDWIN MROZ PRESIDENT AND CEO, EASTWEST INSTITUTE

"If we knew better what cybersecurity was and had a handle on it, then I think we might see that our understandings of it would converge."

STUART GOLDMAN

CHAIR (FMR),
ATIS NETWORK
INTEROPERABILITY
FORUM; BELL LABS
FELLOW (RET.)

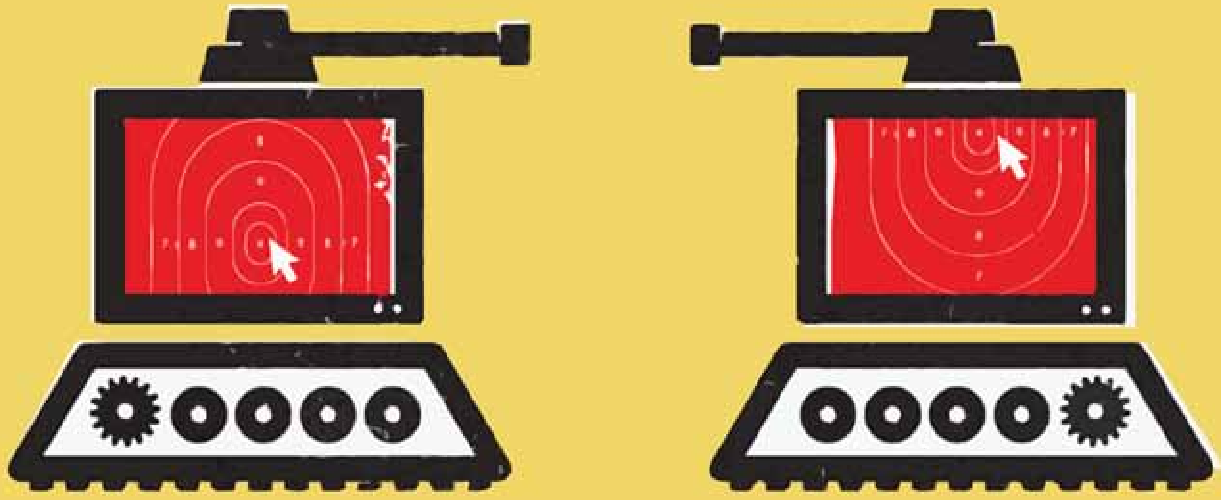
"Submarine cables are often overlooked, but they are very critical and form part of the critical infrastructure. I think if you look at cybersecurity, if that's the virtual gatekeeper of cyberspace, then the submarine cable network is the physical media that connects all that. Without the submarine cable network, you don't have the Internet and you don't have cyberspace."

DEAN VEVERKA

CHAIRMAN, INTERNATIONAL CABLE PROTECTION
COMMITTEE (ICPC); DIRECTOR NETWORKS AND
VICE PRESIDENT OPERATIONS, SOUTHERN CROSS
CABLES LIMITED

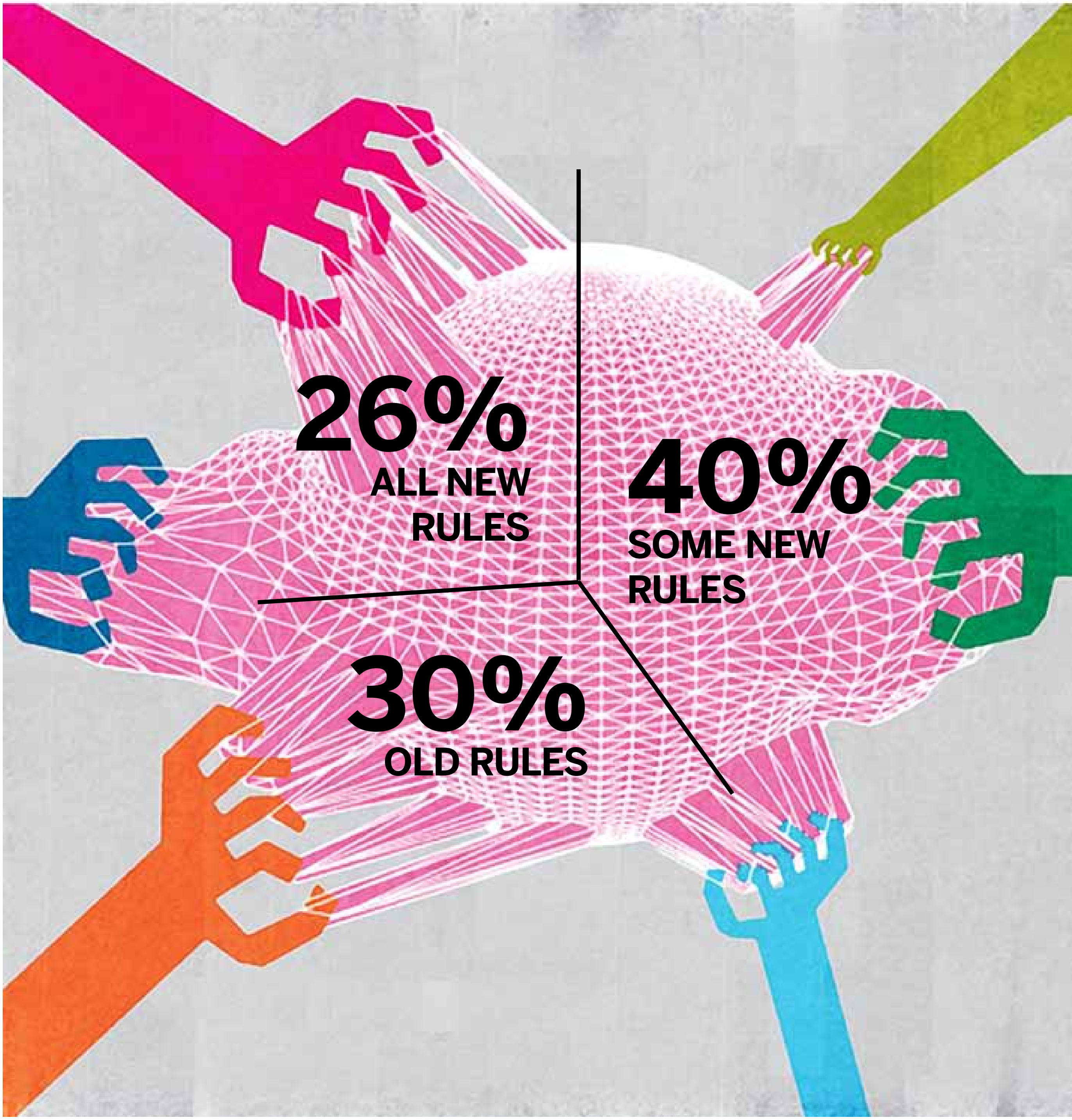
55%

DOUBT THAT THEIR COUNTRY CAN DEFEND ITSELF AGAINST SOPHISTICATED CYBER ATTACKS



WHAT KIND OF RULES SHOULD APPLY IN CYBERSPACE?

Is cyberspace a truly new society that deserves its own rules or an extension of the real world—and should most or all of its rules apply?



"Technologically, cyberspace is without boundaries but the privacy issues are country-specific. The issues which may be very acceptable for open discussion in the U.S. may have their own sensitivities in India. So the whole question is, how do you address all these issues so that the different stakeholders—government, regulators, service providers, civil society, the media—have some common acceptance of cybersecurity?"

ARBIND PRASAD

DIRECTOR GENERAL, FEDERATION OF INDIAN CHAMBERS OF COMMERCE AND INDUSTRY (FICCI)

"We really are operating in concentric circles. First, companies need to protect the data of their customers and themselves, and then around that is industry and, third, at a country-level. But these three circles are not enough, and the world has moved farther. I think global concentricity, where we are intersecting with what happens across the world, becomes even more important."

SOM MITTAL

PRESIDENT, NATIONAL ASSOCIATION OF SOFTWARE AND SERVICE COMPANIES (NASSCOM)

"In the area of theft of intellectual property and espionage, there's been very little progress, and maybe it's the nature of that challenge. That there isn't likely to be very much progress internationally because there are some strikingly different incentives that operate across the globe."

MICHAEL CHERTOFF

CHAIRMAN AND CO-FOUNDER, CHERTOFF GROUP; FORMER U.S. SECRETARY OF HOMELAND SECURITY; MEMBER, BOARD OF DIRECTORS, EWI

Working Togethe

The institute's summit process is oriented around ongoing breakthrough groups, diverse collections of experts assigned to devise solutions to major cybersecurity challenges.

r

The success of EWI's Worldwide Cybersecurity Initiative is measured in part by the policy breakthroughs made in the interactive working sessions, both during the summit meeting and in the follow-up activities throughout the year.

The objective for each of the breakthrough groups is to have actionable recommendations for industry and government that, if implemented, will have significant impact in making cyberspace and the real world safer, more stable and more secure. As in London and Dallas, the format of the New Delhi summit included new and continuing breakthrough groups, immersing participants in interactive sessions with professional peers from around the world. Following consultation with the Indian government and private sector leaders, three new issues, discussed below, emerged as central areas of focus at the New Delhi summit.

Globally Distributed Processing and Data Storage (the "Cloud")

The transition to so-called "cloud" style design and management brings both new efficiencies and new vulnerabilities. While there is much work underway (e.g., IEEE, Cloud Security Alliance) to optimize security within the constraints of distributed processing and storage, fundamental issues at the core of the discussion remain unresolved. Which policies apply to the data of country A when managed by country B? Will country A know if country X has its data? How? These and other questions have made many uneasy. Equally urgent are concerns about governments overreacting with regulations that could stifle innovation or otherwise restrict freedoms.

Agreements, standards, policies and recommendations need to catch up to already introduced innovative services that have befuddled government, legal and social paradigms.

The answers to these and other questions directly impact the safety, security and integrity of phenomena like social networking, information leak posting, personal broadcasting and tracking and profiling the online behavior of netizens. Agreements, standards, policies and recommendations need to catch up to already introduced innovative services that have befuddled government, legal and social paradigms.

This group builds on work that began as an India-U.S. Track 2 bilateral, which put forth voluntary principles that multi-national companies should subscribe to when designing and operating "cloud" applications.

ICT Development/ Supply Chain Integrity

Governments and businesses are unable to determine the integrity of the hardware and software on which they vitally depend for the reliability and security of their critical operations. Major initiatives are underway by national governments to improve their oversight of the technology responsible for national critical infrastructure as well as vital national security operations. The overwhelming majority of expertise and experience resides in the private sector, where much of the hardware and software design, development, deployment and operation occur. Thus governments are typically at a substantial disadvantage, forced to rely on the private sector for insights. That said, private sector insight can be biased as a result of commercial objectives hinging on status quo approaches.

This group builds on work underway within an India-U.S. Track 2 bilateral and is working toward articulating international principles for the integrity of ICT development/supply chains that may be otherwise overlooked or underemphasized within national initiatives.

As essential data now often traverses international borders, the lack of a common understanding of the appropriate rigor for its protection and access is a major obstacle for everyone.

Payload Security

In a perfect world, the government can access the critical information it needs in a timely manner to ensure national security and public welfare, while citizens and private sector enterprises can enjoy cyberspace with safety, security and privacy – i.e. freedom from being needlessly observed or interrupted. Private sector network operators and service providers should meet both needs in an efficient, reliable and collaborative manner. However, neither government nor private sector objectives are met adequately, making the present state acceptable to neither.

As essential data now often traverses international borders, the lack of a common understanding of the appropriate rigor for its protection and access is a major obstacle for everyone. This group builds on work underway within India-U.S. Track 2 bilateral talks to address gaps in international policies affecting monitoring and privacy.

Additional Breakthrough Groups

Pursuing World Class Performance for International Connectivity: Timely Outage Repairs for Global Undersea Communications Cable Infrastructure (GUCCI)
Applying the International Cable Protection Committee's best practices for timely outage repairs of undersea cables is essential to both maintaining stable international connectivity and restoring service as soon as possible in the event of an outage.

Harmonizing Legal Frameworks
Advancing non-partisan, objective recommendations for potential new legal mechanisms is critical to combating cyber crime and cyber attacks.

Priority International Communications: Strategy for Implementation
This breakthrough topic explores the steps the international community must take towards implementing the four recommendations proposed by EWI's report *Priority International Communications (PIC): Staying Connected in Times of Crisis.*

Emergency Preparedness for the Financial Service Sector in Cyberspace
Collaboration in the international financial services sector is imperative to prepare for future crises, such as sophisticated attacks that could occur in cyberspace.

Dealing with the New Power Structure of Non-State Actors in Cyberspace
Proactive measures are needed to promote constructive cooperation with non-state actors in cyberspace, and assure that the existing prescribed instruction and training regarding the Geneva and Hague protections for civilians are sufficient in the event of cyber conflict.

International Aspects of Critical Infrastructure Protection
Despite relevant stipulations in the Geneva and Hague conventions, there are currently no distinctive, clearly visible markers for protected humanitarian entities such as hospitals in cyberspace; this group seeks to devise means of addressing this potentially dangerous problem.

Measuring the Cybersecurity Problem
Producing the first worldwide, standardized, high-level benchmarks for cybersecurity compromises is vital in a world of increased complexity, connectivity and criticality.

Stopping Cyberspace Pollution: International Cooperation on Fighing Spam and Botnets
Botnet creators and spammers have made their identities extremely difficult to uncover, their spam messages more difficult to recognize and needed countermeasures more difficult to apply. International cooperation and policy is crucial to effectively addressing the problem.

Implementing Public Health Models for the Internet
In the face of mounting cyber threats, international cooperation based on a global public health model can improve device health and reduce security risks.

Above, from left: Dean Veverka, Chairman, International Cable Protection Committee (ICPC); Director Networks and Vice President Operations, Southern Cross Cables Limited; Michael O'Reirdan, Chairman, M3AAWG; Distinguished Engineer, Comcast; Karl Frederick Rauscher, Chief Technology Officer and Distinguished Fellow, EastWest Institute; Stuart Goldman, Chair (fmr), ATIS Network Interoperability Forum; Bell Labs Fellow (ret.); Angela McKay, Principal Security Strategist, Microsoft

New Ideas

The 3rd Worldwide Cybersecurity Summit provided an excellent opportunity for experts, stakeholders and decision-makers from industry, government and academia to review papers on the international policy-related aspects of cybersecurity.

Thirteen papers were presented and discussed on topics such as: the worldwide response to a cyber crises (e.g., priority international communications and trusted information sharing); global awareness and education (e.g., protecting youth, spam, and the private-public partnerships needed to secure the global economy); and worldwide governance, frameworks and protocols for day-to-day behavior in cyberspace, and responses to cyber conflict. All of the authors presented their papers at the Poster Session of the summit.

For a full list of presented papers visit the summit website at **www.cybersummit2012.com**.

In the News

The 3rd Worldwide Cybersecurity Summit made it to the front pages of major newspapers in India and attracted wide media interest abroad. Here are some headlines and soundbites from the summit.

"Now, there are no bangs, no explosions and no declarations of war, but cyber crimes can inflict just as much damage. Experts from the U.S. and India are meeting at a summit in Delhi to discuss vital cybersecurity areas."

BBC

"'If we can figure this out here, it's a massive business opportunity across the world,' Mr. Perot told India Real Time on the sidelines of the EastWest Institute's cyber security summit in New Delhi Tuesday. The EastWest Institute is a New York-based think tank that focuses on issues of global security and is chaired by Mr. Perot."

WALL STREET JOURNAL

"India's importance in this domain can be judged from the fact that, after the previous two editions in London and Dallas, Delhi will play host to the Third Worldwide Cybersecurity Summit."

Business India

"'We have 1.2 billion people and will be the largest in terms of population in the world in years to come. Cyber crime affects us perhaps much more than any other country in the world,' Telecom and IT Minister Kapil Sibal said on the sidelines of the 3rd Worldwide Cybersecurity Summit."

THE ECONOMIC TIMES

"John Suffolk, [Huawei]'s global cybersecurity chief, told Reuters at a cybersecurity conference in New Delhi that he was sending a team of engineers to talk to German security researcher Felix Lindner, who has exposed vulnerabilities in the company's routers, from its $100 home Internet devices to multi-million dollar equipment."

REUTERS

"Union Telecom Minister Kapil Sibal on Tuesday called for a global effort to fortify cyber security. Interacting with reporters at the third Worldwide Cybersecurity Summit here, Sibal said that such security is necessary as online space doesn't have a boundary and information could travel miles, affecting or influencing sensitive matters."

ANI NEWS

"The global summit sought to bring more stability and safety into the global cyberspace by identifying critical security areas and ways to address them."

DATAQUEST
The Business of Infotech

"While governments fear crippling cyber-attacks on critical infrastructures such as nuclear power plants and banking systems, citizens have smaller risks like identity theft and credit card fraud to grapple with. The recently concluded Worldwide Cybersecurity Summit, held in Delhi, has done well to throw some light on the enormity of the challenge of fighting this menace."

LIVE RICH FINANCIAL Chronicle International Herald Tribune

New Publications

Two new EWI reports were released to coincide with the convening of the New Delhi Summit.

Priority International Communications

During recent tragedies like Japan's tsunami and nuclear meltdown in 2011, the London bombings in 2005, and the 2008 Mumbai and 9/11 terrorist attacks, some critical communications failed to make it through congested networks. Priority International Communications (PIC) capability is needed to help prevent the loss of lives and property in such crisis situations.

Based on inputs from leading telecommunications industry experts, this publication sets forth straightforward steps needed to set up an international capability for both government officials and private sector leaders. As emerging networks' technologies and services continue to demand greater and greater bandwidth, these congestion scenarios will likely occur more frequently.

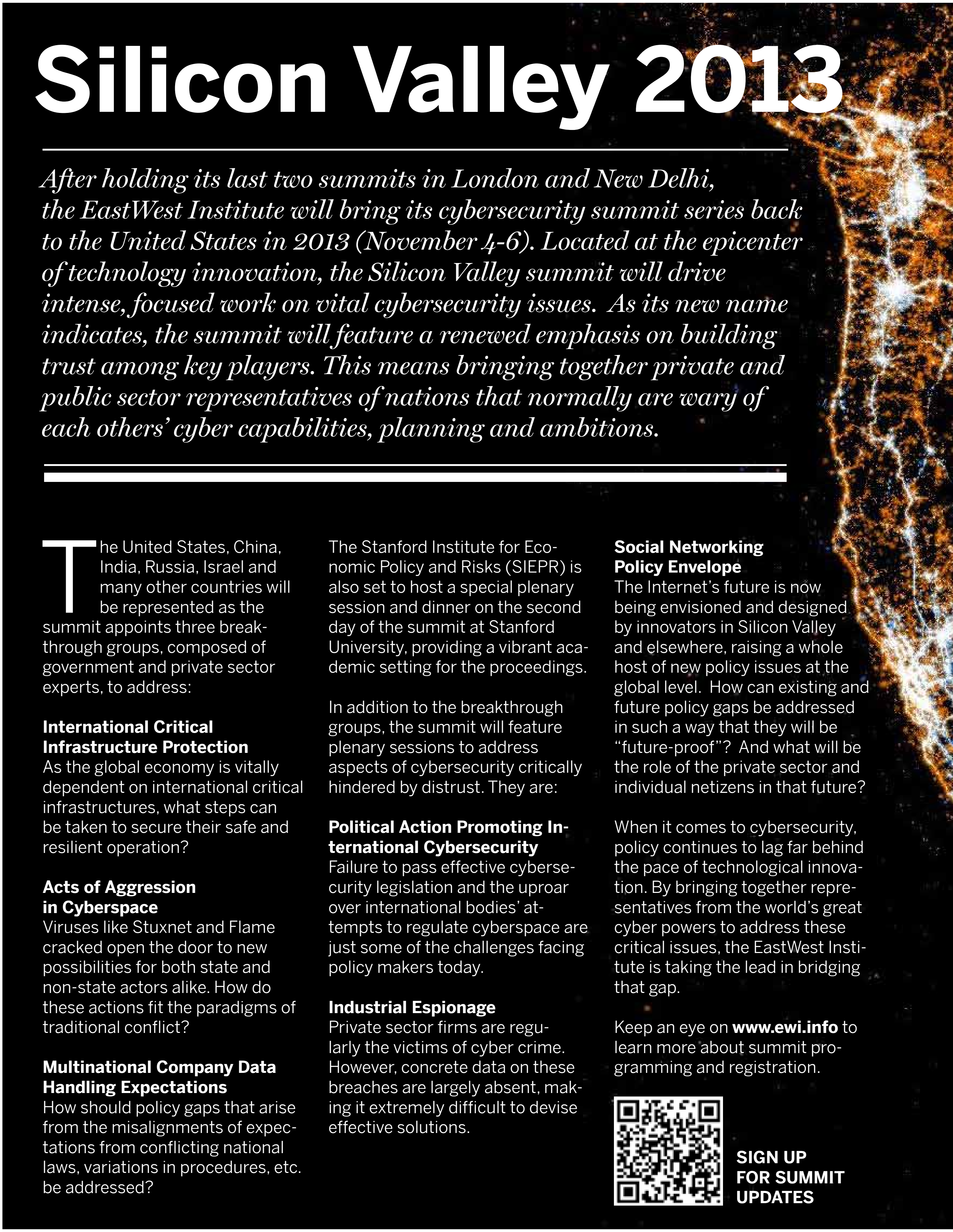
Priority International Communications: Staying Connected in Times of Crises presents four actionable recommendations that, if implemented, would allow government-authorized users to communicate even when networks are jammed. These authorized users include public or private sector individuals with critical roles in times of crises. They are critical infrastructure operators (communications, energy, financial services and transportations); public safety officials (health care, local government, emergency management) and individuals with national security responsibilities.

Cyber Detente Between the United States and China

It's no secret that the United States and China have a contentious relationship when it comes to their cyber capabilities and intentions. But according to *Cyber Detente Between the United States and China: Shaping the Agenda*, these two countries have common cyber concerns that could bring them to the table to lay the groundwork for diplomatic exchanges and solutions, avoiding an escalation of aggressive strategies from either country.

The authors point out that through Track 2 processes some very useful preparatory work has already taken place. However, they argue that the diplomacy—both official and unofficial—needs to be more intense, to cover more concrete problems and to involve a larger number of people on both sides, especially from the military and private sector. The paper calls for a fresh appraisal of the impact of both countries' military cyber policies.

PRIORITY INTERNATIONAL COMMUNICATIONS
CYBER DETENTE BETWEEN THE UNITED STATES AND CHINA



Silicon Valley 2013

After holding its last two summits in London and New Delhi, the EastWest Institute will bring its cybersecurity summit series back to the United States in 2013 (November 4-6). Located at the epicenter of technology innovation, the Silicon Valley summit will drive intense, focused work on vital cybersecurity issues. As its new name indicates, the summit will feature a renewed emphasis on building trust among key players. This means bringing together private and public sector representatives of nations that normally are wary of each others' cyber capabilities, planning and ambitions.

The United States, China, India, Russia, Israel and many other countries will be represented as the summit appoints three breakthrough groups, composed of government and private sector experts, to address:

International Critical Infrastructure Protection
As the global economy is vitally dependent on international critical infrastructures, what steps can be taken to secure their safe and resilient operation?

Acts of Aggression in Cyberspace
Viruses like Stuxnet and Flame cracked open the door to new possibilities for both state and non-state actors alike. How do these actions fit the paradigms of traditional conflict?

Multinational Company Data Handling Expectations
How should policy gaps that arise from the misalignments of expectations from conflicting national laws, variations in procedures, etc. be addressed?

The Stanford Institute for Economic Policy and Risks (SIEPR) is also set to host a special plenary session and dinner on the second day of the summit at Stanford University, providing a vibrant academic setting for the proceedings.

In addition to the breakthrough groups, the summit will feature plenary sessions to address aspects of cybersecurity critically hindered by distrust. They are:

Political Action Promoting International Cybersecurity
Failure to pass effective cybersecurity legislation and the uproar over international bodies' attempts to regulate cyberspace are just some of the challenges facing policy makers today.

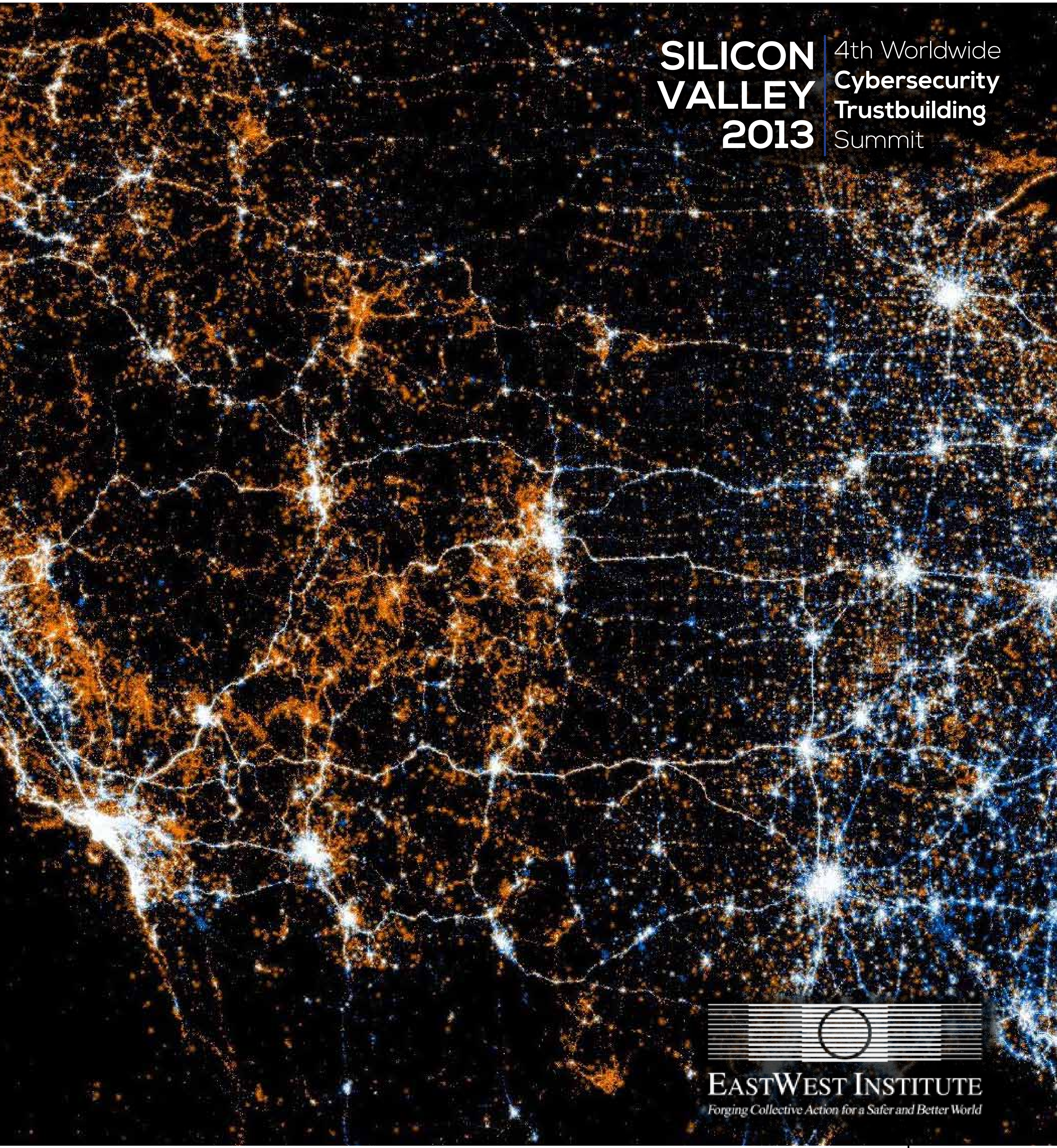
Industrial Espionage
Private sector firms are regularly the victims of cyber crime. However, concrete data on these breaches are largely absent, making it extremely difficult to devise effective solutions.

Social Networking Policy Envelope
The Internet's future is now being envisioned and designed by innovators in Silicon Valley and elsewhere, raising a whole host of new policy issues at the global level. How can existing and future policy gaps be addressed in such a way that they will be "future-proof"? And what will be the role of the private sector and individual netizens in that future?

When it comes to cybersecurity, policy continues to lag far behind the pace of technological innovation. By bringing together representatives from the world's great cyber powers to address these critical issues, the EastWest Institute is taking the lead in bridging that gap.

Keep an eye on **www.ewi.info** to learn more about summit programming and registration.

SIGN UP FOR SUMMIT UPDATES



SILICON VALLEY 2013

4th Worldwide **Cybersecurity Trustbuilding** Summit

EASTWEST INSTITUTE

Forging Collective Action for a Safer and Better World

“See something or say something," Eric Fischer
Orange dots are locations of Flickr pictures, **blue** dots are locations of Twitter tweets.
White dots are locations that have been posted to both.

EWI Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder & CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

R. William Ide III (U.S.)
Counsel & Secretary
EastWest Institute
Partner
McKenna Long & Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman & CEO
Southwest Energy (HK) Ltd.

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Sir Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
CEO
WBE Hong Kong

Robert N. Campbell III (U.S.)
Vice Chairman (Retired)
Deloitte LLP

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Mark Chandler (U.S.)
Chairman & CEO
Biophysical

Angela Chen (U.S.)
Founder and Managing Director
Global Alliance Associates
Partner
Epoch Fund

Michael Chertoff (U.S.)
Co-founder & Managing Principal
Chertoff Group

David Cohen (U.K.)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman & Co-Founder
Planet Heritage Foundation

Adel Ghazzawi (U.A.E.)
Founder
CONEKTAS

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Emil Hubinak (Slovak Republic)
Chairman & CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference
Global Head of
Governmental Affairs
Allianz SE

Anurag Jain (India)
Chairman
Laurus Edutech Pvt. Ltd.

James L. Jones (U.S.)
Former U.S. National Security
Advisor

Haifa Al Kaylani (U.K.)
Founder & Chairperson
Arab International Women's Forum

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

Kevin McGovern (U.S.)
Chairman
The Water Initiative
Co-Founder
SOBE Beverages

General (ret) T. Michael
Moseley (U.S.)
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Tsuneo Nishida (Japan)
Ambassador;
Permanent Representative
of Japan to the U.N.

Ronald P. O'Hanley (U.S.)
President,Asset Management
and Corporate Services
Fidelity Invesments

Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab
Emirates in Washington

Admiral (ret) William A. Owens
(U.S.)
Chairman
AEA Holdings Asia
Former Vice Chairman
U.S. Joint Chiefs of Staff

Sarah Perot (U.S.)
Director & Co-Chair for
Development
Dallas Center for Performing Arts

Louise Richardson (U.S.)
Principal
University of St. Andrews

John Rogers (U.S.)
Managing Director
Goldman Sachs & Co.

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
CEO
Bud Smith Organization Inc.

Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President & CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor & Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill Inc.

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

India Summit Committee

Kapil Sibal
Minister of Union for Communications and Information Technology
Committee Chairman

PUBLIC SECTOR

Sachin Pilot
Minister of State for Communications and IT

Milind Deora
Minister of State for Communications and IT

R. Chandrashekhar
Secretary of the Department of Telecommunications,
Ministry of Communications and IT

J. Satyanarayana
Secretary of the Department of Electronics and IT,
Ministry of Communications and IT

B. K. Gairola
Director General, National Informatics Centre (NIC)

Gulshan Rai
Director General, CERT India

Som Mittal
President, National Association of Software and
Service Companies (NASSCOM)

Nandan Nilekani
Chairman, Unique Identification Authority of India
(UIDAI)
Head, Technology Advisory Group for Unique
Projects (TAGUP)

Arbind Prasad
Director General, Federation of Indian Chambers of
Commerce and Industry (FICCI)

Kamlesh Bajaj
CEO, Data Security Council of India (DSCI)

Dilip Chenoy
CEO, National Skills Development Corporation

PRIVATE SECTOR

Virat Bhatia
Chairman, FICCI Communications &
Digital Economy Committee

Anurag Jain
Chairman, Laurus Edutech Pvt. Ltd.

Sanjay Kapoor
CEO India & South Asia, Bharti Airtel

Marten Pieters
CEO, Vodafone India

C.S. Rao
President, Corporate Affairs and Regulatory
Reliance Communications Ltd.

Udayan Sen
CEO and Managing Partner
Deloitte Haskins & Sells

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

Founded in 1980, the EastWest Institute is a global, action-oriented think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) nonprofit organization with offices in New York, Brussels and Moscow. Our fiercely guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI New York Center
11 East 26th St.
20th Floor
New York, NY 10010
1-212-824-4100

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka St. 7/5,
Building 1, 6th Floor
Moscow 125009
7-495-2347797

EWI Washington Office
1069 Thomas Jefferson St. NW
Washington, DC 20007
1-202-492-0181

www.ewi.info