PROTECTING THE DIGITAL ECONOMY

THE FIRST **WORLDWIDE CYBERSECURITY SUMMIT** IN DALLAS

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

30 YEARS

"WE NEED TO GET MUCH CRISPER IN HOW WE SET
OUR PRIORITIES. OUR RESOURCES ARE LIMITED AND
NO ONE COUNTRY – OR COMPANY – CAN FIGHT THIS WAR ALONE.
AND AS MORE AND MORE PEOPLE ADOPT
SMARTPHONES, TABLETS AND OTHER WIRELESS DEVICES,
MOBILE BROADBAND WILL HAVE A HUGE IMPACT ON CYBERSECURITY."

RANDALL L. STEPHENSON, CHAIRMAN OF THE BOARD,
CHIEF EXECUTIVE OFFICER AND PRESIDENT OF AT&T INC

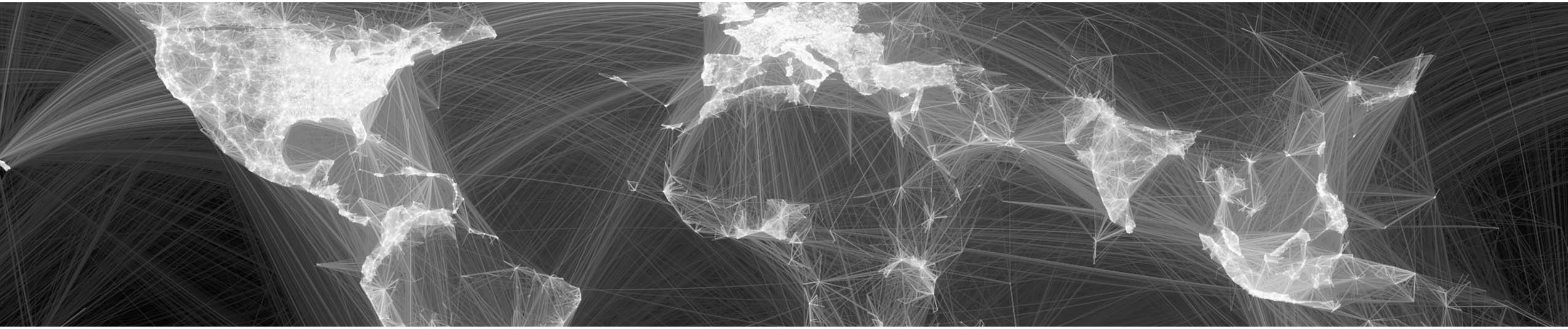


TABLE OF **CONTENTS**

OUR **CYBERSECURITY** INITIATIVE

Imagine a day when you can't access your checking account, use your credit card, get online or make a call from your cellphone - a day when transportation shuts down in a cascade of broken traffic lights and grounded flights. This nightmare scenario is all too possible: the Internet, which hosts the communications, financial and military systems that keep our world connected and safe, is increasingly vulnerable to sweeping attacks, like the one that paralyzed Estonia in 2007. With the availability of mobile Internet access devices, hacking is cheaper and easier than ever, and it's becoming harder to track the criminals who commit online theft and terrorism. Since cyberspace has no borders, a purely national solution to this problem is impossible. We need to work together as a global community to agree on how to secure the world's digital infrastructure.

The EastWest Institute has a thirty-year track record of bringing together powerful players from around the world to achieve change. Concerned by the lack of meaningful discussion on protecting cyberspace, the EastWest Institute established the **Worldwide Cybersecurity Initiative** in 2009, with an advisory group led by General Harry Raduege.

Our goals are to:

- raise awareness of the growing threat to cyberspace.
- build trust and cooperation among national policymakers, business leaders and technical communities.
- host a forum for the creation of an international cyberspace policy (like the agreements that govern use of outer space).

In less than one year, we have engaged the expertise of over 300 companies and government agencies, and formalized partnerships with companies including AT&T, Microsoft, Motorola, Juniper, Deloitte, Huawei, Vimpelcom, Goldman Sachs, Akin Gump, and the Knightsbridge Group. We have formed strong relationships with the IEEE and World Federation of Scientists Permanent Monitoring Panel on Information Security. We have also secured the commitment from China, India, Russia, the European Union, and the United States to support bilateral Track 2 consultations.

AN INTERNATIONAL **FORUM**

We began our cybersecurity initiative's public process with **The First Worldwide Cybersecurity Summit: Protecting the Digital Economy**, held from May 3-May 5, 2010 in Dallas Texas. The summit brought together over four-hundred technical experts, policy elites and national security officials from the Cyber40, an informal grouping of the world's most digitally-advanced countries.

Michael Dell, speaking at the opening ceremony, declared: "Governments and private industry need to work collaboratively to develop the appropriate international framework to secure cyberspace. We should all do this in a way that keeps our global information central nervous system intact and secure." At its heart, the summit's main aim was to answer that call.

Today, policymakers face a wide array of problems in overseeing cyberspace:

- We lack a commonly-agreed upon definition of what "cybersecurity" means.
- The private sector and the public sector have not worked together effectively to protect cyberspace.
- Companies don't have an incentive to build security into network equipment, networks and services, largely because consumers are not aware of their own risk.
- Diplomatic assets assigned to the problem are inadequate, which reflects a lack of political commitment at high levels to protecting cyberspace.
- We lack agreements like the Geneva Convention to govern information warfare.
- States are too parochial in their thinking about online security to collaborate on crafting global cyber regulations.

In order to identify solutions to these problems, the conference broke down into smaller "breakthrough groups," each working to identify specific threats to and recommend policies for seven crucial sectors of the Internet: information & communications technology, financial services, essential government services, energy, transportation, national security and media.

Thanks in large part to these dynamic working groups, experts left the conference with renewed commitment to protecting cyberspace and some solid ideas about how to move forward.

In anticipation of **The Second Worldwide Cybersecurity Summit: Mobilizing for International Action**, to be held from June 1- June 2, 2011 in London, we wanted to share some of the highlights from the Dallas summit – what was said, what we learned and, most importantly, the next steps in our international effort to protect cyberspace.

OUR **SPEAKERS**

In Dallas, we brought together top business and government experts from over forty countries. Here’s a taste of what our speakers had to say.

OUR **SPEAKERS**

"The cyber world depends on a **'web of trust'** that must be preserved by technology and security working together. Reliable and strong authentification mechanisms strengthen the 'web of trust' by exploiting, in the best sense of the word, the technological possibilities of payment and transaction in our economy."

HOWARD A. SCHMIDT, CISSP, CSSLP SPECIAL ASSISTANT TO THE PRESIDENT AND CYBERSECURITY COORDINATOR.

As Special Assistant to the President and the Cybersecurity Coordinator for the United States federal government, Schmidt is responsible for coordinating interagency cybersecurity policy development and implementation and is responsible coordinating engagement with federal, state, local, international, and private sector cybersecurity partners.

"There are no national barriers when it comes to the Internet world. Therefore, in order to develop a fundamental measure which effectively handles cybersecurity, the **global community** has to join hands together and exert collaborated efforts."

BYEONG GI LEE, PRESIDENT, IEEE COMMUNICATIONS SOCIETY; COMMISSIONER OF THE KOREA COMMUNICATIONS COMMISSION (KCC).

Lee is a professor of electronics engineering, Seoul National University, Korea. He has worked for Granger Associates (DSC Communications) and AT&T Bell Laboratories. He was the founding chair of the Joint Conference of Communcations and Information (JCCI)

"Countries will need to decide what constitutes warfare in cyberspace and **what rules apply**. This can only happen through international dialogue."

SCOTT CHARNEY, MICROSOFT CORPORATE VICE PRESIDENT FOR TRUSTWORTHY COMPUTING, ENGINEERING EXCELLENCE, AND ENVIRONMENTAL SUSTAINABILITY.

Trustworthy Computing is Microsoft's effort to help ensure secure, private and reliable computing experiences for everyone. Before joining Microsoft in 2002, Charney served as a principal for PricewaterhouseCoopers and the Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the U.S. Department of Justice, where he was the leading federal prosecutor for computer crimes from 1991 to 1999.

"Criminal innovation outpaces security development. 85 to 90 % of critical infrastructure within the United States is owned by the private sector. Value and productivity improvements in general are largely based on IT. Without IT, businesses could not be run anymore. **Private-public partnerships** will be essential in battling cyber threats, which increasingly undermine trust and confidence in technology."

JAMES H. QUIGLEY, CHIEF EXECUTIVE OFFICER, DELOITTE TOUCHE TOHMATSU (DELOITTE).

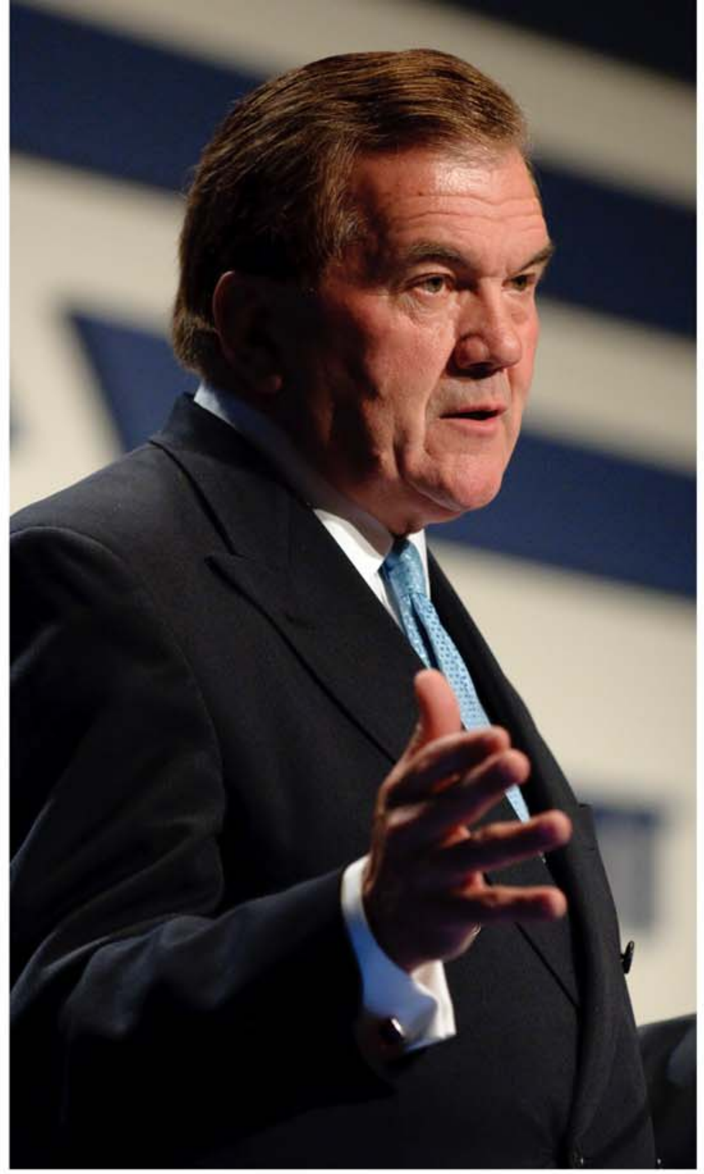
Prior to his current role at Deloitte, which serves public and private clients in over 140 countries, Quigley was the CEO of Deloitte United States. Quigley is actively involved in international business organizations committed to shaping policies for a successful, sustainable global economy, including the TransAtlantic Business Dialogue (TABD,) of which he is co-chairman, and the board of trustees of the U.S. Council for International Business (USCIB).

OUR **SPEAKERS**

"Law enforcement and the judiciary need to be trained and be improved dramatically. The **lack of international cooperation** is to blame for the fact that many cyber crimes are not solved."

KAMLESH BAJAJ, CHIEF EXECUTIVE OFFICER, DATA SECURITY COUNCIL OF INDIA AND HEAD OF NASSCOM SECURITY INITIATIVES.

Bajaj spent the last two years leading the development of Best Practices for Data Protection, promoting their usage by IT and Business Process Outsourcing companies in compliance with regulations of client countries. He was the Founder Director of Computer Emergency Response Team (CERT-In), Ministry of Communications and IT, and served as a Deputy Director General, National Informatics Centre (NIC).



"Virtual attacks have **real life consequences**. There is a stronger than ever imperative for international collaboration. Individuals around the world should be engaged to build an international culture of security."

TOM RIDGE, SENIOR ADVISOR, DELOITTE LLP, PRESIDENT AND CEO, RIDGE GLOBAL LLC.

Ridge leads a team of international experts that counsels businesses and governments on risk management and global trade security, strategic business generation, technology integration, and event security, among other concerns. Following September 11th, 2001, Ridge became the first Assistant to the President for Homeland Security and, in 2003, was appointed as the first Secretary of the U.S. Department of Homeland Security.

"Laws need to be harmonized by agreeing on a minimal level of security at the least, via existing treaties and agreements. Enormous problems still persist in the areas of investigation and extradition. A **new multilevel agreement** is necessary which takes diplomatic and political complexities into consideration."

JODY R. WESTBY, CEO, GLOBAL CYBER RISK, LLC.

Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cybercrime, e-discovery, and outsourcing risk management. She has served as senior managing director for PricewaterhouseCoopers, where she was responsible for information security, and is vice chair of the World Federation of Scientists' Permanent Monitoring Panel on Information Security. She was recently appointed to the United Nations' High Level Experts Group on Cyber Security.

"We need to get much crisper in how we set our priorities. **Our resources are limited** and no one country – or company – can fight this war alone. And as more and more people adopt smartphones, tablets and other wireless devices, mobile broadband will have a huge impact on cybersecurity."

RANDALL L. STEPHENSON, CHAIRMAN OF THE BOARD, CHIEF EXECUTIVE OFFICER AND PRESIDENT, AT&T INC.

Appointed to the position in 2007, Stephenson previously served as the company's chief operating officer, where he was responsible for all wireless and wired operations, and as senior executive vice president and chief financial officer for SBC Communications (today AT&T).

OUR **SPEAKERS**

"It is necessary to involve all stakeholders in the debate surrounding cybersecurity. We are not overestimating the threat of **cyber terrorists**, and there is the possibility of future attacks to come."

PHILIP R. REITINGER, DEPUTY UNDERSECRETARY, DHS NATIONAL PROTECTION AND PROGRAMS DIRECTORATE (NPPD).

As Senior Security Strategist with Microsoft Corporation's Trustworthy Computing Security Team, Reitinger developed and implemented programs that enhanced Microsoft products' security and helped secure our nation's critical infrastructures. Reitinger is also the former Chair of the Group of Eight's High-Tech Crime Subgroup, and the Vision and Policy Committee of the National Cyber Crime Training Partnership.

"The Internet is the new frontline in the struggle for **human rights**. We need to establish new codes of conduct and effective sanctions for non-compliance and rigorously apply human rights standards."

HENNING WEGENER, FORMER AMBASSADOR OF GERMANY.

Wegener served as Ambassador for Disarmament in Geneva between 1981 and 1986, as Assistant Secretary General for Political Affairs at NATO between 1986 and 1991, and later as Ambassador to Spain. From 2001 to 2009, he was Chairman of the Permanent Monitoring Panel on Information Security of the World Federation of Scientists and now serves as the panel's co-chair. Among other degrees, he holds a Doctor of Juridical Science from Yale.

"75 % of all cyber attacks come from outside national boundaries. **International cooperation** therefore is vital."

LT. GENERAL (RET.) HARRY D. RADUEGE JR., CHAIRMAN, DELOITTE CENTER FOR CYBER INNOVATION; HONORARY CHAIR OF THE EWI WORLDWIDE CYBERSECURITY SUMMIT.

Former Director of the Defense Information Systems Agency; Commander, Joint Task Force - Global Network Operations; and Deputy Commander for Global Network Operations and Defense, U.S. Strategic Command Joint Forces Headquarters – Information Operations, Arlington, Va. This organization plans, develops and provides interoperable command, control, communications, computers and intelligence systems to serve the needs of the President, Secretary of Defense, Joint Chiefs of Staff, the combatant commanders, and other Department of Defense components under all conditions from peace through war.

"A new global cybersecurity **legal framework** is very necessary to foster international cooperation and bridge the digital divide."

STEIN SCHJØLBERG, CHIEF JUDGE, MOSS TINGRETT COURT, NORWAY.

An international expert on cyber crime, and one of the founders of the harmonization of national criminal law on computer crime, Judge Schjølberg has served as an expert on cyber crime for several international institutions, serving as Chairman of the global High-Level Experts Group (HLEG) on Cybersecurity and Cybercrime at the International Telecommunication Union (ITU) in Geneva.

OUR **SPEAKERS**

"Technological innovations are fundamentally **changing the way people live**, work, play, share information and communicate with each other."

JOHN N. STEWART,
VICE PRESIDENT AND CHIEF SECURITY OFFICER, CISCO

Stewart is responsible for providing leadership and direction to multiple corporate security teams throughout Cisco, and for leading corporate security practices, policies, and processes. He oversees the security for Cisco Connection Online, the infrastructure supporting Cisco's business.

"Most of the nation's infrastructure is owned, operated, and developed by the **commercial sector**. We depend on this sector to address the nation's broader needs, so we'll need a new information-sharing environment."

MELISSA HATHAWAY,
PRESIDENT, HATHAWAY GLOBAL STRATEGIES LLC

Hathaway is a former Acting Senior Director for Cyberspace in the U.S. National Security Council under the Obama Administration. Previously, Hathaway was a Principal with Booz Allen & Hamilton, Inc., leading two primary business units: information operations and long range strategy and policy support.

"**International cooperation** will be difficult, but it is necessary. Even a bad compromise is better than a good war!"

ANDREY KOROTKOV, HEAD, DEPARTMENT FOR INTERNATIONAL INFORMATION PROCESSES AND RESOURCES, MOSCOW STATE INSTITUTE OF INTERNATIONAL RELATIONS (MGIMO), RUSSIA

Korotkov is known as one of Russia's top technology leaders. Former First Deputy Minister of the Russian Ministry for Telecommunications and Informatization, Korotkov was responsible for several large information systems. He was an ICT adviser to former UN Secretary General Kofi Annan.

"It's sometimes hard to judge where cyber attacks are coming from, but **'Internet sovereignty'** needs to be recognized and respected... When you're speaking on the Internet, you must abide by laws."

LIU ZHENGRONG, DIRECTOR, INTERNET INFORMATION SERVICE COMMISSION, CHINA

Liu is Deputy Director General of the Internet Affairs Bureau of the State Council Information Office, Director General of the China Internet Media Research Center, and Director of China's Internet Information Service Commission. He is the former First Information Secretary in the Chinese Embassy in the United States and was a guest researcher at Harvard University.

69% DOUBT THEIR COUNTRY COULD DEFEND AGAINST A SOPHISTICATED CYBER ATTACK.

66% VIEW THEIR GOVERNMENT'S MATURITY AS LOW REGARDING INTERNATIONAL COOPERATION IN CYBERSECURITY.

70% BELIEVE THAT INTERNATIONAL POLICIES AND REGULATIONS ARE FAR BEHIND TECHNOLOGY ADVANCES.

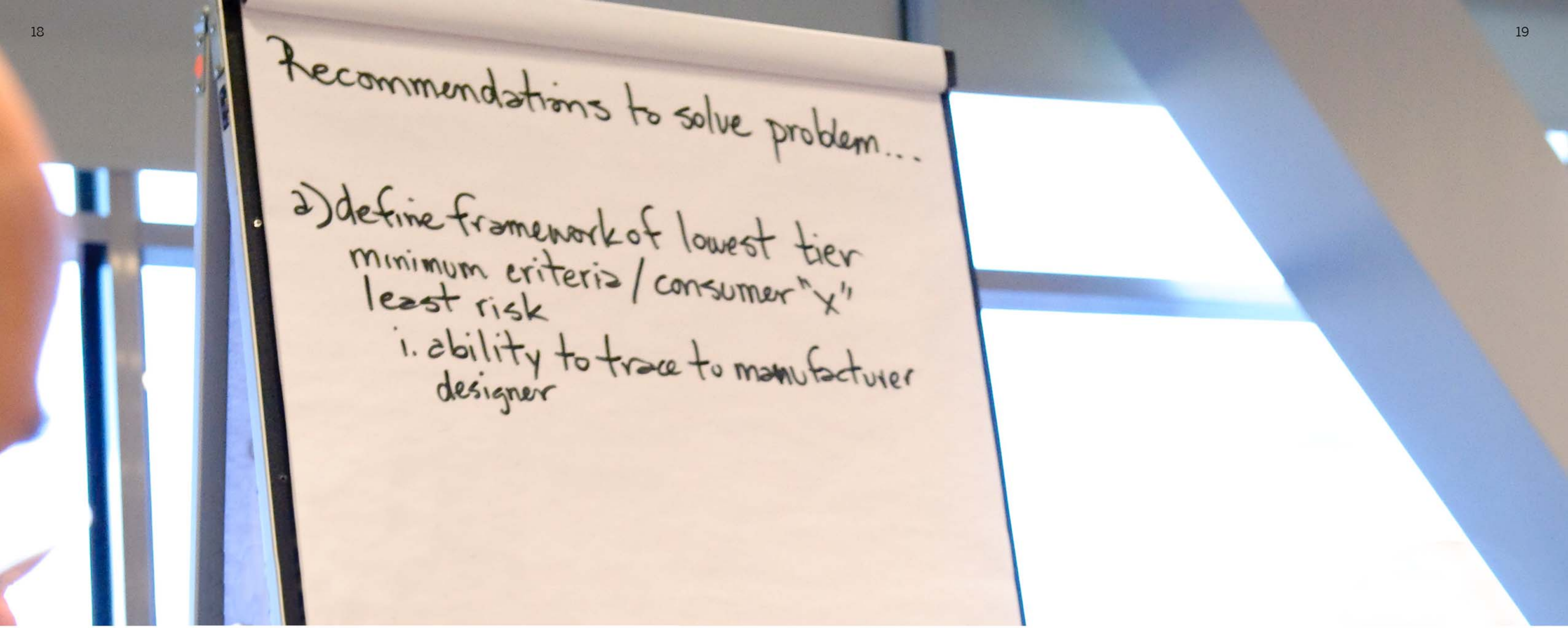
61% ANTICIPATE THE IMPACT OF LOSING GLOBAL CONNECTIVITY FOR AN EXTENDED PERIOD OF TIME TO BE CATASTROPHIC WITH IRREVERSIBLE CONSEQUENCES.

66% THINK HOME USERS NEED TO TAKE MORE RESPONSIBILITY FOR CYBERSECURITY.

66% A 'TREATY ON CYBER WARFARE' IS NEEDED NOW OR IS OVERDUE.

DO WE NEED TO **WORRY** ABOUT CYBERSECURITY?

The experts say yes. During the summit, we polled participants about the current situation in cyberspace and what needs to be done. Here are their concerns.



OUR **CYBERSECURITY AGENDA** AT EWI

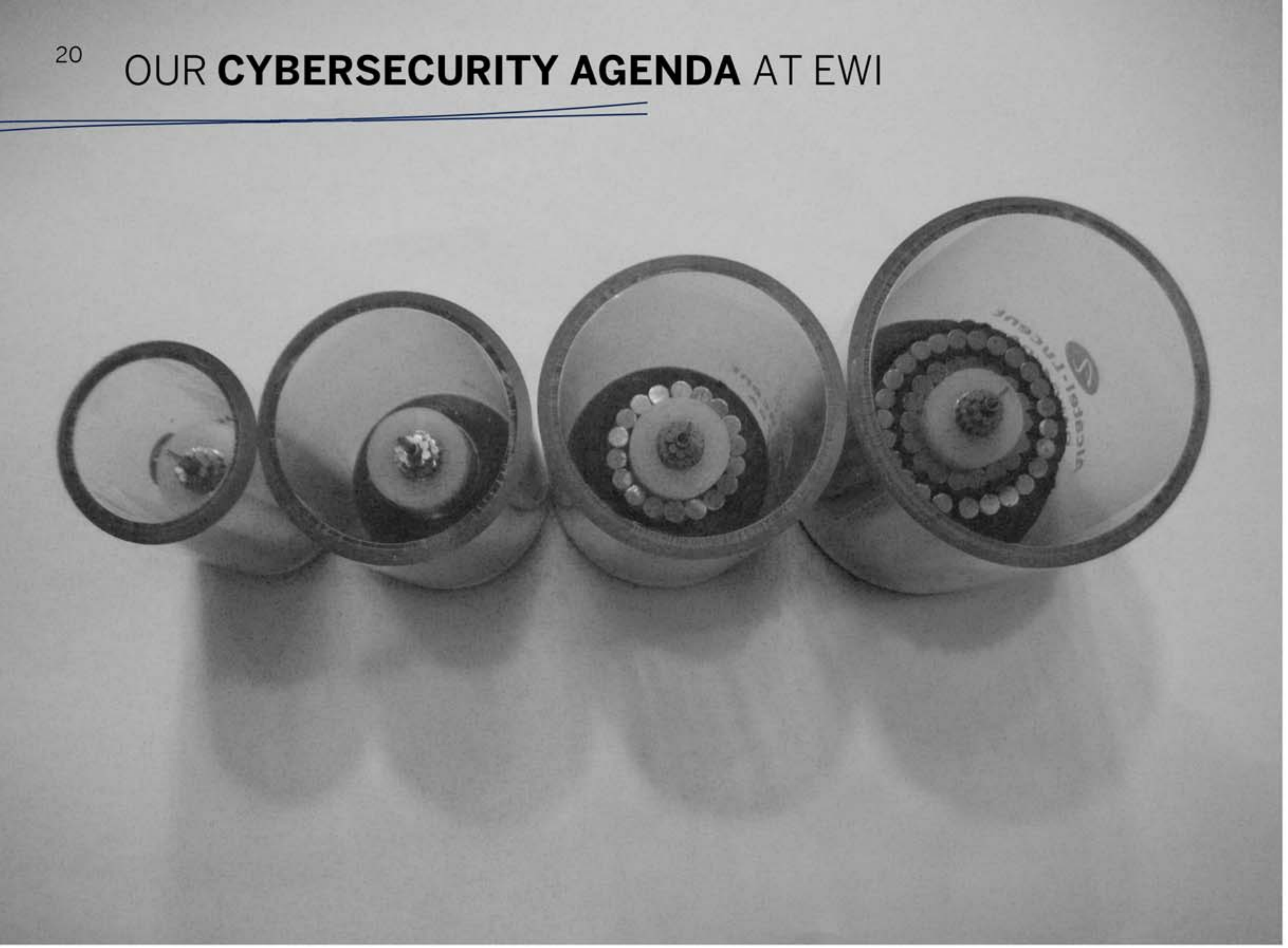
In Dallas, we learned that by bringing together a broad spectrum of experts, clearly framing the issues and guiding the discussion toward realistic recommendations, we can foster international cooperation. But we also realized that it will be difficult to develop global agreements, standards, policies and regulations (ASPR) due to a lack of trust.

In the wake of the summit, we reached out to countries most seriously affected by mistrust. Currently, we are facilitating bilateral processes between the United States and Russia, and the United States and China. We are also working with governmental and technical experts in India. These kinds of bilateral efforts will be the key to helping countries address the attribution problem – that is, to better track and prosecute online crime – and cooperate to protect critical infrastructure and Internet users.

In some ways, the Dallas summit revealed the current limitations of cyber legislation. We left with the clear impression it could take years to arrive at a global treaty on cybersecurity, since many states are not ready for it – and perhaps never will be. As a result, we began to consider voluntary agreements in the private sector and international standards as avenues to change. We decided that the best approach is to target concrete, specific problems while "speaking to the big issues."

So which problems should we tackle first? At the Dallas summit, participants met in smaller working groups. Each group was asked to identify an international cybersecurity issue and to develop solutions. After the summit, we looked at the work of each group and decided which issues to tackle first. How? We prioritized based on the urgency of the problem, the potential impact of a breakthrough and the feasibility of the solution from a business and policy perspective.

These six issues top our cybersecurity agenda at EWI.



UNDERSEA CABLES AT RISK

Undersea fiber-optic cables carry over 99% of all intercontinental Internet traffic, but many people don't even know they exist – let alone underpin the worldwide web. Built and maintained by a handful of private companies, and generally reliable, the cables are vulnerable to natural events like earthquakes and to intentional tampering. Damage to one of the three "cable chokepoints," where undersea cables converge would cause a loss of connectivity lasting anywhere from a few days to a few weeks, and cost the world billions of dollars.

At EWI, we think that the first step for protecting the undersea cables is raising public awareness about our daily dependence on this crucial infrastructure. The next step is engaging private and public sector stakeholders to create best practices for securing and maintaining the cables. To foster this effort, EWI and IEEE have begun a program of advocacy and mobilization called the Reliability of Global Undersea Cable Communications Infrastructure (ROGUCCI). Most recently, we have reached out to government and financial sector leaders in India, China and Hong Kong to discuss an immediate need: assuring the speedy repair of the cables in case of damage.

To learn more about ROGUCCI and our recommendations for securing our global undersea communication cables network, visit http://www.ieee-rogucci.org/.

INTERNATIONAL PRIORITY COMMUNICATIONS POLICY

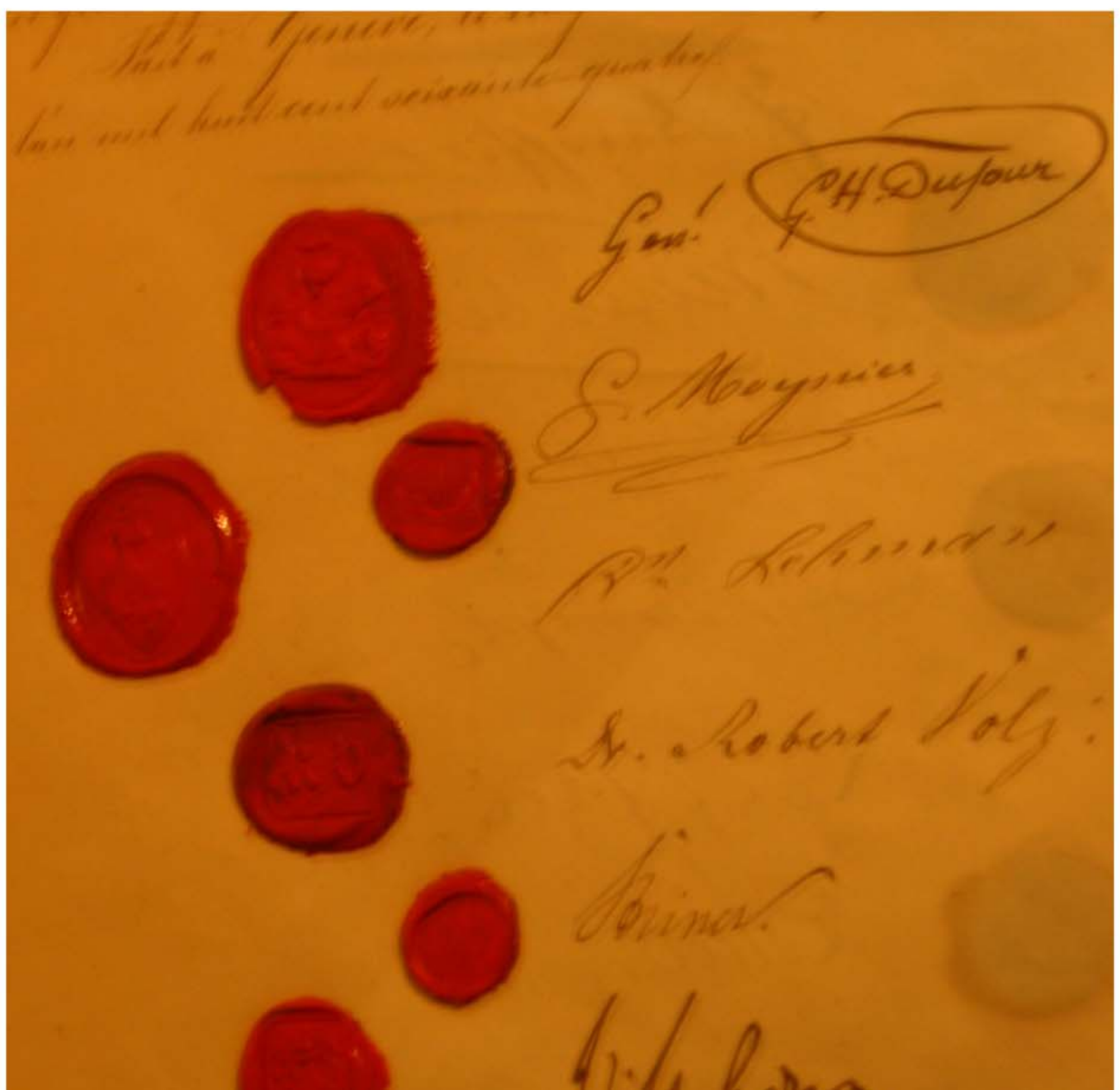
On September 11, 2001, U.S. Federal Reserve Board chairman Alan Greenspan was in Europe and couldn't complete a call to the United States. According to his Chief of Staff, Greenspan had a "fast pass card" that should have allowed his call to jump the queue, but its American code was not recognized in Europe. Just as during a bad traffic jam, an ambulance can still drive down a crowded city street, "priority information" like Greenspan's call should be able to push through a congested worldwide communications network. But during the large-scale crises, priority information doesn't always make it through... and crises are just when it matters most.

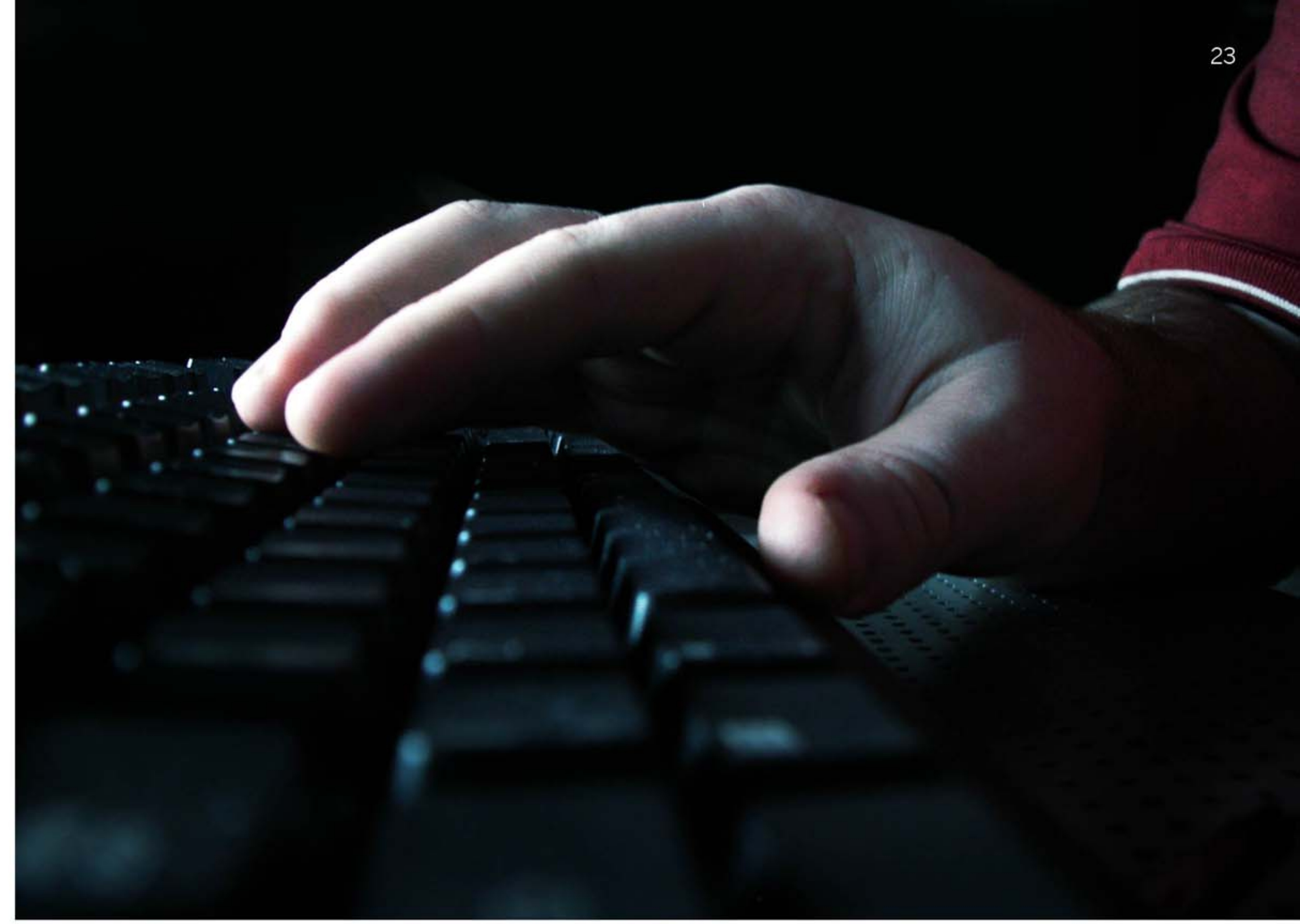
With the rising use of bandwidth-intense applications like imaging, video and gaming, today's networks are increasingly overburdened. Even though the equipment and codes exist to fast-track priority information, there are no policies in place to assure that, say, a Spanish mobile phone company will recognize a code from England. At EWI, we are raising awareness of this problem in governments and communications companies around the world. At events like our Second Worldwide Cybersecurity Summit in London, we are working to create policy recommendations for universal code standards.

CYBER CONFLICT POLICY AND RULES OF ENGAGEMENT

Today's wars are fought on land – tomorrow's may be fought online. In May 2010, the United States government established the Cyber Command as a new military wing. According to William J. Lynn II, the U.S. Deputy Secretary of Defense, "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare." This new idea of war raises troubling questions – for instance, is it acceptable for one country to attack another's hospital databases? How about the flight systems that support passenger planes in the air?

While cyber conflicts have the potential to hurt citizens as profoundly as conventional battles, we do not have a Geneva Convention for cyber war. To help solve the problem, EWI has established Track II bilateral processes with the United States, Russia and other key nations. Working through cooperative dialogue, EWI will continue to help senior officials in governments as well as private sector stakeholders develop "rules of the road" for cyber conflict.

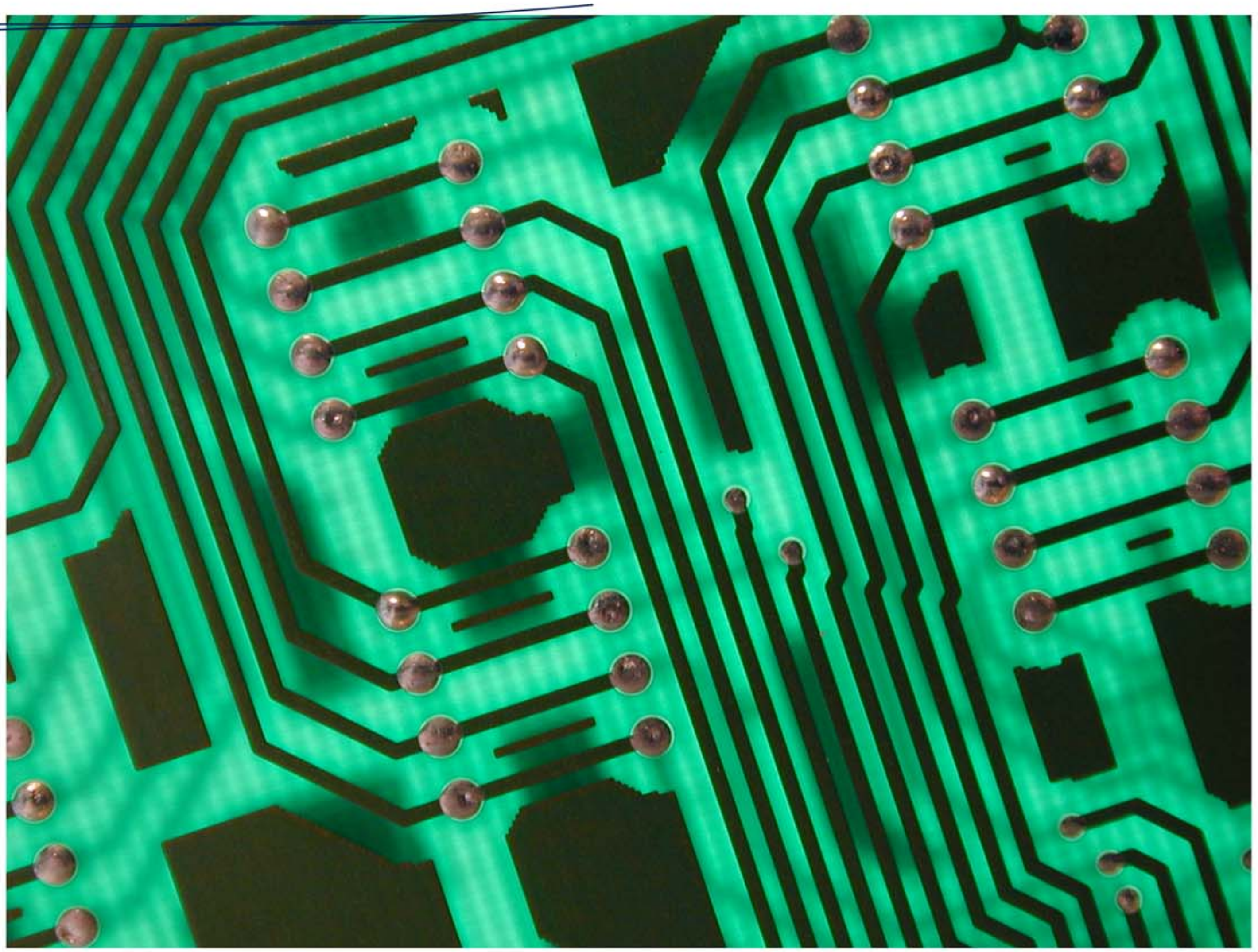




CYBERSECURITY BREACH INFORMATION SHARING

One morning, our Chief Technology Officer at EWI Karl Rauscher got a call like many have had recently. The call was from his bank: his credit card had been compromised after a retail purchase. Which retailer? The bank wouldn't tell him. Why not? Because if a popular retailer were linked with a security breach, they could lose customers, just as if a Wall Street trading company admits it's been hacked, the negative affect on its reputation could be devastating to the trust needed in its operations. For Karl, this story represents a lost opportunity: if this information were reported, we could use it to better understand the real problems individuals, financial institutions, government agencies and retail stores are having right now. Since we lack even an approximate sense of how many breaches occur, there is insufficient motivation to provoke effective measures to correct the problems.

At EWI, we believe that if compromised parties could share information without fear of tarnishing their reputations or losing business, we could aggregate strong statistical data on the number of breaches. We are working to create a trusted environment, where stakeholders can confidently and confidentially report information. One day, this effort could result in a unified database, but for now, we are working to build trust on a person-by-person level – a hub of personal connections spanning the globe.



ICT DEVELOPMENT SUPPLY CHAIN INTEGRITY

In an overseas factory, a foreign agent inserts malicious logic into a batch of computer chips. Months later, a “logic bomb” is activated in the chip, which sits inside a Pentagon computer. While this scenario may seem unlikely, many computer chips are made in insufficiently secured factories. Cyberspace is comprised of hardware and software designed, built and deployed via supply chains spanning the globe. Although the security of this technology is vital for economic stability and national safety, that security is difficult to ensure.

At EWI, we understand the challenges of securing ICT supply chains and the development environment. We understand that competitive, innovative companies have their own ways of securing their products. We understand that giants and smaller start-ups alike would be burdened by overly-rigid international regulations. So we are working to promote international standards – a measurable scale like a thermometer – that governments and businesses can use to assess the integrity of products and services.

WORLDWIDE CYBER EMERGENCY RESPONSE COORDINATION CAPABILITY

If the cyber equivalent of Pearl Harbor strikes, there is a response in place... up to a point. While many countries and companies have Computer Emergency Response or Readiness Teams (CERTs) capable of dealing with worms and virus like Stuxnet, there is still a big gap in our ability to respond to a major cyber emergency. For one, most African and Eurasian countries are excluded from this network of teams. For another, the person-to-person network is still too inefficient to respond swiftly and decisively to a major cyber emergency.

At EWI, we are working to build understanding among nations states, to lay the groundwork for cooperation in case of a major international cyber crisis. Such a capability would complement the existing CERT capabilities with “infrastructure-level emergency response” capabilities in order to better prepare for a catastrophic cyber event.

IF YOU ARE INTERESTED IN LEARNING MORE ABOUT EWI'S CYBERSECURITY AGENDA AND HOW YOU CAN GET INVOLVED – PLEASE VISIT OUR WEBSITE AT **WWW.EWI.INFO/CYBER** OR CONTACT OUR CYBERSECURITY PROGRAM ANALYST **FRANZ-STEFAN GADY** AT FGADY@EWI.INFO

MEDIA ATTENTION

SUMMIT PLEDGES TO FIGHT INTERNET CRIME

Senior officials and private sector leaders pledged to work toward multilateral agreements on cyberwar and cybercrime and stronger authentication for online transactions. Á three-day, 40-nation summit on cybersecurity hosted by the non-profit **EastWest Institute** suggested a series of measures that should be taken by defence officers, law enforcement and by the private sector. ...The presence of 500 people, many with significant standing in countries including the US, Russia and China, indicated impatience with the pace of official efforts to combat what many see as a threat to national and economic security.

FINANCIAL TIMES, MAY 5, 2010

DELL CEO CALLS FOR COLLABORATIVE EFFORT TO SECURE THE INTERNET

Rising cyberattacks are being carried out by cybergangs who control large botnets. These sprawling networks of infected home and workplace PCs are being used to compromise confidential information, taint and cripple websites and swipe financial, commercial and military data. Summit attendees will hear how criminals and terrorists can use botnet-driven cyberattacks to paralyze communications infrastructure, compromise international financial systems and disrupt government services.

USA TODAY, MAY 4, 2010

IS THERE REALLY A CYBERWAR? TERM MIGHT BE MISUSED

Is there a "cyberwar" going on? Some officials and computer security companies say yes, arguing that armies of hackers are stealing online secrets and using the Internet to attack infrastructure such as power grids...Cyberwar is a catchall phrase: It's often used to refer to everything from purely financial crimes to computer attacks that could kill people by blowing up an oil pipeline. The conference was sponsored by the **EastWest Institute** think tank and assembled about 400 security officials and industry executives from dozens of countries.

WASHINGTON POST, MAY 5, 2010

CYBERSECURITY SUMMIT KICKS OFF WITH CALLS TO ACTION

Securing cyberspace needs more public-private cooperation and a greater ability to identify and punish perpetrators, officials and business leaders said as a conference got underway...**The Worldwide Cybersecurity Summit**, hosted by the **EastWest Institute** think tank, features three days of discussions on ways to protect the world's digital infrastructure from electronic threats. Some 400 government officials, business leaders and cybersecurity experts from China, France, Germany, India, Russia, the United States and three dozen other countries are attending the gathering, which is being held in the wake of cyberattacks on Google which the Internet giant said originated in China.

AFP, MAY 3, 2010

UNITING NATIONS AGAINST CYBERCRIME, BUT NOT YET

The first Worldwide Security Summit has attracted people from more than 40 countries to Dallas, but don't expect cybercrime to be wiped out any time soon. Can we do anything about cybercrime? That's the question being addressed in Dallas this week at **the first Worldwide Security Summit** organised by **EastWest Institute**, a global a thinktank. EWI says: "Electronic attacks around the world have compromised confidential information, crippled official web sites and have exposed the vulnerability of financial data. They have heightened fears that criminals or terrorists could use cyberspace to paralyze communications infrastructure, international financial systems or critical government services."

GUARDIAN, MAY 4, 2010

BE PART OF THE **SOLUTION**

SECOND WORLDWIDE CYBERSECURITY SUMMIT, LONDON, JUNE 1-2, 2011

Intrigued by Dallas? **Join us in London**. Co-hosted by the Financial Times and the leading business network London First, the Second Worldwide Cybersecurity summit in London promises a high caliber of participation, media attention and real steps forward.

The goals of the second summit are:

- To take three of the most pressing issues in global management of cybersecurity and showcase them, alongside proposed solutions:
  - a harmonized global framework for cyber crime, with case studies from the financial services sector;
  - an international cyber catastrophe response capability for all 233 countries & territories connected to the Internet, focusing on examples from the financial services sector;
  - multilateral agreement(s) on cyber warfare.
- To test multilateral crisis-response mechanisms through a scenario exercise.
- To identify new areas where there is a need and opportunity for international policy innovation and create breakthrough groups to address them.
- To advance work on the top five breakthrough groups formed at the first Worldwide Cybersecurity Summit in Dallas.
- To showcase best-in-class research and analysis on building trust and other political aspects of cybersecurity policy from China and Russia.
- To provide a platform for non-Western cybersecurity leaders.
- To showcase new examples of cross-border youth engagement in personal protection and privacy issues.

LONDON SUMMIT **REGISTRATION**:

Please submit an application at **WWW.CYBERSUMMIT2011.COM**

REGISTRATION FEES:

REGULAR REGISTRATION	$1,500
EARLY BIRD REGISTRATION (UNTIL FEBRUARY 28, 2011)	$1,250
EWI PARTNERS (including IEEE, World Federation of Scientists and London First members)	$950

Scholarships are available at EWI's discretion.

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World
30 YEARS

BE PART OF THE SOLUTION

SECOND WORLDWIDE
CYBERSECURITY
SUMMIT

MOBILIZING FOR
INTERNATIONAL ACTION

LONDON, JUNE 1-2, 2011

TO REGISTER, VISIT: www.cybersummit2011.com

"**CYBER THREATS** ARE BOTH OVER-AND-UNDERESTIMATED: THEIR SCOPE IS UNDERESTIMATED, WHILE THE ROLE OF MALEVOLENT ACTORS IS EXAGGERATED. MOST USERS ARE LEGITIMATE AND ONLY FEW MALEVOLENT."

MICHAEL DELL, CHAIRMAN OF THE BOARD OF DIRECTORS AND CHIEF EXECUTIVE OFFICER OF DELL.

Dell is the author of *Direct From Dell: Strategies That Revolutionized an Industry*, his story of the rise of the company and the strategies he has refined that apply to all businesses. In 1998, Michael formed MSD Capital, and in 1999, he and his wife formed the Michael & Susan Dell Foundation. Dell serves on the Foundation Board of the World Economic Forum, the executive committee of the International Business Council and is a member of the U.S. Business Council.

Supporters of EWI's Worldwide Cybersecurity Initiative and Summit Series include:

LEAD SPONSORS

at&t
DELL
Microsoft
Deloitte.
KNIGHTSBRIDGE GROUP
FT FINANCIAL TIMES
THE PEROT GROUP
AKIN GUMP STRAUSS HAUER & FELD LLP

SPONSORS

AA
MOTOROLA
VERISIGN
JUNIPER NETWORKS
LOGOMOTION
TeleGeography

IN PARTNERSHIP WITH

London First
IEEE
IEEE COMMUNICATIONS SOCIETY
CONSUMER ELECTRONICS SOCIETY
WORLD FEDERATION OF SCIENTISTS
NEW EUROPE
PUBLIC STRATEGIES INC

EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World
30 YEARS

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) non-profit 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 Brussels
59-61 Rue de Trèves
Brussels 1040
Belgium
32-2-743-4610

EWI Moscow
Sadovaya-Kudrinskaya St.
8-10-12, Building 1
Moscow 123001
Russia, 7-495-691-04949

EWI New York
11 East 26th Street
20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100

www.ewi.info