MOBILIZING FOR INTERNATIONAL ACTION

SECOND WORLDWIDE CYBERSECURITY SUMMIT IN LONDON

EASTWEST INSTITUTE

Forging Collective Action for a Safer and Better World

30 YEARS

At the EastWest Institute's Second Worldwide Cybersecurity Summit, held June 1-2 in London, more than 450 government, industry and technical leaders from 43 countries gathered to craft new solutions for threats facing our digital world.

Globe Encounters

In the Information Age, the flow of Internet traffic between locations is nearly ubiquitous. Globe Encounters visualizes the volumes of Internet data flowing between New York and cities around the world over the past 24 hours. The size of the glow on a particular city location corresponds to the amount of IP traffic flowing between that place and New York City. A larger glow implies a greater IP flow.

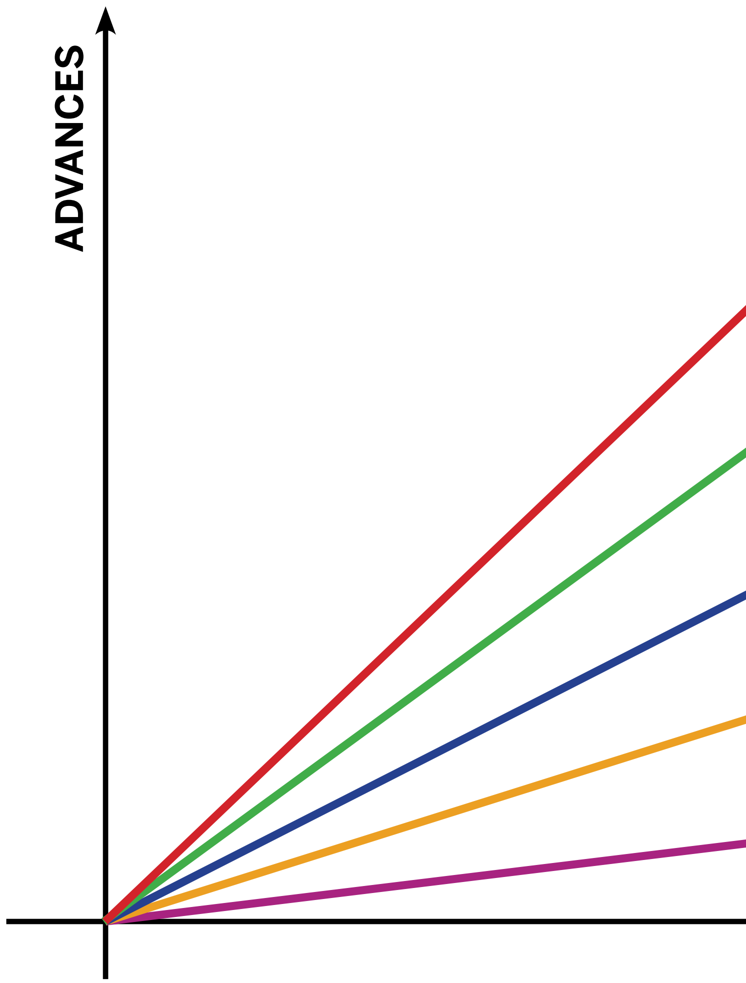
TABLE OF **CONTENTS**

The **Problem**

Every day, billions of phishing emails bombard personal computers, carrying malware and viruses. Hackers steal client data from company websites, accusations of cyber espionage fly and countries uneasily wonder whether cyber attacks can be considered acts of war.

At EWI, here's how we understand the global cybersecurity challenge: As technical innovation has skyrocketed, the global economy has become increasingly digitalized. Every day, we depend more on the worldwide web and its infrastructure, from the undersea cables that carry over 99% of intercontinental Internet traffic to our own mobile web access devices. Cyber crime exploiting these technologies is on the rise, but the agreements, standards, policies and regulations we need to secure cyberspace lag far behind.

To track cyber criminals, protect Internet users and secure critical infrastructure, we must address the growing gap between technology and our controls over it – all of us.



Our **Solution**

Securing cyberspace is a global challenge – one that cannot be solved by a single company or country alone. That is why the EastWest Institute launched the Worldwide Cybersecurity Initiative in 2009, bringing together government and corporate partners to protect our world's digital infrastructure.

Drawing on a thirty-year history of building trust, EWI formed the Cyber40, a coalition of representatives from the world's most digitally-advanced countries. The Cyber40 is working to shape "rules of the road" for cyber conflict and fighting cyber crime through international cooperation. EWI is also helping to build innovative private-public partnerships on cybersecurity, and working towards an effective global cyberspace emergency response capability.

Since 2010, over 1,000 business, government and technical leaders have been involved in EWI's ongoing cybersecurity initiative. Our government partners include Russia, China, the United States, France, Germany, India and Japan, who are all members of an innovative forum known as EWI's Cyber40 Ambassadors group. Our corporate partners and supporters include AT&T, Microsoft, Deloitte, BAE Systems, Goldman Sachs, Huawei, Vodafone, Juniper, the Financial Times, Akin Gump, Knightsbridge Cybersystems, the Chertoff Group, VeriSign and Unisys. EWI and the IEEE Communications Society have established a partnership to support the policy aspects of cybersecurity, and the IEEE Communications Society serves as the technical co-sponsor for EWI annual worldwide summits.

EWI's annual cybersecurity summits provide a crucial forum for building international, private-public partnerships and for shaping the agreements, standards, policies and regulations (ASPR) we need to protect cyberspace.

ASPR = Agreements, Standards, Policy and Reguilations

The **Dallas Process**

EWI held The **First Worldwide Cybersecurity Summit**: Protecting the Digital Economy from May 3-5, 2010 in Dallas Texas. It convened more than 400 members of the policy and law enforcement communities, as well as business and technology leaders from the Cyber40 – a grouping of the G20 countries plus the next 20 most digitally-advanced nations.

Speaking at the opening ceremony, Michael Dell 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."

EWI's summits are designed to answer that call, providing a unique environment in which private and public sector leaders can address specific cybersecurity threats. While tightly-timed plenary sessions are a large attraction, the summit is more than a chance for participants to learn– it's a chance for them to network and actively craft solutions.

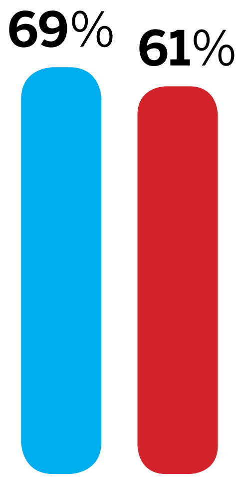
The Dallas Process included bilateral dialogues that continued throughout the year. Talks between U.S. and Chinese experts on regulating spam and U.S.- Russia talks on defining rules of the road for cyber conflicts both produced attention-getting reports. The Dallas summit also created breakthrough groups, small, international groups of experts committed to solving a specific cybersecurity threat. These groups are encouraging practical steps for everything from securing the undersea cables that carry over 99% of intercontinental Internet traffic to ensuring emergency cooperation after disasters.

A year after the summit in Dallas, EWI hosted the **Second Worldwide Cybersecurity Summit** from June 1-2, 2011 at the Queen Elizabeth II Conference Center in London, which drew more than 450 government, industry and technical leaders from 43 countries. The London summit built on the work of the Dallas summit, with meetings of existing breakthrough groups, meetings of new "London Process" breakthrough groups, and informal opportunities for cross-sector collaboration.

In anticipation of the EWI's **Third Worldwide Cybersecurity Summit**, to be held in New Delhi in 2012, this report intends to share highlights from the London summit – key observations, new proposed solutions and next steps for protecting our world's digital infrastructure.

Worrying **Numbers**

Here's a look at how world experts saw the cybersecurity challenge in **Dallas 2010** and how they saw it one year later in **London 2011**.



MAJORITY DOUBTS THAT THEIR COUNTRY COULD DEFEND AGAINST A SOPHISTICATED CYBER ATTACK

84%

THINK THAT THE CYBERSECURITY RISK WE FACE TODAY IS **HIGHER** COMPARED TO ONE YEAR AGO

70%

BELIEVE THAT INTERNATIONAL POLICIES AND REGULATIONS ARE FAR BEHIND TECHNOLOGY ADVANCES

66%

THINK HOME USERS NEED TO TAKE MORE RESPONSIBILITY FOR CYBERSECURITY

54%

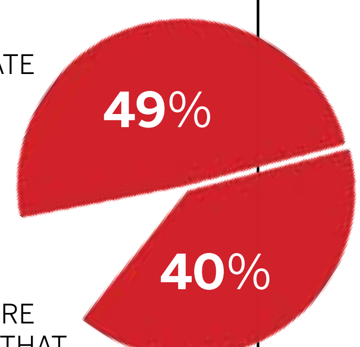
DOUBT THAT THEIR ORGANIZATION (BUSINESS, AGENCY) IS CAPABLE OF DEFENDING ITSELF AGAINST A SOPHISTICATED CYBER ATTACK

MAJORITY DESCRIBES THEIR GOVERNMENT'S LEVEL OF UNDERSTANDING AND COMMITMENT TO INTERNATIONAL COOPERATION IN CYBERSECURITY AS LOW

66%

SAY THAT A 'TREATY ON CYBER WARFARE' IS NEEDED NOW OR IS OVERDUE.

THINK THAT CORPORATE BOARDS GROSSLY UNDERESTIMATE THE CYBERSECURITY PROBLEM



THINK THAT BOARDS ARE 'ARE SO CONFUSED THAT THEY DO NOT KNOW WHAT TO THINK'

81%

AGREE THAT BOLD STEPS ARE NEEDED IMMEDIATELY TO ADDRESS THE LACK OF TRUST IN THE INTEGRITY OF ICT DEVELOPMENT AND SUPPLY

Flags from the **Cyber40**, an informal grouping of the world's most digitally-advanced nations

EWI's **Global Effort**

All around the world, companies, governments and nonprofits are working independently on cybersecurity. EWI's cybersecurity initiative is distinguished by our truly global scope – and our ability to bring experts from different countries and sectors together to forge solutions. The first step to creating collective solutions is building trust – a method that has been at the heart of EWI's activities for the past thirty years.

Established during the Cold War, EWI's original mission was to build trust between what was then called the East and West: The Soviet Union and the Warsaw Pact countries, and the United States and its NATO allies. Forging a unique "Track 2" diplomatic approach, EWI encouraged business, government and civil society leaders from both sides of the Iron Curtain to work together on some of the era's most divisive issues.

Thanks to our legacy, EWI has earned a reputation as a trusted convener and honest broker. In this capacity, EWI has launched cutting-edge cybersecurity collaborations between the United States and Russia, and the United States and China. Looking to the future, EWI is also reaching out to leaders in India and other rising cyber powers.

China

At their meeting in January 2011, President Barack Obama and President Hu Jintao called for the United States and China to cooperate on cybersecurity – a call that, a year earlier, EWI anticipated by bringing together a team of U.S. and Chinese experts on a major cyberspace challenge for the first time ever.

Fighting Spam to Build Trust is a report that makes strong joint recommendations for decreasing spam – an underrated problem in cyberspace according to EWI Chief Technology Officer Karl Rauscher, who led the bilateral process with Zhou Yonglin, Director of the Internet Society of China's Network and Information Security Committee. Spam, which comprises as much as 90% of all email messages, irritates end-users, clogs networks and carries the malicious codes used by hackers for crime.

To fight spam, the experts made two key recommendations: first, the creation of an international forum to deal with spam; second, that network operators, Internet service providers and email providers cooperate to enhance and maintain consensus best practices, beginning with the 46 initially provided in the report.At the Second Worldwide Cybersecurity Summit in London, the experts discussed how to implement these recommendations and conduct outreach to the broader international community. The report is just the beginning of EWI's bilateral work with China and the United States on cybersecurity. EWI's China-U.S. team will continue its collaboration, going on to address a series of more difficult and complex cybersecurity challenges in the months and years ahead.

According to Rauscher and Zhou, "In a time when most can only see a grim, downward spiral of recrimination when it comes to all things cyber, this report is the product of cooperation and offers some hope for an improved relationship between China and the U.S."

"**No single country** can deal with cross-border issues such as hacking, viruses or spam on its own."

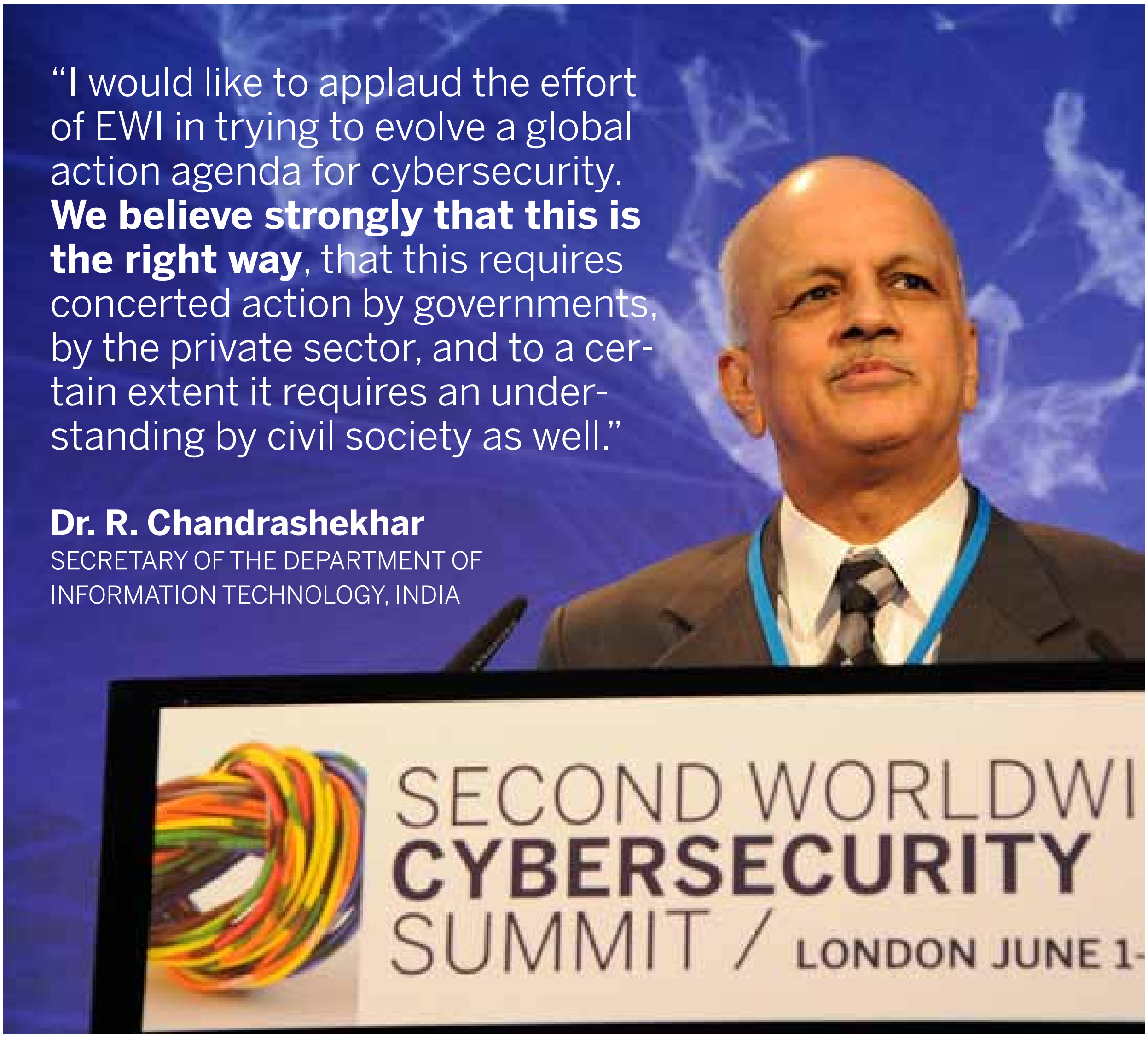
Ambassador Liu Xiaoming
AMBASSADOR OF CHINA TO THE UK

"EWI's China-U.S. bilateral report on *Fighting Spam to Build Trust* is a rare **breakthrough in international cooperation**."

Dr. Byeong Gi Lee
PRESIDENT, IEEE
COMMUNICATIONS SOCIETY

"I would like to applaud the effort of EWI in trying to evolve a global action agenda for cybersecurity. **We believe strongly that this is the right way**, that this requires concerted action by governments, by the private sector, and to a certain extent it requires an understanding by civil society as well."

Dr. R. Chandrashekhar
SECRETARY OF THE DEPARTMENT OF INFORMATION TECHNOLOGY, INDIA



India

Digitalization has been a key ingredient in India's spectacular economic rise over the last two decades, but the public sector is still struggling to implement a comprehensive approach to cybersecurity. Also, private-public cooperation on cybersecurity is still in its infancy in India.

For those reasons, the Indian National Security Council asked EWI to explore avenues for collaboration with its Indian partners: the Federation of Indian Chambers of Commerce and Industry (FICCI), the National Association of Software and Services Companies (NASSCOM), and the Data Security Council of India (DSCI). EWI has secured a commitment from these leading Indian organizations and others to co-host the Third Worldwide Cybersecurity Summit in 2012. This year, EWI has engaged in a number of activities in India to build momentum for the summit.

In April, EWI and FICCI co-hosted an impressive public seminar and a closed door private session on ROGUCCI, an initiative aimed at securing the undersea cables that carry

"I think there is a recognition by all governments, including my own, of the importance of securing cyberspace –the recognition that there has to be cooperation between governments and the private sector…I think we all recognize the threat is immense and **we still have very far to go**."

Latha Reddy
DEPUTY NATIONAL SECURITY ADVISER OF INDIA

"Isn't our own homeland security dependent on India's homeland security and their cybersecurity? These things are becoming interrelated as we gain more **dependence on cyberspace**."

Lt. General (Ret.) Harry D. Raduege, Jr.
CHAIRMAN, DELOITTE CENTER FOR CYBER INNOVATION

over 99% of intercontinental Internet traffic. NASSCOM and DSCI also partnered with EWI to co-host a seminar on cooperative strategies for reducing spam, which garnered impressive attendance from the Indian private sector. Along with the United States, India is a top producer of spam – messages that often carry viruses and malicious codes that can conscript private computers into botnets, a rising problem in India according to government attendees. "India is rapidly becoming one of the most critical players in the global cybersecurity arena," concluded EastWest Institute President John Mroz. "EWI is particularly pleased to be able to facilitate highly productive sessions such as these where representatives from both the private and the public sectors can work closely with their counterparts in the United States and elsewhere to promote best practices on cybersecurity." In the months leading up to the summit, EWI will continue its engagement with India by hosting a range of public seminars, discussions and closed door consultations with the public and private sectors on key cybersecurity issues.

"We do this work very much in the spirit of the reset. These recommendations carry great potential for engaging the international community, because when Russia and the U.S. speak together, **the world listens**."

Karl Frederick Rauscher
CHIEF TECHNOLOGY OFFICER
AND DISTINGUISHED FELLOW,
EASTWEST INSTITUTE

Russia

In February 2011, EWI released the first ever joint U.S.-Russia publication on cyberspace: *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*. This effort brought together a team of experts from the U.S. and Russia to discuss "rules of the road" for cyber conflict, and how to extend the humanitarian principles that govern war to cyberspace.

"Our hope is that these recommendations will provoke a broad international, cross-sector debate on the very hot topic of cyber conflict," said the report's co-author and leader of the Russian experts, Andrey Korotkov.

In that, the report was successful, garnering a great deal of attention at the 2011 Munich Security Conference. In April, another group of U.S.-Russia experts convened by EWI released a joint report defining critical terms for cyber and information security. The twenty terms represented a first step toward an international cyber taxonomy– and a foundation for wording multilateral agreements on cyberspace.

Both threads of work played a major role at EWI's Second Worldwide Cybersecurity Summit in London, where speakers highlighted the need to define terms and make a special effort to protect entities like hospitals online, perhaps with special markers.

Beyond that, both reports modeled the kind of international cooperation that is possible in cyberspace - a process where experts from different countries and sectors come together to create practical solutions for the challenges facing us online.

In the months ahead, EWI will continue to carry the work of these expert groups forward, with the terminology group set to define additional terms for the cyber taxonomy and multilateral meetings on "rules of the road" for cyber conflict scheduled in Changsha, China, in the autumn of 2011.

"There is a general awareness of the breadth, depth and importance of cyber and the way it penetrates everything we do and the effect that it has on the society that we live in. This is a **game-changer**. It is shifting power within the state and to some extent equating power between states in the way that economies will grow in the future."

Baroness Pauline Neville-Jones FORMER MINISTER FOR SECURITY, UK

"The final shape of international cooperation is yet to strike a balance between individual rights and collective responsibility or between individual rights to information and privacy in cyberspace. While domestic laws and structures are in place in India, we feel that **internationally** there is a need to define jurisdictional boundaries more clearly and to create the structures of a framework of cooperation."

Latha Reddy
DEPUTY NATIONAL SECURITY ADVISER OF INDIA

"One of the key things that we and our partners are doing around the world is reaching out to the developing world to make sure that capacity is built— legal capacity, policy capacity, technical capacity—so that **all nations can share** in the prosperity and connectedness that cyberspace offers and all nations can be part of the discussion."

Christopher Painter
COORDINATOR FOR CYBER ISSUES,
U.S. STATE DEPARTMENT

"A small action made somewhere in Asia or Russia or Australia can have a huge **cyber impact on the world** — on Europe and the United States — and vice versa."

Armen Sarkissian
EWI VICE CHAIRMAN, FORMER PRIME MINISTER OF ARMENIA

A NEW WORLD (DIS)ORDER? STUXNET TO WIKILEAKS

The Second Worldwide Cybersecurity Summit took place in an environment that had fundamentally changed since the first summit in Dallas one year previously. Several key markers for this change over the course of the year were Stuxnet, Wikileaks, the emergence of web-based social networks as a game-changer in protest politics at the national level, and dizzying new heights in the scale of criminal cyber attacks and the breaches of confidential consumer data.

"A small state could be absolutely brought to its knees because everything could be closed down — its life systems, its energy systems, its medical systems. So the ability to have a serious impact on a state is there, be it in a total sense, if you had total cyber warfare, or be it in a partial sense. And clearly this means that we are getting into a sort of **cyber technology race** from a warfare point of view, from both a defensive and offensive point of view. "

Sir Michael Rake CHAIRMAN, BT GROUP PLC

"Technology on its own of course is not enough, it needs to be underpinned by genuine confidence in its use — **confidence** that it will work, that the projects will be well managed and will deliver, confidence that it's resilient and confidence that it's secure and that confidence must be shared equally by the providers of these services, the government and contractors on the government's behalf, and by the consumers of these services, industry and the general public."

Rt. Hon. Francis Maude, MP
MINISTER FOR THE CABINET OFFICE, UK

“Technologically we are losing the battle.”

Jason Pontin EDITOR, TECHNOLOGY REVIEW (MIT)

“**We are definitely not on the winning side**. There is no dent in the amount of malware and cyber attacks that we are experiencing in the world. In fact it’s still growing.”

Roel Schouwenberg SENIOR RESEARCHER, KASPERSKY LAB

“Too often, **policies have not kept pace** with the advances of technology. There are mounting international policy problems that complicate cyberspace and expose us to unwanted risks — to our children, our privacy, financial stability, and our nation’s security.”

Dr. Byeong Gi Lee
PRESIDENT, IEEE COMMUNICATIONS SOCIETY

“The analysis of Stuxnet’s malicious code shows that its designers have chosen to invest important human and financial resources in order to reach their objective. We had not observed such **investments from the attackers** that we faced until now.”

Francis Delon
SECRETARY GENERAL FOR DEFENSE AND NATIONAL SECURITY, FRANCE

“The fundamental issue lies in changing the mindset of corporations and businesses and the culture. Because at the end of the day attacks are global, but the **solutions and mindset** are still very local.”

Vartan Sarkissian CEO, KNIGHTSBRIDGE CYBERSYSTEMS

Cybersecurity Is **Transnational** and **Inter-Governmental**

The second summit saw a strong affirmation that the security of our electronic information, our advanced IT machines and related communications networks has an inescapably transnational character.

This was evidenced in remarks from several government speakers about new departments being set up in foreign ministries to handle cyber policy or existing cyber units being strengthened. For example, the Secretary General for Defense and National Security of France, Francis Delon, reported his government's recent decision to double the workforce of the French Network and Information Security Agency, the national authority for the defense of information systems, to 350 people over the next two years. He cited the recent release of the United States's international strategy paper for cyber policy.

Chris Painter, head of the new Office of the Coordinator for Cyber Issues in the U.S. State Department, spoke at the summit, as did Tim Dowse, the recently appointed head of the new Office of Cyber Policy in the UK's Foreign and Commonwealth Office.

This transnational environment is also characterized by rapidly advancing technology, high rewards for cyber crime, high impunity for such crime, new cross-border sabotage with cyber weapons (such as Stuxnet) and massive breaches of private customer data. The summit reflected a near universal consensus that we urgently need new international mechanisms to manage risk and bring a reasonable state of order to the cyber domain.

In five years time, what do we want to see in terms of international and diplomatic arrangements for cybersecurity? There was considerable agreement that existing formulas in traditional diplomacy do not address the needs. The cyber domain has transformed the exercise of state power and formulas for success in business. Cybersecurity is not exclusively what happens with code, machines or operators. Cybersecurity is part of the fabric of our daily lives. As cyber technology advances, it fundamentally alters the broader political, social and economic dimensions of life, including at the transnational and intergovernmental levels.

Policy for cybersecurity is not simply about reacting to threats. It is about shaping creative and sustainable combinations of technological and social responses at an international level. This occurs against the background of competing national legal jurisdictions, un-reconciled concepts of national sovereignty and security, a ravenous hunger by states and others for massive cyber espionage undertakings, and an all-too-visible arms race in development of cyber weapons. Summit participants emphasized time and again the need for purpose-built regimes to address these fundamentally new challenges, even as others recognized the unrealized potential of existing domestic laws and international mechanisms.

As much as private sector interests would like little or no governmental regulation in most aspects of cybersecurity, the emerging realities and, indeed, the urgency of action may be pushing us in a different direction.

"Over a hundred nations have cyber capabilities. Whether it's attacks by hackers or whether it's espionage or whether it's a broader-based, state-sponsored weaponization – there are many involved in this. This is why **many have to participate in the conversation** to address and ensure that it doesn't escalate."

Melissa Hathaway
PRESIDENT, HATHAWAY GLOBAL STRATEGIES LLC; EWI DIRECTOR

"Should we, as the cyberfication of our lives becomes even more deeply present in everything that we do, have a **crisis in confidence** in the infrastructures that we depend on, we could see an effect on a global basis that would make this past liquidity crisis [the global financial crisis] look like child's play."

Matt Bross CTO, HUAWEI

"In the past year, we have identified more than 100,000 threats deployed in **social media networks**, most aimed at gathering information by cyber criminals for largely unknown purposes. Security strategy is a process that must be continually reviewed and modified in response to changing conditions."

Natalia Kaspersky CEO INFOWATCH, CHAIR OF THE BOARD, KASPERSKY LAB

"Our dependence on cyberspace has inevitably increased our exposure to security threats and it is vital that businesses reappraise their approach to risk management accordingly. Cybersecurity is often delegated to IT departments which may put in place generic defenses that are not aimed at specific advanced threats. A more holistic, **business-led approach** to assessing impact and managing risk is required."

Martin Sutherland
MANAGING DIRECTOR, BAE SYSTEMS DETICA

"Everyone who has a computer or a mobile device that connects to the Internet is only going to come under more attacks. What is lagging behind in all of this is the policy, the strategy and approach that **government and private industry** need to take."

Lt. General (Ret.) Harry D. Raduege, Jr.
CHAIRMAN, DELOITTE CENTER FOR CYBER INNOVATION

Business Leadership out of a Cyber Crime Wave?

With strong business leadership at the summit, the stage was set for robust discussion of private sector needs and their cybersecurity practices, especially in the international domain. Few participants were prepared for the grim assessments that emerged. On the one hand, law enforcement mechanisms both domestically and internationally were seen to be on the losing side. Too many cyber criminals appear to be outside the reach of law enforcement. On the other hand, global businesses now face attacks on such a scale and frequency that board leaders are being forced to reevaluate enterprise security strategies and come to terms with new risk management strategies. For major businesses, the risks, vulnerabilities and threats are now as multinational as their corporate footprint, with the added character of being quite complex and difficult to anticipate.

Where do we want to be in five years time in terms of private-public partnerships for enhanced cybersecurity? The unanimous view might be that we want these partnerships to be richer and deeper, and to cover many more sectors. That will happen, but the most

"**We do not have any international accord** – we do not have any commonly accepted incentives to industry, there are no mandates, there are no fines and at the level of the legislative process – what it would take to begin to go and create a common infrastructure, where public and private organizations can work together is not clear."

Jason Pontin EDITOR, TECHNOLOGY REVIEW (MIT)

"Education to our leadership, to the CEO's of our corporations, is critical for them to understand the situation that we face. We need to encourage companies to discuss this openly, to show them that they are not independently suffering, that **this is a worldwide crisis** and that they must report both to law enforcement and/or regulators. "

Shawn Henry EXECUTIVE ASSISTANT DIRECTOR, FBI (U.S.)

interesting evolution in private-public partnerships will be a clearer knowledge of the boundaries of responsibility and of potential operations and actions. Many of the problems that are currently on the table in terms of what needs to be done jointly by governments and the private sector may never be addressed.

It is important to build confidence in those areas where this can be done and, where this cannot be done, to prepare for contingencies. We need to develop international mechanisms and deepen the levels of cooperation between the private and public sectors in a way that gives confidence, allows for flexible responses and, most importantly, provides the points of contact in all countries needed for a credible emergency response. Too many conversations on private-public partnerships assume they are largely American, European or trans-Atlantic. In the next five years, we need to see an evolution in the direction of partnerships that become truly global, involving many different governments, including those currently outside the Western circle of trust.

"It is impossible to build a regional legal framework that will anticipate things yet to come. Therefore I think **flexible regulations**, result-oriented and outcome-oriented rather than prescriptive regulations are needed to allow people to adapt and deal with evolving requirements."

Michael Chertoff
CO-FOUNDER, CHERTOFF GROUP, FMR. U.S. SECRETARY FOR HOMELAND SECURITY

"Individuals move from the periphery to center stage and increasingly this is where the debate about privacy and what it means for us as a society and the growth of our economies is being discussed. So as **individuals move to center stage**, the individual is increasingly taking control over their own information."

Stephen Deadman
GROUP PRIVACY OFFICER AND HEAD OF LEGAL, VODAFONE GROUP

"General security law should describe the **consequences of failure**: penalties, sanctions and rights to compensation. It would be naive to think that all relevant actors will do what is necessary to protect these assets without a clear steer from the law. Ignorance, laziness, apathy, short-sightedness, greed – these are all powerful counter waves to enlightened self interest."

Stewart Room
PARTNER, PRIVACY AND INFORMATION LAW GROUP, FIELD FISHER WATERHOUSE

Individual Users: An Obligation to Secure?

"It is important not to overlook people within an organization, because security ultimately comes down to **people using technology in secure ways**."

Matthew Kirk GROUP EXTERNAL AFFAIRS DIRECTOR, VODAFONE GROUP

In consultations leading up to the summit and in several speakers' presentations, there was a new emphasis on the role of individuals in delivering or undermining cybersecurity. This issue was raised at several levels. First, in terms of social power, some observers noted that individuals are much more able to exercise political influence through modern social media. In some fundamental way, it was suggested, the "personal worlds" of a much larger number of individuals matter more now than ever before.

Second, the new prominence of individuals has pushed privacy law out of low-profile administrative tribunals and occasional, high-profile defamation/libel hearings onto a much wider stage. This has forced changes upon legislators, police forces and courts that could not have been imagined even five years ago.

In devising legal mechanisms to secure cyberspace, several speakers proposed that we pay more attention to understanding the minds of individuals involved in everything from economic crime to harassment and vandalism. They highlighted the issue of disgruntled former employees or their allies, as manifested in the massive leak of national security information through Wikileaks and the ensuing acts of cyber vandalism by supporters of Wikileaks founder Julian Assange. The Wikileaks phenomenon demonstrates the continuing conflict between countries and within countries about the trade-offs to be made between perceived Internet freedoms and, on the one hand, the need to punish transnational cyber crime, on the other.

The "innocent" user did not escape implied criticism, with some attention to the idea that we could not rely on most users to play their part in the cybersecurity ecosystem. The evidence cited for this included the persistence in the IT marketplace of consumers opting for the cheaper price rather than basing their purchasing decisions on the quality of security systems in, or associated with, the product.

The accountability of individual users, with the concept extending to corporations and firms with legal personality, was one of the more challenging notions raised at the summit. One proposal called for the "introduction of a general obligation for security both nationally and internationally by which … holders of sensitive data and the controllers of important networks, systems and infrastructures and their supply chains should face a clear legal obligation to keep these assets safe and secure." Another speaker mentioned the need to begin to impose fines and other administrative penalties to enforce more secure behavior by firms.

Cyber Espionage: Too Big to be Ignored

At the First Worldwide Cybersecurity Summit in Dallas, the massive and increasing scale of cyber espionage was acknowledged, but the prevailing view was that we probably could not do much about it. The main reason was that states would never stop doing it and, since they would not admit to it, cyber espionage could not be controlled. At the London summit, participants argued that espionage is now too massive to ignore at the policy level. Moreover, there are fresh concerns that cyber espionage on such a massive scale has very destabilizing spillover effects, inspiring increased fears about cyber war, on the one hand, and economic insecurity on the other. Underpinning both sets of concerns is the fundamental contradiction that the main players in espionage activity are also dependent on a global supply chain. As in other areas of policy, the globalized world of cyberspace is forcing us to rethink and, in some cases, abandon traditional approaches to the sharing of once-sensitive data across national divides.

"**Cyber industrial espionage**: we know very little about this area. It is not yet compulsory in most territories to report breaches and companies are reluctant to do so for fear of damage to their image and their shareholders' dividends. But according to Verizon's latest cyber threat assessment, this accounts for 34 per cent of malfeasance on the web."

Misha Glenny AUTHOR

"Cybersecurity has nothing to do with the substance of what is being circulating on the networks. Cybersecurity has to do with protecting companies against **espionage**, but also against sabotage, whether it is carried out by possible rebels, by terrorist groups, by organized criminals."

Francis Delon
SECRETARY GENERAL FOR DEFENSE AND NATIONAL SECURITY, FRANCE

"We live in a world where 'the need to know' is still a valid principle but 'the need to share' is even more important. These two are still needed – both of them. There is a tendency at the moment, I think, to let 'the need to know' to get in the way of '**the need to share**."

Baroness Pauline Neville-Jones
FORMER MINISTER FOR SECURITY, UK

"About 60 percent of the ministerial level websites in China faced **security threats** of varying degrees in 2010."

Ambassador Liu Xiaoming AMBASSADOR OF CHINA TO THE UK

"The Internet is different in the sense that you don't have to put assets at risk to engage in **espionage**. Spies can sit in their home country and exfiltrate terabytes of data quickly."

Scott Charney
CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT

Cyber Arms Race: What Confidence Building Measures?

Where should we be in five years time in terms of "rules of the road" for cyber conflict? We should agree that there are certain cyber practices that states should not undertake because they are either threatening and destabilizing, or offensive in character. There are certain obligations in security that exist in international law, including the UN Charter, and we don't necessarily need new treaties. We can actually address most state-to-state cyber operations under existing international law.

Instead of trying to determine new laws for cyber warfare, why don't we start talking about the principles of conflict prevention or preventive diplomacy with respect to cyber operations?

That approach was demonstrated in May 2011, when the United States laid down markers in terms of what would be acceptable or not in terms of cyber conflict and created a positive international agenda. In this, the U.S. government seemed to say, "Let's have a positive conversation that reduces tension and improves mutual understanding." This would be a "preventive" conversation.

In five years time, the discussion about rules of the road is going to be very different. How can we get to that point? The U.S. State Department only recently established an office for cyber issues and the UK foreign office just set up an office of cyber policy. In one or two years, we can imagine that these brand-new offices will come to fully understand the extent of the problem and how it can be addressed, both through existing mechanisms and new mechanisms.

"It is critical to try to move towards some sort of cybersecurity **non-proliferation treaties**. But like with nuclear non-proliferation treaties, it s going to be easier to say it than to do it."

Sir Michael Rake CHAIRMAN, BT GROUP

"The way to make sure that [cyber war] never happens is to make sure that countries have close relationships and connections in place. I think those structures need to be improved and we are working on that... The most important thing is to build **international consensus.** It's not just China that we need to engage with. It is an important part of our agenda with every country."

Christopher Painter
COORDINATOR FOR CYBER ISSUES,
U.S. STATE DEPARTMENT

"A **cyber peace treaty** would be one of a kind. It would have to bring together governments, the private sector and even individuals."

Dr Hamadoun Touré SECRETARY GENERAL, INTERNATIONAL TELECOMMUNICATION UNION

"In terms of **cyber warfare**, there is a lot of strategic and doctrinal thinking not yet done. We don't know when a cyber war starts, how to declare it over, what proportionality means, and if there should be a cyber equivalent of the Geneva Convention. We are fighting on a battlefield created by man as opposed to nature, and one that is 85 percent owned and operated by the private sector."

Scott Charney CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT

"It is important to put a core group together which actually represents **major players in cyberspace** who do have some degree of commonality in terms of their interests and assumptions"

R. Chandrashekhar SECRETARY, DEPARTMENT OF INFORMATION TECHNOLOGY, INDIA

Breakthroughs

During the London summit, experts worked in "breakthrough groups" – small groups of international experts and stakeholders committed to solving a specific cybersecurity problem. Addressing priority areas identified at the First Worldwide Cybersecurity Summit in Dallas, five "Dallas Process" groups met throughout the year: International Priority Communications, Cyber Conflict Policy and Rules of Engagement, Measuring the Cybersecurity Problem, Information and Communications Technology (ICT) Development Supply Chain Integrity, and Worldwide Cyber Emergency Response Coordination Capability.

Another group met to discuss how to increase the resilience of the undersea cables that carry over 99% of intercontinental Internet traffic, basing their work on 12 bold recommendations made by the joint IEEE/EWI *Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI)* report, first presented at the Dallas Summit.

Also, following the Dallas summit, a group of U.S. and Chinese experts undertook breakthrough policy work on building trust by fighting spam. Other multinational teams devised new approaches to protecting youth in cyberspace and international legal approaches to prosecution of cyber crimes.

In the build-up to the London summit, EWI and its partners identified two more core areas where international and cross-sector collaboration was needed and formed "London Process" groups: Collective Action to Improve Global Internet Health, and Emergency Response Coordination for Major Cyber Incidents in the Financial Services Sector.

In London, the breakthrough groups began by measuring progress achieved from May 2010 to June 2011. Many recommendations are being implemented and the most advanced groups' recommendations have been institutionalized – that is, championed by external organizations. After assessing their progress, the groups went on to chart next steps and outline work for the Third Worldwide Cybersecurity Summit, to be held in New Delhi in October 2012.

The Reliability of Global Undersea Communications Cable Infrastructure

Businesses and governments rely on global connectivity for their ongoing operations. Over 99% of intercontinental connectivity is provided by the Global Undersea Communications Infrastructure (GUCCI). Every day, over $5 trillion in transactions traverse this complex network of undersea cables. This infrastructure's ultra-high reliability has enabled our total dependence on the worldwide web, but is GUCCI's reliability proportional to our complete and utter dependence on it?

At the Dallas summit, EWI launched a major advocacy effort to promote the reliability and security of the cables based on the 12 recommendations made in a joined IEEE/EWI report, *The Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI)*. Since the Dallas summit, EWI has championed many of these recommendations and conducted outreach seminars with senior government and industry leaders in Abu Dhabi, Beijing, Brussels, New Delhi, Hong Kong, Honolulu, London, Moscow, Paris and Washington, D.C.

At the London summit, experts focused on recommendations aimed at improving international governance frameworks for the cables and to encourage timely repairs of the cables in territorial waters – specifically, best practices to reduce the time needed to acquire repair ship permits from over ten weeks to a few days.

The International Cable Protection Committee (ICPC), which represents seabed users in 60 countries, has begun to implement a new governance framework to improve cross-sector cooperation. The committee has begun to expand membership, actively recruiting members from the financial services sector. The ICPC is also working to provide clear, accurate communications about the cables. To help governments speed repair ship permit times, the ICPC will recommend that countries appoint a lead agency for issuing repair permits and benchmarking progress in comparison to other countries. The ICPC will call on the end-user financial sector to weigh in on the significant impact of delayed repairs.

>> LEARN MORE: www.ieee-rogucci.org

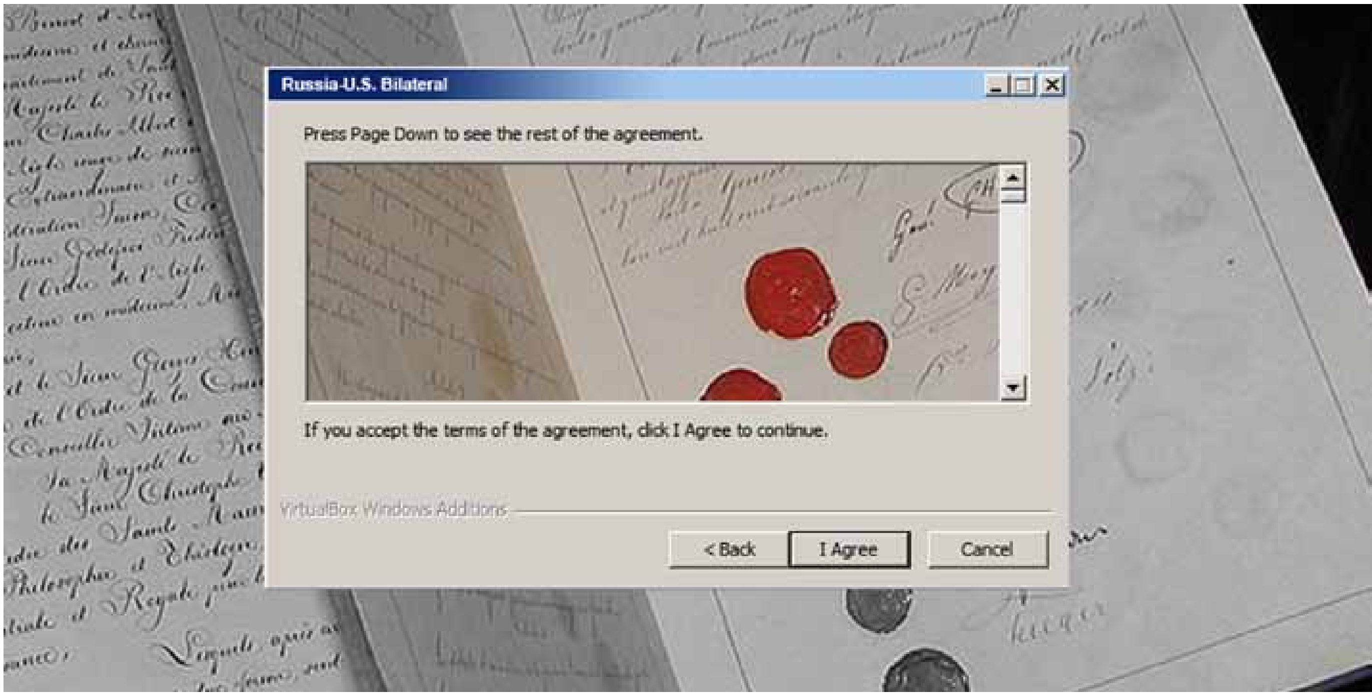
International Priority Communications

During major crises like the earthquakes that devastated Haiti and Japan, communications networks become so congested that critical calls cannot be completed – contributing to loss of life and property. Last year in Dallas, experts and stakeholders agreed that we must ensure that priority messages make it through.

During the past year, a growing team of experts and stakeholders has analyzed the problem of networks' limited capacity, considering existing capabilities, lessons learned from historic events and long-term technology evolution. The group ultimately developed recommendations for the financial services sector, governments, network operators and network equipment suppliers. The overarching recommendation is for governments to ensure that authorized users – that is, users with cell phones equipped with priority codes that fast-track their messages in crowded networks – can communicate wherever they are in times of crisis. To accomplish that, network equipment suppliers should insert software ensuring universal recognition of priority codes into equipment around the world.

In London, the group reviewed benefits to all parties, from governments to suppliers, and discussed how to build momentum for policy agreements. The working group will publicize best practices from countries with an effective priority scheme, create a list of countries that are interested in deploying an IPC system (including a government database identifying authorized users), list agencies that should be involved in each country, identify evolving standards, and determine acceptable call completion rates.

The group will share its recommendations and analysis in a forthcoming EWI report, *International Priority Communications: Making Sure the Most Important Calls Get Through*.



Cyber Conflict Policy and Rules of Engagement

For some time, common wisdom has held that setting "rules of the road" for cyber conflict would be tedious and difficult. In February 2011, EWI defied expectations, publishing *Working Toward sRules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*. The report was prepared jointly by Russian and U.S. experts and released at the 2011 Munich Security Conference, where it garnered attention at the longstanding conference's first-ever session on cybersecurity.

In April 2011, EWI and the Information Security Institute released the first joint Russian-American report to define critical terms for cyber and information security, Critical Terminology Foundations.

This ongoing breakthrough group work and the reports served as a backdrop to the London summit "rules of the road" discussions. In London, working groups discussed how markers in cyberspace can provide protection for non-combatant entities, like hospitals. According to participants, the expansion of address space provides an opportunity for creating such protected addresses.

London working groups discussed how much evidence of a cyber attack is needed to secure international assistance and protocols for collecting related evidence. They noted the lack of international standardized requirements under the UN, NATO, or intergovernmental groups for requiring servers to keep processed data. The group emphasized that the private sector, which maintains and develops the technologies, should take a leading role in resolving these issues. A major challenge yet to be resolved: how to ensure that countries don't respond too hastily to cyber attacks, before the aggressor is properly identified. Incorporating time limits into codes of conduct is a challenge – one of the many that the group will address in the year ahead.

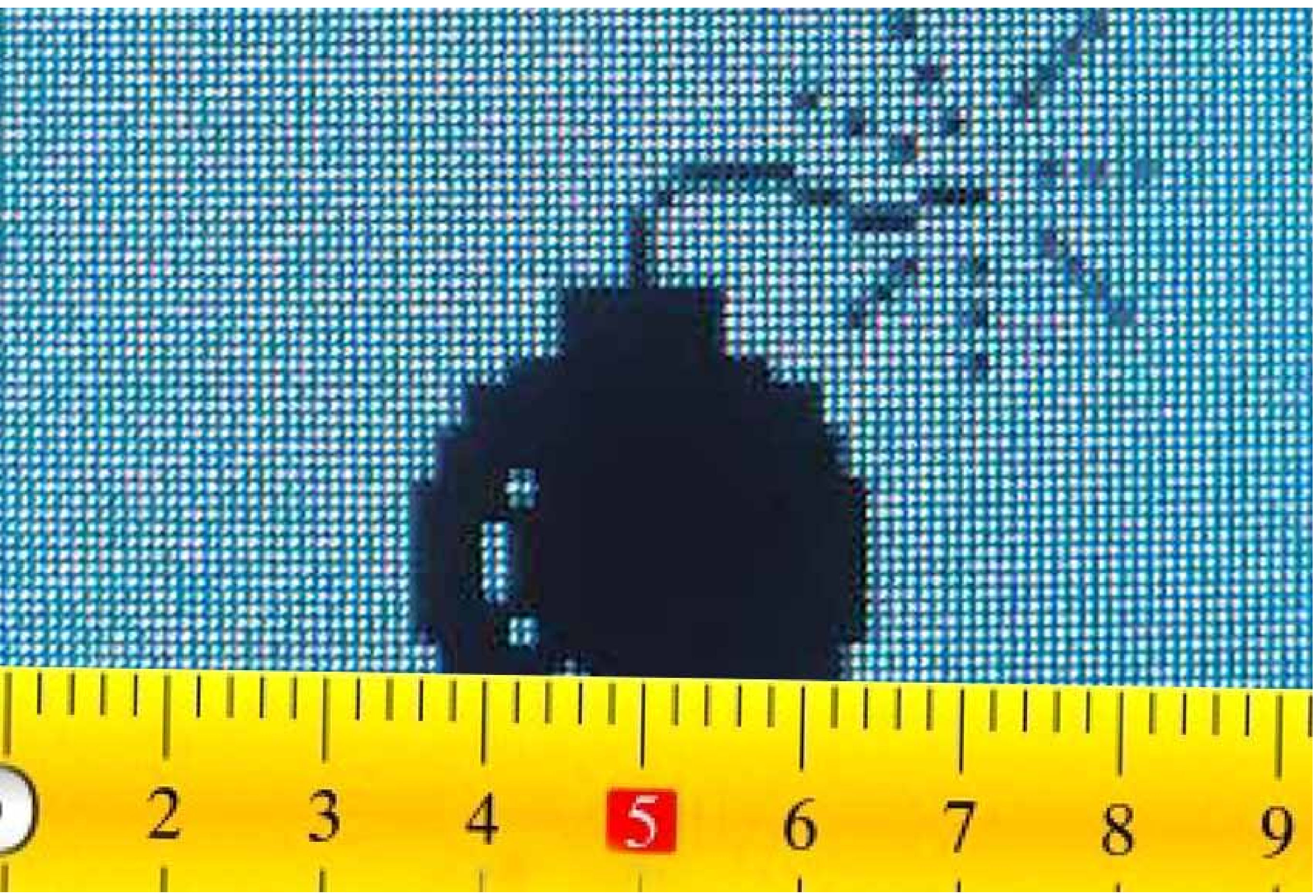
>> LEARN MORE: www.ewi.info/working-towards-rules-governing-cyber-conflict
www.ewi.info/cybersecurity-terminology-foundations

Measuring the Cybersecurity Problem

With the recent wave of corporate hackings and information theft, it is clear that we have a cybersecurity problem on our hands. But how big is the problem? Are our investments in countermeasures paying off or is the problem getting worse? It's tough to say, largely because many companies do not share information about security breaches to protect their reputations. In this environment, many companies underestimate their own security risk, which makes it difficult to justify increased security spending. The solution: accurate measurements of how frequently companies and organizations are subject to cyber attack.

According to the London working group, the private sector should establish a trusted environment in which companies can voluntarily report security breaches. This would enable the aggregation of statistical data to support measurements of the world cybersecurity problem.

A report sharing this group's analysis and recommendations is anticipated for publication in the autumn of 2011. The group will continue to explore the best approach, process design and funding model, determining what data the entity would measure. The group will consider if tax breaks could be used to incentivize participation, how to standardize breach sharing standards internationally, and how to create education campaigns to remove the stigma (and hence the corporate risks) of sharing breach information.

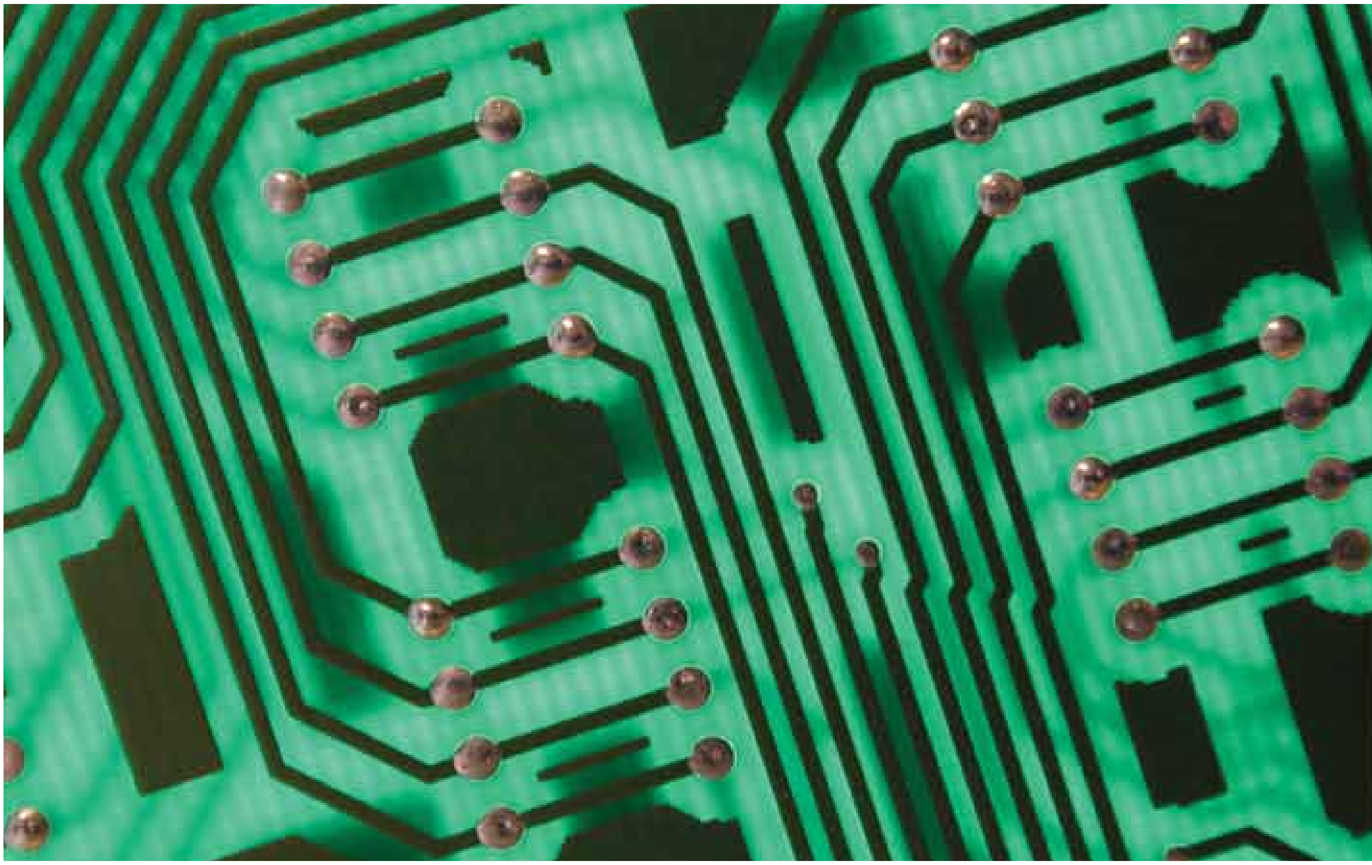


ICT Development Supply Chain Integrity

Governments, businesses and individuals depend on complex global supply chains that provide and support their ICT products. This dependence cuts across all sectors: government, defense, energy, financial services, transportation and health care. Although this reliance is growing dramatically, stakeholders cannot perform due diligence on products. Understandably, many governments are considering measures to protect their national security interests, like demanding that companies share source codes, but this kind of measure actually endangers companies' intellectual property – and lowers the security of their product. Also, company resources are strained by the need to satisfy multiple countries' regulations.

In London, the group advanced on last year's progress by further outlining the problem's scope and making recommendations. Key "takeaways" included better defining, quantifying and prioritizing the supply chain integrity problem, enabling traceability and transparency; setting up guidelines for private-public sector cooperation; and sharing of best practices.

Over the coming year, the group will further analyze the proposed recommendations. The London summit input will be integrated with current principles, which include preserving marketplace competition and encouraging governments to use empirical measures to determine where to source ICT products. The group also favors international cooperation to foster innovation. This breakthrough initiative requires a relatively longer time to complete its work, in part due to limitations in needed technologies.



International Cooperation to Fight Spam

Spam, which accounts for about 90% of all email messages, is a huge problem. Not only does it pollute cyberspace with hundreds of billions of messages every day, it is often the carrier of malicious code, like viruses. A vehicle for fraud, spam funds much of the malicious behavior on the Internet, infecting hosts via web browsers and viruses, and is often used to set up botnets – a host of infected computers taken over by hackers and used to perform malicious tasks. Botnet operators make money by sending spam via black markets and the proceeds fund identify theft and fraud. Spammers take advantage of the lack of international coordination to accomplish their goals.

In London, the group affirmed that the problem is large and on a global scale, and that the spammers' techniques are becoming more complex, and therefore necessitate improved cooperation between governments and service providers. Nearly all of the countries ranked as the top sources of spam participated in the summit.

During the summit, EWI and the Internet Society of China released *Fighting Spam to Build Trust*, a joint report by a team of U.S. and Chinese experts. This report presents two joint recommendations and 46 best practices that, if implemented, would be very effective in reducing spam. The group's working sessions, aimed in part at outreach to the broader international community, focused on how to implement the main recommendations: specifically, the creation of a regular international forum aimed at spam reduction and for stakeholders to cooperate on implementing a host of best practices.

Participants agreed that implementing the report's best practices would result in establishing critical new relationships between Internet service providers worldwide. Benefits would also include increasing the costs for spammers to operate, reducing global spam levels and making for happier netizens around the world.

This initiative is moving very fast, with planned next steps for international cooperation on reducing spam that include collaborative expert meetings in China, India and Russia. Also, the highly regarded international Message Anti-Abuse Working Group (MAAWG) has offered to facilitate the recommendations' implementation, including these next steps for new international cooperation.

>> LEARN MORE: www.ewi.info/fighting-spam-build-trust

Collective Action to Improve Global Internet Health

> "There is currently no global, coordinated approach to protecting people from malware and related threats."

Beginning with this observation, nearly 30 subject matter experts from industry, government, and academia discussed how a public health model (PHM) might be used to imagine new approaches to protecting billions of Internet users.

To begin, the PHM works at all levels from the microbial to world populations. This is necessary for Internet health as well, to represent all components and stakeholders. The public health model also suggests certain roles for stakeholders such as individuals, medical providers and governments. There are several challenging areas where the metaphor does not work perfectly, such as the speed of disease progression, the lack of an immune system for the Internet and the lack of discrete populations.

But overall, the group concluded that the metaphor was useful. Participants discussed several successful initiatives from around the world, including national clean-up programs in Asia and Europe, as well as ISP botnet-notification programs in the U.S. The group concurred that much can be learned from these programs, which could be usefully replicated around the world.

There was also a robust discussion about metrics for tabulating Internet health. The group plans to reconcile measurements at the device level, such as the infection rate of a specific computer, with those that look at entire populations. These areas present an opportunity for thorough academic research on the root causes of Internet "disease" and proper data models.

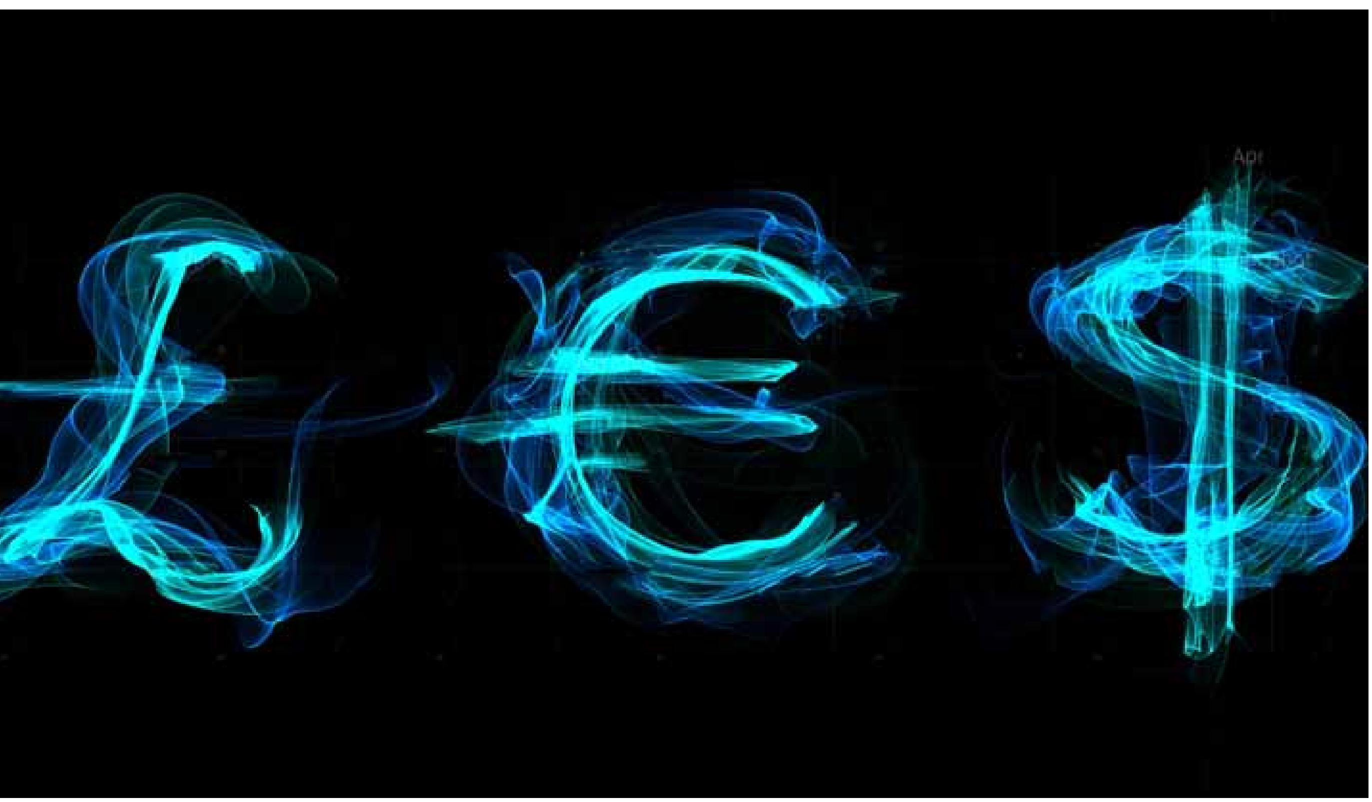
The group plans to continue this exploration of the public health model and to publish a report including recommendations for action.

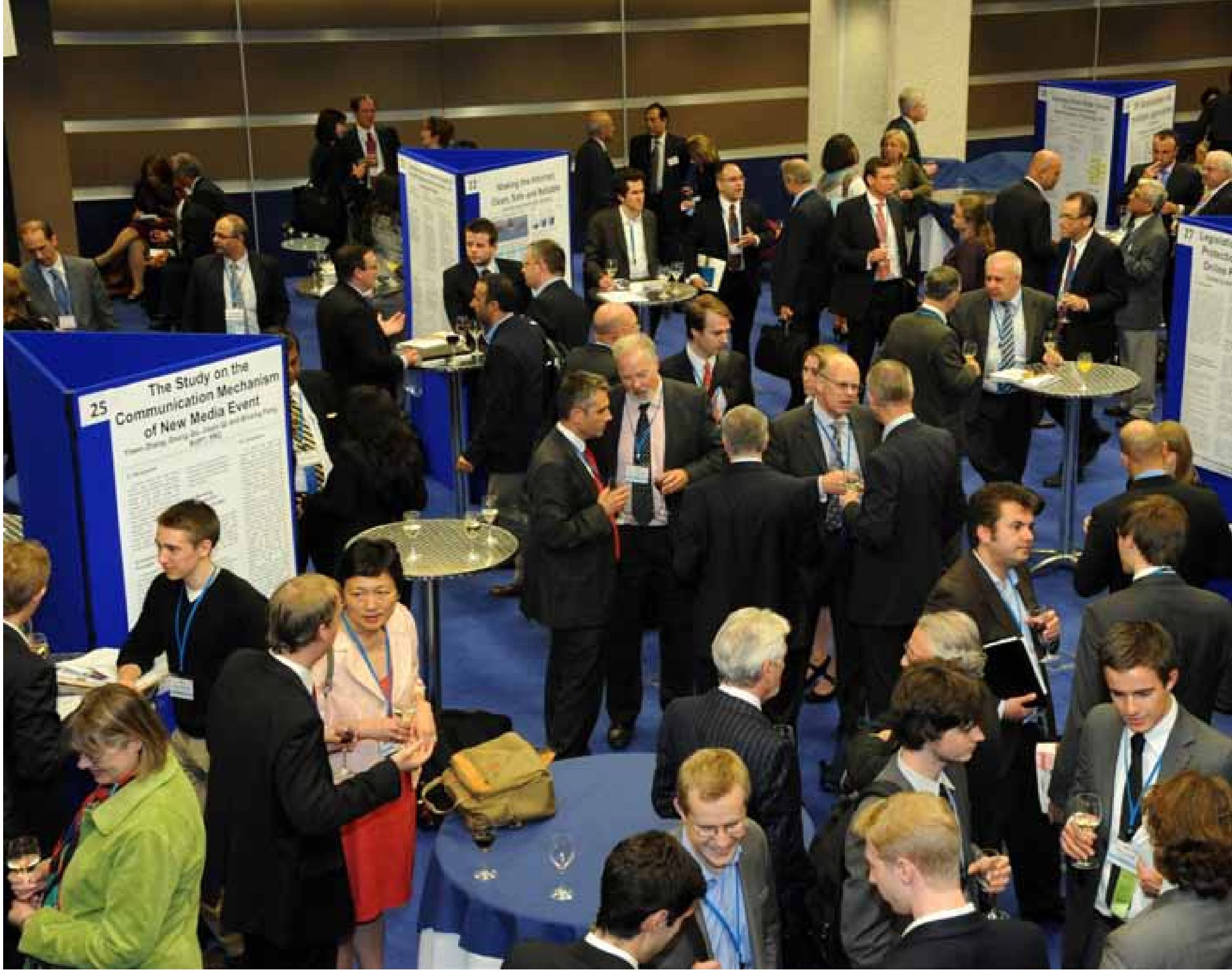
Emergency Response Coordination for the Financial Services Sector

In London, financial sector experts noted that there is no single point of contact for their sector in the event of a major cyber attack. Looking to remedy this, the group concurred that this problem needs to be solved at a local level before it can be solved internationally. For example, financial services firms in the UK must first be able to coordinate with each other before expanding coordination on a global level.

In the United States, information sharing occurs through the Information Sharing and Analysis Center (ISAC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). In Europe, there is the European Network and Information Security Agency (ENISA). A key challenge to coordinating an emergency response to a major cyber incident is that the private sector is reluctant to share information once the government is included. Establishing trust between financial services firms is another challenge. To achieve this trust, decisions must be made about what information firms are willing to share.

The group agreed that the first step for solving the problem is to develop a legal framework with clear scope and objectives. This would include: membership, roles and responsibilities, non-disclosure agreements for individuals and organizations, leadership, governance, and organization. An effective emergency response capability would need to include a network of responders who are able to contact each other 24 hours a day, 7 days a week, along with common language and protocols to be used in a crisis and clearly defined criteria for escalation.





New Ideas: A Call for Papers

How can we fight online child pornography worldwide? How do computer emergency response teams combat cross-border cyber threats? Is there a global cyber arms race going on right now? These are just some of the questions posed by the 28 papers presented at the Second Worldwide Cybersecurity Summit in London. In partnership with its technical co-sponsor, the IEEE Communications Society, EWI issued the call for papers, many of which offer innovative and practical cybersecurity solutions. Following IEEE's rigorous publication standards, EWI formed an ASPR Program Committee to peer-review and edit the papers. Industry, government and academic experts from nine countries, including the United Kingdom, Malaysia, Pakistan, Italy, Japan and China, contributed papers. Here is a sampling of papers submitted:

In "New Approaches to Dealing with Online Child Pornography," John Carr from the Children's Charities' Coalition on Internet Safety in the United Kingdom outlines how the growth of the Internet has allowed for the large increase in child abuse images and, indirectly, organized crime. According to Carr, a system of "notice and take down," with blocking pending deletion, is needed to remove child pornography more efficiently.

Kevin Newmeyer of the Center for Hemispheric Defense Studies in the U.S. offers a proposal for international Internet governance modeled on the Financial Action Task Force (FATF), an intergovernmental policy group that has been successful in countering money laundering. Newmeyer writes that such a model would effectively unite private and public sector efforts in fighting abuse –

if member states can muster the necessary political will.

"The Organisation of Islamic Conference-Computer Emergency Response Team (OIC-CERT)," presented by Rahayu A. Ahmad and Mohd Shamir Hashim of CyberSecurity Malaysia, illustrates how international cooperation can counter vulnerabilities in the information and communication (ICT) systems and network infrastructures. With members from eighteen countries, the OIC-CERT fights cyber threats and shares intelligence, research, and best practices across borders.

Stefano Zanero and Federico Maggi of Politecnico di Milano in Italy write that the rise of cloud computing and replacement of physical disks with space quotas has introduced new vulnerabilities. In "Is the Future Web more Insecure? Distractions and Solutions of New-old Security issues and Measures," the authors propose several simple modifications to current countermeasures to fight off new attacks.

In "Legislation Concerning the Protection of the Right to Online Privacy in China: A Comparative Study with EU," Li Yuxiao and Xu Jinghong compare existing privacy laws in the European Union and mainland China. The authors suggest that, using the EU legal system as a model, China strengthen constitutional protection for online users and instill a more detailed, unified protection of civil privacy rights.

After their presentation to attendees at EWI's summit, the papers will be published in IEEE XPlore Digital Library and EI Index.

Youth Congress on **Digital Citizenship**

On May 31, EWI held the International Youth Congress on Digital Citizenship in London, bringing together young people with government, business and technical leaders. The aim: to improve online safety and empower youth in cyberspace. EWI planned the event with groups including UNICEF, AOL, the Girl Scouts and the Family Online Safety Institute.

There, students in GlobalCyber Ambassadors for Peace (GCAP), a collaboration with UNESCO and the E-World-Wide Group, spoke about problems ranging from pop-up ads to the serious risks posed by pedophiles on social networking sites.

"The Internet allows a rapid and widespread distribution of false and misleading information," Muaaz Patel, 14, pointed out.

Participants made suggestions for self-protection online and also explored the cyber problems faced by youth in developing countres.

To that end, EWI and Movements.org created a series of workshops for young people in Cameroon, Nigeria, the U.S. and Lebanon.

The Youth Congress's main recommendations, shared at the summit, included:

1. More research, particularly on the youth online experience in developing countries;
2. A space for sharing youth-to-youth cybersecurity solutions;
3. Bringing youth into high-level policy discussions;
4. A digital bill of rights drafted by young people;
5. Private sector codes of conduct to protect young people.

"Younger generations are rising to meet tomorrow's challenges with greater connectivity and speed than ever before," says John Kluge, Jr., EWI Associate and Youth Congress founder. EWI aims to create a standing alliance to accomplish these goals.

Cyber Crime Working Group

In June 2010, the EastWest Institute established a Cyber Crime Legal Working Group to advance the discussion of a possible treaty or set of treaties to harmonize national frameworks to better combat cyber crime.

Members include independent non-governmental cyber law experts from Norway, India, Russia, Sri Lanka, Switzerland, the United Kingdom, France and Brazil.

The Cyber Crime Legal Working Group primarily aims to explore new legal mechanisms to combat cybercrime and to "develop a consensus-building set of proposals related to international law," according to EWI Working Group Chair Judge Stein Schjolberg.

During the 2011 London Worldwide Cybersecurity Summit, the group presented discussion papers and held a seminar which covered the following issues:

- A minimal set of standards to apply internationally recognized approaches to cyber crime.
- A treaty to include existing procedural instruments already applied by many states.
- A treaty should develop existing regulation on jurisdiction and standards for international cooperation, and exclude controversial provisions on trans-border searches.
- The world's most serious cybercrimes and attacks should be investigated and prosecuted based on international law, and sentenced by an international court or tribunal for cyberspace.
- A global virtual taskforce to police crimes in cyberspace, including law enforcement, INTERPOL, ICT private sector stakeholders and NGOs.
- A global and interdisciplinary approach to cybersecurity, and lessons from Commonwealth frameworks.
- Blocking child pornography websites.

Summit **in the News**

The summit attracted broad media interest, with continuous coverage by *Reuters, the Associated Press, BBC, Sky News, CBS, the Financial Times* and *the Guardian*. Agencies' reports were published in thousands of outlets around the world, including *ABC News, CNBC, Bloomberg, Forbes, the Huffington Post, MSNBC, China Daily, Xinhua, Global News China, Times of India, DNA* and *CIO India*. A 32-page special report on cybersecurity was published in cooperation with *New Europe* ahead of the summit.

"This week in London, U.S. and Chinese officials spoke at a cybersecurity conference organized by the U.S.-based East-West Institute. The think tank says it has been working at finding common ground between Washington and Beijing on tackling spam, a relatively noncontroversial area. 'Some people say building trust is impossible but it is getting better,' EastWest Institute president and CEO John Edwin Mroz said."

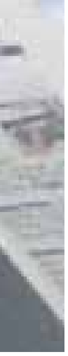
"Cyber attacks run risk of wider instability" REUTERS, JUNE 2, 2011

"The summit opened in London on June 1. More than 400 delegates from 42 countries and regions are attending the meeting. National security issues facing the Internet and how to strengthen international cooperation to safeguard information security are some of the issues that will be discussed."

"London Worldwide Cybersecurity Summit Holds Discussions on Cooperation and Safeguarding of Information Security"
XINHUA, JUNE 1, 2011

"'Everyone who has a computer or a mobile device that connects to the internet is only going to come under more attacks,' says Harry Raduege, a former head of US military information security who is speaking at the EastWest Institute's cybersecurity policy summit in London this week."

"Threats pile up in war that never ends" FINANCIAL TIMES, JUNE 2, 2011



"Hundreds of international delegates from governments and the private sector converged for the two-day conference to try to agree on the basics — how to enforce cybersecurity regulations across borders, what to do about countries that don't want to be regulated, how to protect government and company data and who will ultimately control cyberspace?"

"US Investigating Google Claim of China Hacking" ASSOCIATED PRESS, JUNE 2, 2011

"Computer security and corporate intelligence specialists say they are often sworn to secrecy by firms scared of the potential reaction of corporate partners and investors. Some companies, said experts gathered at a cyber security conference in London last week organized by the EastWest Institute, may not know the extent of their own exposure."

"Stigma puts many firms off reporting cyber attacks"
THE TIMES OF INDIA, JUNE 6, 2011

"Recent high-profile attacks against Sony and Lockheed Martin have made headlines, while experts described last year's discovery of the super-sophisticated Stuxnet virus — thought to have been aimed at sabotaging Iran's disputed nuclear program — as an illustration of the havoc that malicious programs can wreak on infrastructure and industry. How to deal with that threat was the topic of the two-day summit organized by the EastWest Institute, an international think tank which gathered hundreds of law enforcement officials, business leaders, academics and security consultants for talks in the British capital."

"US says no new treaty needed"
BLOOMBERG BUSINESSWEEK, JUNE 1, 2011

"A group of the world's leading cyber security experts has warned that the UK needs to be better protected from online attacks. Delegates at the Worldwide Cyber Security Summit in central London were told that online fraud and hacking costs the British economy around £27bn a year. The conference, only the second worldwide summit of its kind, comes in the midst of a huge surge in digital usage."

"UK Warned To Improve Lax Cyber Security" SKY NEWS, JUNE 1, 2011

NEW DELHI 212

THIRD WORLDWIDE **CYBERSECURITY** SUMMIT

India is among the most dynamic cyber powers on the planet. India's influence flows from a high level of technological expertise and central role in the global supply chain, providing vital digital products and infrastructure. Among Indian citizens, Internet use is growing exponentially. Each of these factors is not only extremely important to India's future, but also to the future of the world.

The EastWest Institute's Worldwide Cybersecurity Initiative will host the Third Worldwide Cybersecurity Summit in New Delhi, from October 30 - 31, 2012.

The aims for the New Delhi Summit will be:

1. To mobilize new commitments by leading businesses and governments of Cyber40 countries to address cross-border cybersecurity challenges.

2. To set in place new models for private sector leadership in addressing inherent vulnerabilities and emerging threats associated with global Internet connectivity and ICT development.

3. To make advances on the most pressing issues in global management of critical information and communications technology infrastructure with collaborative international breakthroughs.

4. To frame an action plan for globally acceptable policies on cyber crime, the associated international investigative procedures and a framework for addressing the related (and very complex) jurisdictional matters.

Byeong Gi Lee, *IEEE*, **Natalya Kaspersky**, *Kaspersky Lab*, **Som Mittal**, *NASSCOM*, **Latha Reddy**, *Indian Deputy National Security Advisor*, and **Kamlesh Bajaj**, *DSCI*, were among 450 private and public sector leaders who took part in the 2011 summit in London.

UNIQUE WORKING STYLE: EWI PROCESS

The Summit is designed to catalyze a quantum leap in international efforts to address specific cybersecurity vulnerabilities and threats. The EastWest Institute works with business and government leaders from around the world, its sponsors, its media partners, and all participants in the Summit to mobilize for international action. This means that **the annual Summit is part of a process, the "EWI Process", and not an end in itself.**

We invite all participants to contribute to the post-summit work in several ways: through their ideas for new measures (agreements and policies); through identification of mechanisms to bring those measures into play; and – after the summit – to be a part of the large community of "change agents" working through EWI or independently to achieve our common purposes.

SUMMIT PROCESS: (Breakthrough Groups)The bulk of the summit will be a highly interactive format. This interactive working program gives participants unique opportunities to collaborate with professional peers from around the world. Participants can expect to be able to work on critical issues identified at the first summit in Dallas and the second summit in London where international policy is stalled. The success of the summit is measured by the breakthroughs made in these groups both during the summit, and in the follow-up activities.

NEW DELHI PROCESS: In addition to the breakthrough groups initiated in Dallas and London, the New Delhi summit will launch new breakthrough groups labelled the "New Delhi Process." These breakthrough groups will expand the discussion in international cooperation on cybersecurity in new fields carefully chosen in advance by the summit ASPR Committee. EWI will work closely with its Indian partners and the IEEE in the next year and a half to identify the highest priority topics for breakthrough groups at the New Delhi summit.

To learn more, please visit **www.ewi.info/cyber**

IN PARTNERSHIP WITH

NASSCOM® DSCI PROMOTING DATA PROTECTION FICCI

EWI Board of Directors

OFFICE OF THE CHAIRMAN

Francis Finlay (U.K.)
EWI Co-Chairman
Former Chairman,
Clay Finlay LLC

Ross Perot, Jr. (U.S.)
EWI Co-Chairman
Chairman, Hillwood Development Company, LLC;
Member of Board of Directors, Dell, Inc.

Armen Sarkissian (Armenia)
EWI Vice-Chairman
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President and CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee of EWI Board of Directors
Senior Fellow, Harvard Business School

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

Leo Schenker (U.S.)
EWI Treasurer
Senior Executive Vice President, Central National-Gottesmann, Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former President of Finland

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

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

Thor Bjorgolfsson (Iceland)
Chairman
Novator

Sir Peter Bonfield (UK)
Chairman
NXP Semiconductors

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

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

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

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

Craig Cogut (U.S.)
Founder & Co-Managing Partner
Pegasus Capital Advisors

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

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

NON-BOARD COMMITTEE MEMBERS

Marshall Bennett (U.S.)
President
Marshall Bennett Enterprises

John A. Roberts, Jr. (U.S.)
President and CEO
Chilmark Enterprises L.L.C.

J. Dickson Rogers (U.S.)
President
Dickson Partners, L.L.C.

Laurent Roux
Founder
Gallatin Wealth Management, LLC

George Sheer (U.S.)
President (retired)
Salamander USA & Canada
Founder & CEO
International Consulting Group, USA

Bengt Westergren (Sweden)
President (ret.)
AIG Central Europe &
the Former Soviet Union

CHAIRMEN EMERITI

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

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

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

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

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

Ira D. Wallach* (U.S.)
EWI Co-Founder

DIRECTORS EMERITI

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

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

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

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

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

William E. Murray* (U.S.)
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)
Former Minister of Foreign
Affairs of Norway

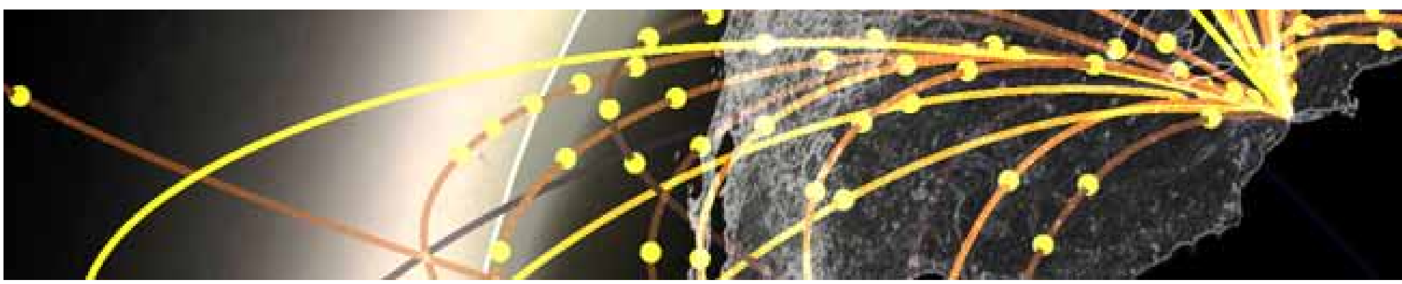
Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

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

* Deceased

EWI's Worldwide Cybersecurity Initiative is made up of a diverse group of professionals, ranging from top government and military advisors to business and technical consultants. We deeply appreciate the leadership and informed perspective of experts like Lt. General (Ret.) **Harry D. Raduege, Jr.**, Chairman of the Deloitte Center for Cyber Innovation and **Melissa Hathaway**, the U.S. National Security Council's former Acting Senior Director for Cyberspace, as well as EWI Vice President of the Worldwide Cybersecurity Initiative **Greg Austin** and EWI Chief Technology Officer and Distinguished Fellow **Karl Rauscher**. We want to thank EWI's Co-Chairmen of the Board **Ross Perot, Jr.**, and **Francis Finlay**, the latter having chaired the London Host Committee, as well as EWI Vice Chairman of the Board **Armen Sarkissian**, for their leadership. EWI's cybersecurity initiative would not be possible without the hard work, dedication and imagination of our staff members, including **Matthew Eckford**, **Anneleen Roggeman**, **Franz-Stefan Gady**, **Alison Kung**, **Nathan Wendt**, **Abigail Rabinowitz**, **Tracy Larsen** and **Dragan Stojanovski**.

EWI would like to acknowledge the support of **London First** in preparing and staging the London Summit. London First remains a committed partner of the Worldwide Cybersecurity Initiative.



New York Talk Exchange graphics (pages 1, 2, 3, 49) by SENSEable City Laboratory,
Massachusetts Insitute of Technology

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely 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, and Moscow.

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

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

OUR SPONSORS

LEADERS' FORUM

Microsoft · Goldman Sachs · Deloitte.

PLATINUM SPONSORS

HUAWEI · KNIGHTSBRIDGE CYBERSYSTEMS

GOLD SPONSORS

AKIN GUMP STRAUSS HAUER & FELD LLP · at&t · vodafone

SILVER SPONSORS

BAE SYSTEMS · VERISIGN™ · UNISYS · CHERTOFF GROUP · FT FINANCIAL TIMES

TECNHICAL CO-SPONSORS

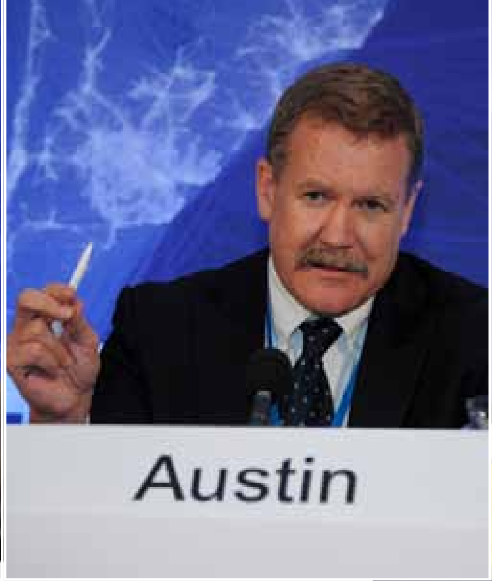
IEEE · IEEE COMMUNICATIONS SOCIETY

OUR PARTNERS

London First

UK Investment Banking Information Security SIG · NASSCOM® · DSCI PROMOTING DATA PROTECTION · intellect REPRESENTING THE UK TECHNOLOGY INDUSTRY

TeleGeography · Institute for Security & Resilience Studies University College London · NEW EUROPE


Austin


SECOND WORLDWIDE
CYBERSECURITY


Mroz


DIGITALCITIZENS
EASTWEST INSTITUTE

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

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

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

EWI DC Office
1069 Thomas Jefferson Street NW
Washington DC 20007
U.S.A. 1-202-492-0181

www.ewi.info