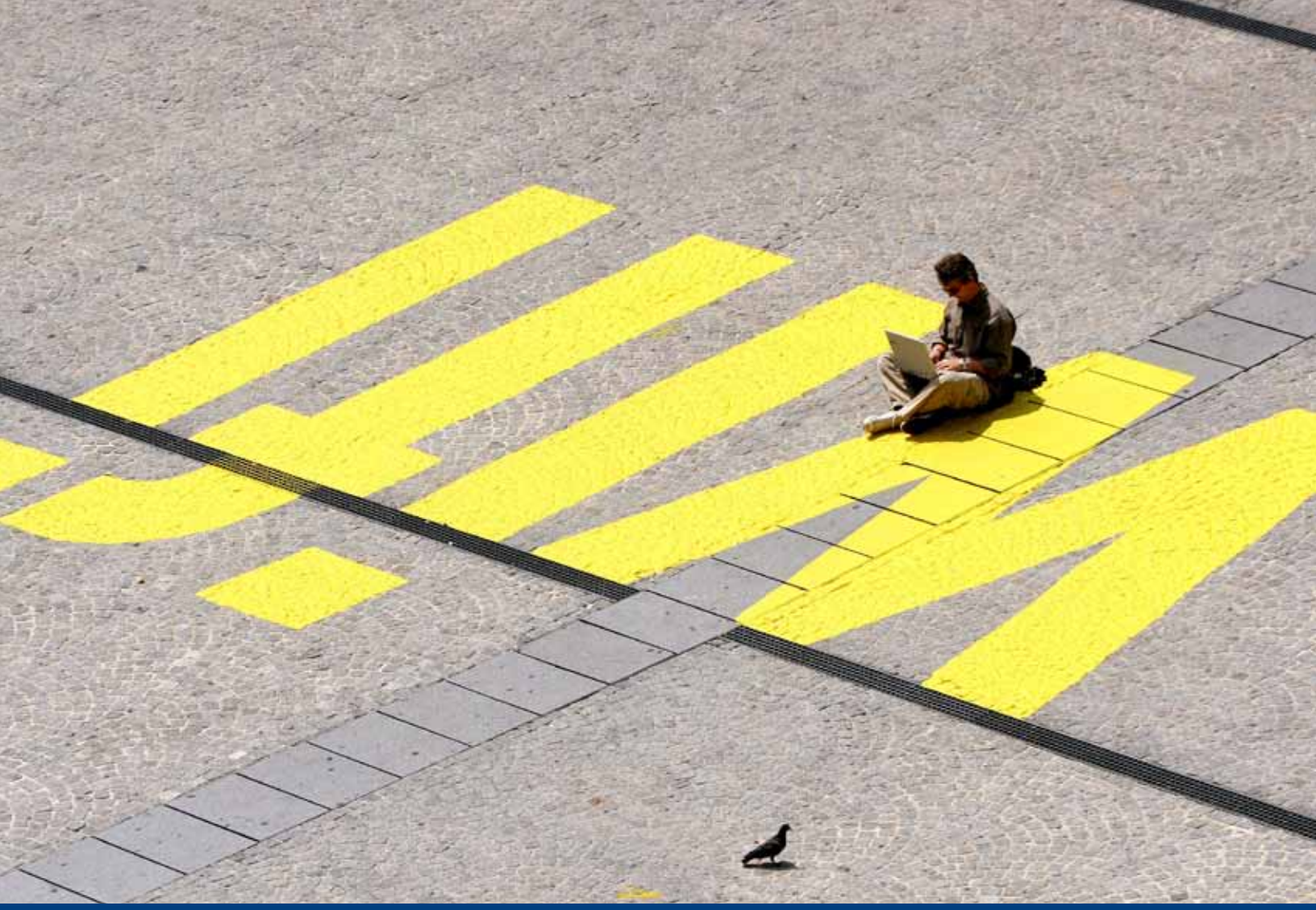


The Cybersecurity Agenda

Mobilizing for International Action

By Kamlesh Bajaj

EastWest Institute
Forging Collective Action for a Safer and Better World
www.ewi.info

DSCI
PROMOTING DATA PROTECTION
www.dsci.in

About the Author

Kamlesh Bajaj is the Chief Executive Officer of the Data Security Council of India and Head of NASSCOM Security Initiatives. He has over 30 years of experience in various capacities in the IT industry. Over the last two years, he has led the development of best practices for data protection, promoted their use by IT and business-process outsourcing companies in compliance with regulations of client countries. He was the Founder Director of the Computer Emergency Response Team in the Indian Ministry of Communications and IT. He has also served as Deputy Director General of the National Informatics Centre. He led several large projects in finance and banking, most notably the Customs EDI Project that introduced near-paperless operations in custom houses in India. Dr. Bajaj began his career as a Software Engineer at CAE Electronics in Canada. He is also a Fellow at the Institution of Electronics and Telecommunication Engineers, India, and at the National Academy of Sciences, India.

The Cybersecurity Agenda

Mobilizing for International Action

By Kamlesh Bajaj

EastWest Institute

Forging Collective Action for a Safer and Better World

www.ewi.info

DSCI

PROMOTING DATA PROTECTION

www.dsci.in/

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 paper, 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

Cover photo: Paris mayor Bertrand Delanoe has unveiled his 'digital program for the capital', which envisages connecting at least 80 percent of all buildings to very high speed internet access by 2010. The mayor's project also calls for there to be 400 free Wi-Fi hotspots across the city within one year, using street lights, buildings, bus stops and other urban furnishings. Pictures here are computer users surfing the net using Wifi netword around Georges Pompidou center in Paris, France on July 5, 2006. Photo by Nicolas Chauveau/ABACAPRESS.COM

Printed in the United States.

Contents

Executive Summary

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. A nation's cyberspace is part of the global cyberspace; it cannot be isolated to define its boundaries since cyberspace is borderless. This is what makes cyberspace unique. Unlike the physical world that is limited by geographical boundaries in space—land, sea, river waters, and air—cyberspace can and is continuing to expand. Increased Internet penetration is leading to growth of cyberspace, since its size is proportional to the activities that are carried through it.

Cyberspace merges seamlessly with the physical world. So do cyber crimes. Cyber attackers can disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in the physical space They can also carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities.

Anyone can exploit vulnerabilities in any system connected to the Internet and attack it from anywhere in the world without being identified. As the Internet and new technologies grow, so do their vulnerabilities. Knowledge about these vulnerabilities and how to exploit them are widely available on the Internet. During the development of the global digital Internet and communications technology (ICT) infrastructure, the key considerations were interoperability and efficiency, not security. The explosion of mobile devices continues to be based on these insecure systems of Internet protocols.

It is increasingly cheap to launch cyber attacks, but security systems are getting more and more expensive. This growing asymmetry is a game changer. It has another dimension, too—individuals, terrorists, criminal gangs, or smaller nations can take on much bigger powers in cyberspace, and through it, in the physical world, as well. The effects of attacks on critical infrastructure such as electricity and water supplies are similar to those that would be caused by weapons of mass destruction, without the need for any physical attacks.

Proving attribution in cyberspace is a great challenge. In most cases, it is extremely difficult to attribute cyber attacks to nation-states, collecting irrefutable evidence. The very nature of botnets and zombies makes it difficult to do so, leading to the conclusion that "the Internet is the perfect platform for plausible deniability."[1]

Nations are developing cyber attack capabilities with a view to dominating cyberspace. However, unilateral dominance in cyberspace is not achievable by any country. But uncontrolled growth of cyber attack capabilities—in effect, cyber attack proliferation—is an increasingly troubling phenomenon. Yet another disturbing reality is that cyber attacks can be launched ever more easily, and propagated faster using the same broadband that nations are building for global e-commerce. Finally, the consequences of a cyber attack are more likely to be indirect and more uncertain than most scenarios currently envision; we may not always recognize the damage inflicted by cyber attackers.

Cybersecurity is a global problem that has to be addressed globally by all governments jointly. No government can fight cybercrime or secure its cyberspace in isolation. Cybersecurity is not a technology problem that can be 'solved'; it is a risk to be managed by a combination of defensive technology, astute analysis and information warfare, and traditional diplomacy. Cyber attacks constitute an instrument of national policy at the nexus of technology, policy, law, ethics, and national security. Such attacks should spur debate and discussion, without any secrecy, both inside and outside governments at national and international levels. This is all the more so because of the growing number of significant actors not tied to, or even loosely affiliated with, nation-states. Over the last few months, events in cyberspace such as the GhostNet attacks on governments and large multinational corporations, whether to steal intellectual property or attack free speech, bear this out. They are not restricted by geographical borders or national laws.

There is an added dimension to this problem: the infrastructures are owned and operated by the private sector, and cyberspace passes through various legal jurisdictions all over the world. Each government has to engage in supporting

1 Scott James Shackelford. 2008. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" ExpressO. Available at: http://works.bepress.com/scott_shackelford/5

its private sector for cybersecurity through effective public-private partnership (PPP) models, with clearly-defined roles for government and industry. Because cyberspace is relatively new, legal concepts for 'standards of care' do not exist. Should governments create incentives to generate collective action? For example, they could reduce liability in exchange for improved security, or introduce tax incentives, new regulatory requirements, and compliance mechanisms. Nations have to take appropriate steps in their respective jurisdictions to create necessary laws, promote the implementation of reasonable security practices, incident management, and information sharing mechanisms, and continuously educate both corporate and home users about cybersecurity.

International cooperation is essential to securing cyberspace. When it comes to tracking cyber criminals, it is not only the laws dealing with cyber crimes that must exist in various countries, but the collection of appropriate cyber forensics data in various jurisdictions and their presentation in courts of law, which are essential to bring criminals to justice in sovereign countries. The term "cybersecurity" depends upon international cooperation at the following levels:

a. **National nodal centers** on information infrastructure, based on public-private partnerships, to cooperate;
b. **Global service providers** such as Google, Microsoft, Twitter, Yahoo, and Facebook to cooperate with law enforcement agencies in all countries and respond to their requests for investigations;
c. **Computer Emergency Response Teams (CERTs) to exchange threats and vulnerabilities data** in an open way to build an early-watch-and-warning system;
d. **Incident management** and sharing of information with a view to building an international incident response system;
e. **Critical-infrastructure protection:** Establishment of an international clearing house for critical-infrastructure protection to share threats, vulnerabilities, and attack vectors;
f. **Sharing and deployment of best practices** for cybersecurity;
g. **Creation of continued awareness on cyber threats,** and international coordination as part of early-watch-and-warning system;
h. **Acceptable legal norms** for dealing with cyber crimes regarding territorial jurisdiction, sovereign responsibility, and use of force to reconcile differing national laws concerning the investigation and prosecution of cyber crimes, data preservation, protection, and privacy. Address the problem of existing cyber laws that do not carry enforcement provisions;
i. **Incident response** and transnational cooperation, including establishment of appropriate mechanisms for cooperation. Such measures must include provisions to respond to counter cyber terrorism, including acts of sabotage of critical infrastructure and cyber espionage through information warfare
j. **Law enforcement agencies** to investigate cases, collect forensic evidence at the behest of other countries, and prosecute cyber criminals to bring them to justice.

It is time for the international community to start debates and discussions to encourage nations to create domestic public-private partnerships for cybersecurity, establishing laws for cyber crimes, and, more importantly, to take steps for international cooperation to secure cyberspace.

Cyberspace and Cyber Crimes

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. They are connected through undersea cables, satellites in outer space, land lines, and radio links. A nation's cyberspace is part of global cyberspace; it cannot be isolated to define its boundaries since cyberspace is borderless. This is what makes cyberspace unique. Unlike the physical world that is limited by geographical boundaries—land, sea, river waters and air—cyberspace can and is continuing to expand. Technology innovations are pushing the speeds of communication and computing to new limits; quantum computers promise to far exceed Moore's Law, which predicts that the processing power of computers doubles every eighteen months. Increased Internet penetration is leading to the rapid growth of the cyberspace, since the size of cyberspace is proportional to the activities that are carried through it. Among those activities: the exchange of goods or services, financial transactions through banks, credit card payments, email communications, social networking, exchange of pictures, videos or music. These activities lead to the seamless merging of cyberspace with the physical world. No wonder that cyber crimes impact the physical world, too. Cyber attacks are used to disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in physical space. Cyber attackers can also carry out identity theft and financial fraud; steal corporate information, including intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities in the world.

Cyber crimes are committed both in the physical world and in cyberspace to exploit the weaknesses of networks and computer resources. What makes cyber crimes possible? The same features that make global e-commerce and national e-governance possible: standardized protocols that enable the accessing of information and services easily from anywhere in the world. Anyone can exploit the vulnerabilities in any system connected to the Internet, using them to launch attacks on it. The attackers could be located anywhere in the world and they can target a particular system or a particular service in a country or a region. Worse still, the attackers can cover their tracks so that they cannot be traced. It is extremely difficult to prove whether the attacker is a criminal, a gang, a host of non-state actors or a nation-state.

With the growth of the Internet and the adoption of new technologies, including the use of open source systems, comes a rapid growth of new vulnerabilities that are exploited well before vendors are aware of them. Interestingly, knowledge about vulnerabilities and how to exploit them is widely available on the Internet; and expanding bandwidths make it possible to propagate attacks at a much faster pace, even before organizations start patching their systems to protect themselves. As a result, it is increasingly cheap to launch destructive cyber attacks anonymously, but increasingly expensive to defend against such attacks. This growing asymmetry is a game changer.

In the globalized world today, national borders still exist and nations take necessary steps to protect them. The physical world, with clearly defined geographic boundaries, makes it relatively easy for nations to protect themselves from physical attacks. But states also have to take proactive steps to secure cyber systems within their borders, even though cyberspace is borderless. Cybersecurity measures include providing for the physical security of systems. Such measures are essential to protect cyberspace and to reduce the chances that physical access to insecure systems will be used to commit crimes. Cybersecurity is thus essential for a nation's internal security. As the world moves towards more and more interconnectivity, where more and more people are linked by devices with all kinds of applications and services, cyberspace is becoming infinitely large. It will soon be the biggest "global commons."

What are the options for nations to protect themselves in cyberspace? At the international level, there are no treaties for cyberspace. Unlike land, sea, and airspace, covered by international treaties, cyberspace poses a unique challenge since it is one big international space that spans across all countries making it difficult to define boundaries of a "nation's cyberspace." In this paper we will review the nature of cyber attacks, the motives of cyber criminals, and attacks on critical infrastructures that can be as damaging as the effects of nuclear attacks. This will be illustrated through the example of Estonia. We will further present the policy issues and steps that nations should take to protect their infrastructures through laws, best practices, training, and public-private partnerships, because large parts of information and communications technologies (ICT) infrastructure are owned and operated by the private sector. But even this is not enough since cybersecurity is a global problem. International cooperation at several levels is critical for making nations secure: law enforcement, information sharing to bring criminals

to trial; incident management; information sharing on threats and vulnerabilities; international cooperation to create an intelligence mechanism to combat cyber threats; and private-sector cooperation across countries.

Cyber Attacks

Cyber attacks are defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[2] Cyber exploitation or cyber espionage, on the other hand, refers to the penetration of adversary computers and networks to obtain information for intelligence purposes; this is espionage, not a destructive activity. Cyber attack weapons are easy to use and they can generate outcomes that range from the simple defacing of a web site to the stealing of data and intellectual property, espionage on target systems and even disruption of critical services. Likewise, cyber attack as a mode of conflict raises many operational issues—for example, how will a country know whether it is the subject of a deliberate cyber attack launched by an enemy government? How will it prove this? Proving attribution in cyberspace is a great challenge. It is extremely difficult to attribute cyber attacks to a nation-state, since collecting irrefutable evidence has proved elusive in almost all cases of this nature in recent years. The very nature of botnets and zombies makes it difficult to do so. This has led many analysts to conclude that the Internet is the perfect platform for plausible deniability.

Cyber attackers can support military operations. They can disrupt the target's command, control, and communications. They can support covert actions to influence governments, events, organizations, or persons, often disguising whoever is launching those actions. Valuable information and state secrets can be obtained through cyber espionage.

Cyber attacks can be carried out in a number of ways. Among them:[3]

a. Computer-network attacks
b. Supply-chain attacks
c. Social-networking-led attacks
d. Attacks on radio networks for GPS and wireless networks
e. Radio frequencies with sufficiently high power to disrupt all unprotected electronics in a given geographical area

Cyberattacks can be launched against the critical infrastructure of nations that includes telecommunications, energy, financial networks, transportation systems, and water distribution, among others. In many countries, such infrastructure is owned and operated by the private sector. Much of it depends on SCADA systems, which are computer-controlled in a networked environment. Taking advantage of vulnerabilities in these systems, attackers can disable them and disrupt essential services. An attack on the air traffic control system could not just wreak havoc with flight schedules but also, in the worst case, cause crashes. The effects are the same as if the infrastructure were bombed or attacked by some other physical measure, without the enemy coming in by air, sea, or land. Likewise, financial networks can be targeted to disrupt a nation's economy. Banks, stock exchanges, trading, online payment systems, and other transactions of all kinds can be brought to a grinding halt as if these were physically bombed. This is cyber war or information warfare. The effects are similar to what would be achieved by Weapons of Mass Destruction (WMD).[4]

Such damage can be caused by cyber criminals, acting on their own or on behalf of mafia and other organized crime gangs; nation-states or terrorists can also be the beneficiaries of their activities. Actors thus range from ordinary cyber criminals to fundamentalist religious, social, and political groups to terrorist organizations. Even single individuals, who may be disgruntled insiders, are capable of launching such attacks. The damage will be similar to what would be caused by national armies in physical attacks. And all this at an insignificant cost!

Cyber espionage is another area that can produce a high payoff for a relatively small investment. All someone needs are a few dedicated hackers who can crawl for information stored on the enemy's servers. Human beings are not exposed; nor do they have to travel to enemy's territory to gather or collect information. Terrorists, irrespective of their motives and location, launch cyber attacks on the Internet even as they use the same medium to mobilize their resources. They have an unprecedented opportunity to access the global community to advance their aims.

2 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors, Committee on Offensive Information Warfare, National Research Council, 2009, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," (executive summary at http://www.nap.edu/catalog/12651.html)

3 Michael N. Schmitt, "Wired warfare: Computer network attack and *jus in bello*," IRRC, June 2002, Vol 84, No. 846 pp 365 – 399

4 Schmitt, pp 365 – 399; Shackelford

Cyber criminals began by committing petty crimes in different parts of the world. But with the expansion of cyberspace, financial payoffs have increased, which, in turn, have led to the emergence of organized gangs spread over different cities across countries. Crime syndicates, which sometimes include terrorists, are increasingly visible. So are fundamentalists of different religious, social, and political groups, who are masquerading in cyberspace as protectors of their rights and the causes of allegedly aggrieved or wronged communities. They have already graduated from defacing websites to causing real damage to their "enemies," especially their critical infrastructure.

Cyber criminals have different motives, but they can command the resources to create attack vectors in order to achieve the results they want. They may commit fraud, identity theft, steal money, commit robbery against corporations, banks, nations, regions and even individuals. They may try to blackmail them, too. The U.S. government reports that intrusions into its digital infrastructure have resulted in cyber criminals stealing intellectual property of economic value of more than $1 trillion in 2008. They also stole sensitive military information, and even caused a multi-city power outage.[5]

The convergence of terrorism and cyberspace is referred to as cyber terrorism. An attack on ICT infrastructure can lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic losses. All such attacks against critical infrastructures would qualify as acts of cyber terrorism.

It is not difficult to visualize a scenario where mercenaries will be willing to carry out cyber crimes for anyone willing to pay them, as happens in the physical world. This will have the added advantage of concealing the national identities of the real perpetrators along with their motives. They will not be restricted by geographical borders or national laws.

Events over the last couple of years have shown that cyberspace can be expected to witness more virulent conflicts that are instigated by political, religious, economic, and national tendencies. A cyber conflict could easily escalate across national borders. Alternatively, physical attacks could precede cyber attacks. Estonia and Georgia provide recent examples. The Dalai Lama's website was targeted by attackers from China. The attackers were a group based in China that was operating a large spy network spanning more than a hundred countries. South Korea's network was brought down by attackers. The Indian Prime Minister's Office has been attacked several times. So have been the Pentagon and the White House. GhostNet of China[6] and its second version called Shadows in the Cloud[7] have received extensive coverage in the global media. Google has gone public with the claim that it has been a victim of targeted attacks originating from China, with the objective of accessing emails of political dissenters in that country.

The Google security team recently revealed that tens of thousands of Vietnamese computer users were infected with malware in a coordinated cyber attack. The users, who downloaded Vietnamese language software for their computers, were unwittingly infected with malicious software, which was then used to spy on and attack political dissenters.

According to "In the Crossfire: Critical Infrastructure in the Age of Cyber War,"[8] a McAfee report based on a survey conducted in December 2009, 36 percent of respondents saw the United States as the most likely attacker in a cyber war and 33 percent saw China that way. The next most likely attacker was found to be Russia, a distant third with just twelve percent. None of the other three developed countries—the UK, France and Germany—reached even six percent. Furthermore, McAfee's "Threat Report: Third Quarter 2009"[9] states that the United States is a leader in zombie production with a total percentage of 13.1 percent, China is next at 12.2 percent, Brazil number three at eight percent, and India in seventh place with 3.4 percent of zombie production worldwide. In so far as hosting malicious servers is concerned, the United States is a leader at 45 percent, while China is a distant second at ten percent. The report also suggested that other nations that contributed to a total of 21 percent of malicious servers are from small islands from Trinidad and Tobago to Aruba and Martinique. For spam, the United States again leads at 25 percent. Brazil came in second place at 12.1 percent and India was number three at 5.3 percent in the third quarter of 2009. The United States also leads in the number of phishing websites, accounting for 46 percent of such sites. Countries such as Netherlands (eleven percent) and Germany (seven percent) were also emerging as top

5 Owens, Dam, and Lin

6 Shishir Nagaraja and Ross Anderson, "The snooping dragon: social-malware surveillance of the Tibetan movement," University of Cambridge, March 2009

7 Information Warfare Monitor and Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," http://shadows-in-the-cloud.net, April 6, 2010

8 Stewart Baker et al, "In the Crossfire – Critical Infrastructure in the Age of Cyber War : A global report on the threats facing key industries," February 2010 (McAfee study)

9 David Marcus, Paula Greve, Sam Masiello, and David Scharoun, "McAfee Threats Report: Third Quarter 2009," McAfee Labs, http://www.mcafee.com/us/local_content/reports/7315rpt_threat_1009.pdf

ten contributors. Romania, which stood 25th in spamming, rose to thirteenth position in phishing. This suggests changing patterns for all threats and a rise of hacker groups in a variety of countries. McAfee points out that more than 120 countries have cyber attack capabilities.

This is a corroboration of the "2008 Data Breach Investigations Report," an earlier study by Verizon.[10] The external data breach sources of attack were assessed to be 24 percent from Eastern Europe, nine percent from Western Europe, and 23 percent from North America, while South East and South Asia constituted fourteen percent of total attacks. The "Symantec Global Internet Security Threat Report-2008" also confirmed that the United States, at 23 percent, is seen as a top originator of malware activity.

What does one conclude from this? Is the United States the biggest perpetrator of malicious activity, phishing, and spam, and hence responsible for cyber crimes in the same proportion? Or is there another way of analyzing targeted cyber attacks that originate from specific geographic locations?

Is cyberspace as borderless as it is made out to be? National boundaries do seem to affect cyberspace activities. This has to be recognized since it has a bearing on finding solutions to protect cyberspace.

Information Warfare and Legal Issues

In April and May of 2007, Estonia was the first victim of large scale information warfare that was believed to have been masterminded by a European country. The entire communications network was under attack; since Estonia was a fully online country, it came to a grinding halt just as might have happened if it were attacked by a traditional nuclear, chemical, or biological weapon of mass destruction. Government services were completely paralyzed, communications were disrupted, banking stopped, newspapers stopped publishing, cell phones died. This was the first case of a country experiencing cyber disruption similar to that caused by armed attacks. The attack was believed to be orchestrated with the help of non-state actors. Ene Ergma, Speaker of Estonian Parliament, said: "Like nuclear radiation, cyber war doesn't make you bleed, but it can destroy everything."[11] In fact, some elements within governments have publicly reserved the right to use nuclear weapons in response to cyber attacks, and they have also observed that the dangers posed by such attacks are analogous to other conventional WMDs. It is not clear what legal rights a state such as Estonia has as a victim of a cyber attack, or whether cyber attacks should be classified as merely criminal or a matter of national security.

While the effect of cyber war is similar to that of a nuclear explosion, a treaty similar to the Nuclear Nonproliferation Treaty is not the answer. This is because cyber weapons are freely available on millions of websites, and there are millions of "soldiers" trained in the art of their use to launch cyber attacks that are capable of causing great harm to their opponents.

In the United States, some view the Presidential National Security Directive, NSPD 16, issued in July 2002, as a directive to prepare potential cyber attacks against enemy computer networks. Internet warfare strategy has a major role in the prevention, detection, and mitigation of cyber attacks. Counterterrorist intelligence using cyber weapons thus seeks to reduce the probability and scope of attacks against valued ICT targets by making the attacker pay a price for targeting a system; the idea is that the best defense is an active offense.

Determining responsibility for a cyber attack is extremely difficult, as was found in the Estonian attack. Chat rooms were full of detailed instructions on how to launch botnet attacks, and thousands of attacks followed from untraceable computers around the world. Estonia did not get help in tracking down the true source of the botnets because existing agreements and treaties lack mandatory enforcement mechanisms.

What are the options for legal analysis of a cyber attack? Is it possible to analyze a cyber attack based on the present notions related to "use of force" and "armed attack"? Should these be judged primarily by the mode of attacks as in the physical world, or by both the direct and indirect effects of the attacks. The principles of the Law of Armed Conflict (LOAC) and the Charter of the United Nations, including both laws governing the legality of going to war (*jus ad bellum*), and laws governing behavior during war (*jus in bello*), should apply to cyber attacks. But the international community needs to debate to how these principles should apply to cyber weapons, particularly, how they relate to traditional notions of territorial integrity. Espionage through cyberspace will have to be suitably accommodated, since it is largely an accepted

10 Wade H. Baker, C. David Hylender, and J. Andrew Valentine, "2008 Data Breach Investigations Report," Verizon Business, 2008. http://www.verizonbusiness.com/resources/security/databreachreport.pdf

11 Shackelford

phenomenon in the physical world. But it may be difficult to define the boundaries of cyber espionage and cyber attack.

Global Data Flows

Companies around the world are outsourcing IT business processes, development, and operations for cost and quality considerations. Global businesses require 24/7 operations with partners working in different time zones in an effort to follow the sun to stay competitive. Global sourcing involves international data flows. Data protection, which requires both data security and data privacy, has emerged as a major challenge in cross-border data flows. Clients who are outsourcing their IT or business process operations to service providers in other countries such as India are demanding greater security as their concerns about cyber crimes, privacy, and identity theft have grown.

Global data flows have now become the norm everywhere. Whether one uses a social networking site or webmail to exchange information, it is not known where the data is stored. Personal information of users could be physically located anywhere around the world where huge data centers are established by service providers. And many of these services are now delivered using "cloud computing" models – some of which are global clouds. For example, Google, Facebook, Orkut, MySpace, and other social networking sites are global clouds. Users are concerned about the security and privacy of their personal data, but they do not know what laws govern them. Such movement of data and services to third-party, network-based servers—the cloud—introduces new policy challenges for the private sector and governments around the globe. Among these challenges:

a. Defining jurisdictional boundaries for law enforcement agencies;
b. Protection of privacy and civil liberties, as required by local laws of countries;
c. Liability in the event of data or network breaches.

Cybersecurity Challenges

As noted above, cyberspace continues to grow. Nations are investing heavily in their ICT infrastructures with a view to providing higher bandwidths, integrate national economies with the global marketplace, and to enable citizens or "netizens" to access more and more e-services. Given the security problems, there is increased emphasis on, and investment in, the security of cyber infrastructure. Core Internet protocols are insecure, and an explosion of mobile devices continues to be based on the same insecure systems. This is adding up to increased usage of the Internet in more vulnerable cyberspace.

Protection of critical infrastructure operations has emerged as a major challenge. This is because trillions of dollars move through the networks every day involving a broad range of activities, including e-commerce, e-governance, travel, hospitality, health care, and general communications. Electricity distribution, water distribution, and several other utility services are based on ICT infrastructures. The defense sector relies heavily on electronic systems. Security challenges have created a new paradigm: A country that becomes a leader in cybersecurity will have big economic advantages both in the short and long term.

Critical infrastructure is largely owned and operated by the private sector. But is security only the private sector's responsibility? Does this mean that government has a lesser role? These are some of the important cybersecurity issues that nations are grappling with. At an organizational level, too, cybersecurity is not merely a technology issue, but a management issue. This is grounded in enterprise risk management, which calls for an understanding of the human, process, legal, network, and ICT security aspects.

It is obvious that multiple agencies are involved in securing ICT infrastructure. These include private operators for their respective pieces of the infrastructure. Their efforts need to be firmly coordinated through an integrated command-and-control entity, which should serve as a unifying structure that is accountable for cybersecurity. Roles and responsibilities of each of the parties need to be clearly defined. At the same time, governments need to establish the appropriate policy and legal structures.

Nations, such as the United States, have advocated for a market-based, voluntary approach to industry cybersecurity as part of the National Strategy to Secure Cyberspace. But this has not worked entirely, because security investments made by industry, as per their corporate needs, are not found to be commensurate with the broader national interest. How will the additional private investments be generated? Is there a case for government incentives, as part of an incentive program to bridge the gap between those security investments already made and those additional ones that are needed to secure critical infrastructure? Several security surveys point to this need. They reveal a lack of adequate knowledge among executives about security policy and incidents, the latest technologi-

cal solutions, data leakage, financial loss, and the training that is needed for their employees.

Since cyberspace is relatively new, legal concepts for "standards of care" do not exist. Is there a case for governments to offer incentives to generate collective action? For example, they could provide reduced liability or tax incentives as a trade off for improved security, new regulatory requirements, and compliance mechanisms.[12] Governments need to provide incentives for industry to invest in security at a level that is not justified by corporate business plans. Citing the example of a social contract entered into by the U.S. government with the private sector for the protection of railroads and telecom lines over a century ago, the Internet Security Alliance advises that "industry and government must construct a mutually beneficial social contract which addresses creatively and pragmatically, the security of our cyber infrastructure".[13]

Government has a key role in setting an example by securing its own infrastructure, including that of government departments dealing with defense and intelligence, as well as the agencies that deliver civilian services. It should also educate itself, create security awareness, embrace public-private partnerships, and coordinate intelligence gathering with industry. Its focus should not be merely on regulation. It should create legal structures to encourage voluntary reporting of security incidents and reasonable data gathering for risk assessments.

Some of the major difficulties in addressing problems related to cybersecurity include the lack of the following: high quality software; management incentives (security expenditures are all too often minimized to keep profits high); coordinated multi-departmental roadmaps; calculations about the impact of insufficient cybersecurity; and cyber insurance.[14]

During the development of the global digital ICT infrastructure, interoperability and efficiency were the prime goals, not security. More and more innovative applications are being added to the Internet in the growing global economy in the same spirit. Furthermore, in an effort to cut costs of services, ICT industry is going through a phase of commoditization of products. As a result there are more security problems. While more and more features are getting added to IT products, there is no money to cover the cost to secure those products, since the margins are lower. Consumers are not demanding security, and are unwilling to pay for security, which only encourages more insecure products. Government has a key role in demanding secure products, especially by demanding higher standards in its procurement contracts. But it must also use its market powers to motivate and sustain cybersecurity in other areas. Regulations alone won't solve the problem, since they will impose unnecessary burdens on users without commensurate results. Instead, governments can encourage lower-cost loans for small and medium businesses that implement best security practices. Above all, government should work with the finance and insurance industries to see to it that they incorporate cybersecurity risk management as an underwriting principle.[15]

Incident Reporting

Notwithstanding the security measures that an organization may take, security incidents will continue to occur, though less frequently than before. Such incidents must be reported to designated government agencies so that the affected consumers may be made aware of the compromising of their data. ICT providers of products and services need to learn about the vulnerabilities of their products so that they can devise security workarounds or more lasting solutions to prevent similar incidents in the future. They also need to learn about the pattern of cyber attacks by persons and groups from various regions of the world. An effective program must include:

1. Development of standards for incident reporting by private sector network operators;
2. Definition of sector-specific cyber incident thresholds that warrant reporting;
3. Development of Breach notification laws to make consumers aware of compromise of their data;

12 "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Executive Office of the President, May 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

13 Internet Security Alliance, "The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress," 2008. http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf

14 Ibid.

15 "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency," Center for Strategic and International Studies, December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Executive Office of the President, May 2009; "Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space." UK Office of Cyber Security and UK Cyber Security Operations Center, June 2009, http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf

4. Government-led processes and rules to share reports on incidents with the private sector. Such processes and rules should be sure to account for classification and privacy issues;
5. Availability of incident data for research communities, enabling them develop tools and test theories;
6. Sharing of information about network incidents and vulnerabilities with international allies, seeking bilateral and multilateral arrangements that improve cybersecurity.

Operational Challenges

Finally, here are the overall challenges a nation faces.

1. ICTs are largely owned and operated by the private sector in most countries. The private sector thus has to directly protect, or be involved in the protection, of this infrastructure.
2. Addressing network security requires a public-private partnership as well as international cooperation and norms.
3. It is important to create mechanisms for intelligence and information sharing.
4. Governments must develop a comprehensive framework to ensure coordinated responses and recovery after a significant incident or threat. This must include a definition of the roles and responsibilities of each player in the PPP.
5. Nations must specify the roles of government and industry even as they identify incentives for businesses that implement best practices and standards.
6. Insider threats must be assessed. Background checks of employees in an organization are essential.
7. Create a predictable legal regime for dealing with cyber crimes, storage and retention of cyber forensics data, and international cooperation across jurisdictions to track cyber criminals.
8. Law enforcement agencies and the judiciary should be trained to understand cyber crimes and the relevance of evidence in the form of cyber forensics,

It must be reiterated that no country can address cybersecurity alone since the Internet is global and is based on universal standards and protocols. ICT products and components of various services are designed, developed, and rolled out for implementation by hundreds of thousands of companies all over the world. None can claim an application or a service as its own technology. And this trend is likely to continue since this is the only way to encourage innovation that generates efficiency and economic prosperity through free trade. The challenge, therefore, is to promote safety and security while preserving civil liberties and privacy rights in cyberspace.

It is thus clear that the global digital infrastructure is vulnerable to attacks from anywhere by anyone. Hence, no government can fight cyber crime or secure cyberspace in isolation. International cooperation to promote deployment of best practices for cybersecurity is essential, along with acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and the use of force, since there exist differing national laws concerning the investigation and prosecution of cyber crimes, data preservation, protection, and privacy.

Policy Considerations for Nations

Governments around the world have enacted laws to mandate use of secure practices to protect information assets and critical information infrastructures, and have made cyber crimes punishable. For example, the Information Technology (Amendment) Act, 2008 that came into force in October, 2009 in India has made cyber terrorism an offence that can lead to life imprisonment, while crimes like identity theft, phishing, and child pornography are serious offences that are punishable by fine and imprisonment. Enterprises have to implement appropriate technical and process safeguards along with physical, legal, and personnel security measures to secure their businesses. Best practices for data protection can help secure organizations. Consumers and employees need to be continuously made aware of threats and advised to use secure ways of conducting online transactions such as banking.

Governments also have to train law enforcements agencies and the judiciary in the handling of cyber crimes. They have to understand cyber forensics and use it effectively to try cyber criminals. Capacity building for these agencies is a continuous process that requires the support of industry; the human-resource challenge is far greater than the legal challenge for governments.

The United States has enacted several laws at the federal and state levels. Some of the prominent federal laws include the following: the Computer Fraud and Abuse Act (CFAA), also known as Title 18 U.S.C Section 1030; the National Information Infrastructure Act (NIIA); the Communications Assistance for Law Enforcement Act (CALEA) (Amendment of ECPA); the Cyber Security

Enhancement Act (CSEA); and the Homeland Security Act of 2002.

The United Kingdom has implemented the following laws to promote cyber security and punish cyber crimes: the Computer Misuse Act (CMA) of 1990, the Data Protection Act of 1998, and Serious and the Organized Crime Act of 2005.

Below are outlined some important points that the governments around the world need to consider when drafting their policies to secure cyberspace.[16]

1. No country can achieve unilateral dominance in cyberspace. Every nation has the option to develop cyber attack capabilities. Over 120 countries already have them. The defensive or offensive intent of cyber operations may be difficult to infer in a given case. The plausible deniability of a cyber attack by any nation-state is an important factor in identifying the cyber attack as an act of cyber war, since it is difficult to prove conclusively the source of the attack and the players behind it.
2. The global proliferation of unrestrained cyber attack capabilities is a highly dangerous trend.
3. The consequences of a cyber attack may be both direct and indirect—the latter may turn out to be more important. They also may be harder to quantify than in the case of conventional attacks. As a result, cyber attacks should be judged on the basis of the total effects that can be identified.
4. The response to cyber attacks has to be a mix of dynamic changes in defensive postures, law enforcement actions, and diplomacy, but counterattacks may not be a deterrent. It requires coordination among nations, and a wide range of public and private entities may be necessary depending on the scope and nature of a cyber attack. A better mutual understanding of various national views of cyber attack is needed, as well as measures to promote transparency and confidence building.
5. The starting point for an international legal regime to govern cyber attacks can be the LOAC and the UN Charter. However, as a National Research Council report put it, "these legal constructs fail to account for non-state actors and for the technical characteristics of some cyberattacks."[17]

16 Heickero, Roland. "Cyber security challenges for Asia in a 2030 timeframe." 12th Asian Security Conference, New Delhi, February 2010; Owens, Dam, and Lin; Shackelford; and Schmitt, pp 365 – 399.

17 Owens, Dam, and Lin

Cybersecurity: A Global Problem

Cybersecurity is clearly a global problem; it has to be addressed globally by all governments jointly. No government can fight cyber crime or secure cyberspace in isolation. But the cyber infrastructure is owned and operated by the private sector, spread over all the countries of the world and passing through various legal jurisdictions. The private sector therefore has to be involved in securing the cyberspace. Each government has to enlist the support of its private sector for cybersecurity. Models of public-private partnerships have to be created that are effective. There are thus two components to cybersecurity: at national level, and at international level.

At the National Level

1. Every country should establish national nodal centers to act as integrated command-and-control entities—as a unifying structure in each country—that are accountable for cybersecurity. Multiple agencies for securing ICT infrastructure including private operators for their respective pieces of the infrastructure need to be firmly coordinated. Roles and responsibilities of each agency need to be clearly defined. At the same time, policy and legal structures essential to enable them perform their missions should be in position.
2. CERTs should be set up to disseminate information on threats and vulnerabilities in each country. CERTs specific to particular sectors may also be set up. They should share information with a view to build an early-watch-and-warning system
3. Public-private partnership : Roles and responsibilities to defend privately-owned critical infrastructures must be defined. Such roles and responsibilities should account for armed attack or from physical intrusion or sabotage by criminals, terrorists or foreign attacks. The core responsibility of governments should be shared by the private sector. But the governments should pursue malicious actors and assist with information and technical support to enable private-sector operators to defend their own networks.
4. The private sector may take care of security risks in its respective organizations, but only to the extent

the market puts demands on it for being competitive. Beyond that, private companies cannot justify additional expenditure to their Boards. Security cannot be left to market forces alone. Moreover, cyber attacks carried out remotely can result in same harms and effects as by direct physical attacks. Does this make protection purely a government responsibility?

5. Governments need to give incentives to industry to encourage cybersecurity. Best Practices for security help mitigate 80 to 90 percent of attacks.[18] Implementation of these practices amounts to the construction of secure cyber systems. But to do this, governments must use their market powers, not regulatory powers to motivate and sustain cybersecurity. A country creating more regulatory pressure will put its industry at a disadvantage in this globalized environment, since the regulation will not reach beyond its borders.
6. Governments need to work with industry to design a secure technology infrastructure from the ground up. This should be driven by a market-based program, but one that is not a completely voluntary model. A voluntary model will result in weak links in cyberspace which are detrimental to corporate and national security.
7. Law enforcement agencies should build cyber forensics and investigation capabilities; train their officers and the judiciary in the handling of cyber crimes; and reach out to other sectors such as financial institutions which are the victims of financial frauds
8. Educating both corporate and home users is essential for any cybersecurity program to succeed; employee carelessness is a key finding of global security surveys worldwide. No outreach program is adequate enough.

At the International Level:

1. National nodal centers on information infrastructure should cooperate across borders.
2. Law enforcement agencies should investigate cases, collect forensics and evidence at the behest of other countries, and prosecute elements involved in cyber criminal gangs.
3. Global Service Providers such as Google, Microsoft, Twitter, Yahoo and Facebook should cooperate with law enforcement agencies in all countries and respond to their requests for investigations.
4. CERTs should exchange data on threats and vulnerabilities in an open way to build an early-watch-and-warning system.
5. Incident Management: Agencies must share information on incidents with a view to build an international incident-response system.
6. Critical Infrastructure Protection: An international clearing house for critical infrastructure protection should be established to share threats, vulnerabilities, and attack vectors.
7. Businesses and governments should share and deploy best practices for cybersecurity.
8. Businesses and governments should continue to raise awareness on cyber threats, and share information as part of an early-watch-and-warning system.
9. Laws should be enacted to deal with cyber crimes and cyber attacks to bring criminals to justice. Clearly defined statutes must be put in place for various crimes; data preservation; presentation of cyber forensics data in courts of law; norms regarding territorial jurisdiction; implementation of reasonable security practices; privacy protection; incident response; and transnational cooperation including establishment of appropriate mechanisms for cooperation. Cyber terrorism and acts of sabotage of critical infrastructure may be addressed as cyber espionage through information warfare. The key problem in existing cyber laws is that most do not carry enforcement provisions.
10. Acceptable legal norms must be established regarding territorial jurisdiction, sovereign responsibility, and use of force, since national laws differ.

Cyber Offense for Defense

All of this is a defensive approach to security. Can there be any defense without offence? Will the adversaries, whether terrorists, criminal gangs, or nation-states engaged in espionage get away without having to pay a price, while organizations around the world spend huge sums to secure their infrastructures and protect valuable information assets? Or, do democratic governments have

18 Internet Security Alliance, "The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress," (2008), quoted in CIA Chief of Information Assurance Robert Bigman, Aerospace Industries Alliance meeting (October, 2008).

the right to engage in information warfare to make cyber attackers pay? This is important because most nations have information-warfare capability, but they must collaborate, share information gathered through information warfare, through a mechanism that may be created as a multinational organization. The key to defense is through such cooperation for information sharing. How will trust be built?

It must be remembered that cybersecurity is not a technology problem that can be 'solved,' it is a risk to be managed by combination of defensive technology, analytic approaches using information warfare, and diplomatic and other channels. At an organizational level, it is a management issue grounded in enterprise risk management, which calls for an understanding of human resources, process, legal, network, and IT security aspects.

Clearly, cyber attack is an instrument of national policy at the nexus of technology, policy, law, ethics, and national security. Debate and discussion, both inside and outside governments at national and international levels, is called for. It is worth observing that public discourse on cyber attacks is analogous to the nuclear debate 50 years ago—at that time, nuclear policy issues were veiled in secrecy and there was little public debate about them. One must appreciate the rise in the significance of actors unconnected or loosely connected to nation-states, and of adversaries that do not share common values and legal traditions with respect to the conduct of conflict. Recent events in cyberspace such as GhostNet and attacks on governments and multinational corporations, whether to steal intellectual property or to attack free speech, bear this out. Such actors are not restricted by geographical borders or national laws. It is time the international community takes note and starts debate and discussions to encourage nations to create domestic PPP for cybersecurity, establish laws for cyber crimes, and, more importantly, take steps for international cooperation to secure cyberspace.

Conclusion

Sun Tzu in The Art of War says "All warfare is based on deception … know your enemy and know yourself and you can fight a hundred battles without disaster…. If you know neither the enemy nor yourself, you will succumb in every battle."[19] It is difficult to know the enemy in cyberspace, because he is an expert in deception. He can only be known through international cooperation. His vulnerability can be learnt of and exploited through such cooperation. The world has to find a way to cooperate so that the cyberspace—the biggest global commons—remains a driver of economic prosperity of nations and a cloud where people from all countries can safely interact and exchange goods and services.

---

19 Sun Tzu, "The Art of War," translated by Lionel Giles at The Internet Classics Archive. http://classics.mit.edu

EWI Board of Directors

EastWest Institute

Forging Collective Action for a Safer and Better World

OFFICE OF THE CHAIRMAN

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

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

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

Thor Bjorgolfsson (Iceland)
Chairman
Novator

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

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

Rohit Desai (U.S.)
President
Desai Capital

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

Melissa Hathaway (U.S.)
President
Hathaway Global Strategies, LLC;
Former Acting Senior Director for Cyberspace
U.S. National Security Council

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

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

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

Donald Kendall, Jr. (U.S.)
Chief Executive Officer
High Country Passage L.P.

Sigrid RVC Kendall (U.S.)
Managing Partner
Kendall-Verwaltungs-GmbH

James A. Lash (U.S.)
Chairman
Manchester Principal LLC

Christine Loh (China)
Chief Executive Officer
Civic Exchange, Hong Kong

Ma Zhengang (China)
President
China Institute of
International Studies

Michael Maples (U.S.)
Former Executive Vice President
Microsoft Corporation

Peter Maurer (Switzerland)
Ambassador
Permanent Mission of Switzerland
to the United Nations

Thomas J. Meredith (U.S.)
Co-Founder and Principal
Meritage Capital, L.P.

Francis Najafi (U.S.)
Chief Executive Officer
Pivotal Group

Frank Neuman (U.S.)
President
AM-TAK International

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

Ross Perot, Jr. (U.S.)
Chairman
Hillwood;
Member of Board of Directors
Dell, Inc.

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

John R. Robinson (U.S.)
Co-Founder
Natural Resources Defense Council

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

Ramzi H. Sanbar (U.K.)
Chairman
Sanbar Development Corporation, S.A.

Ikram Sehgal (Pakistan)
Chairman
Security and Management Services

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
Chief Executive Officer
Bud Smith Organization, Inc.

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., Ltd.

Henrik Torgersen (Norway)
Retired Executive Vice President
Telenor ASA

William Ury (U.S.)
Director
Global Negotiation Project
at Harvard Law School

Pierre Vimont (France)
Ambassador
Embassy of the Republic of
France in the United States

Alexander Voloshin (Russia)
Chairman of the Board of Directors
OJSC MMC Norilsk Nickel

Charles F. Wald (U.S.)
Former Deputy Commander
U.S. European Command

Bengt Westergren (Sweden)
Senior Vice President for Corporate &
Government Affairs, Europe and C.I.S.
AIG Companies

Igor Yurgens (Russia)
Chairman
Institute for Contemporary
Development

Zhang Deguang (China)
President
China Foundation for
International Studies

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.

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

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.

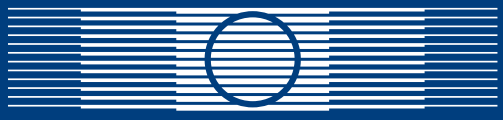
Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

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



EASTWEST INSTITUTE

Forging Collective Action for a Safer and Better World

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

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

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

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

The EastWest Institute is a non-partisan, 501(c)(3) 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
59-61 Rue de Trèves
Brussels 1040
Belgium
32-2-743-4610

EWI Moscow Center
Sadovaya-Kudrinskaya St.
8-10-12, Building 1
Moscow 123001
Russia, 7-495-691-0449

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

www.ewi.info