



GLOBAL CYBER DETERRENCE

Views from China, the U.S.,
Russia, India, and Norway



EASTWEST INSTITUTE
Forging Collective Action for a Safer and Better World

www.ewi.info

GLOBAL CYBER DETERRENCE

Views from China, the U.S., Russia, India, and Norway

Tang Lan, Zhang Xin, Harry D. Raduege, Jr.,
Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg

Edited by Andrew Nagorski

April 2010



EASTWEST INSTITUTE

Forging Collective Action for a Safer and Better World

www.ewi.info

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

Copyright © 2010 by the EastWest Institute.

Cover photo: South Korean computer hackers compete during an information security olympiad at the National Assembly in Seoul, South Korea, Friday, July 10, 2009. South Korea's spy agency told lawmakers that the cyber attacks that caused a wave of Web site outages in the U.S. and South Korea were carried out by using 86 IP addresses in 16 countries, amid suspicions North Korea is behind the effort. (AP Photo/Lee Jin-man)

Printed in the United States.

Contents

Foreword	
<i>by John Edwin Mroz</i>	i
Can Cyber Deterrence Work?	
<i>by Tang Lan and Zhang Xin</i>	1
Fighting Weapons of Mass Disruption: Why America Needs a “Cyber Triad”	
<i>by Harry D. Raduege, Jr., Lieutenant General USAF (Ret.)</i>	3
Russian Priorities and Steps Towards Cybersecurity	
<i>by Dmitry I. Grigoriev</i>	5
Cyber Deterrence: Legal Perspectives	
<i>by Pavan Duggal</i>	8
Wanted: A United Nations Cyberspace Treaty	
<i>by Judge Stein Schjølberg</i>	11

FOREWORD

Cybersecurity looms as the 21st century's most vexing security challenge. The global digital economy hinges on a fragile system of undersea cables and private-sector-led partnerships, while the most sophisticated military command and control systems can be interfered with by non-state as well as state actors. Technology continues to race ahead of the ability of policy and legal communities to keep up. Yet international cooperation remains stubbornly difficult, both among governments as well as between them and the private sector—the natural leaders in everything cyber. In 2007, the International Telecommunication Union (ITU) set up a High-Level Experts Group to try to address the problem but progress is slow. The European Union and Asia-Pacific Economic Cooperation (APEC) are working at the regional level. But it has only been in the past six months that public consciousness has started to grasp the scope and significance of the cybersecurity challenge. Pushed by a spate of revelations about cyber attacks worldwide, the media and key elites now seem to get it: cybersecurity is a fundamental problem that must be addressed across traditional boundaries and borders by the private and public sectors in new and cooperative ways.

Three years ago, the EastWest Institute used its Strategic Dialogue team from the United States led by General (ret.) James Jones and me to challenge senior Chinese and Russian leaders to begin the process of promoting international cooperation to meet cybersecurity challenges. The responses have been favorable and practical in both cases. Since then, we have engaged not just the Chinese and the Russians but also a broader array of “Cyber40” countries—the members of the G20 plus other countries who are key players in the cyber arena—to tackle together issues of cybersecurity. There was an immediate recognition of the lack of awareness of what is involved in protecting cyberspace. This quickly moved to a push for practical solutions that transcend national borders.

In early 2009, these cybersecurity efforts came together in the form of EWI's Worldwide Cybersecurity Initiative. Its purpose is to work across borders to catalyze more rapid and effective responses to cybersecurity challenges identified by industry, governments and international organizations as well as civil society. There's growing recognition—and mounting concern—about the vulnerabilities of today's digital infrastructure, whether it's international financial systems or critical government services. There are also growing dangers posed by criminal and terrorist groups, and the very real risks of cyber warfare, including attacks on states by non-state actors. As a result, top industry and government officials agree on the urgent need for bold new measures to ensure the secure functioning of the cyber dimension that underpins all of our lives in this century.

For this policy paper, EWI asked top cyber experts in five countries—China, the U.S., Russia, India, and Norway—to present their vision of what is needed to build an effective system of cyber deterrence. It is a first step in the process of building trust on tackling cybersecurity challenges—listening, understanding and probing the views, interests and concerns of key players in the global system. The EastWest Institute is not endorsing any of these proposals or taking a position on them. We strongly believe that it is vital for everyone involved in the cybersecurity debate to understand the differing perceptions, concerns and suggested solutions that are emanating from different parts of the globe. This is also a vital first step in the effort to find common ground for joint actions that are so desperately needed.

These essays will help stimulate discussions at EWI's First Worldwide Cybersecurity Summit in Dallas from May 3 to 5, 2010, which will convene hundreds of international business leaders, technical experts, policy

elites and national security officials. Building on earlier EWI consultations, most recently at the Worldwide Security Conference in Brussels in February 2010, we will seek to identify common problems and suggest breakthroughs and new agreements in critical sectors. We cannot allow the technological advances to continue outpacing common sense cybersecurity measures. It is time for the world to confront the challenges of our digital age. Comments and alternative views are warmly welcomed by the EWI cybersecurity team.

A handwritten signature in black ink, appearing to read "John Edwin Mroz". The signature is fluid and cursive, with the first name "John" being the most prominent.

John Edwin Mroz
President and CEO
EastWest Institute

The View from China

Can Cyber Deterrence Work?

By Tang Lan and Zhang Xin

In the wake of the financial crisis, organizations everywhere have looked to the third revolution in information technology to upgrade their infrastructure and spur a new round of growth. The damage caused by cyber crimes and cyber attacks, however, is at the same time growing increasingly serious. As we face a looming “cyber cold war” and a “cyber arms race,” vital individual, business, and even national interests are threatened. At the same time, faith in information technology and information networks continues to slip. As a result, seeking effective ways to counter cyber threats has become an urgent priority across the globe.

In an opinion piece he wrote for the *Washington Post* on February 28, 2010, titled “How to win the cyber-war we’re losing,” Mike McConnell, the former U.S. director of national intelligence, maintains that a combination of cyber deterrence and preemption will be needed to win this cyber war. McConnell’s view represents mainstream opinion in the United States – the belief that the world has “reverted” to the 1950s and that the methods used to contain nuclear proliferation should now be used to deal with cyber threats. The basis for this belief is both the technological and military strength the United States possesses, which should allow it to achieve the four key elements needed for cyber deterrence: what McConnell calls “attribution (understanding who attacked us), location (knowing where a strike came from), response (being able to respond, even if attacked first) and transparency (the enemy’s knowledge of U.S. capability and intent to counter with massive force).” Meanwhile, human intelligence, early-warning radar systems, reconnaissance satellites, and undersea listening posts can be used to determine the source and location of attacks.

Undeniably, information technology and the Internet have now developed to such an extent that they have become a major element—comparable to nuclear forces—of national power. During the Cold War, nuclear deterrence was able to keep the United States and the Soviet Union in check. Based on that logic, then, cyber deterrence should play a similar role in the information age. But the anonymity, the global reach, the scattered nature, and the

interconnectedness of information networks greatly reduce the efficacy of cyber deterrence and can even render it completely useless. The spread of information technology and the Internet also produce an increasing number of vulnerabilities and weaknesses that can easily be exploited. They allow an individual person to more easily obtain the means and capabilities for causing destruction almost anywhere in the world. The kind of asymmetry this presents is completely different from any situation involving the development or acquisition of nuclear weapons. If a nation wants to acquire a nuclear strike capability, it must invest an enormous amount of time and money to do so. Cyber attacks, on the other hand, are much simpler. Citibank at the end of last year suffered tens of millions of dollars in losses at the hands of criminals using “Black Energy” malware, which can be purchased online for only \$40. And the “Zeus Trojan” and its variants that attacked 74,000 computers across 196 countries are also available online for a mere \$700. The low-cost, low-risk nature of all this has now made hiring hackers an ideal means for conducting a cyber attack.

With reconnaissance satellites now covering virtually every corner of the globe, the United States and other major powers can detect any plans to launch a nuclear attack on the basis of the rapid movement of personnel and equipment. But the unique nature of networks means that cyber attacks can be launched by any person, from any place, and at any time. Attackers can easily conceal, erase, or even spoof the original source of an attack, leaving behind no identifiable physical tracks, thereby eliminating retaliatory action as an option. Still, out of fear of possible retaliation, these actors take meticulous steps and additional measures to cover their tracks and destroy any evidence. Consequently, early warning against and tracing of cyber attacks is all but impossible, so the most crucial element of a deterrence strategy—“retaliation”—cannot even be considered.

Another reality of particular import is that networks across the globe are becoming increasingly interconnected. However, as the Chinese saying goes, “while we might not all share in the benefits of this, we will all certainly suffer the losses caused by it.” That is to say, a retaliatory attack on another country’s networks has the potential of harming the security of one’s own networks. The *New York Times* revealed that the Bush administration had initially planned during the Iraq War in 2003 to bring down Saddam Hussein’s financial system with cyber attacks. But it abandoned the idea out of concerns that such attacks would bring disaster to its own systems and those of its allies. In the Japan-South Korea “Netizen War” at the beginning of

March, a Japanese Web site called 2ch was paralyzed by cyber attacks. But a U.S. government department and a few businesses whose websites shared a server with 2ch were also affected by the attacks, leading to \$2.5 million in losses. The potential for indirect damage is the primary problem with cyber deterrence.

Moreover, in stark contrast to the United States, there are some states or non-state actors who are not nearly as developed in terms of their information systems, which in some cases do not even connect to the outside world. Any damage to such systems is unlikely to threaten local political stability. The impact of cyber deterrence on such actors would be miniscule. The “mutual assured destruction” principle of deterrence does not apply to cyberspace.

There are now three major obstacles when it comes to meeting cyber threats: difficult technical hurdles, a lack of social responsibility and security awareness, and inadequate international cooperation. In principle, the first two can be dealt with handily by increasing investment in technological research and development, putting rules in place, stepping up education, and other such measures. Progress in these areas is just a matter of time. But the greatest obstacle preventing international cooperation is the reluctance of states to budge on their perceived cyberspace interests or on differences they have in terms of laws and politics. This is the primary reason why cyber threats cannot be dealt with effectively. So long as there is disagreement between countries about the definition of cyber crime, there will be disputes about transnational lawsuits, penalties, and extradition relating to such crimes.

Furthermore, some states make cracking down on illegal information that harms or damages the stability of state power a part of their cybersecurity efforts. Because of a belief in the free spread of information or other customs and traditions, other states lack a clear stance on what constitutes illegal and harmful information. The “Google incident” at the beginning of the year is a prime example. China and the United States differ greatly on their ideas about whether and how to control the Internet. But differences between China and Western countries on the issue of controlling Internet content should not become a roadblock for cybersecurity cooperation between the two sides, and it certainly should not be the basis for accusing China of tacitly allowing hacking.

China has made rapid progress in information technology over recent years. But in terms of technology research and development, the size of the information technology

industry, and the overall strength of common applications, it still falls far short of the United States. China is also well behind the United States in terms of its cybersecurity assurance capabilities and cybersecurity awareness among its citizens. Recently, hackers and other cyber criminals have become a distinct social problem in China. The annual worth of China’s “hacker industry” is now over 238 million yuan (about \$34.8 million), causing upwards of 7.6 billion yuan (about \$1.1 billion) in losses. Hacker websites and training sites have run rampant on the Internet, and there is a continuous increase in hacker attacks involving threats, retaliation and extortion. The number of computers in China controlled by “botnets” tops the list worldwide.

Cyber crime has seriously interfered with the normal economic order and has affected the normal operations of networks. China’s crackdown on hacker activity is truly needed to protect national interests; it is by no means done “for show,” as the Western media has charged.

China is an information power. As such, it should be a responsible information power. The future information climate, information order, and formulation of regulations cannot be shaped without China’s participation. At the same time, China recognizes that Internet security is a global problem, and hacker attacks and cyber crime are increasingly becoming a public nuisance worldwide. Thus, only international cooperation will enable us to better crack down on cyber crime and ensure the healthy development of the Internet.

China believes there is little cause for criticism when individual states strive to protect their own interests when cooperating with others. However, all nations must also respect the laws, politics, and cultural traditions of others. All nations must voice their opinions, but they must all see to their responsibilities. We believe that through frank and honest communication and exchanges, the international community will be able to come up with effective ways to meet cyber threats.

China has always stood for the peaceful use of the global information space, with the precondition that the national sovereignty, interests, and security of its information domain must be protected. At the 16th World Computer Congress in 2000, the Chinese government proposed an initiative to develop an “International Internet Convention.” It has also cracked down heavily on cyber attacks, network viruses, hacker intrusions, illegal remote control of computers, and other such problems that are harmful to the security of communications networks. It has done so with legislation that calls for strict

“All nations must respect the laws, politics, and cultural traditions of others.”

measures in response to all forms of hacker attacks and cyber crime activity inside China. Such legislation includes a 2008 amendment to the Criminal Law and the Administrative Measures for Communications Network Security Protection, which went into effect in March, 2010.

For many years China has worked to build effective mechanisms for cooperation with many countries on cybersecurity. Some examples include the establishment of the China-Russia information security cooperation relationship under the framework of the Shanghai Cooperation Organization (SCO) as well as the establishment of the SCO Special Working Group on Modern Information and Telecommunication Technologies; the China-UK Internet Roundtable; the China-U.S. Internet Forum; the China-France Joint Working Committee on Information Technology and Communications; the China-Japan-Korea Information and Communications Ministerial; and the China-Pakistan Working Group on Information Industry Cooperation. China's successful experiences with these mechanisms should be applied to future international information security cooperation efforts under the UN framework. All of these cooperative arrangements fully illustrate China's sincere desire to move forward with international cooperation on cybersecurity.

Tang Lan is an Adjunct Research Fellow at the China Reform Forum and Assistant Director of the Institute of Information and Society Development Studies at the China Institutes of Contemporary International Relations. She received her Bachelor's degree in philosophy from Wuhan University in 1993 and a Master's degree from the University of International Relations in 2004. She has been studying cyber-related issues for about 10 years, currently focusing on cybersecurity, cyber warfare, and Internet governance.

Zhang Xin is Deputy Director of the Liaison Office of the China Reform Forum. He was a research assistant at the China Institutes of Contemporary International Relations from 2001 to 2007, where his main field of study was information security strategy. In 2005 and 2006, he twice participated in the Chinese Ministry of Science and Technology's National Project on IT Security Policy.

The View from the United States Fighting Weapons of Mass Disruption: Why America Needs a “Cyber Triad”

*By Harry D. Raduege, Jr.,
Lieutenant General USAF (Ret.)*

In the 21st century, Americans use cyberspace to run industries, share information, control machinery, purchase items, move money, and perform essential government services. Yet, as our nation grows more dependent on information networks, cyberspace also has become a battlefield where adversaries are launching cyber attacks of increasing sophistication. The world has dealt with the threat of weapons of mass destruction—commonly referred to as WMD—in the past. However, in the world of cyberspace, we are now confronted with a new WMD threat: weapons of mass disruption. If we do not prepare now, we could one day face a cyber attack that could cripple our government, our economy, and our society.

Last summer, the United States government faced such a disruptive attack. On a great American holiday -- the Fourth of July -- foreign adversaries launched a coordinated strike, or ‘botnet’ attack, in cyberspace against government agencies ranging from the Treasury Department to the Secret Service. It is still unclear who the ultimate source was for this cyber attack. This is not the first time our government's digital infrastructure has been attacked. The Departments of Defense, Homeland Security, and Commerce, and the National Aeronautics and Space Administration have all suffered major electronic intrusions from unknown foreign entities. Corporate America faces a similar predicament. Every day, public and private companies throughout the United States are confronted with the challenges of managing cyber risks. The disruption can have huge financial implications for corporations and consumers. One current example is the dispute between Google and China, which burst into the headlines after Google's networks were hacked.

The same aggressors who hack into our computer systems to steal information can also leave behind viruses and malicious code that can be triggered in the event of a conflict or crisis. Foreign adversaries or cyber terrorists could shut down our information systems and deprive our

country of electricity, communications, and financial services. And it's all too easy to imagine the destruction our enemies could wreak if they broke into the military's blue force tracking system, which tells our commanders where friendly forces are located. The result might be changed designations, possibly producing a situation where commanders would unknowingly call in attacks on their own forces.

The time has come for the United States to begin treating cybersecurity as one of the most important national security challenges it faces. In December 2008, the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency highlighted the fact that the United States lacks a comprehensive national strategy to address cyber threats; it also laid out a set of recommendations, including the appointment of a White House point person to lead the government's efforts on cybersecurity. Those recommendations were well received. On May 29, 2009, President Obama announced a series of initiatives that included the establishment of a Cybersecurity Coordinator at the White House, who will orchestrate and integrate cybersecurity policy across the entire federal government. Howard Schmidt has since been appointed as the first White House Cybersecurity Coordinator. This is a positive step and positions the United States well to continue making significant progress in securing cyberspace.

A top priority for Mr. Schmidt must be establishing a clear strategy to not only protect against cyber attacks, but also deter such attacks in the first place. During the Cold War, we built a "Strategic Triad" of land, sea, and airborne nuclear weapons that deterred an attack on our country involving weapons of mass destruction. In the digital age, we need a "Cyber Triad" that will similarly deter cyberspace attacks on our information networks using weapons of mass disruption.

The first leg of this new Cyber Triad is resilience. During the Cold War, our adversaries knew that a nuclear first strike was futile, because if they hit our land-based missiles, we still had missiles at sea and in the air with which to retaliate. We must build similar resilience into our information systems, so our adversaries know that they cannot succeed in crippling our economy, our government, or our military with cyber attacks. Cyber resilience means such things as redundancy of critical connectivity; the ability to handle increased traffic loads, even under the most stressed conditions; and the ability to protect and se-

cure sensitive and private information. Building resilience into information networks requires proper resourcing but the increased costs will pale in comparison to the negative consequences of not making the commitment.

The second leg of the new Cyber Triad is attribution. As last July's cyber attack on the United States demonstrated, it is difficult to identify the ultimate source of cyber attacks. In the future, we might be able to trace a cyber attack on America to one nation, without realizing that it came from a computer that had been surreptitiously taken over by another nation. Our continuing inability to attribute attacks is tantamount to an open invitation to those who would like to do us harm, whatever their motives. If enemies can attack our information networks without fingerprints, they can attack without consequences – and that means

they cannot be deterred or countered. To deter cyber attacks, we need to improve our capability to attribute these attacks to their ultimate source.

The third leg of the Cyber Triad is offensive capabilities. Just as with kinetic weapons, our enemies must know that America possess an effectively balanced set of offensive and defensive capabilities. If terrorists and rogue regimes know that our digital infrastructure is resilient, that we accurately can identify any attackers, and that we can fully defend ourselves in

cyberspace or through other means, they can be deterred from initiating cyber attacks.

Unlike nuclear deterrence, cyber deterrence cannot be undertaken by government alone. We need to involve the general public. Today, a significant number of home computers in our country have no firewall or anti-virus software installed. Cyber criminals exploit these vulnerabilities each day to secretly take over and remotely operate thousands of computers, turning them into "bots" for cyber crime and cyber attacks. Experts estimate that about 11 percent of machines worldwide – some 65 million to 90 million PCs – are compromised. We need to launch a public information and awareness campaign, on par with the Year 2000 (Y2K) campaign, to encourage every American with a computer to get a firewall and anti-virus software installed – now!

We also need to involve the private sector. Private industry owns 85 percent of our nation's information infrastructure. According to McAfee estimates, businesses worldwide saw up to \$1 trillion in data stolen through cyber espionage last year. This is an unparalleled loss of intellectual property. To protect our information networks

“To protect our information networks against espionage, crime, and attacks in cyberspace, we need an unprecedented private-public partnership.”

against espionage, crime, and attacks in cyberspace, we need an unprecedented private-public partnership. We also need to work internationally in countering cyber-crime by identifying the operating locations, apprehending the suspects, and prosecuting the criminals. Working together, we need concerted efforts to appropriately punish criminal activity, which will aid in deterrence and in countering syndicated global criminal activity.

Finally, we need to involve the international community in a broad range of other areas as well. Many of the developed nations of the world are as dependent on a healthy, secure Internet as we are, so this is a multi-dimensional, global problem. It's not just the United States; all of our allies and other nations of the world are interested in peaceful coexistence on the Internet. So, we all have work to do in achieving peaceful coexistence in cyberspace and we've got to get to work on that now.

Our cyberspace capabilities must be robust but they must abide by our nation's laws, comply with the policies that we have in place now and identify new policies that need to be established. In the same way that we have worked out agreements with other nations regarding land, sea, air and space, it's a natural extension that we will have to work on relationships, increased understanding, alliances and agreements for cyberspace. We must realize that globally we have entered an age of interdependence where each nation's security and prosperity is increasingly dependent on the actions of the other nations of the world.

Achieving peaceful coexistence in cyberspace will be expensive – but the costs of inaction will be even greater. Today, there are approximately 1.5 billion people around the world online – and more are joining the information age each day. Cyberspace has become an engine of economic growth, but it is also a growing source of vulnerability. Unlike during the Cold War, our adversaries don't need nuclear weapons to attack us: all they need is a laptop and an internet connection to cause immense disruption and destruction. To preserve our way of life in the digital age, we must summon the will, and the resources, to meet this challenge. Investing in a robust 'Cyber Triad' is a crucial first step.

Lieutenant General (ret.) Harry D. Raduege, Jr., is chairman of the Deloitte Center for Cyber Innovation. He served in the U.S. military for 35 years, working in the areas of telecommunications, space, information and network operations. In his last position, he led Department of Defense netcentric operations as the director of the Defense Information Systems Agency. He also served as the commander of the Joint Task Force for Global Network

Operations, and as deputy commander for Global Network Operations and Defense for the U.S. Strategic Command.

The View from Russia Russian Priorities and Steps Towards Cybersecurity

By Dmitry I. Grigoriev

For many years the Institute of Information Security Issues at Moscow State University has been collaborating with leading Russian government and research organizations to study problems of international information security (IIS). The increasing awareness of the reality of existing threats in cyberspace has led the world community to intensify cooperation aimed at safeguarding IIS. Today, most actors in world politics recognize the need for a comprehensive solution to these problems. The Russian Federation has long been in favor of dealing with existing disagreements on cybersecurity at bilateral and multilateral levels, and it is advocating concrete steps in negotiations, international forums, scientific conferences, and seminars.

First, it is important to begin the process of unifying terminology concerning IIS, which would enable all stakeholders to speak the same language when discussing existing problems. This applies in particular to the concept of "cybersecurity," which continues to generate much debate. Different countries attach different meanings to the term. Russia insists that cybersecurity involves coping with three basic areas: criminal, terrorist, and military-political threats. Each may differ in terms of the capabilities for mounting cyberattacks and the scale of potential damage. Russian experts believe that it is criminals and terrorists who present the greatest threat to the security of transnational cyberspace.

Military-political threats involve the use of Information and Communication Technology (ICT) to achieve political objectives through coercive pressure on the leadership of opposing states—in essence, the "hostile" use of these technologies. This is evident in the structure of the armed forces of some nations, which set up special units to conduct cyber warfare. For such units, ICT takes on the characteristics of offensive weapons, designed to attack

the enemy in an armed conflict. As ICT becomes more sophisticated, so does the destructive potential of these weapons.

The specific features of these weapons are their capacity for cross-border use, the covert and anonymous nature of the preparations they allow for hostile actions in cyberspace, and the difficulty of averting and appropriately responding to such attacks. When repelling a cyberattack, the target will not be aware of the motives of its source, and therefore will not be able to identify what is occurring as a criminal, terrorist, or military-political act. Military cyber attacks can easily be disguised as criminal or terrorist acts. Moreover, it is often very difficult to reliably determine precisely what country such actions were carried out from. And even if the country is identified, it is very difficult to prove that the attack was carried out specifically by its armed forces. This underscores the need for the world community to safeguard IIS with a systemic approach that factors in the entire array of threats to cyberspace and their asymmetric nature. It would be helpful to study the possibilities of creating an international system for identifying the source of any “hostile” action involving the use of ICT.

In order to safeguard the security of cyberspace at the national level, we should identify and study the actors in cyberspace, including the “enemies” operating there. Today we can identify the following such actors:

- **Users, Operators, Administrators:** These groups do not have a negative influence on cybersecurity. They are actors who lawfully provide cyberspace resources or consume them.
- **Non-hostile Hackers:** As a rule, they unintentionally have a negative impact on cybersecurity, whether they are doing so “just for fun” (settling a bet or dispute, for example) or to show off.
- **Hostile Hackers:** Their motives include revenge, envy, and self-interest.
- **Network Combatants:** They can have a positive or negative impact on cybersecurity for their own purposes. In network law enforcement, activities are prescribed by law and financed by the state. Other combatants may be secretly financed by state or private entities pursuing covert agendas.
- **Cyber Criminals:** Criminals using cyber as their

weapons of choice.

- **Cyber Terrorists:** Terrorists using cyber as their weapons of choice.
- **Governments:** State bodies that may use cyberspace for military-political purposes.
- **Nongovernmental organizations:** Groups that may use cyberspace to promote their political agendas.

All of these actors are growing stronger, building up their capacity to have an impact on cyberspace. As a result, the makeup of a system of international and regional cybersecurity needs to be based on the idea of establishing a universal and comprehensive regime of international law that does not allow the use of the Internet for military-political purposes and ensures that it functions in a stable, secure and continuous manner. To achieve these

objectives, according to Russian experts, Russia must move to carry out the following tasks:

- Create an international system of Internet governance, which would call for the transfer of such functions as managing the system of domain names and root servers to the International Telecommunication Union. In this context, it is essential to take steps to increase the influence of intergovernmental bodies on the creation of Internet protocols, so as to improve the security of their use and to make it possible to identify perpetrators of information attacks;

- Adopt a universal international political-legal pact that condemns the use of the Internet for military-political purposes. It should also contain definitions recognized by the world community for

aggression in information space and for information weapons; ascertain the aggressor’s liability under international law; and implement joint measures to minimize the damage to global cyberspace and a specific country’s cyberspace. The purpose of this pact would be to bolster the confidence of members of the international community in the global information infrastructure and to reduce the threat of hostile uses of information;

- Create regional information security systems that include international legal norms and threat monitoring, including identification and assessment centers within the framework of such organizations as the Collective Security Treaty Organization (CSTO) and the Shanghai Cooperation Organization (SCO).

“A system of international and regional cybersecurity needs to be based on the idea of establishing a universal and comprehensive regime of international law that does not allow the use of the Internet for military-political purposes.”

Also enlist the EU's cooperation, organizing joint measures to suppress and repel aggressive activities in cyberspace;

- Within the framework of thematic and regional forums such as UNESCO, the G8, the Council of Europe, etc., form a friendly global and regional information space based on principles of trust, in order to prevent the concerted dissemination of inaccurate and deliberately false socio-political information;
- Harmonize legislation and establish unified agencies for the investigation of cybercrimes in order to prevent the use of the Internet for criminal and terrorist purposes.

In bilateral and multilateral negotiations, Russia defines the following areas as priorities:

1. The regulation of relations and the practice of law enforcement with regard to the use of information technologies as a means to force a settlement for intergovernmental conflicts. Agreements on this problem could become an important factor in the task of strengthening international peace and security.
2. Management of stable functioning and secure use of global information and communication networks for national development. This activity will bolster confidence in global networks as a factor in the economic, social, political, and cultural development of national societies and in preserving their cultural identity and spiritual unity.
3. Raising the standard of cybersecurity by educating users to observe basic practices that best ensure the secure use of information technologies in all areas of human activity.
4. Developing the mechanisms to identify hostile users of information technologies and ensuring that liability is prescribed by international law.
5. Developing countermeasures against the use of information technologies for the preparation and commission of terrorist acts and other types of terrorist activities. Cooperation in this area will help to strengthen government guarantees of human rights and freedoms in the realm of security.
6. Bolstering cooperation between regional and bloc information security systems to reduce the risk of the use of information technologies for breaches of international peace and security. The Russian Federation is actively working in this area by promoting political consultations and joint academic seminars on these issues within the framework of

the CSTO, the SCO and the informal BRIC group.

7. In pursuing the above areas of cooperation, Russia is guided by the following universally recognized tenets of international law: strictly complying with the principles of the sovereign equality of states and non-interference in the internal affairs of other states; conducting activities solely on the basis of the principles of international cooperation; respecting basic human rights and freedoms; and respecting the sovereignty of states in the national information space.

Russia proposes the following as the basic mechanisms for carrying out cooperation in the field of IIS:

- Development of norms of international law with regard to IIS and mechanisms for complying with them;
- Expansion of international contacts between national academic and educational institutions and between national experts in the field of IIS;
- Development of mechanisms for international governance of the global information infrastructure;
- Harmonization of national educational standards with regard to safeguarding information security;
- Development of international mechanisms for consultations on the most complex problems of safeguarding IIS;
- Publication of a journal on problems of IIS under the aegis of the UN;
- Joint research on ways to solve the most pressing problems of IIS.

In order to establish worldwide mechanisms of cooperation in safeguarding IIS, the Russian Federation is prepared to consider signing a number of international legal pacts that regulate relations in the following areas: countermeasures against hostile use of information technologies; the dissemination of standards of cybersecurity; international cooperation in conducting research and implementing educational programs on IIS issues; and creation of a mechanism for regular discussions at the expert level under UN aegis of problems of developing a system for safeguarding IIS.

Russia's position on this matter is based on the principles of international law and the spirit and letter of the UN Charter—to wit, respect for national sovereignty, the inadmissibility of aggression and the peaceful settlement of disputes.

These principles in the context of the Internet have already been enshrined in part in international legal documents—in the UN General Assembly Resolution “Developments in the Field of Information and

Telecommunications in the Context of International Security” and in documents from the final phase of the World Internet Governance Forum. These documents point out that it is inadmissible to use ICT for purposes that are incompatible with international stability and that could have a negative impact on the security of states.

After the Obama administration came into office in 2009, there was some intensification of the negotiating process regarding IIS at the bilateral Russia-U.S. level. As a result, the Russian Federation has stepped up its actions aimed at developing common approaches at both the bilateral and multilateral levels. Among the most recent activities:

- In March 2009, the Organization on Security and Cooperation in Europe held a workshop on a comprehensive OSCE approach to enhance cybersecurity.
- In April 2009, the third international forum on Partnership Among State, Business Community and Civil Society in Ensuring Information Security was held in Garmisch, Germany. As a result of the forum, Russia reached specific agreements on cooperation to safeguard Internet security with the management of the International Corporation for Assigned Names and Numbers (ICANN) and an array of European research centers.
- In October 2009, the Fifth International Conference on Problems of Security and Countermeasures Against Terrorism was held in Moscow, which included examination of cybersecurity issues.
- In November 2009, based on a decision by the UN General Assembly adopted on Russia’s initiative, a UN Group of Government Experts on Problems of International Information Security began its work. The group’s mandate calls for continuing research on existing and potential threats in the field of information security and possible joint measures to remove them. Based on the results of this work, the group is to prepare a report by the UN Secretary General in 2010 for the 65th session of the General Assembly.
- In November 2009, talks took place in the United States between a Russian delegation and leaders of the U.S. National Security Council, the State Department and the Department of Homeland Security on intensifying bilateral cooperation in the field of IIS.
- At the EastWest Institute’s Seventh Worldwide Security Conference in Brussels in February 2010, the Russian delegation presented a report on

Russia’s approaches to problems of safeguarding IIS.

- In April 2010, the fourth international forum of Moscow University on Partnership among State, Business Community and Civil Society in Ensuring Information Security was held. Representatives of Moscow University and leading research centers in Germany, Bulgaria, the U.S., China and India, as well as ICANN, discussed the draft Declaration on the Creation of an International Research Consortium of Information Security, which was proposed by Moscow University. The purpose of the consortium is to conduct joint research on problems of IIS.

Taken together, these activities demonstrate the scope and commitment of the Russian Federation to giving true meaning to the concept of cybersecurity on a global level.

Dmitry I. Grigoriev is Director of the Center for International Cooperation in Security and Countering Terrorism Studies at Lomonosov Moscow State University’s (LMSU’s) Institute of Information Security Issues. He is a permanent member of the Organizing Committee Presidium of the annual LMSU International Scientific Conference of Security and Countering Terrorism Issues and of the annual LMSU International Forum, “Partnership of State Authorities, Civil Society and the Business Community in Ensuring Information Security and Combating Terrorism,” in Germany. He is also a regular participant of the OSCE’s Action Against Terrorism Unit conferences and workshops.

The View from India

Cyber Deterrence: Legal Perspectives

By Pavan Duggal

The coming of the Internet has made our world a much smaller place and opened the way for tremendously positive interactions across borders. But at the same time, the lack of boundaries on the Internet has ensured that cyberspace has become a fertile breeding ground for terrorists and cyber criminals. Over the last decade and a half, we have seen not only tremendous jumps in the

number of cyber crimes but also growing sophistication in their character, specialization and delivery mechanisms. Consequently, countries across the globe have been looking at a variety of ways to legislate an effective system of cyber deterrence.

India has seen dramatic growth in the sector of Information Technology, and the IT brains of the country have already won broad international recognition. India was also one of the few countries to reach for the tools of cyber law as a means of creating effective cyber deterrence. In 1997 the General Assembly of the United Nations endorsed the Model Law On Electronic Commerce. Keeping that model in mind, India enacted the Information Technology Act, 2000, becoming the twelfth nation in the world to enact cyber law.

Indian cyber law is primarily designed to promote e-commerce, but it also introduced key elements of cyber deterrence. It defines a variety of activities as cyber crimes, making them punishable by imprisonment and fines. Among the provisions:

- Tampering with source code documents was made a crime punishable by up to three years in prison or a fine of up to 200,000 rupees, or by both.
- Hacking was made an offense that is similarly punishable with imprisonment of up to three years or a fine of up to 200,000 rupees, or by both.
- The law prohibits the publishing and transmitting of obscene electronic information, or causing such information to be published or transmitted. This crime is punishable with up to five years in prison and with a fine of up to 100,000 rupees.
- Misrepresentation of any material facts while obtaining any license to act as a Certifying Authority or procuring a digital signature certificate was made a crime. The publishing of false digital signature certificates for fraudulent or unlawful purposes is punishable by up to two years in prison or by a fine of up to 100,000 rupees, or by both.

The Indian law also introduced the concept of a protected system. The central government was given the power to declare any computer, computer system or computer network to be a protected system by notification in the official Gazette. Despite all these provisions, it soon became evident that the initial Indian regulations weren't sufficient, since the law contained several loopholes. As a result, the Indian government enacted the Information Technology (Amendment) Act, 2008, which amended the Information Technology Act, 2000. The new amendments came into force on October 27, 2009. With these new amendments, India's cyber law has begun to focus more

on the concept of cyber deterrence.

For the first time in the legislative history of India, cybersecurity has not only been given tremendous focus but also has been given a distinct legal definition. The amended Information Technology Act defined cybersecurity as "protecting information equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction."

The new amended Indian cyber law has identified far more kinds of cyber crimes than its predecessor. Thus, various computer-related offenses, which involve dishonest and fraudulent activities, have been brought within the ambit of the Indian law. In addition, a variety of new kinds of crimes involving the sending of offensive messages through communications services or communication devices now have penalty provisions. Thus, offenses like cyber defamation, cyber nuisance, cyber harassment, and cyber stalking have been brought within the ambit of Indian cyber law. Identity theft, an increasingly common practice, is now also subject to criminal penalty. All of the above acts are now punishable by prison terms of up to three years and fines of up to 100,000 rupees.

One of the crowning glories of the new focus on cyber deterrence under the amended Information Technology Act is the masterstroke of the Indian legislature in providing for a distinct new kind of offense which deals with cyber terrorism. Cyber terrorism has been defined in the widest possible terms and has been now made a heinous crime punishable by up to lifetime imprisonment and fines.

To ensure respect for the private space of people and that Multimedia Messaging Services (MMSs) and spy cameras do not invade the privacy of individuals, the law makes violation of privacy a criminal offense. Thus, anyone who intentionally or knowingly captures, publishes or transmits the image of the private area of any person without his or her consent, violating the privacy of that person, commits an offense. The offense is punishable by up to three years in prison or a fine of up to 200,000 rupees, or by both.

Publishing or transmitting material in an electronic form containing sexually explicit acts has been made a cyber crime punishable by up to five years in prison and a fine of up to one million rupees. In addition, there is a new kind of cyber crime pertaining to child pornography. Thus, if any person commits cyber crimes involving child pornography, this offense is also punishable with up to five years in prison and a fine of up to one million rupees.

The law includes provisions to strengthen cyber deter-

rence further by providing for compensation to victims. The amount of damages that can be granted under the Indian cyber law are 50 million rupees per contravention. However, an aggrieved person or a victim can even claim damages beyond 50 million Indian rupees by filing a legal action in a court of competent jurisdiction. These damages are provided by means of summary proceedings, which are expected to be concluded in a short period of time.

It isn't just the laws that have changed to build up a system of cyber deterrence; the private sector in India, which is equally concerned about cybersecurity issues, has launched its own initiatives. The Indian banking and financial sectors have been particularly active in this area. The Reserve Bank of India has mandated all banks to follow Internet banking guidelines, which are aimed at enhancing security and reducing risks, and private banks are putting in place added security safeguards to protect third party data.

The government is also paying serious attention to cyber deterrence, but it needs to dedicate far more resources, time, effort, and energy to tackling the problems—first of all, by allocating more funds for improving and strengthening cybersecurity. More needs to be done at the national, regional, and local levels by both the private and public sectors. At the national level, there is need for a comprehensive cybersecurity plan, which should outline how all the components of India's actions should be coordinated to produce the most effective system of cyber deterrence possible.

All countries need to realize that the Internet and cyberspace are shared by all of us, and that we need collaboration at the international level to counter the broad range of threats. The Council of Europe's Convention on Cyber Crime is one example of an effective international treaty. While there is talk about the need for new international treaties, the reality is that the world's nations do not have the luxury of time to formulate new sweeping international agreements. A more practical measure would be greater international cooperation between cyber crime units and law-enforcement agencies, not limited by national borders.

There are large numbers of practical obstacles to progress, particularly at the international level. There is a huge level of mistrust between governments, who do not wish to share information related to their national secu-

urity or internal policies. There are also different legislative approaches to dealing with cyber deterrence in different countries, and dramatically different legislative approaches to such issues as freedom of expression and human rights. Often, these differences become stumbling blocks for nations to work together as a cohesive unit to fight cyber attacks.

I believe that the only way forward is by discussion, debate and collaboration. Countries have to learn to share their strategies for cyber deterrence, thus contributing to a far more cohesive international approach to the subject that should produce more cybersecurity for all in the future.

As far as India is concerned, here are my key recommendations:

1. India needs to come up with a cohesive national plan on cybersecurity.
2. A lot of government and private money, time, and effort need to be allocated for cybersecurity.
3. A broader awareness campaign is needed for all the relevant stakeholders.
4. India needs to participate actively in all forms of international cooperation on cybersecurity to promote more unified policies in the face of cyber threats.
5. India needs to further strengthen its laws pertaining to cybersecurity and make them into a more effective deterrent.
6. India needs to ensure that its existing laws are effectively implemented and do not remain mere paper tigers.

In conclusion, it can be safely stated that the future growth and development of our civilization is linked with the growth and development of cyberspace, and we need to build much greater public awareness of that fact. The next war is not going to be fought on the ground but in cyberspace. All countries, including India, need to take the necessary steps to foster an international consensus on cyber deterrence strategies.

The ancient Indian *Vedas* talked about the concept of Vasudev Kutumbkum—namely, that the world is one family. India considers the entire world in cyberspace as one big family and is happy and willing to contribute everything it can ensure the peaceful coexistence of all the members of this global, cyber family.

Pavan Duggal is an Advocate at the Supreme Court of India. He is an expert and authority on cyber law and

“All countries need to realize that the Internet and cyberspace are shared by all of us, and that we need collaboration at the international level to counter the broad range of threats.”

e-commerce law. He is a consultant to UNCTAD on cyber law and to UNESCAP and the Council of Europe on cyber crime. He is also a member of the AFACT Legal Working Group of the UN/CEFAT and of the Board of Experts of the European Commission's Dr. E-Commerce. He has worked on a cyber law primer for the e-ASEAN Task Force and as a reviewer for Asian Development Bank. Duggal is the President of Cyberlaw Asia, an organization committed to the passing of dynamic cyber laws in the Asia.

The View from Norway Wanted: A United Nations Cyberspace Treaty

By Judge Stein Schjøberg

Cyberspace is the fifth common space, after land, sea, air and outer space. As much as the other domains, it needs coordination, cooperation and legal measures among all nations to function smoothly. And when it comes to constructing an effective system of deterrence against cyber threats, the best means to that end would be the construction and utilization of a global United Nations framework. The ultimate goal would be to establish a Cyberspace Treaty, which would spell out what constitutes acceptable and unacceptable behavior. This would go a long way towards ensuring peace and security in cyberspace.

The specter of mounting cyber threats against sovereign states, including massive and coordinated attacks against critical communications infrastructure, will necessitate a global response. Regional and bilateral agreements will not be enough. A broader view of international law is needed to facilitate the development of a global strategy to deter cyber threats from any direction.

The process of working towards a United Nations Cyberspace Treaty should help develop a common understanding of all aspects of cybersecurity among countries at various stages of economic development. All stakeholders need to come to a common understanding on what constitutes cyber crime, cyber terrorism and other forms of cyber threats. That is a prerequisite for developing national and international solutions that harmonize cybersecurity measures. Those kinds of common understandings will also help reduce the divide between developed- and

developing-country perceptions on cybersecurity.

The United Nations International Law Commission should consider drafting a Cyberspace Treaty – a convention or a protocol on cybersecurity and cyber crime.

Due to the urgency of this global challenge, I recommend that the International Law Commission establish a working group to handle this issue. This group would undertake the preliminary work aimed at defining the scope of responsibilities of the working group and its main goals.

The Record on Cybersecurity to Date

At its forty-eighth session in 1996, The International Law Commission adopted the Draft Code of Crimes against Peace and Security of Mankind, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable under national law.

Serious crimes against peace and security in cyberspace should be established as crimes under international law through a Cyberspace Treaty on the United Nations level, whether or not they were punishable under national law.

In May 2007, The International Telecommunication Union (ITU) launched the Global Cybercrime Agenda to create a framework to coordinate international responses to growing challenges of cybersecurity. In order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons delivered the Chairman's Report in August 2008 with several recommendations, including recommendations for cyber crime legislation. The same group delivered the Global Strategic Report in November 2008. It outlined strategies in five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, and International Cooperation.

As a follow-up to the HLEG reports, a paper on a Global Protocol on Cybersecurity and Cyber Crime was presented at the Internet Governance Forum (IGF) in Sharm El Sheikh, Egypt, in November 2009.

Criminal conduct in cyberspace is global by nature and requires global harmonization of cyber crime legislation as part of a Cyberspace Treaty. The 2001 Council of Europe Convention on Cybercrime is based on criminal cyber behavior in the late 1990s, and is not necessarily suited to deal with the challenges of the current decade. It also fails to have a global reach.

Substantive criminal law and procedural law in a Cyberspace Treaty

The Council of Europe Convention on Cybercrime is a regional initiative on legal measures that may serve as a useful reference point for a broader treaty. The basic standards and principles in this convention may be implemented in a Cyberspace Treaty, taking into consideration the reservations and policies of individual countries. Some provisions of this convention could also encroach on a country's sovereignty and national security policies. Another reference point could be the HLEG recommendations and proposals. Below are some of the major cyber threats that any new treaty will have to contend with:

- Terrorism in cyberspace consists of both cyber crime and cyber terrorism. But terrorist attacks in cyberspace are also a category of cyber crime and a criminal misuse of information technologies. Recent developments have blurred the differences between cyber crime and cyber terrorism.
- Cyber attacks may include the use of botnets that are designed to destroy or seriously disrupt critical information infrastructure of vital importance to a country.
- Public provocation, recruitment, or training on the Internet for terrorism or for a coordinated cyber attack, whether or not inspired by terrorist groups, to destroy or seriously disrupt information technology systems or networks of vital importance to the society should be regarded as a criminal offence. In many countries, no legal provisions exist that aim to criminalize preparations for actions with terrorist and/or destructive intent.
- Phishing may be carried out through the use of botnets. Botnets may include thousands of compromised computers, and their services are offered on the market for sale or lease, enabling criminals to plan and launch cyber attacks. The victims of phishing may be lured to counterfeit or fake Web sites that look identical to legitimate websites.
- Identity theft is the misuse of someone else's personal information to commit fraud. The theft or identity infringement of the information itself does not ordinarily constitute a criminal offence; it is the fraud that follows that is illegal. A great number of

people around the world suffer the financial and emotional trauma of identity theft. In most countries, no legislation exists covering the phishing that enables identity theft. A global cyberspace treaty is needed to criminalize the first part of this process.

- Crime in social networks and virtual worlds. Social networks provide online communities for individuals who share common interests or activities, or for the simple exchange of information among friends. The most important global social networks are Facebook, MySpace, and Twitter, which have several hundred million users. Social networks are also used by criminals, mostly for identity theft and fraud.

“Criminal conduct in cyberspace is global by nature and requires global harmonization of cyber crime legislation as part of a Cyberspace Treaty.”

Procedural law

The real-time collection and recording of traffic data, interception of content data, data retention, and the use of key-loggers are among the top challenges today. A special problem has been caused by Voice over Internet Protocol (VoIP). The old methods of recording human voices are no longer used. In most countries, no procedural legislation exists covering all these new powers and procedures in

cyberspace.

Cloud computing is a means to provide remote computer services in cyberspace. Users often have no knowledge of, expertise in, or control over, the technology infrastructure in the “cloud” that supports them. Cloud computing does not allow users to physically possess the storage of their data, and the user leaves the responsibility of data storage and control to the provider.

The “cloud” may be the ultimate example of globalization, since it could cover many borders and regions. Users could be offered selected “availability zones” around the world. That can easily lead to multi-jurisdictional crime scenarios, with all the obvious complications that implies for the investigation and prosecution of criminal acts. This once again underscores the need for global harmonization of procedural laws in a cyberspace treaty. These problems may only be solved through a global Convention or Protocol that includes necessary jurisdictional provisions under international law, whether or not they are possible to prosecute under national law.

An International Criminal Court

Criminal prosecution based on international law needs an international criminal court for any proceedings. The International Criminal Court (ICC) was established in 1998 as the first ever permanent, treaty-based, fully independent international criminal court. It was meant to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The ICC does not replace national courts, since its jurisdiction is only complementary to national criminal jurisdictions. It will investigate and prosecute if a state that is party to the Rome Statute that entered into force in 2002 is unwilling or unable to prosecute. Anyone who commits any of the crimes under the statute can be prosecuted by the court.

A State may be unwilling to prosecute a crime for any number of reasons—in cases when its judicial system has collapsed, or when, for some reason, it is unable to capture the accused person or gather the necessary evidence and testimony.

The jurisdiction of the International Criminal Court is limited to states that become parties to the Rome Statute. The maximum term of imprisonment is 30 years, and a life sentence may be imposed.

In the final diplomatic conference in Rome, serious crimes such as terrorism were discussed, but the conference conceded that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of major concern to the international community, and recommended that a review conference, pursuant to article 123 of the Statute of the International Criminal Court, consider such crimes with a view to include them in the list of crimes within the jurisdiction of the Court. Massive and coordinated cyber attacks against critical information infrastructure may also qualify as a “serious crime,” even if it may not be considered terrorism. Any expansion of the jurisdiction of the court should also cover other serious crimes in cyberspace.

A Forum for Regional Organizations

The individual countries in each region are members of the United Nations. In addition, countries are also members of regional organizations, but no umbrella organization or institution exists only for the regional organizations. A conference of regional organizations on cybersecurity and cyber crime would promote a broader cyber deterrence initiative.

A conference would provide a forum for discussion and the exchange of information, encouraging a common understanding of the issues and the coordination of principles and standards for cybersecurity. The regional organizations may then be able to assist and provide guidelines for their member states, taking into account regional traditions.

There are at least 13 recognized organizations that could play a significant role in establishing and coordinating the principles and standards for the global battle against cyber crime. These are, but are not limited to:

- The G8;
- The Council of Europe;
- The Organization of American States;
- Asia-Pacific Economic Cooperation;
- The League of Arab States;
- African Union;
- The G20;
- The Organization for Economic Cooperation and Development;
- The Commonwealth;
- The European Union;
- The Association of South East Asian Nations;
- NATO;
- The Shanghai Cooperation Organization.

In addition, global organizations such as the ITU, INTERPOL, and the United Nations Office on Drugs and Crime (UNODC) should establish partnerships with these organizations.

A forum should promote regional and global research and development on cybersecurity and cyber crime. Any successful strategy will unite the existing regional initiatives, bringing the organizations together with the goal of proposing common global solutions. Those solutions must also involve private industries, who build, control, and maintain most cyber infrastructure.

Conclusion

Cyber deterrence may best be achieved within a global framework of a United Nations Cyberspace Treaty on cybersecurity and cyber crime. Regional and bilateral conventions or treaties will not be sufficient. International law should provide the framework for peace and security in cyberspace.

Due to the urgency of the global challenges in our cyber age, I recommend that the United Nations International Law Commission establish a working group to examine these issues. This group may undertake the preliminary

work on a new international treaty, or, at a minimum, help to define the scope and direction of the work that is needed to achieve that goal.

***Judge Stein Schjølberg** is an international expert on harmonizing cyber crime legislation. Since 1980, he has served as an expert for several international institutions dealing with this issue. In 2007 and 2008, he served as the Chairman of the High-Level Experts Group (HLEG) at the International Telecommunication Union (ITU) in Geneva. He is the editor of a Web site on the subject: www.cybercrimelaw.net.*

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. Baldrige (U.S.)

Chairman
Republic Energy Inc.

Thor Bjorgolfsson (Iceland)

Chairman
Novator

Peter Castenfelt (U.K.)

Chairman
Archipelago Enterprises, Ltd.

Maria Livanos Cattai (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

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

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
1040 Brussels
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