Rights and Responsibilities in Cyberspace

Balancing the Need for Security and Liberty

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

World Federation of Scientists
Founded in Erice
Beijing Geneva Moscow New York
World Federation of Scientists
www.federationofscientists.org

About the Authors

Jody R. Westby is CEO of Global Cyber Risk LLC, located in Washington, D.C. She serves as Adjunct Distinguished Fellow to Carnegie Mellon University's CyLab. She chairs the American Bar Association's Privacy & Computer Crime Committee, is co-chair of the World Federation of Scientists Permanent Monitoring Panel on Information Security, and is a member of the ITU Secretary-General's High-Level Experts Group on Cybersecurity.

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

William Barletta is Director of the United States Particle Accelerator School and Adjunct Professor at the Department of Physics at the Massachusetts Institute of Technology and at the University of California at Los Angeles. He is also Director Emeritus of the Accelerator Fusion Research Division and of the Homeland Security Office, which he founded, at Lawrence Berkeley National Laboratory. He is a Vice Chairman of the American Physical Society Forum on International Physics, and an active member of the American Bar Association Privacy & Computer Crime Committee. His professional research activities span a broad range from instruments for accelerator-based science, to nanotechnology using ion beams, to technologies for cargo inspection, to international legal and policy aspects of cybersecurity.

Rights and Responsibilities in Cyberspace

Balancing the Need for Security and Liberty

Jody R. Westby, Henning Wegener, and William Barletta

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

World Federation of Scientists
Founded in Erice
Beijing Geneva Moscow New York
World Federation of Scientists
www.federationofscientists.org

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.

The World Federation of Scientists is a free association, which has grown to include more than 10,000 scientists drawn from 110 countries. All members share the same aims and ideals and contribute voluntarily to uphold the Federation's Principles. The Federation promotes international collaboration in science and technology between scientists and researchers from all parts of the world - North, South, East and West.

For more information about the EastWest Institute, the World Federation of Scientists, 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

World Federation of Scientists
c/o ICSC-World Laboratory
CERN Building # 29
1211 Geneva 23 – Switzerland
e-mail: info@federationofscientists.org
Tel: +41227679957 Fax: b+41227679965
Main contact: Claude G. Manoli – Secretary General

Cover photo: A woman uses the internet at a computer store in Beijing in this July 21, 2004 file photo. (Photo by Greg Baker/AP Photo)

Printed in the United States.

Contents

Foreword

Diplomacy—the art of promoting and defending state interests—is several thousand years old. The pervasive connectivity that now dominates global commerce and communication through the Internet is, by contrast, brand new—barely two decades, depending on the start date we choose. Foreign ministries are conservative institutions. Almost without exception, they have not adjusted their more traditional practices of diplomacy to promote and defend their national cyber interests on the world stage. Cyber diplomacy has been birthed but is facing existential challenges in its early development.

The diplomatic posture of most states on issues of network and information security betrays a fortress mentality, emphasizing physical defenses. It's a mindset more worthy of the medieval era than the modern world. The idea of physical defenses akin to walls will hardly disappear—and remains fully justifiable in many cases. But given the high levels of cross-border connectivity in the cyber world, national security approaches need to adjust quite radically to take into account international vulnerabilities, threats and opportunities. If ever there was a case for "common security" or "indivisible security," the cyber domain is it.

The policy papers in this short collection, written by leading members of the World Federation of Scientists' (WFS) Permanent Monitoring Panel on Information Security, spell out this urgent need for cyber diplomacy. More importantly, they also call for innovations in international law appropriate to the new cyber era to promote cyber stability and cyber peace. A common thread is the need for states to adopt new standards of responsibility for the conduct of activities emanating from their jurisdiction. There are three main takeaways from these papers:

- States must develop a legal framework applicable to cyber conflict that assures a minimum level of geo-cyber stability;
- Existing international legal obligations of states to protect human rights need to be applied more creatively and more comprehensively to the Internet;
- New agreements must impose an obligation on states to cooperate on activities that emanate from networks that operate within their borders.

These recommendations are not likely to be welcomed by all states, and there is indeed some tension between the second and third conclusions. State control of networks might allow state interference in the exercise of the right to freedom of expression. Nevertheless, states need to work through these contradictions to arrive at new minimum standards of regulation—or public and private sector self-regulation.

The EastWest Institute (EWI) has partnered with the WFS to "collaborate in mutual efforts aimed at ensuring the peaceful, free, and secure use of information and communication technologies (ICTs) in a well coordinated and trusted global environment." We promote confidence building and dispute resolution. Many states retreat behind their fortress

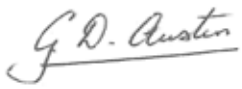
walls and claim national security sensitivities or irreconcilable differences in their political systems rather than talk seriously through diplomatic channels to address some of the most pressing problems.

These papers highlight the need to apply more diplomatic resources for inter-state dispute management in cybersecurity. This cannot have the desired effect until there is a new acceptance, enshrined in law, of how states and private sector actors assign responsibility. The authors have no illusions about the technical and political difficulties in reaching such agreements. But they offer their practical recommendations based on their conviction that this goal must be pursued.

The papers have been jointly published by EWI's Worldwide Cybersecurity Initiative and WFS as part of an EWI series to help catalyze awareness among key stakeholders of the need for more rapid progress in international cooperation. Through such work, EWI's main goals are to:

- Reframe the most divisive or contentious issues to enable consensus proposals for new agreements, policies and regulations;
- Champion high-impact proposals through effective advocacy and mobilization of stakeholders and expert groups;
- Work with stakeholders to create new and effective international mechanisms to solve the most serious problems.

EWI and WFS will leverage their collaborative relationship to address these goals in a multidisciplinary manner that bridges the associated scientific, legal, and diplomatic issues.



Greg Austin
Vice President
EastWest Institute

Antonino Zichichi
President
World Federation of Scientists

The Path to Cyber Stability

By Jody R. Westby, Esq.

Cyber war has become the drumbeat of the day. Nation-states are developing national strategies, creating offensive and defensive cyber war capabilities, conducting cyber reconnaissance missions, and engaging in cyber attacks, all with alarming frequency. What is blatantly apparent is that far more financial resources and intellectual capital are being spent figuring out how to conduct cyber warfare than are being spent figuring out how to prevent it. The lack of international dialogue and activity with respect to the containment of cyber warfare is simply stunning. As Winston Churchill famously noted, "It is better to jaw-jaw than to war-war." It is time for governments to begin discussions aimed at assuring an agreed-upon level of geo-cyber stability through mutual cooperation and international law.

"Geo-cyber stability" is defined by the author as the ability of all countries to utilize the Internet for economic, political, and demographic benefit while refraining from activities that could cause unnecessary suffering and destruction. With 1.8 billion online users[1] in 246 countries and territories connected to the Internet,[2] cyber attacks have become so commonplace and the capabilities to exploit the full range of information and communication technologies (ICTs) so great, that government systems, military networks, and business operations are in a continual state of risk.

The threat of cyber warfare is not new. In fact, the United States has exercised cyber warfare tactics probably more than any other nation. Two excellent examples of U.S. cyber war tactics are Operation Desert Storm and a successful Central Intelligence Agency plot to disrupt Soviet pipelines. In 1982, U.S. President Ronald Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. "The result was the most monumental non-nuclear explosion and fire ever seen from space," noted former Air Force Secretary Thomas C. Reed in his book At the Abyss: An Insider's History of the Cold War.[3] The attack had an enormous economic and psychological impact in the Soviet Union and is credited with helping to end the Cold War.[4] The United States deployed cyber warfare tactics again when it invaded Iraq in 1991. Phase I of Operation Desert Storm was a strategic air campaign that would "attack Iraq's strategic air defenses; aircraft/airfields; . . . command and control systems; . . . telecommunications facilities; and key elements of the national infrastructure, such as critical . . . electric grids. . . ."[5] The United States also used its extensive communication and satellite systems to support its Desert Storm activities.[6]

Recent Attacks That Undermined Geo-Cyber Stability

Although cyber attacks have been commonplace for the past decade, the frequency and sophistication of them over the past two years has caused a shift in the stability of the Internet and uncertainty whether nations will be able to secure and control their infrastructure, systems, and information. The 2007 attacks on government and private sector networks in Estonia were the watershed event that served as a government wake-up call. The attacks demonstrated the rapid pace at which a cyber attack can become a national security issue, involve other nation-states, and raise the issue of collective defense.

The attacks quickly escalated, seriously impacting government Web sites and systems and shutting down newspaper and financial networks.[7] The Estonian government was forced to close large parts of the country's network to outside traffic to gain control of the situation. Estonia blamed the attacks on Russia and claimed that it had tracked some communications to an Internet address belonging to a Kremlin official.[8] Notably, Russia refused to

1 "Internet Usage Statistics: The Internet Big Picture World Internet Users and Population Stats," http://www.internetworldstats.com/stats.htm.

2 "Internet World Stats: List of Countries Classified by Internet Penetration Rates," http://www.internetworldstats.com/list4.htm.

3 David E. Hoffman, "CIA slipped bugs to Soviets," *Washington Post*, Feb. 27, 2004, http://www.msnbc.msn.com/id/4394002.

4 Ibid.

5 *Operation Desert Storm: Evaluation of the Air Campaign,* U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, June 12, 1997, at Appendix V, http://www.fas.org/man/gao/nsiad97134/app_05.htm.

6 Jon Trux, "Desert Storm: A space-age war," *NewScientist,* July 27, 1991, http://www.newscientist.com/article/mg13117794.900-desert-storm-a-spaceage-war--one-year-ago-next-week-iraqinvaded-kuwait-provoking-a-war-with-the-us-and-its-allies-but-withoutanarmada-of-snooping-satellites-iraqs-battle-was-lost-almost-before-it-began.html.

7 Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times,* May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=print&oref=slogin.

8 Ibid.

cooperate in the investigation of the attacks even though it strongly denied any responsibility for them.[9] "They won't even pick up the phone," complained Rein Lang, Estonia's minister of justice, regarding Russia's refusal to help end the attacks or investigate evidence that Russian state employees were behind them.[10]

The attacks were also significant because Estonia quickly had to call international experts for help, even though it is one of the most "wired" countries in the world. The head of Estonia's Computer Emergency Response Team (CERT) initially summoned security experts from Estonia's Internet service providers, financial institutions, government agencies, and police and called on contacts in other countries to help track and block suspicious Internet addresses and traffic. Before the attacks ended, computer security experts from the United States, Israel, the European Union, and the North Atlantic Treaty Organization (NATO) were assisting Estonia—and learning its lessons.[11]

The attacks also highlighted the global nature of cyber crime and the difficulty of tracking and tracing cyber activities. Traffic involved in the attacks was traced to countries as diverse as the United States, China, Vietnam, Egypt, and Peru.[12] The Estonian attacks also may have represented a situation in which rogue actors, such as bot herders or organized cyber criminals, were aligned with a nation-state in conducting and concealing such attacks, though this has not been proven. (Bot herders are persons who control thousands to millions of computers on which they have surreptitiously planted software that can be activated at a chosen time. Once activated, the software can cause the infected computers to take certain actions, such as send repeated communications to a network as part of a denial-of-service attack.)

A few months after the Estonia attacks, U.S. Pentagon computer networks were allegedly hacked by the Chinese military in what has been called "the most successful cyber attack on the U.S. defense department,"[13] shutting down parts of the Pentagon's systems for more than a week.[14] Chinese hackers have also been blamed for attacks that compromised German government systems and for cyber espionage incidents against the United Kingdom's government systems.[15] The director-general of the United Kingdom's counterintelligence and security agency, MI5, posted a confidential letter to three hundred CEOs and security officers on the Web site of the Centre for the Protection of National Infrastructure, warning them that their infrastructure was being targeted by "Chinese state organizations" and that the attacks were designed to defeat security best practices.[16] Like the Estonian events, these attacks raised profound legal questions with respect to nation-states' use of cyber mercenaries to conduct intelligence or military activities.

The 2008 attacks on Georgian systems that were interspersed with kinetic attacks during the Russia-Georgia conflict over South Ossetia were a more obvious example of cyber warfare that demonstrated the degree to which governments are dependent upon computers and communications networks, especially during crisis management. A sequence of distributed denial-of-service (DDOS) attacks against Georgian government Web sites essentially shut down government communications. The Georgian government quickly obtained assistance from other countries and companies. Estonia sent cybersecurity experts to Georgia and took over the hosting of the Web site of the Georgian Ministry of Foreign Affairs. The Polish government made space on its Web site for Georgian updates on its conflict with Russia,[17] and U.S. companies, such as Google and Tulip Systems, helped the Georgian government move some of its Web content to the United States, where it would be protected.[18]

While the Estonia attacks raised questions whether the cyber attacks could trigger NATO's Article V protections of collective defense, the Georgian attacks raised issues regarding other aspects of international law. Stephen Korns and Joshua Kastenberg analyzed the assistance provided to Georgia and pondered whether Georgia violated the United States' right of neutrality under the

9 David J. Smith, "Cyber-war!" *24 Saati*, Tblisi, Sept. 25, 2007, http://www.potomacinstitute.org/media/mediaclips/2007/Smith_24Hours_092507.pdf.

10 Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, May 19, 2007, p. 1, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

11 Landler and Markoff, "Digital Fears Emerge."

12 Finn, "Cyber Assaults on Estonia," p. A14.

13 Demetri Sevastopulo, "China 'hacked' into Pentagon defence system," *Financial Times*, Sept. 6, 2007, p. 1.

14 Demetri Sevastopulo, "Real security fear over virtual invasions," *Financial Times*, Sept. 4, 2007, p. 2.

15 "China's cyber-spies spread their net," *Financial Times*, Sept. 4, 2007, p. 12; Andrew Ward and Demetri Sevastopulo, "US concedes danger of cyber-attack," *Financial Times*, Sept. 6, 2007, p. 3.

16 Rhys Blakely, "MI5 alert on China's cyberspace spy threat," *Times Online*, Dec. 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece.

17 Jeremy Kirk, "Estonia, Poland Help Georgia Fight Cyber Attacks," *PCWorld*, Aug. 12, 2008, http://www.pcworld.com/businesscenter/article/149700/estonia_poland_help_georgia_fight_cyber_attacks.html.

18 Thomas Claburn, "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google and Elsewhere," *InformationWeek*, Aug. 12, 2008, http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702.

Hague Convention when it took the "unorthodox step of seeking cyber refuge" in the United States without first seeking the permission of the U.S. government. The chief executive officer of Tulip Systems, a Georgian who happened to be visiting Georgia at the time of the attacks, called the Georgian government and volunteered Tulip's services. Korns and Kastenberg note:

> During a cyber conflict, the unregulated actions of third-party actors have the potential of unintentionally impacting U.S. cyber policy, including U.S. cyber neutrality. There is little, if any, modern legal precedent.[19]

The Estonia and Georgia cyber attacks serve as sterling examples of the chaos surrounding cyber attacks and the uncertainty of the legal frameworks that govern actions taken during such events. Theory gives way to reality in the chaos that follows such crises: neither NATO nor the countries that came to the assistance of Estonia had clear legal authority to engage in defensive measures to aid Estonia. *The Estonian and Georgian attacks highlight the need to revise the doctrines and laws that traditionally support diplomatic, policy, and military decisions to accommodate new cyber threats and asymmetrical challenges that often link national and economic security.*

More recent cyber attacks highlight the interconnected nature of cyber vulnerabilities and accentuate the need for multilateral dialogue aimed at defining an agreed-upon level of geo-cyber stability. Researchers at the Centre for International Studies, at the University of Toronto's Munk School for Global Affairs, conducted a ten-month investigation into allegations of Chinese computer network attacks on the Tibetan community. The Information Warfare Monitor's March 2009 report on this investigation, Tracking GhostNet, indicated that the researchers uncovered a network of 1,295 infected computers in 103 countries that were controlled from commercial Internet access accounts in China. According to the report, the GhostNet system commanded computers to download malware that enabled the attackers to "gain complete, real-time control" that included "searching and downloading specific files, and covertly operating attached devices, including microphones and Web cameras."[20] The report noted:

> Significantly, close to 30% of the infected computers can be considered high-value and include ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.[21]

In early 2009, cyber researchers from three hundred organizations and 110 countries joined together to fight the Conficker worm, which had infected at least five million systems in 211 countries. Conficker is contained for the moment, but not eradicated. The threat looms that those behind the worm could break through and take control of these systems. SRI International reported that Conficker first appeared in September 2008, and Chinese hackers were the first to market it, for thirty-eight U.S. dollars.[22] According to Rick Wesson, CEO of Support Intelligence and one of the researchers deeply involved in this effort to contain Conficker, the sophistication of this worm is unprecedented and targets the infrastructure of the Internet. In part, Conficker has relied upon the inability of infected parties to collaborate—one of the gravest weaknesses in the international legal framework, yet one of the easiest to fix through international agreements.

As recently as July 2009, at least thirty-five government and commercial Web sites in South Korea and the United States, including the NASDAQ and the New York Stock Exchange, suffered denial-of-service attacks. South Korean intelligence officials have unofficially blamed North Korea. Former U.S. officials have publicly named

19 Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008–2009, U.S. Army War College, 2008, p. 61, http://www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf.

20 *Tracking GhostNet: Investigating a Cyber Espionage Network*, Information Warfare Monitor, March 29, 2009, at 5, http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/.

21 Ibid.

22 Phillip Porras, Hassen Saidi, and Vinod Yegneswaran, "An Analysis of Conficker's Logic and Rendezvous Points," Feb. 4, 2009 (updated March 19, 2009), SRI Int'l, http://mtc.sri.com/Conficker/index.html#ref-5, citing Haowei Ren and Geok Meng Ong, "Exploit MS-08-067 Bundled in Commercial Malware Kit," Nov. 14, 2008, http://www.avertlabs.com/research/blog/index.php/2008/11/14/exploit-ms08-067-bundled-in-commercial-malware-kit/.

Iran and North Korea among nations perfecting cyber warfare capabilities.

These examples are only the beginning of the list of countries focusing on cyber warfare. As early as 1996, U.S. government officials estimated that more than 120 countries either had or were developing computer attack capabilities that could enable them to take over the Department of Defense's information systems and "seriously degrade the nation's ability to deploy and sustain military forces."[23] Considering that the entire planet is now wired, the number of countries with such capabilities is likely higher.

The political and economic shifts caused by the Internet and globalization have introduced considerations that impact the more fundamental approaches to national security based on geopolitical interests, spheres of influence, and correlation of forces. Foreign policy is far more complex in an interconnected world where cyberspace knows no borders, packets hop from country to country, and laws governing collective assistance and armed conflict were intended for traditional warfare, not cyber conflict. Although geopolitical considerations still must be afforded great weight, threats to critical infrastructure must be evaluated in a broader policy paradigm that is based on maintaining global cyber stability.

Countries certainly need to be able to protect their infrastructure, systems, and information from intrusion, attack, espionage, sabotage, unauthorized access or disclosure, or other forms of negative or criminal activity that could undermine national and economic security. They also, however, need some certainty regarding everyday operations and a legal framework upon which to rely when making decisions about national and economic security. Such a framework is lacking in the cyber realm.

Today, all countries need the certainty of a minimum level of cyber stability that is assured through international agreements. At its core, this minimum level of cyber stability means that a country's critical infrastructure shall not be disrupted in a manner inconsistent with the laws of armed conflict and other applicable treaties and conventions, such as the Hague, which requires nations at war to respect the neutrality of other nations, and the Geneva Convention.

23 *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* U.S. Government Accountability Office, GAO/AIMD-96-84, May 22, 1996, http://www.fas.org/irp/gao/aim96084.htm.

Legal and Policy Issues

The laws of armed conflict regulate the conduct of armed hostilities and are intended to prevent unnecessary suffering and destruction. They also protect civilians, prisoners, and the wounded, sick, and shipwrecked. Under the laws of armed conflict, combat forces can engage in only those actions necessary to achieve legitimate military objectives (the principle of necessity), and they must distinguish between lawful and unlawful targets, such as civilians, civilian property, and the wounded and sick (the principle of distinction). The amount of force cannot exceed that needed to accomplish military objectives (the principle of proportionality). Lawful combatants are those authorized by the government to engage in military actions, and they must bear distinctive emblems and be recognizable at a distance. Unlawful combatants are those who participate in hostilities without authorization by government authority or under international law.

In a cyber context, the first obvious issue is: what constitutes an act of cyber warfare? Other issues concern the attack of communication systems and other critical infrastructures owned by the private sector that support civilian life, including hospitals and treatment for the sick, wounded, elderly, and very young. Should these and the systems of targets protected by the Geneva Convention be off-limits? Are attacks on these systems really necessary to achieve military objectives? Is the damage to the networks proportional to the military objective? When an attack occurs, no one knows who is attacking until it can be tracked and attribution can be determined. Legitimate cyber soldiers are indistinguishable from young hackers seeking ego gratification (often known as script kiddies) or any rogue actor on the Internet. How does one determine whether attackers are military combatants? What international cooperation is required? Likewise, how is it to be known if third parties are acting at the behest of a nation-state? They certainly do not have distinctive emblems, nor are they recognizable from a distance. Do cyber soldiers and engaged third parties need to wear cyber uniforms or have recognizable characteristics? What is excessive force in cyberspace?

These and numerous other legal and policy questions arise in the context of cyber warfare. The two principal legal instruments that would govern nation-state action in a conflict situation are the NATO Treaty and the United Nations (U.N.) Charter. Each document is more than fifty years old and their provisions do not accommodate cyber scenarios. They both use similar language and are equally

ambiguous regarding cyber attacks. The NATO Treaty uses terms such as "armed attack," "territorial integrity and political independence," and "territory, forces, vessels, and aircraft." The terms "self-help," "mutual assistance," and "collective assistance" are used only in the context of an "armed attack."

Estonian Defense Minister Jaak Aaviksoo pinpointed the gaps in the NATO Treaty with respect to cyber attacks, stating:

> At present, NATO does not define cyber attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country. Not a single NATO defense minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future.[24]

Article XII of the NATO Treaty allows for consultation of NATO members for the purpose of reviewing the treaty with respect to "factors then affecting peace and security." Thus, this article could be used as the mechanism by which cyber attacks, collective defense, and geo-cyber security are considered by NATO nations.

The U.N. Charter, applicable to its 192 member countries, serves as the foundation in international laws for state conduct, including armed conflict. The language in the charter is closely aligned with that in the NATO Treaty, using terms such as "territorial integrity and political independence," "the use of armed force," "action by air, sea, or land forces," and "armed attack." The self-defense provisions confuse more than clarify. Article 51 states that nothing shall block a nation or group of nations from engaging in collective self-defense if an armed attack occurs, raising the question of whether a cyber attack could be deemed to be an "armed attack." Article 41 cuts against the interpretation that a cyber attack is an armed attack, however, because it specifically lists the partial or complete interruption of communications as a measure "not involving the use of armed force" that is an allowable means of enforcing Security Council decisions.

Quite simply, the U.N. Charter and the NATO Treaty do not accommodate the electronic capabilities of the twenty-first century. The need to update these legal instruments to govern the actions of nation-states with respect to cyber warfare and attack capabilities has never been more urgent. The rule of law is already in a precarious state due to disruptions caused by terrorist activities. The ominous threat of cyber attacks by nation-states and rogue actors has become a reality, and this issue can no longer be ignored by nation-states that find it more desirable to war-war than to jaw-jaw. Governments, the private sector, and multinational organizations must begin an international dialogue in this area to accommodate new military capabilities, collective action, and geo-cyber considerations.

If left unattended, by 2015, cyber instability will pose a significant threat to the national and economic security interests of all countries. The Estonian attacks prompted a prediction by Christopher Rhoads of the Wall Street Journal that the attacks "will likely shape a debate inside many governments over how such attacks should be considered in the context of international law and what sort of response is appropriate."[25]

Although some actions have been taken, they fall woefully short of assuring any sort of geo-cyber stability. Following Estonia, NATO adopted a Cyber Defence Policy in 2008. According to the Bucharest Summit Declaration, the policy "emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities: share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack." NATO's Cyber Defence Policy does not address collective defense under Article V.[26] NATO's newly established Cyber Defence Management Authority coordinates cyber defense among NATO allies. In addition, seven NATO members (Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain) and the NATO Allied Command Transformation have established a Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. The steps taken by NATO are positive and make an important contribution to cyber stability, but they do not help define what level of cyber stability is sacrosanct and how cyber actions would fit within the NATO framework.

---

24 Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *Guardian*, May 17, 2007, http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

25 Christopher Rhoads, "Estonia Gauges Best Response to Cyber Attack," *Wall Street Journal*, May 18, 2007, p. A6.

26 Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on April 3, 2008, para. 47, http://www.nato.int/docu/pr/2008/p08-049e.html.

Where to Begin

Countries need to begin the dialogue on global cyber stability by addressing international cooperation. Such cooperation is almost always needed in tracking and tracing cyber communications simply due to the interconnected nature of the Internet and the manner in which the Internet Protocol breaks a communication into packets and routes those across many networks—and countries—before reassembling them at their destination point. The previous examples also highlight the need for assistance from other nation-states in defending against cyber attacks. The Council of Europe (CoE) Convention on Cybercrime, which contains excellent provisions regarding mutual cooperation and assistance, was originally believed to be the best vehicle for reaching such agreement. However, since it opened for signature in 2001, it only has been signed by forty-six countries and ratified by twenty-nine.[27] Considering there are 246 countries and territories connected to the Internet, the CoE Convention hardly appears to be the answer.

The U.N. clearly needs to take the lead in working toward an international agreement on cooperation and containment of cyber conflict. A 2005 report of the United Nations' International Telecommunication Union (ITU) noted:

> Attacks that do breach the confidentiality, integrity, or availability of information systems could in theory be treated as acts of war and be brought within the scope of arms control or the laws of armed conflict. In this approach, existing mechanisms and methods such as the Laws of Armed Conflict and arms control/verification regimes could be applied to this new "weapon system."[28]

Although the United States invented the Internet, it is unlikely that it will step up to take a leading role in any such effort. The United States has openly criticized the ITU for addressing cyber crime in its Global Cybersecurity Agenda and has refused to support the ITU Toolkit for Cybercrime Legislation, which contains sample language for cyber crime laws and provisions for mutual cooperation and assistance (consistent with the CoE Convention). U.S. opposition to U.N. activity in the cyber realm has gone on for more than a decade, with representatives from the U.S. Departments of State and Justice pushing the CoE Convention and claiming that defensive action and cyber crime laws are the solution.

Ironically, Russia—one of the most active countries engaging in cyber warfare—has shown the greatest leadership in this area. Since 1998, Russia has introduced an annual U.N. resolution concerning "developments in the field of information and telecommunications in the context of international security" calling for multilateral consideration of threats emerging in the field of cybersecurity, the definition of basic notions related to the unauthorized interference of information and telecommunication systems, and consideration of international principles to help combat cyber crime and terrorism. The 1999 resolution included the military potential of ICTs. These resolutions have regularly been adopted by the U.N. General Assembly, and the United States has regularly voted against them. Russia's 2008 resolution was adopted by both the U.N.'s First Committee and the General Assembly—over the sole objection of the United States.[29] In a recent turnabout, the United States reportedly has reached agreement with Russia on the resolution and is prepared to support it in the First Committee and General Assembly votes.

Conclusion

The international community must come together and realize that the enormous benefits of the Internet will be lost if it is used as an instrument of harm outside the rule of law. Governments have an obligation to help protect the Internet and systems that support their economies, enrich the lives of their citizens, and support government and military operations. They also have an obligation to assist in tracking and tracing cyber crime activities. A legal framework applicable to cyber conflict that assures a minimum level of geo-cyber stability must be developed, lest the Wild Wild Web become the twenty-first-century

27 Convention on Cybercrime, CETS No. 185, Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

28 *A Comparative Analysis of Cybersecurity Initiatives Worldwide,* International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Document: CYB/05, June 10, 2005 at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

29 *Disarmament Diplomacy*, 2008 First Committee Resolutions: Other Disarmament Measures and International Security, 63/37 (L.45) "Developments in the field of information and telecommunications in the context of international security," http://www.acronym.org.uk/dd/dd89/89unodis.htm.

tool of destruction and impede the rule of law regarding armed conflict, human rights, and friendly relations among nation-states.

Cyber Repression: Framing the Problem, Assessing the State of Debate, and Thinking of Counter-Strategies

By Henning Wegener

Since time immemorial, free expression of opinion and free access to information have been key elements in building civilized societies. They are an essential part of human rights and civil liberties, and are consequently anchored in almost all modern democratic constitutions: in the famous Fifth Amendment of the U.S. Constitution, Article 5 of the German Basic Law, or Article 20 of the post-Franco Spanish Constitution, for example. Indeed, the freedom of the individual to hold and communicate opinions could serve as a yardstick of human progress. And the definition of the limits this principal freedom must undergo for reasons of public security, decency, and ordre public are an equally vital and necessary element of internal political debate, a fertile, never-ending effort, a struggle for balance between individual liberty and the public interest.

In the Internet age, this basic constellation of principles has not changed, but the form it takes indeed has. Digital technologies have catapulted the opportunities for access to information and communication into a new dimension. As in every other aspect, the Internet enlarges amplitudes and favors extremes, changes traditional measures of quantity and quality, negates distance and time, and, as all new technologies do, creates ambivalences. The issue of freedom of opinion and information as a human right must be considered afresh. As has rightly been stated before, "the Internet is the new front in the struggle for human rights and freedom of opinion."

While the Internet exponentially increases information and its free availability, it also increases the potential to intervene in the underlying technical processes and manipulate that information. Digital technology allows for filtering software that can block any area of information, allowing governments to introduce state censorship on a massive scale. The number of industrial suppliers of such filter techniques is legion. They include not only most of the grand names of information technology, but also specialized companies. There are several Web pages dedicated to comparatively evaluating and rating the efficiency of such software, while other pages, operated by advocates of total freedom of expression on the Internet, criticize the emergence of this technology.

Yet one must not overlook that filtering also serves an important societal protection function. Blocking pages of child pornography, incitement to violence, racial hatred, and crime in general would appear legitimate to anyone, and the same holds true for the increasing utilization of the Internet by national and international terrorism. Content that may not be disseminated legally outside the Internet needs to be susceptible to legal sanctions and interdiction also within the Internet. The fact that current filters, like search engines generally, react only mechanically to certain words or phrases and often overshoot their target ("overblocking") is a mere technical aspect. More important are the possibilities of avoiding, circumventing, or damaging the filters. Regardless of the efficiency of Internet filters and their censorship effect, "free" societies, mainly of the so-called West, with their high degree of consensus on values, restrictions on freedom of expression and access to information, are clearly regulated by law. Thus, the scope of such filtering is governed by rules of adequacy and proportionality, and it can be evaluated in transparent and publicly available legal review procedures.[30]

Given the borderless nature of the Internet, national legislation is not sufficient to protect freedom of expression. The European Union has therefore put in place since 1999 a comprehensive regime to regulate legitimate inroads to Internet contents and procedures. It relies mainly on self-regulation by the Internet industry and search engines to exclude illegal or damaging content and to ensure conformity with national legislation. This self-regulation functions satisfactorily, even though complementary legislation may occasionally be required.

Globally speaking, legal standards are set in particular by the two great human rights resolutions from the early years of the United Nations—the Universal Declaration of

30 It is worth noting that many countries with an impeccable democratic record have ordained, on *ordre public* grounds, a very sweeping, if "selective" blocking of Internet contents, not least as part of their antiterrorism campaigns. This leads to vivid domestic debates and revolt by the advocates of a free Internet. The crucial criteria is the availability of an independent review procedure.

Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966. Practically all nations have joined these pacts, which are now considered international customary law. By coincidence, the principle of freedom of expression and opinion is recognized in Article 19 of both documents, as is the right of anybody to receive and impart information of all types, regardless of frontiers and through any chosen medium. There is no doubt that this principle also includes the reception of information through the Internet. Thus the World Summit on the Information Society (WSIS) has solemnly confirmed these principles as central to and an indispensable pillar of the information society, specifically in the Geneva Declaration of Principles (principles 4, 5, and 55). It is worth noting that the WSIS text emphasizes the liberty aspect, deemphasizing the caveats added in the International Covenant.

What in "free" societies boils down to a problem of an admittedly difficult, permanent political balance between freedom and state intervention under clear legal criteria, becomes in many other states a problem of human rights and the extension of a global information order. Internet censorship by governments via filter technologies without legal constraints, and with grave consequences for the individual seeking and imparting information, becomes a growing human rights problem. An aggravating component of this development is that Western technology companies not only provide their filtering technology to censorship-prone governments but also collaborate willingly in their use, thus establishing effective censorship systems and facilitating prosecution and punishment. This phenomenon is a particular concern of this article, which also aims at suggesting possibilities of international action against such practices that are damaging from a human rights perspective.

This article is written at a time of growth, both in the number of governments that practice Internet censorship, mostly to the detriment of political rights and freedoms, and in the proficiency of filtering techniques. The list of states prone to these practices is long—at least twenty-five governments deprive their citizens of access to the full range of information available online. Most concentrate their intervention on banning political content—freedom, democracy, free elections, legal remedies—which their own system of government does not allow, but many go further. Some Arab and Muslim governments concentrate their restrictions in the area of moral themes based on their inherited moral and cultural order. The intensity and thoroughness of control varies. There are some Arab countries where the censor blocks certain pages, but redirects users to an explanatory page, providing access only if special "legitimate" interest in the information is shown, thus affording at least some degree of transparency. In other countries, censorship is practiced sporadically and ineffectively, with no sanctions in case of a breach of government filters.

The rule, however, is that government censorship is exercised without limits and over a broad segment of human knowledge, without any explanation of the underlying rationale. In most public comments, China, with more than 300 million Internet users, and Iran, which possesses a filtering infrastructure of high sophistication, are cited as prime examples of government censorship. Other countries with active censorship policies include Cuba, North Korea, Myanmar, Zimbabwe, Vietnam, countries formerly under communist influence, and some otherwise quite respectable countries like Tunisia or Egypt. The further away from Western-style democracy a country is, the higher the incidence of censorship through Internet filtering. There is no doubt that China pushes the indoctrination of its population through Internet censorship to particular extremes: Internet users caught accessing prohibited pages are subject to severe punishment and persecuted by an aggressive cyber police. Criminal punishment is also practiced elsewhere. Western companies providing filtering software have to live with the accusation that they actively aid and abet such measures of prosecution, and thus contribute to the resulting human suffering.

The consequences of comprehensive censorship are grave and cannot be overestimated. Citizens are not only curtailed in their rights under international law, they are also cut off from important benefits of the information age. They receive a skewed view of world reality, and their ability to benefit from global communication processes is diminished. Massive cyber repression can alter the collective state of mind of a nation.

This state of affairs and the worsening record of Internet censorship urgently call for action. The European Union (EU) has recognized this and has taken action. It does not accept that repressive governments should be assisted by Western technology companies in solidifying their mental dictatorship. We also should praise the EU for coining the highly appropriate term "cyber repression" to define these practices.

The EU is not alone. The international Internet lobby, which commendably fights for the freedom of information and the integrity of the Internet worldwide, is active and vigilant. Especially in the United States, there are many prominent institutions that monitor cyber repression and denounce it publicly. An example is the OpenNet

Initiative,[31] in which major North American (and British) universities have pooled their knowledge and run an observatory for these repressive practices. Many international defenders of Internet freedom have gone so far as to provide citizens of censorship-prone countries with software to bypass government filters, helping them access censored sites and pages. These anti-filter technologies have developed into a veritable industry that helps diminish the effectiveness of government censorship, without being able to eliminate it entirely.

The result of this mesh between filters, circumvention software, and sophisticated measures of individuals to outwit government filters is a permanent battle between censorship and Internet freedom, fraught with risk for those who seek to escape censorship. One member of the OpenNet Initiative, the University of Toronto, has developed Psiphon, a system of particular effectiveness designed to allow Chinese users to jump the obligatory firewalls introduced by the government and to navigate freely in the global Internet.[32] However, the application of this device is being actively fought by filter providers like Cisco. This again demonstrates the need for many multinational industries to evaluate carefully the effects of their commercial policies on the freedom of expression and on the tenets of international law, an obligation that in many cases is not honored. Apart from Cisco, technology suppliers like Nortel, 3Com, Alcatel, Juniper Networks, Sun Microsystems, MSN, MySpace, Google, Yahoo, and Nokia-Siemens, to varying degrees, have to face the same criticism.[33]

Obviously one has to add that China, as a country advanced in digital technologies, is able to develop filters domestically, and is already doing so in great quantities. At present, the Chinese government is contemplating an obligation for all Internet users to work with "Green Dam," domestically supplied software that already includes Internet filters, imposing the insertion of these devices even on foreign computer suppliers.[34]

This is not the place for a detailed country-by-country analysis; the Internet provides ample information to that effect. But even the brief references here and the nascent public discussion raise questions about how the obvious need for action can be met, and what the international community can do to counteract cyber repression as a continued violation of international law.

The legal and political problems involved in defining the limits of internationally acceptable Internet filtering and possible sanctions are evident and they are huge. Questions of national jurisdiction and sovereignty, the near impossibility of developing broadly valid borderlines between civil liberties and overriding public interests, questions of choice of law and means of enforcement, and the larger issue of Internet governance, inter alia, render an attempt at international codification unfeasible and probably futile. As is often the case in international law, there are no rapidly effective sanctions. Any reform of global Internet filtering must thus be looked upon in terms of process and strategies over time. One should think in terms of procedures that raise the world's consciousness, generate public awareness and pressure, and—for the governments affected—a public-opinion challenge and a motive to provide detailed justifications for their actions.[35]

---

31 http://www.opennet.net. The project employs an international network of investigators to determine the extent and nature of government-run Internet filtering programs. Participating academic institutions include the Centre for International Studies at the University of Toronto's Munk School of Global Affairs, the Berkman Center for Internet & Society at Harvard Law School, the Oxford Internet Institute at the University of Oxford, and the SecDev Group, which took over from the Advanced Network Research Group at the University of Cambridge's Cambridge Security Programme.

32 Psiphon is "a censorship circumvention solution that allows users to access blocked web pages in countries where the Internet is censored. Psiphon allows a regular home computer to act as a personal, encrypted proxy server that allows the administrator to specify a username and password that is, in turn, given to someone in a country where Internet censorship is prevalent so that users in that country will be able to browse the Internet in a secure, uncensored manner." In Iran, anti-censorship activists grouped around the Global Internet Freedom Consortium, which closely cooperates with the Falon Gong sect, apply similarly effective systems.

33 This list has been taken from the current literature, and the companies have not been individually verified. In the meantime, Google has at least partially rectified its policies. In January 2010, following Chinese attacks on its corporate infrastructure, the company decided to stop censorship on its Chinese-language Google.cn site, and thereafter shut down its filter services, redirecting traffic to Google.com.hk, its unfiltered site hosted in the Hong Kong SAR. Google had already avoided operating its search engine in Vietnam to avoid a censorship regime as strict as China's. Nokia-Siemens is suspected to have equipped Iran with effective "Deep Packet Inspection" technology, although this has been denied, if somewhat halfheartedly.

34 After pervasive public criticism from abroad and resistance from within, the plans for obligatory installation of the software were put on hold. However, at the same time, China's authorities are setting the groundwork for the forced inclusion of filter software in cellular phones.

35 This procedural approach was first suggested by the World Federation of Scientists in *Information Security in the Context of the Digital Divide.* Recommendations submitted to the World Summit on the Information Society at its Tunis phase (November 16–18, 2005), Doc. WSI05/TUNIS/CONTR/01-E, Sept 2, 2005.

An important responsibility lies with national governments, industry, and the institutions of civil society with their ability to influence public opinion. Governments can promote—as the U.S. government has been doing in an exemplary way[36]—the development and availability of anti-filter technologies. They can subject the export of filter technologies to appropriate export controls and use diplomatic means to pressure censoring governments, in the interest of transparency, to lay open and justify their restrictive policies.

The information technology industry, including software producers, Internet service providers, and their associations, bears obvious responsibilities and should thus proceed to adopt a code of conduct that excludes the use of their technologies for political censorship. This self-regulation policy, providing clear common standards, has produced good results in the EU and can strengthen the power of individual companies to withstand pressure from censorship-prone governments eager to do business with them. But this moral responsibility pertains also to the private sector as a whole. Companies should react to the infringement of Internet freedom in their international business transactions.[37]

Academic institutions and human rights organizations such as the OpenNet Initiative, the Yale Center for the Study of Globalization, Amnesty International, and Reporters Without Borders tirelessly denounce cyber repression. Such organizations should be encouraged and supported by well-meaning governments. In this vein, some governments, such as that of the United States, provide funds to groups that aid users in censorship-prone countries with circumvention techniques to enable the largest possible numbers of citizens to access the Internet safely.

But given the trans-frontier and international nature of the Internet, and the global human rights relevance of cyber repression, the most important task may be to put the issue in a major new way on the agenda of international organizations.

A first step could be to reach in these bodies a broader international understanding of the development and technical underpinning of current Internet filtering, and to create an international monitoring mechanism.

As a second step, one might consider the introduction of an international complaint procedure, broadly accessible to all concerned and following a number of summary reporting standards.

Which international fora could be put to the service of this struggle?

In the first place, one could consider the Internet Governance Forum (IGF), created in 2006 pursuant to decisions by the WSIS's so-called Tunis Agenda. The restrictions that Internet political censorship places on the functioning and management of the Internet are of obvious relevance to the assignment of the forum, and could easily be subsumed under its mandate (article 72, sections a, b, e, and k of the Tunis Agenda), even though the problem of cyber repression is not specifically mentioned in these texts. Regretfully, the IGF, in its four years of existence, has limited itself to admittedly rich and meaningful discussions on topics such as the freedom of the Internet, but operational activities have not been initiated. The establishment of a monitoring procedure where filter practices could be followed, analyzed, and critically evaluated would be possible and desirable under the terms of reference of the forum. UNESCO proudly proclaims itself, under its founding act, the unique international guardian of freedom of information, and has received from the WSIS clear tasks under the headings "Access to Information and Knowledge" and "Ethical Dimension of the Internet." Nothing would be more logical than, as a means of fulfilling these tasks, to initiate a dialogue, and then, as an outcome, to periodically examine censorship practices.

As we are dealing with human rights and the two basic international covenants that define states' obligations to protect them, the principal venue for international action should be the human rights organizations within the United Nations: the Human Rights Council (HRC), established in 2006 as the special body dealing with violations of the International Covenant on Civil and Political Rights. The HRC, with its broad mandate, would be entitled to put in place a formal complaint procedure available to all U.N. member governments. One possibility would also be to insert the topic of Internet freedom and censorship in the Universal Periodic Review process, where countries' human rights records are peer-reviewed.

Whatever procedural form is chosen, the collective highlighting of human rights abuses in this sphere could generate welcome pressure on governments suspected of illegality, requiring them to provide arguments justifying

36 There have been congressional initiatives leading to comprehensive draft legislation, and the U.S. government is firmly committed "to devoting the diplomatic, economic and technological resources necessary" to advance Internet freedom. The State Department operates a Global Internet Freedom Task Force, which it plans to reinvigorate. See the important speech of Secretary of State Hillary Clinton of January 21, 2010, at www.foreignpolicy.com/articles/2010/01/21/Internet_freedom.

37 The Global Network Initiative, a voluntary effort by U.S. technological companies, thus reacts to government requests for censorship and promotes Internet freedom. Secretary Clinton: "Censorship should not be in any way accepted by any company from anywhere".

their actions. Within the complaint procedure, the dubious role of the international IT industry in allowing cyber repression could also be adequately illuminated. As in the HRC, the periodic country reviews in the U.N. Human Rights Committee could also include Internet freedom. However deficient such procedural devices, they could, over time and with adequate perseverance by freedom-oriented governments, create a highly visible comply-or-explain regime, resulting in public pressure and public opprobrium, thus paving the way for more global awareness of the problem and for an eventual streamlining of behavior in the digital world.

Cyber War or Cyber Terrorism: The Attack on Estonia

By William A. Barletta

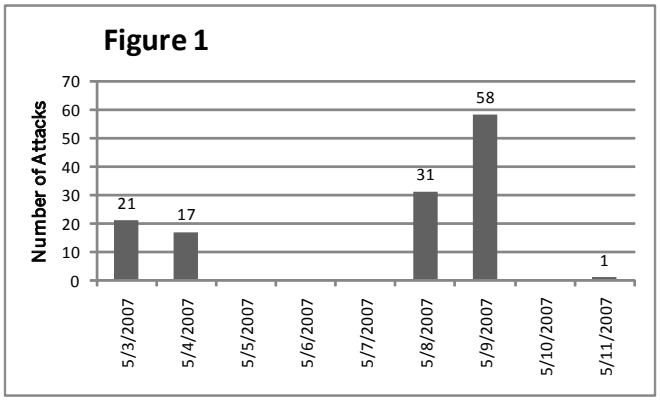
Abstract: This paper reviews the vulnerabilities of information societies to deliberate, sustained cyber attacks at a level which—if conducted in physical space by a nation-state—would likely be called armed aggression. The attack on Estonia in the spring of 2007 offers a sobering example of the nature of cyber aggression and the uncertainties and ambivalence in the international community, especially the United States, on how to respond to such attacks.

Introduction

The information age, especially in the manifestation of e-government, promises to enhance national prosperity, influence, and power. At the same time, the information society presents a tempting target to miscreants, be they criminals, subnational terrorist groups, or hostile nation-states. I analyzed the structural basis of the vulnerability of information societies in "Evolving Face of Cyber-conflict and Information Warfare."[38] As discussed in that report, "the concepts of deterrence developed during the Cold War may have little value. . . . In the intermediate case of cyber-terrorism . . . the model of deterrence at the level of civil and criminal penalties [also] fails." The attack[39] on the national information infrastructure of Estonia[40] in April 2007 clearly demonstrates both the predicted vulnerability of an e-government and the limited ability to deter an attacker.

Chronology

On April 27, data floods began on Estonia's computer network, coinciding with two nights of violent demonstrations to protest the Estonian government's decision to relocate the "Bronze Soldier," a Soviet-era memorial to an unknown World War II Russian soldier. Estonia had previously discussed moving the memorial with the Russian government, which not only denounced the relocation, but also warned of dire consequences if the plan was carried out. "In the days that followed," the New York Times reported, "Russia suspended rail service, ostensibly for track repairs, while protesters in Moscow staged raucous demonstrations, harassing Estonia's ambassador in one instance."[41]



In Estonia, violent riots following the movement of the monument were accompanied by widespread vandalism in the center of Tallinn, leaving one dead, forty injured, and more than three hundred arrested. The Web sites under attack in the initial wave included those of Parliament, the president, the prime minister, and major political parties.

38 W. A. Barletta, "Evolving Face of Cyber-conflict and Information Warfare," Proceedings of the 36th International Seminars on Planetary Emergencies, Erice, Sicily, 2006, World Scientific, 2007.

39 The attack has been widely reported in the international press. For example, see Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *Guardian*, May 17, 2007.

40 Estonia has made a concerted commitment of e-government to such an extent that it is sometimes called e-Stonia.

41 Steven Lee Myers, "Estonia Computers Blitzed, Possibly by the Russians," *New York Times*, May 19, 2007.

The initial attacks included denials of service and Web site defacement.[42] From the outset, the highly visible nature of the attacks strongly suggests that the data floods were intended to cripple Estonia's online public administration and to erode public confidence in the government and its institutions.

By April 30, additional government sites were hit, and the attacks spread to several daily newspapers. In response the Estonian government began blocking all traffic from .ru domains.[43] By the next day, attackers directly targeted Estonian Internet service providers (ISPs). The government convened emergency meetings of computer experts from the Estonia Computer Emergency Response Team (CERT), ISPs, banks, and several government agencies, including law enforcement agencies.

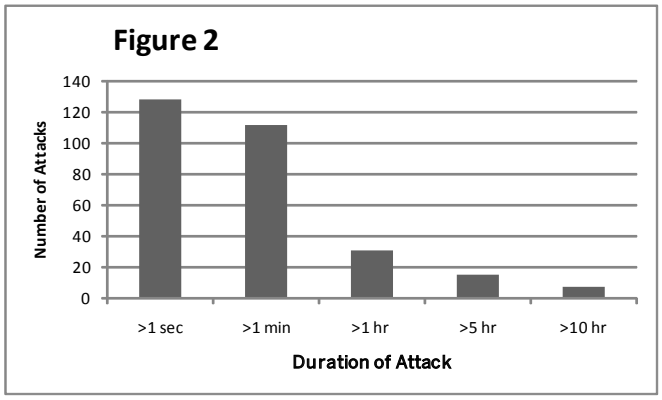
Plans were set in motion, anticipating a wave of attacks on financial services such as online banking. Within a few days, "private sector banking and online media were also heavily targeted and the attacks affected the functioning of the rest of the network infrastructure in Estonia."[44] During the period from May 2 to 5, the countermeasures, undertaken with the cooperation of ISPs worldwide, were to expand blocking of traffic from specified groups of IP addresses and to wall off the banking system from all international traffic.

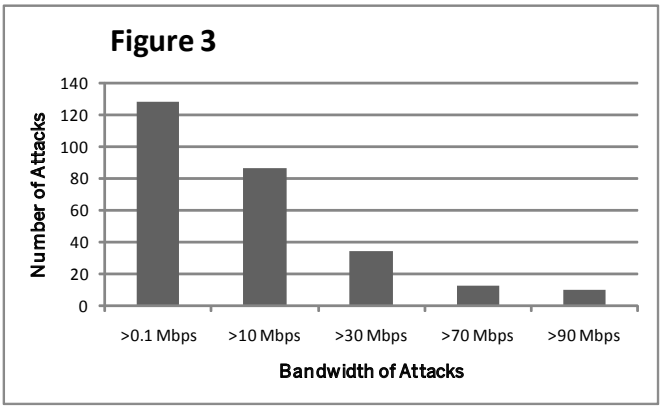
Estonia's government accused Russia of organizing the attacks and began its preparations to defend against another anticipated cyber attack to coincide with Russian Victory Day on May 9. As displayed in the first figure,[45] that same period (from May 5 to 7) saw a lull in the cyber attacks, as recorded by Arbor Networks' ATLAS system.[46] As was anticipated, Victory Day saw a sharp increase in the number of individual attacks. The last major attack was on May 18.

Following the Victory Day attack, Estonia's Public Prosecutor's Office formally requested legal assistance from the Office of the Russian Prosecutor General, asking for help finding the perpetrators of the attacks, who may have been living in Russia. "In its reply," according to Baltic Business News, "the Office of the Russian Prosecutor-General refused to comply with the Estonian request. . . . The request for legal assistance was sent in accordance with the Estonian-Russian legal assistance and legal relations treaty."[47] The request was officially turned down on the grounds that the treaty did not cover such incidents.

Modality

The attacks on Estonia began with simple uncoordinated pinging of sites and Web site defacement. It is likely that many of these attacks were launched by individuals using malicious scripts from Russian-language chat rooms to target Estonian Web sites. By early May, the attacks had changed to distributed denial-of-service attacks by botnet swarms. From May 3 to 10, the ATLAS system recorded 128 unique attacks, several of which lasted more than ten hours (figure 2). The attacks ceased on May 18; no physical casualties have been directly attributed to the attacks.





42 Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, May 19, 2007.

43 Ibid.

44 "ENISA commenting on massive cyber attacks in Estonia," ENISA press release, May 24, 2007, http://www.enisa.europa.eu.

45 Data for all figures are taken from Jose Nazario, "Estonian DDoS Attacks—A summary to date," http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

46 http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=9.

47 *Baltic Business News*, July 20, 2007, www.balticbusinessnews.com/newsletter/070720_bbn_newsletter.pdf.

The intermittent but persistent attacks were frequently of large bandwidth, as illustrated in figure 3, with the largest ten attacks measured at 90 Mbps, lasting approximately ten hours. The attacks were at minimum a clear indication of an ability to inflict serious damage on or disruption to Estonian society.

The Estonian government claimed that several Russian government IP addresses were involved in the attack, including "an Internet address . . . [of] an official who works in the administration of Russia's president."[48] But Russia has denied any involvement in the attacks. While some attacking IP sites were in Russia, other sites were spread widely across the globe. "The attackers used a giant network of bots—perhaps as many as one million computers in places as far away as the United States and Vietnam—to amplify the impact of their assault. In a sign of their financial resources, there is evidence that they rented time on other so-called botnets."[49] In none of the reports of the incident is there any suggestion that the attacks were launched or coordinated by dissident elements from within Estonia.

National Security Implications

The connectivity of e-government and information infrastructure that has imparted many benefits to Estonian society has also expanded its vulnerability to a new form of concerted asymmetric attack on critical information systems. The mode of attack is what a RAND Corporation study has labeled "netwar,"[50] an intermediate level of networked attacks on a society via its information networks. The attacks appeared to employ asymmetric swarming tactics executed by multiple groups with no absolute master controller as in normal botnets. In the netwar paradigm, any machine can be the controller.

The aims of netwar attacks may range from cyber warfare[51] to cyber terrorism to cyber criminality and hooliganism. However, even in the most extreme cases, neither the European Union nor the United Nations Charter recognizes cyber attacks as "armed attack" or "armed aggression."

Many experts have claimed that the technical sophistication of the attack exceeded that of previous known incidents. While some go so far as to say that the knowledge or collusion of a national entity was required, several U.S. experts have pooh-poohed such speculation. One should, however, note that the Estonian episode was not accompanied by political or monetary demands or by manifestos from the putative leaders of the attack,[52] making mere criminality unlikely. In contrast, the events showed a suspicious correlation with multiple political events and were conducted at a level that constituted a convincing show of force and intent. This is not to say that the Russian government was behind the episode. Indeed, a third party could have staged events to exploit existing tensions between the two countries. Organized, transnational Internet crime rings are acquiring sufficient resources to make disruption-for-hire a possibility, giving nations and subnational groups ample plausible deniability. That fact alone should give pause to supporters of anonymity on the Internet.

Overall, Estonia mounted a credible defense with the assistance and cooperation of private-sector computer-security experts and ISPs in Europe, the United States, and Israel. The attacks appear to have failed in permanently damaging the national information infrastructure of the country. Direct government-to-government support of Estonia's defense by other nation-states was, however, absent or at least has not been officially acknowledged. Without question, more massive and more sustained attacks are increasingly likely anywhere in the world.

48 Landler and Markoff, "Digital Fears Emerge."

49 Ibid. Such botnets-for-rent are most frequently used for spam distribution.

50 "Netwar is the lower-intensity, societal-level counterpart to our earlier, mostly military concept of cyberwar. Netwar has a dual nature . . . it is composed of conflicts waged, on the one hand, by terrorists, criminals, and ethno-nationalist extremists; and by civil-society activists on the other. What distinguishes netwar as a form of conflict is the networked organizational structure of its practitioners—with many groups actually being leaderless—and the suppleness in their ability to come together quickly in swarming attacks. The concepts of cyberwar and netwar encompass a new spectrum of conflict that is emerging in the wake of the information revolution." Summary in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, J. Arquilla and D. Ronfeldt, ed., National Defense Research Institute, RAND, 2001.

51 "[T]he status of information operations under Article 51 of the UN Charter, i.e. the definition of what constitutes a 'force' or 'armed attack' is as yet undetermined, and that the justification of the use of legitimate self-defense is, as a consequence, equally unclear . . . [N]ew, extended criteria for the definition of weapons and armed aggression should be sought. Cyber attacks on other states could then be considered acts of armed aggression under the UN Charter, and, applying the principles of proportionality and necessity, thresholds for responsive actions in self-defense could be defined, taking into account the direct as well as the indirect damage cyber attacks can cause." *Information Security in the Context of the Digital Divide*, Information Security Permanent Monitoring Panel (ISPMP) of the World Federation of Scientists, Document WSIS-05/TUNIS/CONTR/01-E, September 2005, p. 35, http://www.itu.int/wsis/documents/listing-all-en-s|2.asp.

52 By early June a leader of the pro-Putin Russian youth group, Nashi, had claimed credit for the attack; http://www.sbcc-chamber.com/index.php?lng=en&page_id=60&news_id=888. The veracity of the claim is unknown.

Miscreants in cyberspace are adept at hiding their tracks. The difficulties of tracking information packets through transmission networks and the technical security limitations of the present Internet Protocol version 4 make the job of cyber sleuths all the more challenging.

Until the full adoption of the next generation of Internet Protocol, version 6 (IPv6),[53] tracking the course of attacks will be far from complete enough to publicly justify state action. Under IPv6, with 128-bit addresses, every network device can be assigned a unique, static IP address. This difference will make tracking and tracing of communications[54] far easier, assuming that packet contents (or a part thereof) are stored for a limited but sufficient time.

To go beyond passive self-defense, states are likely to seek strong international support. On May 24, the European Parliament adopted a resolution[55] strongly condemning the siege of the Estonian embassy in Moscow, the cyber attack on Estonia, and the refusal of Russian authorities to cooperate with Estonia. The resolution further "regards attacks targeting one of the smallest EU Member States as a test case for the European Union's solidarity" and calls for "a study on how such attacks and threats can be addressed at EU level." Nonetheless, the European Parliament refrained from comment on the obvious conclusion that this attack was facilitated by anonymity[56] in cyberspace.

Internationally sanctioned actions[57] beyond statements of solidarity typically require a determination to appropriate evidentiary standards[58] of a) what is damaged or lost, b) who launched the attack, c) when and from where was the attack launched, and d) how was the attack accomplished. In the case of the cyber attack on Estonia, determination of from, where, and how is, at best, incomplete and ambiguous.

Conclusions: What Can Be Done

On a technological level, groups such as the Asymmetric Threats Contingency Alliance are advocating an international task force of counterattack experts to monitor extensive "surveillance and reconnaissance dashboards of digital systems . . . on a 24/7 basis." The Australian CERT has launched an Australian Internet Security Initiative (ISI), which includes the development of a botnet mitigation toolkit: databases of infected computers and work with major ISPs to shut them down. Operationally, such tools would require developing a "cyber-warfare paradigm shift" —a methodology and military doctrine of using swarming white-hat counterattack forces that could respond in kind to offensive swarming attacks. In this concept, reserves of experts would be brought into responsive action in a short period of time.

On the political side, "the grave potential of international cyber conflict calls for immediate attention. The dual-use nature of the technology precludes the kind of international control regime used to control nuclear technology. What one can hope for is the creation of transnational legal framework that lays down the rules and penalties for cyber conflict in a set of structured, internationally negotiated binding agreements. Such rules must specify the obligations of the signatory nations with respect to controlling nongovernmental organizations or networks that physically operate within their borders."

The sophisticated nature of modern communications technology demands equally sophisticated measures to maximize benefits and minimize dangers without imposing excessive drag on operational utility (e.g. data storage, system management, and human interface time). Such measures must engage technical, economic, and policy

53 Unfortunately, the adoption of IPv6 is significantly impeded by owners of information transmission networks that have sunk large investments into routers incompatible with IPv6 and that therefore have near-term economic interests often contrary to the long-tern benefit of their own enterprises. Absent legal and policy checks on perverse incentives, legal externalities can actually encourage, if not amplify, negative effects of information attacks. Where such perverse financial incentives exist, fiduciary responsibilities of managers legally require them to exploit such incentives for proximate gain of their enterprise rather than to search for approaches more consistent with broader community interests.

54 Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", p. 61, www.cert.org/archive/pdf/02sr009.pdf.

55 European Parliament resolution of May 24, 2007, on Estonia, P6_TA-PROV(2007)0215, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//EN&language=EN.

56 The Council of Europe Convention on Cybercrime recognizes a legitimate right to Internet anonymity. "In order to . . . enhance the free expression of information and ideas, member states should respect the will of users not to disclose their identity." Declaration on freedom of communication on the Internet (Strasbourg, 28.05.2003), adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies.

57 In the context of information warfare, such actions span prophylactic-defense measures against future attack to legal prosecution to diplomatic or even military measures.

58 Actionable information (evidence) must be sufficiently relevant, reliable, complete, accurate, and verifiable whether in a judicial or political sense. While there are now many national and international organizations devoted to developing standard procedures for the collection, retention, testing, and display of digital evidence, the legal framework of digital evidence is still evolving. In the United States, "there is debate about whether digital evidence falls under the Daubert guidelines as scientific evidence or the Federal Rules of Evidence as nonscientific technical testimony." Brian Carrier, "Open Source Digital Forensics Tools: The Legal Argument," September 2003, www.digital-evidence.org/papers/opensrc_legal.pdf.

expertise to clarify the offensive and defensive dynamics of computer security development as matter of return on investment. But above all, they must be coordinated across borders to clarify norms and expectations in cyberspace and eliminate the threat of a crippling cyber war.

Erice Declaration on Principles for Cyber Stability and Cyber Peace

The Erice Declaration on Principles for Cyber Stability and Cyber Peace was drafted by the Permanent Monitoring Panel on Information Security of the World Federation of Scientists (WFS), Geneva, and adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice (Sicily) on August 20, 2009.

It is an unprecedented triumph of science that mankind, through the use of modern information and communication technologies (ICTs), now has the means to expand economic resources for all countries, to enhance the intellectual capabilities of their citizens, and to develop their culture and trust in other societies. The Internet, like science itself, is fundamentally transnational and ubiquitous in character. The Internet, and its attendant information tools, is the indispensable channel of scientific discourse nationally and internationally, offering to all the benefits of open science, without secrecy and without borders.

In the twenty-first century, the Internet and other interconnected networks (cyberspace) have become critical to human well-being and the political independence and territorial integrity of nation states.

The danger is that the world has become so interconnected and the risks and threats so sophisticated and pervasive that they have grown exponentially in comparison to the ability to counter them. There is now the capability for nation states or rogue actors to significantly disrupt life and society in all countries; cybercrime and its offspring, cyber conflict, threatens peaceful existence of mankind and the beneficial use of cyberspace.

Information and communication systems and networks underpin national and economic security for all countries and serve as a central nervous system for response capabilities, business and government operations, human services, public health, and individual enrichment.

Information infrastructures and systems are becoming crucial to human health, safety, and well-being, especially for the elderly, the disabled, the infirm, and the very young. Significant disruptions of cyberspace can cause unnecessary suffering and destruction.

ICTs support tenets of human rights guaranteed under international law, including the Universal Declaration of Human Rights (Articles 12, 18 and 19) and the International Covenant on Civil and Political Rights (Articles 17, 18, and 19). Disruption of cyberspace (a) impairs the individual's right to privacy, family, home, and correspondence without interference or attacks, (b) interferes with the right to freedom of thought, conscience, and religion, (c) abridges the right to freedom of opinion and expression, and (d) limits the right to receive and impart information and ideas to any media and regardless of frontiers.

ICTs can be a means for beneficence or harm, hence also as an instrument for peace or for conflict. Reaping the benefits of the information age requires that information networks and systems be stable, reliable, available, and trusted. Assuring the integrity, security, and stability of cyberspace in general requires concerted international action.

Therefore, we advocate the following principles for achieving and maintaining cyber stability and peace:

1. All governments should recognize that international law guarantees individuals the free flow of information and ideas; these guarantees also apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.
2. All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding investigative assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.
3. All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.
4. Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.
5. Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.
6. Governments should actively participate in United Nations' efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.

Selected Bibliography of WFS Permanent Monitoring Panel on Information Security Documents[1]

Main Documents

"Top Cyber Security Problems That Need Resolution: The Planetary Emergency Regarding the InSecurity of Global Communications," WFS PMP on Information Security, 2009

Wegener, Henning, "Overview of Stakeholder Activities: Who is doing what in Cybersecurity?" 3rd Facilitation Meeting for WSIS Action Line C5, 2008

"Information Security in the Context of the Digital Divide: Recommendations submitted to the World Summit on the Information Society at its Tunis Phase," WFS PMP on Information Security, 2005

"Information Security: The Development Imperative Executive Summary of Recommendations submitted to the WSIS," WFS PMP on Information Security, paper (summary), 2005

"Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar," WFS PMP on Information Security, Report & Recommendations, Submitted to World Summit on the Information Society, WSIS-03/GENEVA/CONTR/6-E, Geneva, 2003

Papers

Wegener, Henning, "Uncharted Waters: Cyber Conflict as a New Challenge to World Peace," 2008

Touré, Hamadoun I, Dr., "Cyber Conflict and Cyber Defense in the Framework of the Global Cybersecurity Agenda: An Invitation to the Global Negotiating Table," 2008

Helmbrecht, Udo, Rainer Plaga, "New Challenges for IT-Securtiy Research in ICT," Federal Office for Information Security (BSI), Bonn, Germany, 2008

Helmbrecht, Udo, "Electronic Identity Cards and Citizens' Portals Contributions to a Culture of Cybersecurity," Federal Office for Information Security (BSI), Bonn, Germany, 2008

Wegener, Henning "Perils in Cyberspace: Cancerous Growth?," 2008

Westby, Jody R. "Homeland Security v. Homeland Defense: Gaps Galore," 2008

Wegener, Henning, "Harnessing the Perils in Cyberspace: Who is in Charge?" Disarmament Forum, ICTs and International Security, 2007

Westby, Jody R. "Countering Terrorism With Cyber Security," *Jurimetrics Journal*, Vol. 47 at 297-313, 2007

Supporting Books, Articles, and Papers

Barletta, William A., "Cyberwar or Cyber-terrorism: The attack on Estonia,"

Barletta, William A., "The Evolving Face of Cyber-conflict and Information Warfare," 2006

Axel Lehmann, Prof. Dr., "Innovations in Information and Communication Technologies: Benefits and Threats," Neubiberg, Germany, 2005

Chereshkin, Dmitry, Prof., "New Security Challenges in the Information Age," , 2005

Britkov, Vladimir, "Safety as a Result of of Information Providing," , 2005

Wegener, Henning, "Learning Lessons from Cyber Attacks: Broadening the CERT Framework," 2004

Wegener, Henning, "Guidelines for National Criminal Codes on Cybercrime in the Field of Information Security and their Application throughout the International Community," 2003

1 Documents are located at http://www.unibw.de/infosecur/publications.

Kroutskikh, Andrei Ph.D., Prof., "International Information Security and Negotiations," Russia, 2003

Lehmann, Axel Prof. Dr., "Heightening Public Awareness and Education on Information Security," Neubiberg, Germany, 2002

Bosch, Olivia, "International Monitoring Mechanisms for Critical Information Infrastructure Protection," International Insittute for Strategic Studies, 2002

Westby, Jody R. and William A. Barletta, "Consequence Management of Acts of Disruption," 2002

Tsygichko, Vitali, "Cyber Weapons as a New Means of Combat," Russian Federation Academy of Natural Sciences, 2002

Kamal, Ahmed, "*New Forms of Confrontation: Cyber Terrorism and Cyber-crime*," United Nations Institute of Training and Research, 2002

Gelbstein, Eduardo and Ahmed Kamal, "Information Insecurity: A survival guide to the uncharted territories of cyber-threats and cyber-security," 2002

Westby, Jody R., "A Shift in Geo-Cyber Stability & Security," The Work-IT Group, 2002

About the World Federation of Scientists

The World Federation of Scientists (WFS) was founded in Erice, Sicily, in 1973, by a group of eminent scientists led by Isidor Isaac Rabi and Antonino Zichichi. Since then, many other scientists have affiliated themselves with the Federation, among them T. D. Lee, Laura Fermi, Eugene Wigner, Paul Dirac and Piotr Kapitza.

The WFS is a free association, which has grown to include more than 10,000 scientists drawn from 110 countries. All members share the same aims and ideals and contribute voluntarily to uphold the Federation's Principles. The Federation promotes international collaboration in science and technology between scientists and researchers from all parts of the world - North, South, East and West. The Federation and its members strive towards an ideal of free exchange of information, where scientific discoveries and advances are no longer restricted to a select few. The aim is to share this knowledge among the people of all nations, so that everyone may experience the benefits of the progress of science.

The creation of the World Federation of Scientists was made possible by the existence, in Erice, of a centre for scientific culture named after the physicist Ettore Majorana, the Ettore Majorana Foundation and Centre for Scientific Culture. This Centre, which has been dubbed "The University of the Third Millennium", has attracted over 100,000 scientists from all over the world since its founding in 1963. The Ettore Majorana Centre was a precursor of the World Federation of Scientists and its action to mitigate planetary emergencies.

The World Federation of Scientists rapidly identified 15 classes of Planetary Emergencies and began to organise the fight against these threats. One of its main achievements was the drawing up of the Erice Statement, in 1982, by Paul Dirac, Piotr Kapitza and Antonino Zichichi, clearly setting out the ideals of the Federation and putting forward a set of proposals for putting these ideals into practice. Another milestone was the holding of a series of International Seminars on Nuclear War which have had a tremendous impact on reducing the danger of a planet-wide nuclear disaster and have ultimately contributed to the end of the Cold War. In 1986, through the action of a group of eminent scientists (most of whom were members of the WFS) the International Centre for Scientific Culture ICSC-World Laboratory was founded in Geneva to help achieve the goals outlined in the Erice Statement.

WFS established its Permanent Monitoring Panel on Information Security in 2001. Its report, Toward A Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, was one of the leading documents filed by the civil society in the United Nations' World Summit on the Information Society (WSIS) first held in Geneva in 2003. The PMP has published numerous papers on cybersecurity and cyber warfare and regularly presents information security issues as a critical planetary emergency issue in WFS plenary sessions held each August in Erice, Sicily. In August 2009, the PMP was so alarmed by the potential of cyber warfare to disrupt society and cause unnecessary harm and suffering, that it drafted the Erice Declaration on Principles of Cyber Stability and Cyber Peace, which was adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice (Sicily) on August 20, 2009. The Declaration has been distributed to every member country of the United Nations.

The PMP is co-chaired by Amb. Henning Wegener of Berlin & Madrid and Dr. Jody R. Westby, CEO of Global Cyber Risk LLC in Washington, DC.

EWI and WFS Cooperative Agreement

- On April 19, 2010, The EastWest Institute and the World Federation of Scientists signed a Memorandum of Understanding to collaborate in mutual efforts aimed at ensuring the peaceful, free, and secure use of information and communication technologies (ICTs) in a well coordinated and trusted global environment. The collaboration includes WFS's collabaoration with EWI on its Worldwide Cybersecurity Summit in May, 2010, and the advancement of work in the cyber area developed by either EWI or WFS.
- This joint publication of selected documents of the WFS Permanent Monitoring Panel on Information Security provides recognition of the cutting-edge work that the PMP has conducted in the area of cybersecurity, and it helps advance EWI's cybersecurity initiative and stimulate thought leadership at the Worldwide Cybersecurity Summit.

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

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

NON-BOARD COMMITTEE MEMBERS

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

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

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

Laurent Roux (U.S.)
President
Gallatin Wealth Management, LLC

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.

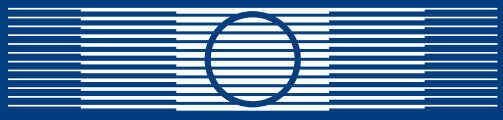
Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

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