Georgia Institute of Technology

Carnegie Mellon University

Workshop on Exploring International Dimensions of Cybersecurity

April 6 - 7
2005

Workshop on Exploring International Dimensions of Cybersecurity

April 6 -7, 2005
Atlanta, GA

Co-sponsored by

The Sam Nunn School of International Affairs,

And

The Georgia Tech Information Security Center,
Georgia Institute of Technology

And

The School of Engineering,
Carnegie Mellon University

Compiled by Benoit Morel (Carnegie Mellon University)[#]

Draft Report
06.23.2005

[#] These notes are based on those taken by a variety of participants. They do not reflect the totality of what was discussed in the workshop and put the emphasis on a few selected subjects. The text has been greatly improved by the editing of Ryan Ricks.

Introduction

The intent of the workshop was to elicit major issues associated with the international dimension of cybersecurity. Participants hailed from academia, government and the private sector. This report focuses on a few key issues which offer the best prospects for research and represented areas of urgent concerns.

Cybersecurity is a complex topic, one in which it is difficult to agree on basic definitions. Cyberspace includes "all the large computer and telecommunications networks in the world, including the IP Internet." Cybersecurity also concerns the Public Switched Telecommunication Networks (PSTN), mobile cellular networks, transport networks, and various data networks.

This report is divided into the following sections: The Internet and its Vulnerabilities, The International Dimension of Early Warning, Cybersecurity and International Security, Information Security and the Developing World, The Atlanta Declaration, International Regime for Cybersecurity and Final Comments.

The Internet and its Vulnerabilities

The Internet, like other communications infrastructures, derives much of its value from its global character; it is a critical infrastructure shared by all nations. The Internet facilitates economic, cultural and many other forms of interaction. It is a major driver of globalization. Despite the benefits, the Internet has also become a breeding ground for criminals and all sorts of malicious activities.

Security was not a major concern at the Internet's creation. Nobody expected it would evolve into its current form. Today there are approximately one billion internet users. None of them are completely immune from attacks.

Cyberspace is owned, equipped and managed mostly by private companies. Out of the thousands of Internet Service Providers (ISPs), a few are transnational, connecting users across continents and borders. Cyberspace itself has many borders, being divided into autonomous systems connected by "border gateways."

National borders, which define the limits of sovereignty, are not natural partitions for cyberspace. The Internet binds nations together outside the jurisdiction of governments. This forces nations to cooperate in ways they are not accustomed to, such as harmonizing and continuously reviewing their laws on subjects like crime, among others.

The Internet has serious vulnerabilities which threaten all nations. BGP (Border Gateway Protocol) is widely used across the Internet although it is a major source of vulnerability. BGP allows different autonomous systems to share routing tables. This plays an essential role in the routing of packets from their source to their destination. The problem with BGP is that it is possible to interfere with the routing table system and as a result, packets may be misrouted.

This vulnerability was accidentally exploited. In that incident (AS7007), a single configuration error in two routers disrupted large parts of the Internet for two hours. Done on a large scale this would lead to the loss of all packets, bringing the Internet down. Today there is no real protection against this vulnerability.

Solutions exist on paper, but the Internet's exponential growth makes the situation intractable. The political will needed to muster necessary resources is lacking. This story is representative of the difficulties in addressing cybersecurity on a global scale.

Had this problem been anticipated when the internet was in its infancy, this vulnerability would presumably not exist today. The BGP vulnerability represents a much larger theme in software development. Security should be part of the original design, not something that can be added later or a patch.

Among the multitude of problems the Internet faces is cyber-crime. Comparatively rare a few decades ago, the concept of cyber-crime has added a new dimension to law enforcement. Criminals often do not reside in the country in which they perpetrate their crime.

The concept of dual-criminality is an important aspect of the international solution to cyber-crime. When attacks cross national jurisdictions, the event must be illegal in each country to legally prosecute. Otherwise the activity is not criminal, and the perpetrator may not be arrested.

Two examples illustrated the importance of dual-criminality. During the mid 1980's, Pacific Bell was hacked by a 16-year-old boy from The Netherlands. Lacking dual-criminality, the US and Dutch authorities were forced to speak with the boy's mother, who disciplined him as a result.[1]

The Love Bug Virus was released onto the Internet in May 2000. The perpetrator was located in the Philippines, which had not criminalized such activities. As a result, the Philippines outlawed most computer crimes as part of an e-commerce statute.[2]

Criminals are not the only group that may perpetrate attacks. Nation states or terrorist groups could also be perpetrators. There has been no evidence of significant attacks from either group to date, however. When this occurs, the problem shifts from law enforcement to national security.

[1] Malik, William. 2005. "National Information Security Governance." Unpublished.

[2] Nain, Delphine, Neal Donaghy, and Seymour Goodman. 2005. "The International Landscape of Cybersecurity." Unpublished.

The distinction between law enforcement and national security is a bit like the sunset. Whereas some parts are clearly blue or red, there is no clear line distinguishing them. So far hardly any incidents have posed a threat to national security. Still, cybersecurity is an important part of national security.

There are at least two instances of this. First, one of the main goals of US cybersecurity policy is to protect critical infrastructures such as the power grid. Secondly, the US military is becoming more dependent upon information technology. Network centric warfare and information operations are central components of US military doctrine.

Another unresolved issue is the role of the government in cybersecurity. The government has let the Internet grow on its own with limited intervention. Most of our security measures have been outsourced to the private sector. Many tools to combat malware and other security technologies, such as firewalls, have been developed commercially.

The private sector is on the front line and has to take care of its defense against cyberattacks. There are few if any built in defenses between attackers and their targets, which range from multinational corporations (MNCS) to small home users. All classes of Internet users are expected to secure their assets, often at a non-negligible cost.

The question is how much of the burden should be carried by the private sector. Should critical infrastructure providers be held to higher standards than other organizations that use the Internet? Should they be required to have adequate defenses against attacks launched by nation-states? Should the government work more to protect critical infrastructure providers?

Corporations cannot be expected to expend resources necessary to defend themselves against a nation-state attack. There are situations where the government should be part of the solution, like for extreme events such as natural disasters.

The role and responsibility of the government is not well defined. There is no mechanism to decide when an attack crosses the threshold where government intervention is necessary. One government representative at the workshop stated, “From a government perspective the focus on cybersecurity competes with other issues. It is unlikely that much progress will happen unless a strong case can be made, showing that the benefits outweigh the costs of investing in cybersecurity.”

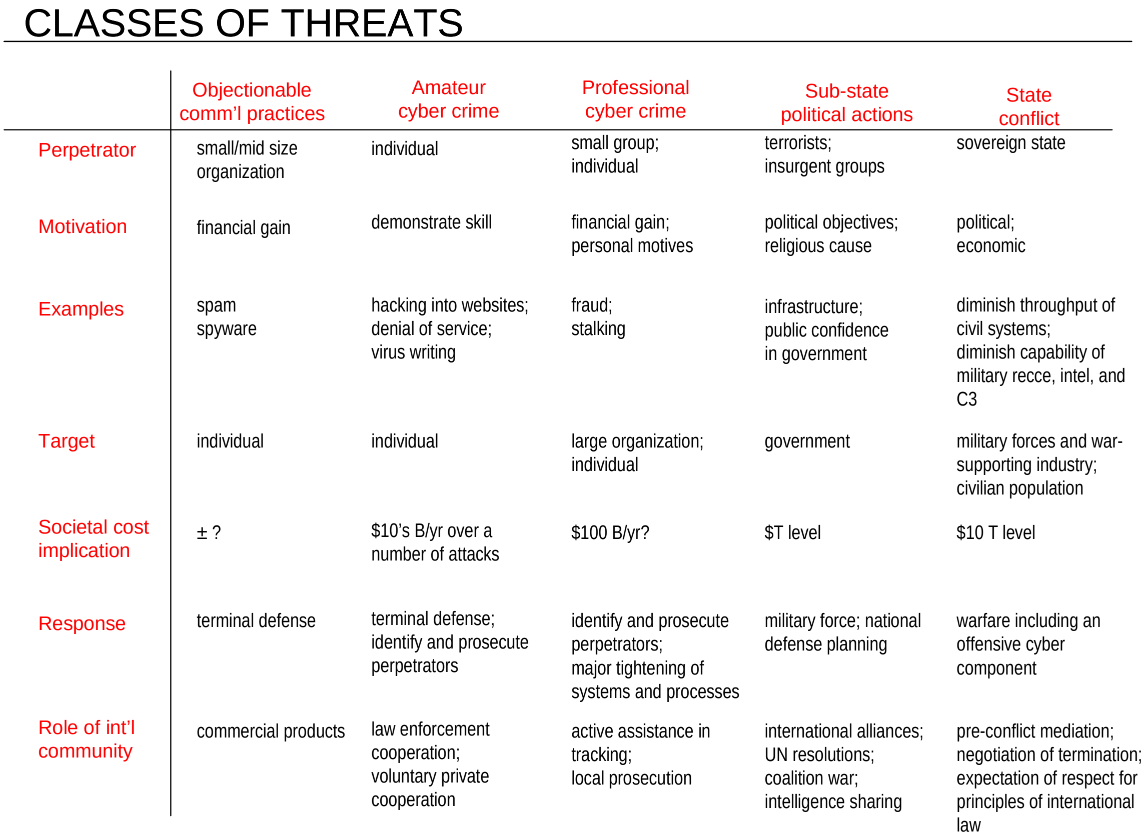
For example, it is well-known that the Internet provides foreign hackers access to our society. These agents may act on their own or for a foreign government. It is unclear if the government has legal responsibility to protect US citizens from privacy violations at the hands of foreign governments. Another unresolved issue is when attacks can be construed as an act of war or aggression.

The lack of cybersecurity has challenged the status quo so profoundly that society is still painfully adjusting to its revolutionary changes. Computers, software, and the Internet change at a rate which far outstrips society's ability to adapt. Hacking methods are progressing faster than the ability to defend systems.

There has been a dramatic increase in the scope, scale, and efficiency of attacks since the Robert Morris worm of 1988. Password cracking, self replicating malware, Trojan horses, the glamorization of hackers, exploitation of buffer overflows, and distributed of denial of service attacks are examples of evolving attack methods. Today, flash threats, bot-nets, and spam rank among society's chief concerns.

How do these compare with future threats? Attacks of the future could be far more destructive than anything we have seen yet (cf Table 1). This concern is compounded when contemplating how society increasingly relies upon information technology (IT).

One lesson from the Internet is that security must be an initial design criterion. Despite the government's rhetoric, many workshop participants would like to see more concrete actions.



CLASSES OF THREATS

	Objectionable comm'l practices	Amateur cyber crime	Professional cyber crime	Sub-state political actions	State conflict
Perpetrator	small/mid size organization	individual	small group; individual	terrorists; insurgent groups	sovereign state
Motivation	financial gain	demonstrate skill	financial gain; personal motives	political objectives; religious cause	political; economic

Examples	spam
	spyware
		hacking into websites;
		denial of service;
		virus writing
			fraud;
			stalking
				infrastructure;
				public confidence in government
					diminish throughput of civil systems;
					diminish capability of military recce, intel, and C3

Target	individual	individual	large organization; individual	government	military forces and war-supporting industry; civilian population
Societal cost implication	± ?	$10's B/yr over a number of attacks	$100 B/yr?	$T level	$10 T level
Response	terminal defense	terminal defense; identify and prosecute perpetrators	identify and prosecute perpetrators; major tightening of systems and processes	military force; national defense planning	warfare including an offensive cyber component

Role of int'l community	commercial products	law enforcement cooperation;
		voluntary private cooperation
			active assistance in tracking;
			local prosecution
				international alliances;
				UN resolutions;
				coalition war;
				intelligence sharing
					pre-conflict mediation;
					negotiation of termination;
					expectation of respect for principles of international law

Table 1: This shows that the spectrum of possible attacks encompasses far more than what has taken place so far. Terrorist attacks and other high consequence threats are possible.

The International Dimension of Early Warning

Many new viruses or worms are released every day. Malware represents only one form of attack. Spam, Distributed Denial of Service Attacks (DDOS), and bot-nets are more recent threats. In most cases, the ability to detect the attack early on would sometimes help preventing it and most of the times reduce significantly the inflicted damage. Currently attacks tend to be detected only when in progress, if they are detected at all.

The example of Slammer (sometimes called Sapphire) illustrates the difference a potent early warning capability could make, but also how difficult it will be to achieve. The Slammer worm was unleashed in January 2003; its victims were SQL servers. The worm exploited a vulnerability for which a patch had been released several months before. Slammer was unprecedented for the speed at which it spread, ushering in the era of flash threats.

When Slammer struck, it is estimated that about 100,000 servers were un-patched. 90% of them were infected in less than fifteen minutes. The speed of transmission resulted from a combination of factors. The worm used UDP packets which allows for faster transmission than TCP. Slammer was very small, carrying a 376 byte payload. Packets were sent at a high rate because the victims were powerful servers.

The worm achieved its full scanning rate of over 55 million random scans per second after approximately three minutes. Subsequently, the growth rate slowed down somewhat due to a lack of bandwidth, which was Slammer's major constraint. As a result, many parts of the Internet were bogged down with the worm's traffic. Slammer caused many hosts to be shut down, resulting in denial of various services, from the cancellation of airline flights to ATM failures.

Despite its destructive capabilities, Slammer was sub-optimal from a design view. It could have spread even faster had it used a more efficient way to find its victims. Slammer made society realize the future utility of the Internet is dependent upon a reliable early warning system. Flash threats spread too fast to be stopped by human intervention. They call for automated detection, identification and response. The technology needed is far from mature and may not exist for a very long time.

Developing enhanced early warning capabilities has an international component. A global early warning system could pick up precursor signs, which may or may not exist. In the case of Slammer, it turns out that there were precursor signs. An early warning system that can pick up subtle precursor signs has to be based on efficient traffic analysis.

Activity preceding the Slammer release was detected retrospectively using a tool called System for Internet-Level Knowledge (SiLK). Fortunately the tool had been deployed shortly before Slammer was released by the Computer Emergency Response Team/Network Situational Awareness Team (CERT/NetSA) to facilitate security analysis in large networks.

SiLK consists of two sets of tools: a packing system and analysis suite. The packing system records the packets and converts them into service-specific binary flat files. The analysis suite consists of tools which can read these flat files and then perform various query operations, ranging from per-record filtering to statistical analysis on groups of records. Efficient early warning capability begins with powerful monitoring techniques and the ability to interpret results

Some private companies are better equipped to monitor Internet traffic than public agencies. Symantec probably has the most powerful capability to monitor Internet traffic and detect malware worldwide. It boasts “over 20,000 registered sensors monitoring worldwide network activity in more than 180 countries."[3] It has deployed and is developing an early detection system for worms called Deepsight. Not much is known about the level of system performance except that information provided by Deepsight is used commercially. Its data are distributed only to paying customers. Significant losses could be avoided if those data were publicly available.

Symantec is not the only private company with significant monitoring capabilities. Microsoft with its ubiquitous network presence also has a lot of information on Internet activities. It shares data with law enforcement agencies when appropriate.

Public sector institutions like CERT have significantly less traffic monitoring capabilities. CERT is working to increase its reach by purchasing IP addresses worldwide and using them to deploy sensors. It has access to 7% of all internet address traffic. That represents an enormous amount of traffic to analyze, but this is not sufficient for high level situational awareness and early warning.

A hybrid solution to improve worldwide monitoring capability based on public-private sector seems to be the most pragmatic approach. Private companies such as Microsoft and Symantec could establish an information sharing regime with public sector organizations such as CERT, the FBI, and Homeland Security.

Aside from technical issues, privacy laws are also an obstacle to an effective international traffic monitoring system. The laws tend to set limits on traffic monitoring due to perceived intrusiveness. They can create situations where those

[3] J.W. Thompson, Chairman of Symantec, in a testimony before The House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet. (November 6, 2003)

in charge of monitoring the traffic may be powerless to take action to prevent disasters.

Early warning is clearly a critical component of a more secure cyberspace. More than just responding to everyday incidents, early warning is about detecting previously unknown attacks. Situational awareness is a critical component of any early warning system.

The limits of the possible for situational awareness and early warning are unclear. Achieving advanced situational awareness is challenging in relatively small networks. Considering the size of the Internet and the amount of traffic it carries, spectacular advances will be needed in intrusion detection and traffic monitoring for an effective early warning system. This does not account for the complicating effects of political and legal constraints. Today a global early warning capability is not even on the international agenda.

Cybersecurity and International Security

The intersection between cybersecurity and international security is a rather poorly studied area. The observation that in cybersecurity offense is significantly easier than defense has inspired to adopt an offensive posture as far as possible. This may not be a practical in many situations, but it could be useful when thinking about how cybersecurity can serve national security.

Cybersecurity has strategic importance. It is well-known that China, among others, is developing information warfare capabilities. China's government publicizes books explaining how to execute well-designed and coordinated cyberattacks, which could effectively supplement more traditional military operations. The US, along with many other nations, is also developing information warfare capabilities.

Even if information warfare is not an important part of military doctrine it is still critical for information operations. Cyber-warfare was discussed as an option in military conflicts such as Kosovo and the Persian Gulf wars. The vague legal status of that form of warfare has hampered its use.

Information warfare rarely plays a prominent role in any current world conflicts. China defaced a news website in Taiwan. The act spread the misinformation that China had shot down a Taiwanese fighter in its airspace. As a result, the Taipei stock exchange fell by many percentage points. It took quite some time before it came back to its original value.

Information warfare will most likely play a much greater role in conflicts of the future. The US military is especially concerned with the development of its network centric warfare doctrine. This concept has a huge cybersecurity component. Other militaries may not be changing their doctrine as deliberately as the US. Still, like most other aspects of society, they increasingly rely on IT. Although uncommon, the rising possibility of information warfare between nations is a potential factor of substantial change in their strategic relations.

The US is among the most IT-dependent countries on earth, and therefore has the most to fear from information warfare. As a result, the US is probably the most aware of the national security dimension of cybersecurity. Concerns are spreading to other countries. The more cybersecurity is seen as part of national security, the more difficult it will be for nations to enter into binding international agreements.

The increasing relevance to international security raises the question: “when does a cyberattack constitute an act of war?” At this stage the answer seems to be the same as for pornography: states can recognize it when we see it, even if they cannot define it.

Cyber-crime and terrorism constitute a breach of international peace and security, yet there is little or no mention of this in international law. On the other hand, information operations figures into international law, however vaguely. The status of information operations as a force or tactic is not precisely defined.

The UN charter could be interpreted as allowing some interruption of communications in peace time (Article 41). In line with how techniques for interfering with information operations are defined, information attacks on other states could be defined as acts of “aggression.” However, this is basically uncharted legal territory. The legal answer must be found in Article 51 of the UN Charter, which allows states to take actions in self defense, without precisely defining means of attack or defense. It is likely that the legal status of information warfare will remain vague until it takes place on a large scale.

From the UN Charter

Article 41

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.

Article 51

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Information Security and the Developing Economies

Developing countries perceive IT as an essential component for growth. It facilitates the spread of information and education at all levels of society. IT makes it possible to reach farmers deep in rural areas and inform them about alternative crops or to train health workers in remote areas. Perhaps IT's most important role is encouraging e-governance.

IT is also a conduit of interaction with the rest of the world, not only for access to information, but also for economic activity. IT has the potential to speed up economic growth in developing countries and help them jump start their economic development. One should not be surprised that 85% to 90% of World Bank projects have an IT component.

Cybersecurity on the other hand is not given sufficient importance. Developing countries are provided with IT, but cybersecurity is not considered. Firms from more advanced countries are reluctant to engage with partners from developing countries because they lack data protection. This in turn partially defeats the purpose of having an IT infrastructure. Ensuring that developing countries enjoy the full benefit of the Internet for their development is not the only reason to raise their level of cybersecurity. There is some truth to the statement that “we are as secure as the weakest link.”

Today in African countries up to 95% of network traffic can be spam and viruses. In Nigeria, the internet is so out of control that it has become dangerous to do any financial transaction over the internet. Cyberspace has become basically inhospitable to e-commerce. In order to get full use of their IT infrastructure, the level of cybersecurity in those countries has to be seriously improved.

One purpose of international cooperation is to make cyberspace a place where it is difficult for attackers to hide. Accomplishing that is still a long way off. The effort to improve the security worldwide could be impeded if developing countries can be used as a sanctuary by attackers.

Improving the security of cyberspace in developing countries is not a simple task. The more their computer infrastructure grows unchecked, the more difficult it will be to correct the problem. The question therefore is not whether some corrective action is needed but what exactly is to be done.

In more developed societies, the level of cybersecurity has plenty of room for improvement. Still, elements of a culture of security have been successfully introduced. System administrators in particular play a central role to enforce some minimum standard of security. Developing countries should have personnel with the same expertise. They need experts who stay abreast of the latest threats, and are able to protect their assets.

Experience and savvy are essential. Even in more developed countries it is difficult to find competent system administrators. There is a global need for many more experts than exist today. The situation is acute worldwide but particularly in developing countries. Very often, system administrators are self-taught. Many that have had training were taught by instructors with no system administration experience. Instructors tend to be engineers, which is only one aspect of a competent system administrator.

Another obstacle to improving cybersecurity is the amount of resources needed for data protection. Antivirus software, the most basic tool of defense, is not cheap for developing countries. Because the cost of data protection is more tangible than the amount of losses anti-virus software prevents, there is a tendency to under-invest. This is also true in the developed world. Aid in the field of cybersecurity seems to be necessary before IT can reach its full potential.

A third complication is that IT is not used exactly the same way in developing countries. In developing countries, the economy does not rely on the Internet in the same way as in more developed countries, and will not for quite some time. The losses due to malware and DDOS attacks are felt less. There is little incentive for governments under budget pressure to spend much energy in the pursuit of a level of security which will benefit more advanced countries. The level of security the developed world would like to see in developing countries, is often times unnecessary for these countries.

The establishment of international standards is problematic. First, cybersecurity changes quickly. Standards must evolve rapidly to keep pace with technological development. Without the creation of an international organization whose mission includes setting standards and enforcing them, it is difficult to imagine how cybersecurity could co-evolve with the threat. Second, there is no international body to set standards with the authority to enforce them. Currently there is not much desire for such a body.

Whatever form this international involvement takes, it will have to accommodate the huge difference between nations and the diversity of technological and political cultures. Any hypothetical international governing body must take care not to propose "one size fits all solutions."

CERTs for Developing Countries?

Could the creation of national Computer Emergency Response Teams (CERTs) improve the cybersecurity situation in some developing countries? The answer depends upon how a CERT would function. If one means a replica of US-CERT, the answer is no. CERTs would be tailored to the needs of developing countries, and would play a central role in the design and implementation of an information security policy in those countries. The original US-CERT has never had the mandate to design or implement policy.

US-CERT was created in 1988 as a policy response to the Robert Morris worm, which wreaked havoc on the Internet and revealed its deep vulnerabilities. When US-CERT began to work, it realized that “the government would not do anything significant in cybersecurity for at least 10 years.”

US-CERT was a place to call for advice and support. Today US-CERT gets so many queries that it can answer only around 10% of them. It produces influential advisories and is one of the most authoritative sources of data on security incidents. US-CERT also plays an important role in the management of software vulnerabilities by putting pressure on vendors to develop patches and responsibly inform the public on how best to deal with them. It is also a center for analysis and contributes to the marketplace of ideas in cybersecurity.

What may be more relevant for the developing countries is the fact that US-CERT encourages the creation of CERTs in other countries, with which it can collaborate. US-CERT could play a very useful role in the design and operation of foreign CERTs.

National CERTs would introduce, maintain, and enforce standard security in their own country. This would make them safer than is the case today. Although there are few similarities with the mission of other CERTs, to a large extent their mission would be unprecedented for a government agency.

National CERTs would have many benefits. If that leads to a successful growth of international e-commerce, those countries would greatly benefit. CERTs could cooperate to increase worldwide monitoring capability and situational awareness. This may be somewhat overoptimistic, however. A potential drawback is the fact that many countries do not welcome a government agency with close ties to similar agencies in foreign countries. This could be problematic because the domestic government would have little say in what their CERT does.

The Atlanta Declaration

The “Atlanta Declaration” was a high point of the workshop. It is inspired by the belief shared by many participants that much more need to be done by the government now.

The Atlanta Declaration outlines the origins of major vulnerabilities in the world's IT infrastructure and lists urgently required corrective actions. A major motivation behind the declaration is the widespread feeling that not enough is done nationally or internationally to reduce the probability of a major disaster. Cybersecurity is far more important than government actions suggest. We are only beginning to appreciate the nature and scope of our vulnerability, but there is still much to discover.

Furthermore, a report entitled “A Crisis of Prioritization” was delivered to the US President in February 2005 by top cybersecurity experts on the President's Information Technology Advisory Committee (PITAC). It states that “today we simply do not know how to model, design, and build systems incorporating integral security attributes.”

It is difficult enough to secure wired networks. Wireless technology, however offers many more challenges to information security professionals. These networks broadcast data that are often unencrypted, threatening the confidentiality of an organization's intellectual property and other important data. Furthermore, wireless networks are easily penetrated, and often times are used as a stepping stone to break into an organization's wired network.

One effect of the information revolution is an irresistible technological push for the increasing reliance on IT. Most everything, in particular the critical infrastructures, have become more IT dependent. This is an international phenomenon, but nowhere as manifest as in the US. This raises new challenges for maintenance and management.

It is not obvious that the transition to this new technological era will be smooth. Interdependencies between different infrastructures will increase, compounding the security problem. Hidden bugs in software create uncertainty as to the reliability of critical infrastructure. Even if this growing dependence upon IT was taking place in a benign environment, we should expect growing pains. But we cannot assume a benign environment, and critical infrastructures are exposed to attacks from the Internet.

The US is progressively exposing its economy to threats at a time of terrorist activity. The increasing vulnerability of critical infrastructures has not escaped the government. It has made the protection of critical infrastructures the first priority of its cybersecurity policy, under the auspices of The National Cyber Security Division (NCSD). The NCSD is a subdivision of the Information Analysis and Infrastructure Protection (IAIP) Directorate, in the Department of Homeland Security. This does not mean that cybersecurity has a high enough priority, however.

This attitude inspired the first article of the Atlanta Declaration, which follows:

1. National public communication network infrastructures generally – and that of the U.S. in particular - have over the past decade become significantly more vulnerable and are likely to become even more so unless urgent responsive actions are taken

---

The authors believe the problem calls for a very determined and immediate policy response. The present security policy tends to be reactive. In fact this is not specific to cybersecurity; government policy seems that way more often than not. This is partially due to the political and administrative constraints within which the government functions.

The growing security threat to critical infrastructures should be taken more seriously. Security should not be an afterthought. This attitude leads to buggy software and communications protocols full of vulnerabilities. Patching systems after vulnerabilities are discovered is not a solution, it is a band-aid.

A strategic initiative called the Software Assurance Program seeks to achieve “trustworthiness that no exploitable vulnerabilities exist, either maliciously or unintentionally inserted.” This is not a realistic goal. Not all vulnerabilities are due to sloppiness; complicated software often can be made to do something completely different from its designated purpose.

Having absolutely reliable software as a policy goal, does not prepare society for the future. A more appropriate goal would be to increase the reliability of software while making society less dependent on flawless information systems. We are at the beginning of a new era where software will be omnipresent. Most technologies will have bugs and exploitable vulnerabilities. Policy should strive to limit the consequences of these vulnerabilities.

Security, resilience, robustness, and fault tolerance should be key design criteria for critical infrastructures. This means taking precautions in design and implementation that were not taken when the Internet was created. It is well known that today's problems arose because security was not a concern when the Internet was designed.

The mechanism by which this lack of concern translated into vulnerabilities has not been precisely studied. Otherwise, there would be a better sense that the mere networking of computers generates vulnerabilities. There are exploitable holes, with varying consequences, throughout the Internet, from TCP, to the Domain Name System, to the Border Gateway Protocol.

So far most of the reported hacking has been done by small groups, often individual teenagers. No significant terrorist incident using the Internet has been reported. The assumption that terrorists prefer bombs is obviously not prudent policy and may not apply to all of them. A terrorist could find many weaknesses in our IT dependent society. Hardening systems against terrorists or criminals would be a worthwhile policy goal.

Instead of preparing for a future where software has no exploitable vulnerabilities, society should prepare for a future where IT will be ubiquitous. This means our infrastructures will be more intelligent, but also not necessarily more reliable. More clever design and management is critical. We should prepare for the possibility of major breakdowns, accidental or malicious. Modern societies will be more functional if they are fault tolerant. Encouraging a fault-tolerant society is an important policy goal.

Hence the second part of the declaration reads:

2. The origins of these vulnerabilities arise from

a. the confluence of more complex computer-based networks

b. the rapid expansion and use of a DARPA/NSF internet platforms not originally designed and administered for public infrastructure use

c. the proliferation of public network architectures, operations, protocols, and user practices that provide end users with significantly greater access to network resources

d. the substantial incentives to criminals and terrorists to exploit the emerging vulnerabilities

e. the lack of appreciation and understanding of these serious infrastructure vulnerabilities by regulatory and national security authorities and instituting the necessary responsive corrective processes and requirements

The third and final part of the declaration outlines urgent corrective actions. Cybersecurity will be a long term issue. The best possible policy initiatives are part of an evolutionary process. Although there are a plethora of initiatives, workshop attendees felt two were prominent: The Next Generation Network (NGN) and the ratification of the Convention of Cyber-crime of the Council of Europe.

Society tries to identify the vulnerabilities and fortify the weakest points. Fixing vulnerabilities is unattractive strategy for the long term. Learning to build solid networks is a more promising approach.

Next Generation Networks proceed from this vision. They reflect a technological change of an even more profound nature. "The general concept is to evolve global telecommunications networks to packet-switched facilities that will support fixed and mobile voice, data, text and video services in addition to other Internet applications on interoperable Internet Protocol (IP) based infrastructures."[4]

NGNs are discussed in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), which created a NGN focus group: The ITU-T NGN Focus Group to address the telecommunication industry's urgent need for NGN specifications. The need for global standards is critical. Setting those standards is the mission of ITU-T. It is "bringing all players together in an environment where they can create truly global specifications for the service-aware network of the future, to deliver dynamic, customized services on a massive scale." The major goals of this initiative, launched in May 2004, are to translate security and the other functionality requirements into global standards. If successful this initiative could pave the way to a world where all telecommunication will go through something like a more secure Internet.

NGNs are being discussed in many forums, governmental (such as Congress, FCC, DOJ, FBI, DHS, NSTAC), private (ultimately the private sector is commercializing the technology) and international (ITU, WTO, G8). NGNs are relevant for critical infrastructures but also for private use. Many countries agree on the need for some form of regulation or NGN regulatory mandates.

The US government has voiced serious policy concerns:

> "Policy decisions that arise from the transition to NGNs are matters for national determination. In the United States' view, NGN infrastructures and services should be, to the greatest extent

[4] T. Rutkowski,: "Toward Next Generation Networks: global industry collaboration; regulatory models and capability requirements" Briefing at FCC June 2005.

[7] United States' Initial Comments on Requirements for NGN, expressed at ITU-T meeting April-May 2005.

> possible, subject to a minimal amount of regulation. In addition, market forces rather than mandated government choices should drive technological advances and innovation in the NGN platforms. Care will need to be taken to ensure NGN Recommendations do not introduce barriers to competition and open markets. Market barriers could arise, for example, from poorly framed NGN Recommendations regarding network capabilities, user access to NGN platforms, interoperability, user information, intellectual property rights, and jurisdictional oversight.[7]"

NGNs raise significant technical and security issues. The "National Security Telecommunication Advisory Committee" (NSTAC) has put together a NGN Task Force focusing on the national security implications of NGNs. It seems that NSTAC's work should play a larger role in shaping policy vis à vis NGNs.

The apparent reluctance of the US to let itself be bound by international agreements can hinder progress. NGNs are about changing the way telecommunications will work. It is an inherently and primarily international initiative. It is difficult to see how issues like quality of service or security will be better served in the absence of worldwide standards. This remark is not limited to NGNs. The establishment of any cybersecurity regime will unavoidably involve some form of international arrangement or even treaty.

The Convention on Cyber-crime of the Council of Europe (CoE) is an interesting example of such international agreement. In a world where "criminals are often located in places other than where their acts produce their effects, and where domestic laws are generally confined to a specific territory, there is a need to find solutions pertaining to international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society."[8]

The convention is far from perfect; it tends to deal with content-related offenses. Our aim and interests are to protect the system itself in a politically neutral way. Some of the convention's provisions are excessively vague. They seem to be designed to enable everybody to join *even* if they do not agree on what constitutes an offence.

The CoE Convention lacks a regulatory mechanism. Regulations may not be politically correct, but they are necessary to promote a secure environment. The proposals in the National Strategy to Secure Cyberspace for strengthening the protocols will never be adopted internationally unless there is some kind of regulatory framework. In the case of cybersecurity, this framework would need private sector involvement to be successful.

[8] Convention on Cybercrime, Council of Europe, Budapest 2001. URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm Accessed: 06.25.05

Also, there is no serious incentive for non-European countries to join. The convention must be global to be effective. The claim that the CoE Convention is not global was perceived at the workshop as a red herring: many CoE conventions are in fact global. The CoE recognized that reaching an international consensus might not be possible, so it provides a standard to which other countries can aspire.

The convention opened for signatures in Budapest in November 2001. It has been signed by 38 out of the 46 member states and by the four non-member states, including the US. No states outside the Council of Europe signed. The convention has been ratified by only 10 nations, all of them member states. Only five ratifications were needed for the convention to enter into force.

There was a consensus at the workshop that the weaknesses of the CoE Convention should not stop the US Senate from ratifying it. The convention provides a framework and a legal instrument that could be used by all. The US did in fact participate in the convention. Ratification by the US would go a long way to providing legitimacy. The advantages of ratifying the CoE convention far outweigh the disadvantages.

Hence the third and last part of the declaration reads:

3. The following corrective actions are urgently required

a. Make protection of the national public communication network infrastructure a principal priority of the Federal Communications Commission and Executive Branch agencies generally, and in the context of every significant regulatory proceeding

b. Institute continuing mechanisms to analyze and understand existing and potential vulnerabilities of the nation's communication network infrastructure, including especially its signaling and security capabilities

c. Give full consideration and effect to the pending report of the NSTAC Next Generation Network task force recommendations

d. Work through international treaty based mechanisms and organizations to institute collective global steps and cooperative actions to reduce communication network vulnerabilities of existing and next generation networks

e. Ratify the Convention on Cyber-crime and create a permanent secretariat to implement and evolve its global infrastructure protection role

The Declaration is repeated in entirety at the end of this report.

International Regime for Cybersecurity

The Internet overcomes geographical boundaries, provides instant worldwide communication, increases business productivity, and creates more effective markets. Unfortunately, all of these benefits are at risk. Criminals and terrorists, including both state-sponsored and individuals, are attacking IT systems at an increasing rate. Security problems affect all nations and a solution will require a global effort. Despite this, there is no institutional organization where nations can meet to debate and join forces.

Not all countries perceive the threat in the same way, nor are they affected by it in the same way. Developing countries have different security needs from other countries. Attacks can originate in any country, so each has a role to play. Furthermore, not all countries have the resources to keep abreast with the latest technology, and most do not have enough trained and experienced personnel. Lack of adequate expertise is a global problem. Even the US suffers from a shortage of trained and experienced personnel.

The US government treats cybersecurity as an aspect of national security. It emphasizes the protection of critical infrastructure. The US government seems to be less concerned with helping nations build security capabilities to protect and stimulate e-commerce and world wide.

Unlike chess players who react to threats, policymakers often wait for the crisis to react. It was observed at the Atlanta workshop that the Chinese ideogram for crisis mixes the ideograms for danger and for opportunity. It is not uncommon in the world of policy that times of crisis also contain opportunities. Security policy will probably also be shaped by crisis. Arguably this has been the case already.

The sluggishness at which a common international front against attacks is being built is painfully slow compared to the advance in attack techniques. Society is exposed to the possibility of mega-disasters, up to an Internet black-out. It is unrealistic to expect protection against such disasters to be developed before the event occurs. This could be construed as a crisis situation.

What does the US Government Do?

The government tries to deflect criticism that it disregards international cooperation by pointing to important documents such as The National Strategy to Secure Cyberspace which recognize the need to work with other countries. Some critics are not swayed, however. They point out that the international cooperation is mentioned in only two out of fifty-one pages. Furthermore, out of the six points on that subject, the first three are vague and only one directly mentions international cooperation.

That is not to say that the US government is isolationist. It is actively promoting the spread of a "culture of security" advocated by OECD and the UN. It has also participated in several international conferences:

- The US was represented by the Assistant Secretary of State for Politico-Military affairs, in an international conference on cybersecurity in the Balkans, which took place in Sofia, Bulgaria in September 2003.

- Through its Telecommunications Working Group, the Asia Pacific Economic Cooperation (APEC) has been a beehive of activity for strengthening critical infrastructures. The US government plays an active role in those efforts.

- The US also led the G8 development of principles to protect cyberspace.

- A US initiative in June 2004 led to the adoption by the OAS General Assembly of a comprehensive Inter-American strategy to combat threats to cybersecurity, developing computer security incident response teams, addressing standards and industry issues, and also to address legal infrastructures for cyber crime.

- Germany and the US co-hosted a multilateral cybersecurity conference in October 2004 in Berlin to address the issue of global cooperation.

When it comes to active cooperation, the US seems to favor the bilateral approach, focusing on countries of greatest strategic importance, such as Australia, New Zealand, UK, India, and Japan. International cooperation is difficult. There is agreement about the ends to a large extent, but not necessarily the means. Countries are aware of the need to secure cyberspace and are eager to do their share, but the leaders face challenges adapting the need to their domestic conditions.

Countries tend to have different legal cultures, which cannot be changed easily. When one realizes how slow and complicated bilateral negotiations are, multilateral approaches do not seem promising or attractive. A common international front is developing far too slowly as a result.

"We are only secure as the least secure country," said the US Assistant Secretary of State for Politico-Military affairs at the Sofia meeting of September 2003. This seems to imply that a sound international regime requires that no country be allowed to fall below a minimum level of security. Considering the dynamic nature of cybersecurity, international standards would need to be revised frequently. Their implementation requires resources and in the case of some developing countries, more than they can afford. This seems to call for some form of international enforcement mechanisms, which presumably would have to be coordinated by an international agency.

The situation would look a bit less hopeless if there was a mechanism or an organization in place to set and enforce international standards. The existence of an international institution coordinating the technological response and its implementation would not provide fool proof protection. This must be compared to the present system of voluntary arrangements between selected countries.

An International Organization for Cybersecurity?

Today, the idea of an international organization with the mission to promulgate and enforce security standards is not a realistic policy option. The creation of such an organization may only come about after a major cyber-crisis. Therefore, discussing and planning such a body is not an exercise in futility. Policy makers will be grateful to have a foundation upon which to build.

The responsibility of such an organization will be to identify the best existing technologies and spur further research. The Internet Engineering Task Force (IETF) is an example; it helped foster technological excellence. IETF together with its satellite organizations sets Internet standards specifications. IETF was originally a self-appointed group, composed of a few American computer experts. This was a reflection of the fact that the Internet was originally a US technology.

IETF managed to promote a culture of technological excellence which underlies the growth of the Internet. It produced “Request For Comments” (RFC), which were de facto technological standards. IETF never had the authority to impose any standard. IETF can contribute only when the problem has a technological answer, however.

Is the IETF a promising model for a hypothetical international cybersecurity organization? Should the international organization have an IETF-like structure, i.e. consensus-based, but with universal participation? IETF is a way to promote openness, but it has no real responsibility or accountability. Could an organization with limited authority create the information-sharing basis and have enough legitimacy to get the job done? This is unclear.

There is a precedent of an international regime enforced worldwide: Airline security. The International Civil Aviation Organization (ICAO) decides the rules but it has very little enforcement power. Nations are ultimately responsible for enforcing the safety rules by denying the right of planes to land if they come from a country which does not abide by the safety rules. This system of enforcement would not work with cyberspace. Nations which do not abide by the rules would have to be physically cut-off from the rest of the Internet. This would have to be a collective decision, not a choice made by individual nations.

Considering that the Internet has a very large intersection with telecommunications, it seems natural to ask what role or relevance the International Telecommunication Union (ITU) could have. ITU is already involved with information and communication technologies (ICTs) and cyberspace. It also has the International Telecommunication Regulations and Art. 9.1b as a treaty basis for protecting infrastructures. Furthermore ITU hosts the World Summit on Information Systems (WSIS) set of conferences. The ITU is better able to deal with the private sector than most organizations, an important benefit since most of the Internet is privately owned and operated.

ITU already deals with standards. One provision of a resolution[9] states that "in accordance with Article 17 of the ITU Constitution, the duties of the ITU Telecommunication Standardization Sector (ITU-T) shall be to study technical, operating and tariff questions and to adopt recommendations with a view to standardizing telecommunications on a worldwide basis." This concerns all ICTs.

Internet technology is the subject of another resolution, resolution 46, adopted at the same time. It "establishes a short-lived group for the purpose of providing the first meeting of the Council Working Group on WSIS in 2005 with a definition relevant to the technical aspects of the telecommunication networks used by the Internet."

ITU like IETF has the right technological culture. Also like IETF it does not have much enforcement power. 90% of ITU work involves standards setting in both the radio and telecom sectors and it has a very successful history over many generations of high technical excellence. The 10% left is for negotiations between nations.

If a hypothetical international cybersecurity agency was created, it would have to find its niche among the existing institutions such as ITU. In fact some of the organizers of the workshop have already worked at a proposal for an international Agency for Information Infrastructure Protection (AIIP), which would meet most of the criteria mentioned above. AIIP may be the most detailed proposal for such an organization.

An Agency for Information Infrastructure Protection (AIIP)

AIIP would be created by a convention of states, who would agree to share the burden of the protecting of the Internet, and help those needing assistance. The mission of AIIP would not be limited to technical issues that enhance system protection. It would also be concerned with procedural issues and be seen as part of an international law enforcement community whose objective is to punish abusers of information systems. In other words, AIIP would protect as well as punish.

[9] Florianopolis, 2004 World Telecommunication Standardization Assembly

AIIP would have to be a value-adding organization, not an international bureaucratic sinecure. It would be highly distributed, in terms of both geography and constituencies. AIIP would be on the cutting edge of information technology. Its staff must be world class. It should be small, relying on its technology to create a web of correspondents. Operations would be highly networked, not just in the use of IT for its administrative functions, but for its reach. AIIP's small size and worldwide connectivity would enable it to respond quickly, effectively and efficiently. A useful organizational model may be the Internet itself. Its processes are open, networked, and focus on consensus.

The organizational structure would include three elements: a secretariat, an assembly and a council. The secretariat would be the day-to-day management arm of the AIIP, directing its staff and supporting the Committees and Working Groups.

The front office would be located somewhere such as Brussels, or New York. AIIP would also have three field locations, Reston, London, and Tokyo, which are reminiscent of the three ITU regions. Field staff would be recruited locally. About half the staff at each field location would be professionals from industry or universities on term appointments.

The Secretary General would be located at the front office. The organization would work through standing and ad hoc committees and working groups. Standing committees would complete about two-thirds of the activity, and about one-third by ad hoc groups addressing emerging needs.

The Assembly would be the forum for Member States to deal with their sovereign interests. The Assembly could meet infrequently, e.g. every three years and address higher-level policy, not working level detail. It would identify issues for the Secretariat to address during the next “cycle” (cf. FCC’s NRIC).

The Assembly would approve recommendations from the Secretariat/Council, or hold them over for the next cycle. It would be the primary mechanism for long-term political input. The Assembly would be the link to the Member States’ governments. Member States would be expected to make organizational and human resources under their jurisdiction available to the AIIP.

Then there would also be a Council. It would be the liaison between the operational Secretariat and the political Assembly. The Council would be elected by the Assembly, and would serve as an Executive Committee for the Assembly. It would operate through authority delegated by the Assembly. The Council would oversee the management actions of the Secretariat and meet annually or more frequently if required.

The AIIP would have several operational functions:

- Establish and support the operation of a Technical Committee to recommend standards for the collection and preservation of forensic evidence. The process would be modeled after the Internet's RFC 2026.

- Establish definitions to govern the estimation and reporting of the consequences of cyber-crimes, probably through an ad hoc committee.

- Recommend such changes to the list of offenses as may be suggested by the evolution of technology.

- Collect and maintain a database of information related to attack profiles voluntarily provided by Members. Such information would be restricted to those authorized by the Member States. It could be run as a contractor-operated service. However it is accomplished, it would be overseen by an Operations Committee.

- Facilitate and coordinate international responses to security incidents through the operation of a registry of certified incident response individuals and organizations. This will require a Certification Committee concerned with defining professional qualifications and training, required technical capabilities, and tracking adequacy of performance to maintain certification.

- Define standards for the initial and continuing certification of incident-response individuals and organizations.

- Define the specifications for a near-realtime incident reporting network for use in expediting tracking and pursuit of violators.

- Establish a secure and anonymous communication facility and clearing house for the exchange of information during the investigation of security incidents by incident response teams.

- Establish a Virus Working Group of the Technical Committee to assist in the coordination of global actions to detect viruses and to distribute patches.

- Encourage, through the establishment of a Tool Integration Working Group under the Technical Committee, the integration of intrusion detection tools by security product vendors.

- Encourage, through an R&D Working Group of the Technical Committee, the establishment of test beds to explore new technical approaches to network security.

- Establish a Measurements and Analysis Working Group under the Technical Committee to assist in reaching agreement on metrics to assist in understanding Internet behavior and use; serving to alert operators to the emergence of new attack modes; and to recognize and characterize emergent properties of the Internet.

- Assist in the identification of individuals and organizations recommended for participation in red teams.

- Work with the Operations Committee, R&D Working Group of the Technical Committee, and the Privacy Committee to explore the technical basis for proposals to implement packet and session tracking capabilities and to make appropriate recommendations to the Council.

- Establish, under the Operations Committee, a Working Group consisting of industry representatives from the ISPs, providers of router hardware and software, and providers of security product software to explore potential solutions to infrastructure protection problems and to recommend best security practices.

- Establish, under the Operations Committee, a Working Group to recommend an architecture for a global indications and warning capability.

A detailed draft of the AIIP Convention exists, as well as estimates of the budget. AIIP is designed in such a way that it can adjust to changes in the landscape of cybersecurity. It should coordinate, lead and implement whatever is needed to improve global cybersecurity.

Today the government’s view is that unless the externalities from cybersecurity are so bad that cooperation is necessary, there will not be enough support to form such an international agency.

Final Comments

One can argue that cybersecurity did not start with the Internet, but with telephony. In the early 1980’s John Draper was using toy whistles from boxes of Cap'n Crunch cereal, which happen to blow at exactly 2600 Hz, the tone necessary to authorize a call, in conjunction with a bluebox to make phone calls for free (known as “phreaking”). This could be considered an early form of cyber-attack. Kevin Poulsen won a Porsche by exploiting this technique; this could be construed as a form of cybercrime.

Phreaking did not need the kind of international response that cybersecurity calls for today. Cybersecurity is only in its infancy. The attacks of tomorrow may be far more deadly and damaging than anything we have seen. Adjusting to the possibility of far more serious engagement is one of today's policy challenges.

In a similar vein, the Internet is not the first telecommunications technology which forced nations to cooperate. Satellite networks, X.25 data networks, and the OSI internet in the 1970s brought the entire array of problems and concerns to international organizations at that time, especially the ITU. In fact, since the inception of telecommunications around 1850, nations had to agree on technological standards and international regulations. The ITU, under whose aegis this international activity takes place, is only the latest organization dealing with ICTs at the international level.

The importance of cybersecurity is unprecedented. It is such a significant disruption for the present international order that it has deep ramifications in the lives of nations, their relations, and their security. International cooperation cannot be limited to technological considerations. Law enforcement and national security are also important.

In many respects the international dimension of cybersecurity is uncharted territory. Malware, hacking, spam, bot-nets and the like are not confined to the territory of one nation. They affect the whole of cyberspace. The targets of the attacks so far tend to be individual users or private companies.

At the national and international level we are only slowly coming to grips with the nature of the situation. The cooperation between nations must overcome a variety of obstacles, such as changing internal laws.

Developing countries are an important piece of the puzzle. Lack of security has the potential to spoil most of the benefits of the Internet. Furthermore, failing to ensure that their portion of cyberspace meets minimum standards could negatively affect the rest of the world. Not much may happen if these countries are left on their own.

A major complication is the central role the private sector plays in the Internet, especially ownership, management and control. Transnational or multinational companies may have to comply with very different laws simultaneously. International standards must also apply to MNCs, and they should be included as participants.

Today there is no international emergency response system, but there is a bottom up effort to build capabilities between selected national CERTs, with little or no involvement of governments.

Fighting cyber-crime with some hope of success requires an international law enforcement system. A new organization could help, such as the AIIP. Governments are not enthusiastic about the emergence of an international institution which would implement and enforce a cybersecurity regime. It seems that only a serious crisis could change this situation.

Ultimately national governmental and inter-governmental bodies must protect the public infrastructures. Governments seem to have difficulty articulating long term coherent policies, especially when it comes to the international dimension of cybersecurity. These difficulties must be overcome.

Lack of security has ramifications everywhere, even embedded systems. We still do not know the full extent of the problem, and certainly do not take adequate precautions. A far more aggressive, systematic and long term analysis of our vulnerabilities is critical. New vulnerabilities are potentially created with each new product. US cybersecurity policy should more seriously mobilize resources and involve far more federal agencies.

Among many of the workshop participants there was a shared concern that behind the official rhetoric the US Government is not taking cybersecurity seriously enough. That is what motivated the Atlanta Declaration.

The Atlanta Declaration

on global protection of public of communication network infrastructure

1. National public communication network infrastructures generally – and that of the U.S. in particular - have over the past decade become significantly more vulnerable and are likely to become even more so unless urgent responsive actions are taken
2. The origins of these vulnerabilities arise from
    a. the confluence of more complex computer-based networks
    b. the rapid expansion and use of a DARPA/NSF internet platforms not originally designed and administered for public infrastructure use
    c. the proliferation of public network architectures, operations, protocols, and user practices that provide end users with significantly greater access to network resources
    d. the substantial incentives to criminals and terrorists to exploit the emerging vulnerabilities
    e. the lack of appreciation and understanding of these serious infrastructure vulnerabilities by regulatory and national security authorities and instituting the necessary responsive corrective processes and requirements
3. The following corrective actions are urgently required
    a. Make protection of the national public communication network infrastructure a principal priority of the Federal Communications Commission and Executive Branch agencies generally, and in the context of every significant regulatory proceeding
    b. Institute continuing mechanisms to analyze and understand existing and potential vulnerabilities of the nation's communication network infrastructure, including especially its signaling and security capabilities
    c. Give full consideration and effect to the pending report of the NSTAC Next Generation Network task force recommendations
    d. Work through international treaty based mechanisms and organizations to institute collective global steps and cooperative actions to reduce communication network vulnerabilities of existing and next generation networks
    e. Ratify the Convention on Cybercrime and create a permanent secretariat to implement and evolve its global infrastructure protection role

Workshop on Exploring the International Dimensions of Cybersecurity

April 6 – 7, 2005
Atlanta, GA

Wednesday, April 6, 2005	
Morning Sessions	
8:15 a.m.	Continental Breakfast
9:00 – 9:15 a.m.	Welcoming Remarks **Seymour Goodman,** Professor, College of Computing and the School of International Affairs, Georgia Institute of Technology
9:15 – 10:30 a.m.	Session 1: Setting the Stage
	Session Chair: **Benoît Morel,** Senior Lecturer, Department of Engineering and Public Policy, Carnegie Mellon University
10:30 a.m.	Coffee Break
11:00 – 12:30 p.m.	Session 2: Early Warning
	Panel Chair: **Herbert Lin,** Senior Scientist, Computer Science and Telecommunications Board (CSTB), National Research Council, National Academies Panelists: **Bill Cook,** Partner, Intellectual Property Practice Group, Wildman Harrold **Tom Longstaff,** Survivable Network Technologies Manager, Carnegie Mellon Software Engineering Institute
12:30 p.m.	Lunch Luncheon Speaker: **David Aucsmith,** Security Architect and Chief Technology

	Officer, Security Business and Technology Unit, Microsoft Corp.
Afternoon Sessions	
2:00 – 3:30 p.m.	Session 3: Private International Initiatives
	Panel Chair: **Roger Callahan,** Senior Vice President, Corporate Information Security, Bank of America Panelists: **Mary Riley,** Senior Vice President, Corporate Information Security, Bank of America **Tony Rutkowski,** Vice-President, Regulatory Affairs, Communication Services Division, Verisign, Inc. **Philip Reitinger,** Senior Security Analyst, Trustworthy Computing Team, Microsoft Corp. **Lawrence Baldwin,** President, myNetWatchman.com
3:30 p.m.	Coffee Break
3:45 – 5:30 p.m.	Session 4: Government International Initiatives
	Panel Chair: **Paul Kozemchak,** Special Assistant to the Director, Defense Advanced Research Projects Agency (DARPA) Panelists: **Paul Syverson,** Mathematician, Center for High Assurance Computer Systems (CHACS), Naval Research Laboratory (NRL) **Dan Hurley,** Director, Critical Infrastructure Protection, United States Department of Commerce
5:30 p.m.	Reception
6:00 p.m.	Dinner
Morning Sessions	
8:15 a.m.	
8:30 – 10:15 a.m.	Continental Breakfast
	Session 5: Strategies to Secure Cyberspace
10:15 a.m.	Panel Chair: **Steve Lukasik,** Consultant Panelists: **William Foster,** Assistant Professor, School of Management, Arizona State University

	Bob Balzer, Chief Technical Officer, Teknowledge Corporation **Neal Pollard,** Information Warfare Analyst, Strategic Assessment Center, Science Applications International Corporation (SAIC)
10:30 – 12:00 p.m.	Coffee Break
	Session 6: International Cybersecurity Arrangements
12:00 p.m.	Panel Chair: **Abraham Sofaer,** George P. Shultz Distinguished Scholar and Senior Fellow, Hoover Institution, Stanford University Panelists: **Slawomir Redo,** Senior Crime Prevention and Criminal Justice Expert, United Nations Office on Drugs and Crime **Joseph Richardson,** Director of APEC and OECD, Office of Multilateral Affairs, International Communications and Information Policy, United States Department of State **Jody Westby,** Managing Director, Advisory, PricewaterhouseCoopers, LLP
Afternoon Session	Lunch
1:00 – 2:30 p.m.	
	Session 7: Agenda for the Future
2:30 p.m.	Session Chair: **Seymour Goodman** Panelists: **Roger Callahan, Paul Kozemchak, Herbert Lin, Steve Lukasik, Benoît Morel and Abraham Sofaer**

Panel Chair Biographies

Roger M. Callahan

Roger Callahan is Senior Vice President within the Corporate Information Security Organization at Bank of America. He is currently responsible for the Corporate-wide Awareness, Communication and Infrastructure Protection efforts for the information security organization. Prior to his current responsibilities, he supported the financial services industry’s Critical Infrastructure Protection (CIP) efforts. He was the Program Manager for the Financial Services Sector Coordinating Council (FSSCC) supporting the Director of Corporate Information Security, Rhonda MacLean, in her role as Treasury's appointed private sector coordinator for CIP and Homeland Security (HLS) during 2002 - 2004. Presently, Mr. Callahan is the Bank of America National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee member, and he has previously served as co-vice chair of the NSTAC Financial Services Task Force.

Mr. Callahan has over 33 years of prior experience in various roles with the National Security Agency (NSA). In 1995, as a member of the Senior Executive Service, he was assigned to the Pentagon and was the Director for Information Assurance in the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. During both his government and private sector careers, he has served as an advisor to DOD's Defense Science Board on the subject of Defensive Information Warfare.

He is a 1968 Electrical Engineering graduate of Northeastern University, Boston Massachusetts; a graduate of the National Defense University, Industrial College of the Armed Forces, Washington DC in 1985; and a graduate of the John F. Kennedy School of Government "Senior Officials in National Security Program" at Harvard University, Cambridge, Massachusetts.

Seymour E. Goodman

Seymour (Sy) Goodman is Professor of International Affairs and Computing, jointly at the Sam Nunn School of International Affairs and the College of Computing at the Georgia Institute of Technology. He serves as Co-Director of both the Georgia Tech Information Security Center (GTISC) and the Center for International Strategy, Technology and Policy (CISTP), and is currently principal investigator on two large grants from the National Science Foundation and the MacArthur Foundation, the latter with John Endicott.

Professor Goodman’s research interests include international developments in the information technologies (IT), technology diffusion, IT and national security, and related public policy issues. His current work includes research on the global diffusion of the Internet and the protection of large IT-based infrastructures.

Immediately before coming to Georgia Tech, Professor Goodman was Director of the Consortium for Research on Information Security and Policy (CRISP) at the Center for International Security and Cooperation, with an appointment in the Department of Engineering Economic Systems and Operations Research, both at Stanford University; and Professor of MIS and a member of the Center for Middle Eastern Studies at the University of Arizona.

Professor Goodman was co-editor with Abraham Sofaer of a volume of essays dealing with the transnational dimension of cyber crime and terrorism, based on a conference on that subject which they co-chaired at Stanford University. The volume includes a proposed multilateral treaty.

Professor Goodman was an undergraduate at Columbia University, where he started as an aspiring English major, and obtained his Ph.D. from the California Institute of Technology, where he worked on problems of applied mathematics and mathematical physics. He is the author of numerous journal articles, books and chapters in edited volumes, and International Perspectives editor for the *Communications of the Association of Computing Machinery (CACM)* since 1990.

Paul Kozemchak

Paul Kozemchak serves as Special Assistant to the Director of the Defense Advanced Research Projects Agency (DARPA). In this position Mr. Kozemchak is primarily responsible for interacting with the intelligence community, including advising DARPA on strategic developments that affect its investments, participating in the Quadrennial Defense Review, the Quadrennial Intelligence Community Review, Joint Vision 2010 and the Defense Science Board.

Mr. Kozemchak is a member of the Director of Central Intelligence’s (DCI) Scientific and Technical Intelligence Committee and the Advanced Research and Development Committee. He works with the National Intelligence Council (NIC) and Intelligence Science Board on matters related to science and technology. This includes the NIC's 2020 project, Mapping the Global Future (the follow-on to Global Trends 2015) and estimates of cybersecurity and biotechnology. He is a member of the Critical Information Infrastructure Protection Interagency Working Group, which is responsible for coordinating all United States government research and development related to cybersecurity.

Prior to joining DARPA, Mr. Kozemchak served as Director of Washington operations for Pan Heuristics. During this time he was the Research Advisor to the President's Commission on Integrated Long-Term Strategy, and was appointed Task Leader for the DOD Future Security Strategy Study. Mr. Kozemchak served as Senior Analyst at

Science Applications International Corporation (SAIC) and Research Analyst at Battelle Columbus Laboratories before his term at Pan Heuristics.

Mr. Kozemchak has received a Master’s of Art degree in Engineering Science from the University of Florida, and a Master’s of Art in International Relations from Lehigh University where he was awarded a Packard Fellowship.

Herbert S. Lin

Herbert (Herb) Lin is senior scientist and senior staff officer at the Computer Science and Telecommunications Board (CSTB), National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a 1996 study on national cryptography policy (*Cryptography's Role in Securing the Information Society*), a 1991 study on the future of computer science (*Computing the Future*), a 1999 study of Defense Department systems for command, control, communications, computing, and intelligence (*Realizing the Potential of C4I: Fundamental Challenges*), a 2000 study on workforce issues in high-technology (*Building a Workforce for the Information Economy*), and a 2002 study on protecting kids from Internet pornography and sexual exploitation (*Youth, Pornography, and the Internet*). His recent projects include Frontiers at the Interface between Computing and Biology and Science & Technology for Countering Terrorism: Panel on Information Technology.

Prior to his NRC service, Dr. Lin was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He also has significant expertise in math and science education. He received his doctorate in physics from MIT. Apart from his CSTB work, he is the author of numerous publications on cognitive science, science education, biophysics, and arms control and defense policy.

Steve Lukasik

Dr. Lukasik received a B.S. in physics from Rensselaer Polytechnic Institute and a Ph.D. in physics from the Massachusetts Institute of Technology. His early research at Stevens Institute of Technology was on the physics of fluids and plasmas. While a member of the Department of Defense Advanced Research Projects Agency (ARPA), he was responsible for research in support of nuclear test ban negotiations and subsequently served from 1967–1974 as Deputy Director and Director of the Agency. Later government service was as Chief Scientist of the Federal Communications Commission, 1979–1982. Dr. Lukasik has been Vice President and Manager of the Systems Development Division at the Xerox Corporation, Vice President for National Security Research and Chief Scientist at the RAND Corporation, Vice President and Manager of the Northrop Research and Technology Center, Corporate Vice President for Technology at Northrop, and Vice President for Technology at the TRW Space and Defense Sector.

He has served on numerous advisory committees of the federal government, several universities, and the National Research Council. He is a founder of the Software Productivity Consortium and Chairman of its Board of Directors in 1988.

Dr. Lukasik's current work on terrorism includes consideration of terrorist behavior, terrorist tactics, terrorist organization, and the design of systems for countering terrorist attacks to include the interaction of attackers and defenders in their mutual adaptation to each others' actions. Central to this work is the construction of detailed scenarios and attack plans that enable one to exercise vulnerability analyses, risk management, and asset allocation models from both the offense and defense perspectives.

He is a member of the International Institute for Strategic Studies, the American Physical Society, and the American Association for the Advancement of Science. Dr Lukasik was awarded the Department of Defense Distinguished Service Medal in 1973 and 1974, and a D. Eng. (Hon.) from Stevens Institute of Technology. He is a founder of *The Information Society: An International Journal*, and a member of the Board of Trustees of Harvey Mudd College.

Benoît Morel

Benoît Morel is senior lecturer jointly in the Department of Engineering and Public Policy, and Department of Physics at Carnegie Mellon University. Dr. Morel's research interests include high technology, biotechnology, information technology, and their impact on security and the economy; and mathematical modeling for policy analysis (complex systems, stochastic processes).

Since earning his Ph.D., Dr. Morel has held appointments in physics at Harvard University as a Post-Doctoral Fellow, at CERN and University of Geneva, and at California Institute of Technology. After attending Caltech, he went to Stanford as a Science Fellow in arms control where he pursued research in the security implications and the technology of anti-ballistic missile defense.

Dr. Morel joined the faculty at Carnegie Mellon University in 1987 in the Department of Engineering and Public Policy, with the Program on International Peace and Security. At Carnegie Mellon, his research interests have focused on military high technology, its technical details and structure, and its impact on security and arms control, as well as its effects on American defense policy.

Dr. Morel is also interested in non-linear dynamic models, and the study of complex systems and chaos, with application to a variety of areas, such as immunology, fluid mechanics, organization theory, economics, pollution, and environment. Dr. Morel received his Baccalaureat in Physics, Diplome de Physique in Physics, and Ph.D. in theoretical high energy physics) at the University of Geneva, Switzerland.

Anthony Rutkowski

Anthony Rutkowski is Currently the Vice-President for Regulatory Affairs within the Communication Services Division at Verisign, Inc - the leading global provider of trusted infrastructure and identity services for the Internet, telecommunications, and ECommerce sectors. A highly visible and well-known global enterprise strategist, public official, organization leader, consultant, lecturer, and author in both the Internet and telecom worlds - with a career spanning 40 years of diverse positions in the business, public, and education sectors, in many different facets of the computer networking, telecom, publishing, and mass media industries, domestically and internationally. This includes employment with: General Magic, Sprint International, Horizon House, Pan American Engineering, General Electric, Evening News Association, the Federal Communications Commission, the International Telecommunication Union, Cape Canaveral City Council, Internet Society, MIT, and NY Law School, as well as consulting with NGI Associates.

He is an engineer-lawyer who extensively uses and innovates with many of these technologies; and developed a career of following strategically important developments and turning them into business opportunities.

He currently serves President of the Global LI Industry Forum and participates in numerous Lawful Access and Interception forums. He also participates on the advisory boards for *Telecommunications Policy* and *Info* magazines.

Over recent years he has participated in such diverse activities a Guest Editor of the IEEE Internet Computing special Millennium Edition, co-producer of the Global Next Generation Internet Conference, and a columnist for *Communications Week International;* co-founded diverse international organizations: Internet Law and Policy Forum (founding member), and has participated in Internet projects preparing reports by the Aspen Institute, the Rand Corp, the International World Wide Web Conference Committee (Board), Register of Copyrights, the President's Framework for Global Electronic Commerce task force, and the Harvard Kennedy School GII Project. Featured twice in the Washington Post, and listed in the 1996 roundup issue of Inter@ctive Week as one the 25 "Driving Forces of Cyberspace," and recognized at the White House in the USA. and internationally for analyzing and shaping the global commercial, public policy, legal, economic, and societal directions.

Abraham D. Sofaer

Abraham D. Sofaer, who served as legal adviser to the U.S. Department of State from 1985 to 1990, was appointed the first George P. Shultz Distinguished Scholar and Senior Fellow at the Hoover Institution in 1994. Professor Sofaer's work has focused on issues related to international law, terrorism, diplomacy, national security, the Middle East conflict, and water resources. During his distinguished career, Sofaer has been a prosecutor, legal educator, judge, government official, and attorney in private practice.

From 1985 to 1990, Professor Sofaer was legal adviser to the U.S. Department of State. His tenure at the State Department followed previous appointments as U.S. district judge in the Southern District of New York, and as professor of law at Columbia University School of Law. Prior to these appointments, Professor Sofaer served as New York state administrative judge, assistant U.S. attorney in the Southern District of New York, and clerk to Judge J. Skelly Wright on the U.S. Court of Appeals in Washington, D.C., and to the Honorable William J. Brennan Jr., associate justice of the U.S. Supreme Court from 1965 to 1967. After leaving the Department of State, he practiced law at Hughes, Hubbard and Reed.

Mr. Sofaer was co-editor with Seymour Goodman of a volume of essays dealing with the transnational dimension of cyber crime and terrorism, based on a conference on that subject which they co-chaired at Stanford University. The volume includes a proposed multilateral treaty.

A veteran of the U.S. Air Force, Professor Sofaer received an LL.B. degree from New York University School of Law. He holds a B.A. in history from Yeshiva College (1962). He was awarded the degree Doctor of Laws, *honoris causa*, in 1980 by Yeshiva University.

Organizational affiliations for participants in the Workshop on Exploring the International Dimensions of Cybersecurity are provided for identification purposes only. None of the participants officially represent any organization at the workshop. This workshop is a not for attribution meeting.