

Remarks by Michele G. Markoff Senior Coordinator for International Critical Infrastructure Protection Policy, U.S. Department of State To the Committee on Hemispheric Security of the Organization of American States

December 3, 2002

INTRODUCTION

I would like to thank the committee for the opportunity to speak today.

Ensuring the safety of networked information systems, what we call cyber security, is a high priority for the U.S. As nations become increasingly reliant on information systems for every aspect of their daily life, it will be an issue of concern for all.

Critical telecommunications and energy distribution systems depend on information networks. The Internet is opening markets for small businesses that never dreamed of selling outside their own countries, and e-government initiatives offer the promise of reliable and swift means of interaction between citizens and their governments.

I am here today because the U.S. is concerned that the benefits this technology can bring may never be realized as the reliability and security of these systems are increasingly threatened. Every day brings a new story of software vulnerabilities that are exploited by someone, resulting in loss of time and money.

The U. S. has concluded that, no matter what steps individual states might take to safeguard their own critical information infrastructures, none of us will be secure until the least secure nation to which we are connected, has also addressed the issue. I have asked to speak to you today because the U.S. wants to ensure that together this hemisphere takes those cooperative steps necessary to secure the critical information systems on which we rely.

OUTLINE

First, I would to offer our view of the threats to these systems and how the U.S. is trying to address them. Then, I want to outline some of the international dimensions of the issue. Finally, I want to offer some ideas on what we may do together in the OAS to enhance our preparedness to deal with this problem.

THREATS

Many focus their attention on the source of the threat. And while it is important that we be able to stop the perpetrators of cyber attacks whoever they may be, from the point of view of defending against them, it is not necessary to differentiate between attacks by terrorists, criminals, or teenagers getting their kicks. Regardless of motivation, these attackers use the same tools, exploit the same vulnerabilities, and cause similar sorts of damage. Most importantly, these attacks require the same defensive measures to prevent.

I would like to use a few examples to highlight this point and also the international dimensions of the problem we face.

- In 1998, the United States wake-up call to the national security dimensions of the cyberspace threat was an incident eventually called "Solar Sunrise." During this event, U.S. military systems were under electronic assault, apparently by someone on a computer in the United Arab Emirates.
- Being attacked were unclassified logistics, administrative, and accounting systems essential to the management and deployment of military forces. These were being penetrated at the same moment that we were contemplating military action against Iraq due to its failure to comply with UN inspection teams trying to uncover evidence of its weapons of mass destruction programs. The timing of the attacks raised suspicions that this was the first wave of a major cyber attack by a hostile nation.
- As it turned out, two teenagers from California, under the direction of a sophisticated Israeli hacker, also a teenager had orchestrated the attacks using hacker tools readily available on the Internet. They had tried to hide their involvement by routing their attack through computers in a variety of countries.
- The technical problem is such that if something like this happened again today, almost five years later, we would still not likely know in any timely way whether this was a prank perpetrated by teenagers or a concerted attempt by Iraq designed to forestall a potential U. S. attack.

In another incident in early February, 2000, computer servers hosting several of the largest commercial websites on the Internet were flooded with connection requests, overwhelming systems. These so-called "distributed denial-of-service attacks" paralyzed parts of the Internet.

- Only through close cooperation between the U.S. and Canadian law enforcement investigators was it discovered that a Canadian teenager, operating under the Internet name "Mafiaboy," had been breaking into legions of computers around the world for many months.
- After he broke in, he arranged to retain control over these compromised servers, creating a "zombie army" which on his command would flood the servers of his next corporate victim. The slowdowns and outages that occurred resulted in more than an estimated \$1 billion in economic losses.

I would also remind you of the May 4, 2000 "I love you" virus that infected computers around the globe. First detected in Asia, this virus quickly swept the globe in a wave of indiscriminate attacks on government and private sector networks. By the time the destructive pace of the virus had been slowed, it had infected nearly 60 million computers and caused an estimated \$13 billion in damage.

- Cooperation among law enforcement authorities around the world finally led to the identification of the perpetrator, a computer science student from the Philippines. He

could be neither charged nor punished for his deeds because the Philippine criminal code at the time did not explicitly outlaw such actions.

Just over a month ago, a series of sophisticated, simultaneous distributed denial of service attacks were aimed at the thirteen "root servers" - the main computers that manage global Internet traffic.

- The attack was fairly short-lived, partially because appropriate security measures were invoked, but also because the unknown perpetrator suddenly decided to stop the attack.
- These attacks demonstrate that threats can target particularly critical nerve centers of the global information grid, and remain tremendously difficult to track. Whoever it was, had they sought to paralyze the Internet, they probably could have, and they used a well-known form of attack.

I would also note that transnational criminal groups are increasingly using information systems to support their operations. The United Nations International Narcotics Control Board issued a report last year stating that narcotics traffickers worldwide are increasingly using IT and the Internet to conduct surveillance of law enforcement, to communicate amongst them, and to facilitate the transport and sale of illegal drugs.

- In many cases, transnational crime groups have levels of cyber skills and access to technology far greater than law enforcement and security forces.

We also know from computers recovered in Afghanistan that Al Qaeda was at minimum investigating possible methodologies for cyber attack and was looking at possible targets in the United States.

- Al Qaeda operatives were visiting many of the sites that teen-aged hackers visit on the Internet - downloading tools and reading strategies for how to break into computer networks.
- Al Qaeda also conducted surveillance of the computer networks that help to run power, water, transport, and communications grids in the United States, and this reconnaissance took place from computers located half-way around the world.
- Like traditional criminal groups, Al Qaeda also utilizes the Internet for recruiting, fund raising, and communications among its cells.

We have drawn a few conclusions and related lessons from these incidents that are relevant.

- First, the tools to conduct these types of attacks are widely available to any individual or group - regardless of their motivation.
- Because tools and methods of attack are so similar across the threat spectrum (from hackers to terrorists to criminals), many of the methods of thwarting attacks are similar as well. Good computer security practices make successful attacks difficult.

- Second, cyber attacks do not respect national boundaries. In fact, perpetrators are likely to purposely route attacks through foreign countries to decrease probability of detection or prosecution if caught.
- This fact plus the increasing interconnectedness of the globe suggests that we will only be as secure as the least secure country or business to which we are - even remotely - connected. This means that everyone has a responsibility for cybersecurity.
- In addition, it suggests that attempts to track and capture perpetrators will require international cooperation on a fairly significant scale.
- Third, because most of the information infrastructures that we rely upon both for government functions and our economic well-being are in the hands of the private sector, security cannot be a government-only responsibility. A broad partnership between government and industry in all countries is required.
- Finally, because the exact interdependence of global infrastructures is highly complex, we do not have a good understanding of the potential impact of cyber attacks. Therefore, we must think of this problem in not only economic terms but also in national security terms as cascading failures can be significant enough to have national security implications.

POLICY RESPONSE

In 1998, the U.S. government issued its first directive setting a national goal of having the United States be able to protect the nation's critical infrastructures from intentional acts of sabotage.

The goal outlined in the directive was to make interruptions or manipulations of these critical infrastructures brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the country.

The order directed the government to work directly with the private sector to achieve this goal, again, recognizing that the vast majority of the infrastructures in question resided in private hands.

New structures and responsibilities were established within the United States government, including designating agencies to have responsibility for each infrastructure sector, such as energy or telecommunications.

While much of the activity focused on U. S. domestic protection, it was quickly recognized that there was an important international dimension to the problem as well that required collective action.

INTERNATIONAL COOPERATION

Directly in the aftermath of the events of 9/11, President Bush issued a new directive giving greater priority to the initiative to protect critical information infrastructures. This established the President's Critical Infrastructure Protection Board, under the chairmanship of the President's Advisor

on Cyberspace Security, Richard Clarke. The Board is an interagency governmental body that oversees policy on cyber security.

The Board and its standing Committees undertook nine critical activities:

1. Awareness raising to the private sector and state and local governments
2. Information sharing (with the private sector and among government agencies)
3. Incident coordination and crisis response
4. Recruitment, retention and training executive branch security professionals
5. Research and development
6. Law enforcement coordination with national security components
7. International information infrastructure protection
8. Legislation
9. Coordination with the Office of Homeland Security

As you are probably aware, the new Department of Homeland Security will incorporate elements of many federal agencies with responsibility for cyber security issues, although not the international portion.

The Undersecretary of State for Arms Control and International Security Affairs, John Bolton, chairs the Critical Infrastructure Protection International Affairs Committee. Mr. Bolton oversees our international efforts to take cooperative action with our friends and allies.

At the heart of our outreach strategy is a desire for international action: We want all states to take tangible steps to reduce the risk to critical national and global information infrastructures. The U.S. feels that it is particularly important that the states of the OAS demonstrate early cooperative progress in this area as a model for all regions.

- Risk reduction includes both prevention/protection efforts and incident mitigation - that is, managing consequences and getting networks back up and functioning if prevention fails.
- Risk reduction also requires early warning or prediction of imminent - threats - a goal in which international cooperation is essential.
- Risk reduction is aided by deterrence. Both to deter future attacks and to mete out justice, effective prosecution and punishment of offenses is a key element of risk reduction.

ELEMENTS OF INTERNATIONAL STRATEGY

Achieving these goals requires a multifaceted strategy. There are several critical elements to our approach, and we offer them to the OAS as a possible way forward for hemispheric cooperation.

- First, each nation should begin to examine its infrastructures, understand where its vulnerabilities lie, and establish a program to address them. From the U. S. experience, the appointment of a central coordinator capable of bringing together all the infrastructure stakeholders is essential.
- Second, each nation should review its legal code to affirm whether it effectively

criminalizes misuse of information technology, and whether rules are in place that permits transborder law enforcement cooperation.

- Third, each nation should identify or establish a national capability for 24/7 real-time tactical warning, cyber threat assessment, and mitigation in order to facilitate global information sharing.
- Fourth, each nation should promote cyber security education and awareness, fostering a "culture of security" at every level of society.
- And finally, each nation must foster a partnership with private industry, as it is they who must bear the greatest responsibility in implementing cyber security measures.

I would like to talk about each of these briefly.

LEGAL FRAMEWORKS/LAW ENFORCEMENT

The OAS has already recognized the imperative for modern legislative approaches to cybercrime, as contained in the lengthy list of recommendations made by the Third REMJA, based on those of the 1999 Group of Government Experts on Cybercrime. It remains unclear to what degree these recommendations have been implemented.

Combating the misuse of information technology requires more than criminalization. When cyber attacks are detected and investigations begin, rules and procedures that facilitate transborder law enforcement cooperation must be in place. Here in the OAS, there are models of cooperation such as those in the Inter-American Committee Against Terrorism (CICTE) and REMJA -- which can be helpful.

- CICTE has been a particularly important venue for information exchange and training cooperation. Law enforcement cooperation on cyber security could be built along similar lines or in other ways that make sense given the issue and its complexities.

In addition to cooperation, special expertise has to be developed in law enforcement communities in this area to adequately perform investigative tasks. Most law enforcement officials are simply not familiar enough with the technical aspects of conducting an investigation in cyberspace to gather evidence, and successfully prosecute cases. This shortcoming needs to be remedied.

INFORMATION SHARING

A second element of this strategy is the creation of a robust international information sharing system for tactical warning and threat assessment. If attacks can either be anticipated or detected early, and if that information can be quickly passed around the world, steps can be taken to prevent damage or at least to minimize it.

We do not have a single prescription for what this system should look like. However, we do know that traditional methods of information collection and dissemination are insufficient given the breadth of the threat and the speed with which attacks can occur. The concept is to ensure that any state connected to this information sharing system realize value from their participation - getting more information back than they put in.

In the United States, the National Infrastructure Protection Center (located in the Federal Bureau of Investigation) is the central point for collecting and disseminating this information, but we need similar points of contact in your countries.

The first step would be for each OAS member to designate or establish a capability that can share information with other national centers on a 24 hour a day, 7 day a week basis. This is not such a daunting task as it may seem. Many, if not all, of you already have a CERT (Computer Emergency Response Team) in an academic or research institution performing the technical aspects of threat assessment that could contribute to or perform such a function.

The U.S. is not seeking to burden you with expensive new bureaucracy but rather to establish an efficient system that gathers, assesses, and disseminates information swiftly enough to be of use to both governments and the private sector.

EDUCATION AND AWARENESS

A third element of this cybersecurity strategy, national education and awareness, is arguably the most important. With our increasing connectivity and our goal of universal access to information technology comes a responsibility at every level of society to adopt a "culture of security" when using and interacting with information technology and networks.

A worthwhile reference in this regard is the OECD's recently issued "Guidelines for the Security of Information Systems and Networks." These guidelines provide a common sense framework that has application from the government to business to private citizens. The U.S. recently proposed a resolution in the Second Committee of the United Nations General Assembly that summarizes these guidelines.

These guidelines emphasize that everyone has a role to play in ensuring the security of these systems, whether a government, business, or individual user regardless of whether they develop, own, provide, manage or use them.

PUBLIC-PRIVATE SECTOR PARTNERSHIP

In the U.S., little that we have proposed here would be possible to implement without the support and participation of the private sector. The reason for this is simple - the private sector owns the vast majority of the infrastructures that we are seeking to have protected.

The private sector not only owns the systems, they also own the important information about incidents - it is their systems that slow down, crash, or detect intruders. In order to stop such attacks, that information must be shared with other businesses and with governments.

In the U.S., there are many obstacles to sharing that information - some legal, some cultural, and they must be overcome through partnership, cooperation and sometimes by removing legislative barriers.

To spur private industry to partner with us on this issue, we have sought to ensure that a credible "business case" is made for investing in cyber security. This is an increasingly less difficult sell as time passes in light of the mounting financial losses due to computer down time resulting from

attacks. Each government concerned about cyber security must take the lead in engaging its private sector in a similar collaborative effort.

THE OAS AND CYBER SECURITY

Some regional and international organizations have begun to address these issues, from APEC - where some of you are very actively involved - to the United Nations.

As I noted earlier, the OAS has taken some important steps in trying to ensure that misuse of information technology is effectively criminalized. REMJA has devoted experts groups to this matter since 1999.

Many other policy areas affect elements of the cyber security problem: national security, counter-terrorism, and telecommunications, among others. The U.S. believes that other groups within the OAS, such as CICTE and CITEL, have roles to play in the development of hemispheric approaches to cyber security.

We were pleased to note that in the recent restructuring of its work program, CITEL included the issue of cyber security in the agenda for the core group covering future network technologies. This is exactly the type of involvement that we see as critical - building security into both current and future endeavors as part of a broader culture of cyber security.

It is hoped that this agenda item is an indication that OAS is prepared to work in earnest on this subject. The OAS can and should play a key role in the development of hemispheric policies and practices on cyber security. We would like to offer some ideas on how we might spur this process along.

A WAY FORWARD

Although responsibility for cyber security ultimately rests in many hands - government must play a leadership role. High-level political impetus is often necessary to bring unfamiliar players together for a new, common purpose.

For this reason, we believe that it may be useful to have the OAS General Assembly build on existing work and consider adopting a resolution setting out cyber security goals for the member states. If there were interest, the U.S. would be very happy to work with the Committee and with interested member states on this idea.

Another lesson we have learned is that cyber security is a problem now, and waiting to some future time to grapple with these issues will only leave us open to increasing peril. Therefore, we commend the work of the REMJA on cyber crime, and we would like to indicate our willingness to work with other member states to ensure the swift implementation of the recommendations that the REMJA experts group made in March 2002.

Similarly, we would urge all member states to ensure that their laws and procedures are at least as comprehensive as those in the Council of Europe Cybercrime Convention and to accede to that convention, when, as is expected, it is opened to non-Council of Europe states.

Finally, we would urge the OAS to look at plans of action adopted by other regional bodies on this issue, particularly the Asia Pacific Economic Cooperation Telecommunication Ministers' (APEC/TEL) May 2002 statement, and to work to adopt a similar plan of action with concrete work programs and deadlines for actions.

As part of this plan of action, competent bodies within the OAS, such as this group, CICTE, and REMJA, should follow CITELE's lead and add cyber security to their own supporting work plans, as appropriate.

We view this as the beginning of a dialogue with the OAS on an issue that affects us all. We stand ready to discuss this issue in greater depth in a variety of venues, such as the Third Regular Session of CICTE in January 2003, or other venues as deemed appropriate.

CONCLUSIONS

I hope that I have been able to impress upon you that the protection of our critical information infrastructures is as essential to the safety and well being of our citizens and economies as is the physical protection of government buildings, airlines, or public gathering places.

Nevertheless, cyber security is a very different national security issue than those we long have grappled with, one where every individual has an important contribution to make.

It is an issue so new that U. S. strategy on both a national and an international level continues to evolve. The White House only recently released a draft U.S. national plan for cyberspace security, designed to elicit comments and input. This strategy is intended to be a living document that will evolve as we learn more about this issue area.

What we are sure of is that national efforts alone are not enough if the rest of the world remains unprotected. We hope that we can work together in the OAS so that all the benefits promised by information technology can be realized.