Cybersecurity: Ensuring the Safety and Security of Networked Information Systems

Lincoln P. Bloomfield, Jr., Assistant Secretary for Political-Military Affairs
Remarks at the Southeastern European Cybersecurity Conference
Sofia, Bulgaria
September 8, 2003

I would like to thank the government of Bulgaria for its hospitality as co-host of this conference and for the opportunity to speak here today on a topic of great importance to the United States and to other states in this region and around the world.

Ensuring the safety and security of networked information systems, what we call cybersecurity is very important to the United States. Our national critical infrastructures – power grids, water systems, and telecommunications networks – all depend on information networks. The smooth and reliable functioning of these systems is essential to the day-to-day well being of our citizens and to the ability of my government to perform its duties. As each of our nations becomes more reliant on information systems for every aspect of daily life, their reliability, and therefore their security, will be an ever-greater priority for all of us.

The “information society” is spreading globally, and it brings many benefits. The Internet is opening markets for small businesses that never had any possibility 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. In fact, I understand that Minister for State Administration Kalchev recently announced that Bulgaria will team with IBM to build the country’s e-government initiative.

At the same time as we are increasing our reliance on information technology for critical services, we are seriously concerned that the reliability and availability of these systems is threatened on a daily basis. Every day brings another story of a system vulnerability being criminally exploited, resulting in downtime and economic losses. If these vulnerabilities were to be exploited systematically by hostile individuals or terrorist groups, our national security could be threatened.

The United States 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 among us has addressed the issue. This technology gives us a shared opportunity, but also a shared vulnerability and a shared responsibility.

I am here today because the United States wants to ensure that the states in Southeastern Europe take the steps necessary to secure their national critical information systems and thereby enhance their security and that of the global information networks on which we all rely.

First, I will describe the threats to these systems and how the U.S. is trying to address them. Then, I will speak about the international dimensions of the issue. Finally, I will offer my government’s thoughts on what the states in this region can do to enhance their preparedness to deal with this problem.

THREATS

When we speak of threats, many focus their attention on the source of the threat. We certainly need to try to stop the perpetrators of cyber attacks, whoever they may be. However, in one respect, it makes no difference whether the source of an attack is a terrorist, criminal, or teenager playing pranks. All these attackers tend to use the same tools, exploit the same vulnerabilities, and even cause similar damage. Most importantly, these attacks require the same defensive measures to prevent.

I would like to cite a few examples to highlight this point and the international dimensions of this problem.

Our first major exposure to the national security dimensions of the cyberspace threat was an incident in 1998 that came to be known as “Solar Sunrise.” During this event, U.S. military systems were under electronic assault, apparently by someone using a computer in the United Arab Emirates.

The attack was against unclassified logistics, administrative, and accounting systems essential to the management and deployment of U.S. military forces. These systems were being penetrated at the same moment that the U.S. and several other governments were contemplating military action against Iraq due to its failure to comply with UN resolutions. The timing of the cyber attacks raised our suspicions that this might be the first wave of an attack on the U.S. by a hostile nation.

As it turned out, two teenagers from California, under the direction of a third individual, a sophisticated Israeli hacker, 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 several countries.

It is technically very difficult to identify the origin of electronic attack. If something like this happened again today, almost five years later, I suspect we would still not know in any timely way whether this was a prank perpetrated by teenagers or a deliberate attack by a hostile country intended to impair our military operations.

We all remember the May 4, 2000, “I love you” virus that infected computers around the globe. This virus began in Asia and quickly traveled around the world, attacking government and private sector networks. By the time the virus had been slowed, it had infected nearly 60 million computers and caused an estimated $13 billion in damage and economic losses.

That virus led to unprecedented law enforcement cooperation around the world, and we found the perpetrator, a computer science student from the Philippines. He could be neither charged nor punished for his deeds, because at that time, creating computer viruses was not a crime under Philippine law.

Today, we find transnational criminal groups 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 computers and the Internet to conduct surveillance of law enforcement, to communicate, and to arrange the transport and sale of illegal drugs.

We already know that terrorist groups use computers, email, and the Internet to coordinate their activities. We learned from computers recovered in Afghanistan that Al Qaeda was investigating possible methods of cyber attack and was conducting surveillance of critical infrastructure sites in the United States including the computer networks that help to operate our power, water, transportation and communications systems.

From all these developments, we have drawn some conclusions:

- First, the tools to conduct cyber attacks are widely available to any person or group – regardless of their motivation. And because the methods of attack are so similar regardless of the attacker, the methods of defending against cyber attacks are similar as well. Good computer security practices are helpful against all these types of attackers.

- Second, cyber attacks pay no attention to national boundaries. In fact, perpetrators are likely to route attacks through several countries to decrease the probability of being caught. That is why our cybersecurity depends on the security practices of every country, every business, and every citizen to which we are connected. It is also why we all depend on effective international law enforcement cooperation on a very wide scale, if we are to find and capture perpetrators. As with terrorism, there must be no safe-havens.

- Third, because most of the information infrastructures that we rely upon, even for many government functions, are in the private sector, security cannot be achieved by governments alone. We need a broad partnership between government and industry in all of our countries.

- Finally, what we have learned is that this problem is both an economic threat and a national security threat.

POLICY RESPONSE

Now, the question is, what to do about it. In 1998, the U.S. Government issued a directive setting a new goal of protecting our nation’s critical infrastructures from intentional acts of sabotage. The objective was to ensure that any

interruptions or manipulations of these critical infrastructures would be brief, infrequent, manageable, geographically isolated and thus minimally damaging to our country.

The order directed the government to work directly with the private sector to achieve this goal. New offices and responsibilities were established within our government, and agencies were given responsibility for protecting each infrastructure sector, such as energy or telecommunications.

While the initial focus was protecting infrastructure within the U.S., it soon became clear that there was an important international dimension to the problem, one that required cooperation and joint approaches with other countries.

Soon after 9/11, President Bush issued a new directive assigning a high priority o the protection of critical information infrastructures. A Critical Infrastructure Protection Board was established by the President to oversee policy on cybersecurity. We are very fortunate to have with us here this morning the former chairman of that board, Howard Schmidt, who will discuss how the Bush Administration addressed this challenge. The Board managed nine essential activities.

1. Raising awareness in 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 security professionals for the government;
5. Research and development;
6. Law enforcement coordination with national security offices;
7. International information infrastructure protection;
8. Legislation; and
9. Coordination of all these activities with the new Office of Homeland Security in the White House, which has since become The Department of Homeland Security.

Today, the President's CIP Board is gone. The new Department of Homeland Security has a 400-person office to manage national infrastructure protection issues. A special division will focus on cybersecurity issues. Many other government offices with cybersecurity duties have moved into this new organization.

International coordination on cybersecurity issues remains my responsibility in the State Department, but as you see here, it is an activity conducted with the full participation of all relevant U.S. departments and agencies.

ELEMENTS OF INTERNATIONAL STRATEGY

At the heart of our international strategy is one basic message: We need all states to take tangible steps to reduce the risks to critical information infrastructures around the world.

- Risk reduction means preventing and protecting against incidents. It is not enough simply to wait for networks to be disabled and to manage the consequences of these threats.

- Risk reduction means early warning and prediction of imminent threats; this is a goal we can advance greatly today and tomorrow, working together.

- And, risk reduction means deterrence. When governments work together, they will be far more successful in investigating, prosecuting and punishing those who attack our systems.

Achieving these goals requires a dedicated strategy of international cooperation. Permit me to offer my government's suggestions on how we might advance our collective cybersecurity:

- First, each nation should survey its infrastructures, determine 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 infrastructure stakeholders at the national level is essential.

- Second, each government should identify or establish a national capability for 24 hour-a-day, 7 day-a-week real-time tactical warning, cyber threat assessment, and mitigation in order to facilitate effective global information sharing on cyber threats.

- Third, each country should review its legal code to assure that it effectively criminalizes misuse of information technology and that it has in place the domestic tools to investigate and prosecute cyber crime, and rules to facilitate transborder law enforcement.

- Fourth, each nation should promote cybersecurity education and awareness, fostering a “culture of security” at every level of society.

- And finally, each government should foster a partnership with private industry, since the owners and operators of major information infrastructure are the ones who must bear the greatest responsibility in implementing cyber security measures.

I would like to talk about each of these briefly.

ORGANIZING FOR CYBERSECURITY

The lesson that we in Washington have learned from our efforts in this area over the last four years is that cybersecurity can be improved only when the entire nation participates in the solution. Each sector of the economy, whether energy, telecommunications, banking, commerce, or defense, must be mobilized to assess and understand the nature of their critical infrastructure vulnerabilities as well as their interdependencies, and to work with government on a strategy to address them.

This requires strong leadership to produce action among the many public and private entities that oversee these infrastructures. Our experience is that a national coordinating mechanism has been essential to our effort in the U.S., and I would urge all of you to consider a similar arrangement.

INFORMATION SHARING

The second element of this strategy is a robust international information sharing system for tactical warning of cyber incidents and threat assessment. We do not have a single prescription for what a tactical watch and warning system should look like. However, we do know that cyber attacks cross borders much faster than traditional military threats, so we all need new and faster warning and response mechanisms.

In the United States, the new cyber division, NCSD, will be the central point for collecting and disseminating this information. To be effective, NCSD must be connected to similar contact centers in your countries.

Our countries need to share cybersecurity information with each other on a 24-hour a day, 7-day a week basis. Many, if not all, of your countries already have a Computer Emergency Response Team, or CERT, in an academic or research institution, conducting technical threat assessments, that could contribute to or even perform such a function.

So we are not suggesting expensive new bureaucracy, but rather practical and efficient ways to gather, assess, and disseminate information swiftly for government and the private sector alike. No country will regret making this effort.

LEGAL FRAMEWORKS/LAW ENFORCEMENT

The third element is the legal aspect. Damaging misuse of information technology must be made a criminal offense everywhere. My recommendation here is that you ensure that your legislation effectively covers cybercrime. In this regard, we commend to all member states the example of the laws and procedures in the Council of Europe Cybercrime Convention as a model for individual states’ legal regimes. I would ask that your governments consider acceding when, as is expected, the Convention is opened to non-Council of Europe states.

But combating cyber attacks requires more than criminalization. We need each other’s help to identify those who are guilty of such acts. That means when cyber attacks are detected and investigations begin, we will all benefit from rules and procedures that facilitate transborder law enforcement cooperation. In time, our law enforcement personnel will need to develop special technical expertise in conducting investigations in cyberspace. That is also an area for future international collaboration.

EDUCATION AND AWARENESS

A fourth element of cybersecurity, national education and awareness, may be the most important of all. With our increasing connectivity driven by the 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.

The current crop of bugs infecting the Internet is a case in point. In July, we learned about a critical vulnerability in Microsoft code that permits computers to be remotely accessed and would allow a hacker to gain control. Microsoft quickly made the repair patch available.

By early August, we had the “Blaster” worm circulating rapidly through the Internet, its speed accelerated by the vast

numbers of private unprotected computers. Within a few weeks, we had “Welchia,” which was supposed to be a “good worm” trying to fix “Blaster” effects but which created its own problems by adding access doors to infected computers. I understand that not only an American teenager, but also a Romanian young man, was arrested recently for creating a variant of this virus.

The latest worm, “Sobig F.,” capitalizing on this vulnerability, infected millions of computers and did the most damage by replicating itself and creating denials of service by choking networks with emails. This worm is set to deactivate only on Wednesday.

The frustrating reality is that this destruction could have been averted by taking advantage of the available patch and by using up-to-date anti-virus software.

In this regard, I commend to your attention the recently adopted United Nations General Assembly Resolution 57/239, “Creation of a Global Culture of Cybersecurity” and the OECD’s “Guidelines for the Security of Information Systems and Networks” on which the resolution is based. Many of the governments in this room made a substantial effort to get this UN resolution passed last fall, and for that I commend you. These documents underscore that everyone has a role to play in ensuring the security of information systems -- whether government, business, or the individual user -- regardless of whether they develop, own, provide, manage or simply use these systems. The documents provide a common sense roadmap of action.

The U.S. intends to introduce another resolution on cyber security to the UNGA this fall based on significant work undertaken within the G-8, and has proposed cybersecurity language for documents to be considered this December at the World Summit on the Information Society.

The lesson we have learned is that we can best encourage private entities and citizens to take cybersecurity seriously when we lead by example. Once the U.S. adopted sound cybersecurity practices on our government information systems and networks, private industry took greater notice, and the “culture of security” began to spread throughout the user community.

PUBLIC-PRIVATE SECTOR PARTNERSHIP

This underscores the next point, namely the indispensable role of the private sector, which owns the vast majority of the infrastructures that we are seeking to protect.

The private sector not only owns the systems, they also own the vital information about incidents – for it is their systems that slow down, crash, or detect intruders. In order to stop these attacks, that information must be shared with other businesses and with government. Indeed, my government needs to share that information with your governments, and in turn with your companies and individual users.

In the United States, we face some obstacles to sharing private sector information – some legal, some cultural – and they must be overcome through partnership, cooperation and sometimes by legislation. To encourage our industry to work with government, we have tried to present a credible “business case” for investing in cybersecurity. As time passes, and businesses suffer financial losses due to computer down time resulting from attacks, our private sector becomes more receptive to collaboration. We believe every government must engage its private sector in this kind of collaborative effort.

THE WAY FORWARD

High-level political impetus is often the best way, and maybe the only way, to bring unfamiliar players together for a new, common purpose. We hope that this meeting creates the necessary momentum for action where it is needed. We will only increase the risks by waiting. I encourage you to work together, on a regional basis, to address cybersecurity problems, particularly where there are shared infrastructures across borders.

In conclusion, I hope that I have been able to communicate the American perspective that protecting our critical information infrastructures has, in just a few short years, become as essential to the safety and well being of our citizens and our economy as the physical protection of government buildings, airlines, or public gathering places.

So we now understand that it is very important. But we also know that cybersecurity is very different from traditional national security issues. The government alone cannot ensure security — we must have partnerships within our societies and around the world. It is a new issue, and U.S. strategy on both the national and international level continues to evolve. I and the U.S. delegation here in Sofia are honored to have the chance to consult with you, compare experiences, and hopefully set a course for national, international and public-private cybersecurity cooperation that will allow our citizens to gain all the extraordinary benefits of information technology in the 21st Century.

Thank you for your kind attention.

Released on September 8, 2003