RONALD L. DICK

"THE LEGAL ASPECTS OF INFRASTRUCTURE PROTECTION"

September 5, 2001
INFOWARCON 2001, WASHINGTON, D C

Thank you very much for the kind introduction. I'm happy to be with you today to discuss the legal aspects of infrastructure protection. I'm pleased, although not at all surprised, to see this level of interest, both in terms of those who have taken the time to attend, and in terms of those who are speaking on the wide range of topics you have ahead of you. In this regard, there are a number of other representatives from the NIPC who are sitting on panels today and tomorrow and I hope that if you have an opportunity to see them you will find their sessions informative.

I suspect that the speakers and the attendees alike are here based on a common understanding that, at some level, our security is at risk. For some of us, the focus is on an individual company's information systems. For others it is on one or more segments of the national security, a concept that includes our nation's overall economic well-being.

There is no doubt that as individuals, as businesses, and as a nation as a whole, we are *increasingly* at risk if we choose to do nothing in the face of our growing infrastructure vulnerabilities. These risks are real. We don't need to wait for a catastrophe to occur—indeed we must not allow a catastrophe to occur—in order to recognize that much work needs to be done. The recent Code Red Worm demonstrates quite clearly that an individual out to harm our infrastructure can infect hundreds of thousands of computers within a matter of hours, and that he can find ready targets even when the vulnerabilities are long known, well-known, further publicized, and easily fixed.

We now must work towards solving the problems. An increasingly large number of our systems are vulnerable and interdependent. The capabilities to exploit many of these weaknesses are commonly understood and inexpensive. And, there is no shortage of people intent on taking advantage of these flaws. Sometimes they are motivated by political ideology. Sometimes by profit. Sometimes by a desire merely to show off. And sometimes they are motivated by pure hatred.

Whatever their motives, their actions are oftentimes impossible to distinguish from one another and, from a government perspective, catching criminals, terrorists, and intelligence operatives has never been more difficult than it has become in today's cyber environment. In today's environment, attacks and intrusions are often encrypted, broken into packets, and routed throughout the world, where they anonymously pass through Internet and telecommunications providers that have no obligation to keep track of how their systems are used or, more importantly, how they are misused.

If there is a single overarching legal aspect to the current infrastructure debate, one issue that bears most heavily on how the landscape will look five years from today, it is how we as a democratic society ultimately resolve the oftentimes competing interests of privacy, business, and public safety. Of these, the most difficult decision involves properly balancing our right to privacy or, in my view, simply reestablishing the traditional balance between privacy rights on one hand and the demands of public safety and national security on the other.

Americans have always recognized privacy as among the most fundamental of all human rights, especially as between people and the government. The Constitution demands that, unless there is some legitimate and compelling need, the government must not interfere with our individually held rights to speak and to associate freely. And, unless there is a similarly overriding and appropriate interest, the government must not search our persons or our property. These principles within the First and Fourth Amendments are firmly etched into our collective memory during grade school and remain part of our strongly held views of democracy forevermore as adults.

The NIPC, on behalf of each of its partner agencies, is firmly committed to the fundamental proposition that the investigation of cyber crimes and national security events must be achieved in a manner that protects the privacy rights of our citizens, which is an essential Constitutional right. We know that we can only be successful if we remain true to these core values.

However, there is reason for concern that cyber intruders are gaining the ability to remain anonymous, regardless of their impact on human life and national security, and regardless of whether the government can make a showing that it should be able to get the information necessary to catch them. Quite simply, the balance described in the Constitution, which provides the government with the capacity to protect the public, is eroding. In its place, the privacy of criminals and foreign enemies is edging towards the absolute. If we continue down this path, no identifying information will be available when the government shows up, as specifically contemplated in the Fourth Amendment, with a warrant issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

As a result of this shifting in the balance between privacy, public safety, and national security, the list of victims is growing and the world wide web is being referred to as the Wild Wild West. As time goes on, I find that more and more of the individuals I meet have firsthand knowledge of computer crime. Their own computers—not just computers of people they know—have been infected with a virus or worm, their company website has been defaced or its presence crippled by a denial of service attack, or their information systems have been infiltrated and their company's proprietary data has fallen into the hands of an unidentified intruder.

Indeed, as time passes, amongst those that actively use computers, I meet fewer and fewer organizations that have proven immune to these growing threats. And, I suspect that the people in this room, and the groups you represent, are no different. If you don't think that you or your company has ever been affected by some form of cybercrime, either you just aren't aware of it, or you are a lucky member of a rapidly narrowing class. An annual computer crime survey conducted jointly between the Computer Security Institute and the FBI bears this out. In 1996, when we asked systems administrators if anybody had gained unauthorized access to their computers, less than half, 42 percent, answered yes. Last year, when asked the same question, well over half of the respondents, a full 70 percent, answered yes. And there lies the irony to the privacy debate. Law abiding citizens are finding that their privacy is increasingly being intruded upon by criminals. Meanwhile, the criminals are gaining privacy.

I've been the Director of the NIPC for a little over eight months now, having held a number of different management positions at the Center since arriving there in 1998. I have watched it grow and develop almost from its inception. Bear in mind that, just three years ago, infrastructure protection was relatively new ground for the Federal government. President Clinton issued Presidential Decision Directive 63 in May of 1998. It was a wake up call which established a new framework for doing business. For the first time, the Federal government created an interagency entity, the National Infrastructure Protection Center—combining the United States law enforcement, military, and intelligence communities—to work directly with the private sector to achieve what many to this day say is impossible: The elimination of all vulnerabilities to our nation's critical infrastructures.

Eliminating all of these vulnerabilities, stated the President, would necessarily require "flexible, evolutionary approaches" spanning both the public and private sectors, and protecting both domestic and international security.

As flexible as we want to be, bringing together the U.S. law enforcement, military, and intelligence communities, as well as the private sector, is not as easy as you might think. But the reason has nothing to do with turf wars. In fact, I continue to be impressed by the strong sense of common purpose and dedication that is reflected day in and day out by our multi-agency partners. Rather, blending these elements together, although absolutely necessary to fulfill our infrastructure protection mission, must as a matter of law be done carefully in order to preserve the privacy rights and civil rights of all Americans.

I will start with the NIPC's integration of the military. As a matter of infrastructure protection, the military has huge equities. Its systems are targeted every day by outsiders. Not only must the military remain vigilant from an information security perspective, the military also must be prepared to respond in case a cyber attack is determined by the President and Congress to constitute an act of war. The military's staffing commitment to the NIPC, as you would imagine, is strong. Department of Defense personnel consistently make up the second largest contingent of NIPC employees, right after the FBI. Put simply, if the NIPC is not responsive to the military, the NIPC is not fulfilling its mission. And so, on a daily basis, the NIPC provides warning information to the military and coordinates with the Defense Department's Joint Task Force for Computer Network Operations. In case of a foreign threat or attack, the NIPC also stands ready to be placed in a direct support role to the Secretary of Defense.

However, there are legal limitations that we strictly adhere to while including the military in our country's domestic infrastructure protection efforts. Unlike in many other areas of the world, in the United States the military does not actively participate in civilian law enforcement. Barring extreme circumstances, the Army, Air Force, Navy, and Marines do not take to the streets bearing arms, conducting searches, or making arrests. In fact, these activities are strictly prohibited by a law dating back to 1878, known as the Posse Comitatus Act. The history of the Act is interesting. By 1878 the Civil War had been over for more than a decade, yet it took this Act of Congress to finally break up the substantial military presence that had remained throughout the South not one or two years, but thirteen years, later.

Those familiar with federal law will find it interesting and telling to know that the limitation on using the military for civilian law enforcement purposes is not found within Title 10 of the U.S. Code, which generally describes the organization and powers of the armed forces. Rather, the prohibition is found at Section 1385 of Title 18, the portion of the U.S. Code which sets forth federal criminal law. The Posse Comitatus Act remains fundamental to our concept of civil rights and due process, and is faithfully integrated into the way the NIPC operates. The Deputy Director of the NIPC is a Two Star Navy Rear Admiral. He has chain-of-command authority for almost every aspect of the NIPC's mission, he is privy to everything that goes on in the Center. But, he does not supervise or conduct domestic investigations. That function is left to law enforcement officers acting under the authority and ultimate control of the Attorney General.

And, just as there are restrictions on the domestic and international use of our military forces, there are also restrictions on how the intelligence community operates within and outside our borders. Congress created the Central Intelligence Agency in 1947 to collect intelligence through human sources and by other appropriate means. Congress also made sure, again as an express matter of federal law, that the CIA had absolutely "no police, subpoena, or law enforcement powers or internal security functions." That restriction is found in Title 50 of the United States Code. Specifically at Section 403-3, for those of you who enjoy that kind of reading.

In order to further protect our First and Fourth Amendment rights, President Reagan issued Executive Order 12,333, making it abundantly clear that the CIA and the NSA are severely restricted from collecting, retaining or disseminating information concerning United States persons. As such, CIA and NSA participation within the National Infrastructure Protection Center—which is absolutely necessary to the NIPC's success since many of the greatest threats come from abroad—is conditioned on a corresponding restriction that these personnel arrive as detailees who are generally prohibited from disclosing to their home agencies any U.S. person information they might have access to at the Center.

These restrictions do not, however, impair the NIPC's strong domestic national security focus. This is because, also pursuant to Executive Order 12,333, when acting within the United States or against a United States person abroad, the Attorney General (rather than the Director of Central Intelligence) is authorized to approve the use for intelligence purposes of any technique for which a warrant would be required if undertaken for law enforcement purposes.

It is also worth pointing out that, although most people think of the FBI solely in terms of being the nation's lead law enforcement agency, as a matter of Presidential Order the FBI is also the lead agency for coordinating and conducting foreign intelligence and counterintelligence investigations within the United States.

Now, looking at the government's infrastructure protection efforts from a legal authorities perspective, you can better see why the NIPC is housed within the Department of Justice at the FBI. Being inside the FBI gives the NIPC access to law enforcement, intelligence, counter-intelligence, and open source information that—for privacy and civil rights reasons—is unavailable in its aggregate to any other federal agency. Given that cyber intrusions cross state and international boundaries nearly at the speed of light, the NIPC relies on the FBI's ability to gather and retain information from domestic and international sources, and from both a law enforcement and an intelligence community perspective.

But, it is equally important to recognize that infrastructure protection is an issue that is bigger than any one agency or any one private sector entity. Therefore, the NIPC has developed meaningful partnerships within government, between the government and private sectors, and internationally.

As I alluded to, the NIPC management structure itself represents a broad cross section of the federal campaign to protect our infrastructures. I am from the FBI. Our deputy is a two-star Navy Rear Admiral. The chief of the NIPC's analysis section is a Senior Intelligence Officer from the CIA. We have representatives from a dozen agencies as well as three foreign partners in the Center: the United Kingdom, Canada, and Australia. Determining which agency has seniority for an infrastructure protection matter must depend on the nature of the incident or threat. The NIPC coordinates to make sure that every entity that needs the information to conduct its own mission gets it. The lead entity in charge of the U.S. government's response will depend on what the threat is. Most often different entities work on the problem simultaneously.

For example, the General Services Administration's Federal Computer Incident Response Capability "FedCIRC" works on the government network security portions of an incident while the FBI might simultaneously conduct an investigation. Many times the military also is brought in to protect its systems and may need to be prepared in case the incident is determined to be an act of war. The intelligence community, whether it is the FBI acting domestically or the CIA and NSA acting abroad, or both, might take the lead role when a matter is believed to be conducted by or on behalf of a foreign power or terrorist group.

Most often, we see simultaneous actions being undertaken by those who are responsible from an information security perspective and those who are responsible for determining attribution and determining an appropriate response to an incident.

The Security Phase and the Incident Response Phase, although distinct, are not mutually exclusive or contradictory. I have often heard people say that those who are responsible for protecting systems want simply to shut out the intruder and get on with their business, while those charged with determining attribution are more interested in keeping the intruder active on the network so they can monitor and catch him.

In practice, I have found that those systems administrators who have suffered root compromises usually have limited abilities on their own, or no ability at all, to shut out the intruder short of reinstalling their entire system from scratch . . . which they seldom will do. I have found in practice that blocking an intruder often tends only to tip him off. The intruder may be shut out from the one path the systems administrator was monitoring, but there is no reasonable assurance that the intruder hasn't by that time

already established a backdoor. Therefore, the best comfort for a system administrator is establishing attribution, making sure that the intrusions are stopped at their source, and fully understanding the extent of the compromise. Usually, similar to other crimes, identifying and stopping the criminal requires a call to law enforcement.

In this regard, I am encouraged by the fact that the NIPC has been seeing far greater private sector reporting and an increase in the voluntary sharing of network security information. As many of you already know, the NIPC and the FBI have joined forces with the private sector in an initiative called InfraGard. Today, there are 65 InfraGard chapters throughout the country, with over 1800 members nationwide. It is the most extensive government-private sector partnership for infrastructure protection in the world. And, InfraGard is getting recognized for its achievements. Just this past May, for example, the InfraGard initiative received the 2001 WorldSafe Internet Safety Award from the Safe America Foundation.

And, I am proud to note that the private sector is finally seeing some positive results in terms of the government's ability to track down and arrest cyber-criminals. Many used to think that nobody would get caught and serve any jail time for these crimes, and that only kids were committing these crimes. In fact there have been a good number of successful prosecutions, and both juveniles and adults are being held accountable.

As a matter of federal criminal law, the Computer Fraud and Abuse Act, codified at 18 U.S.C. 1030, makes it a felony for anyone to "knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer." The same statute also makes it illegal to break into somebody's computer on the Internet and obtain information. First-time offenders can be sent to prison for anywhere up to ten years, depending on what they did. And, for people who launch computer viruses and worms, there is a minimum mandatory prison sentence of six months. In other words, when they get caught and convicted they are sentenced to go to jail for no less than half a year.

A good resource if you are interested in learning more about some of those who have been arrested for computer crimes and the sentences they are serving is a website hosted by the Department of Justice at www.cybercrime.gov. Just go to that page and click on the part that refers to computer crime cases. You'll see that we are catching criminals ranging from disgruntled employees who live and work in the same towns as their victims, all the way to White Collar thieves who have preyed upon American businesses from Europe. And people are being locked up for years. Not months. Not days. Years.

In short, reporting computer crime to the government is a good idea, and increases the likelihood that you and others will not be further victimized, and that somebody will be brought to justice for violating your rights.

I will conclude my remarks by emphasizing the fact that our nation has made tremendous strides in infrastructure protection over the past three years. United States policy is to ensure that any physical or cyber disruption of the critical infrastructure should be rare, brief, limited geographically, manageable, and minimally detrimental to our economy, essential services, and national security. It is the NIPC's mission to vigorously support this policy, and to do so firmly committed to our Constitutional rights.

There is much work to be done. I am confident that each of you here today can be part of the solution. Through our combined vigilance and dedication, we will build a safer environment that will serve to protect all of our freedoms.