Center for Strategic & International Studies
Washington, DC

Cyber Attack:
The National Protection Plan and its Privacy Implications

Testimony of Frank J. Cilluffo

Deputy Director, Organized Crime Project Director,
Task Force on Information Warfare & Information Assurance
Center for Strategic & International Studies

Before the Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary

1 February 2000

Mr. Chairman, Senator Feinstein, distinguished Members of the Committee, I appreciate the opportunity to appear before you today to discuss some of the policy implications with respect to the recently released "National Plan for Information Systems Protection." I would also like to address the difficult challenge of simultaneously ensuring the security of our nation's critical infrastructures while preserving personal privacy.

I commend you for your leadership on these issues and the recognition that they extend far beyond the nation's capital. Indeed, they must be brought before the American people - and soon. Many of these issues are misunderstood and give rise to skepticism, distrust and confusion between individuals, industry and the government - the initial media accounts of the proposed Federal Intrusion Detection Network (FIDNET) to cite one example. We must encourage any initiatives aimed at advancing a meaningful dialogue between our citizens, industry, and government.

One of the advantages of working for a think tank is that *we don't have to stand where we sit,* a rare luxury for someone inside the Beltway. Another is that we are simply in the ideas business and are not responsible or held accountable for implementing our ideas.

With that in mind, I would like to make a few brief observations on:

- cyber threats in general;
- the need to strike an appropriate balance between privacy and security; and
- the "National Plan for Information Systems Protection."

The information technology revolution has given us an unrivalled, perhaps unsurpassable, lead over the rest of the world in virtually every facet of modern life. Information technology's impact on society has been profound and touches everyone, whether we examine our economy, our quality of life, or our national security. Unfortunately there is a "dark side" to this revolution. Along with the clear rewards come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders. These risks range from the national security considerations involving threats to, and vulnerabilities of, our critical infrastructures from cyber attacks and information operations, to protecting the confidentiality and integrity of our personal information such as medical records, credit histories, or even our

identities, from unauthorized use. If we do not understand these potential consequences, widespread cyber threats - once the domain of science fiction - will become a reality for us all.

Our highly complex and inter-networked environment is based on insecure foundations. It is not widely understood that the Internet's predecessor, ARPANET, was never intended to be "secure." In fact its very design schematic was based on openness - to facilitate the sharing of information between scientists and researchers.

It is also problematic that the *ability* to network has far outpaced the *ability to protect* networks. In some cases, new systems are being integrated on top of one another - hence a fail-safe system on one day becomes a loophole the next. The established cliché about the "weakest link in the chain" has never been more acute or applicable. Additionally, according the Final Report of the President's Commission on Critical Infrastructure Protection (PCCIP), it is estimated that by 2002, a worldwide population of approximately 19 million will have the skills to mount a cyber attack.

All of this interconnection leads to the origins of our problem. Modern societies are dependent upon critical infrastructures such as telecommunications, electric power, health services, banking and finance, transportation, and defense systems, to provide us with a comfortable standard of living. These systems are increasingly interdependent on one another and damage to one can potentially cascade and impact others - with single point failures being of greatest concern. To compound the problem, military and law enforcement authorities report that every month assailants make thousands of unauthorized attempts to gain access to these systems, amounting to a nearly continuous assault.

And yet, many in public life and among our citizenry remain skeptical or downright dismissive of any potential dangers. After all, it is difficult to visualize a cyber threat in the same way that we saw film clips of Hitler's legions marching across Europe, the results of Japan's attack on Pearl Harbor, or Soviet missiles on parade in Red Square. There are other problems with getting people to take these threats seriously. For example, how can you "see" a cyber threat developing? While it may be scary in the abstract, it does not easily lend itself to images of fear, making it difficult to personalize for most Americans.

Today our real assets are stored electronically, not in Fort Knox and the targets are increasingly not government and military installations, but rather public and private computer network systems. Information warfare extends the battlefield to incorporate all of society. The myth persists that the United States has not been invaded since 1812, but invasion through cyberspace is now a daily occurrence. We can no longer afford to rely on the two oceans that have historically protected our country; instead we must develop the means to mitigate risk in an electronic environment that knows no borders.

The threat spectrum ranges from "ankle biters " to nations, with currently no readily available means to discern who is committing the attack. Additionally, "smoking keyboards" are hard to find as an assailant can loop and weave from country to country in a matter of nanoseconds. Thus, an attack initiated a couple of blocks away can be made to appear to come from halfway around the world. All of this happens while law enforcement is forced to stop at jurisdictional boundaries, defined by the physical world which have no meaning in cyberspace. In essence, we have created a global village without a police department.

According to a recent public report by the Department of Defense (the National Communications System), currently at least ten countries possess offensive information warfare capabilities comparable to our own. Moreover, a 1996 Government Accounting Office (GAO) report references that approximately 120 nations have some sort of computer attack capability. The reality of this potential threat was illustrated in an article published this fall in the Liberation Army Daily; the official newspaper of the Chinese People's Liberation Army (PLA) titled "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power." In this article, the authors discuss Chinese preparations to carry out high-technology warfare over

the Internet and advocate the creation of a fourth branch of the armed services within the PLA devoted to information warfare.

Bits and bytes will never replace bullets and bombs. Conventional terrorist organizations, for example, will never abandon car bombs or pipe bombs, which have already proven highly effective, relatively low in cost and risk and still generate headline news. As a force multiplier, however, information warfare increases the lethality of the terrorist when used in concert with other more conventional means. For example, one scenario we created at CSIS involved a malcontent first detonating a conventional explosive followed up by denial of service cyber attacks on the same city's emergency communications network, thereby preventing the first responders and authorities from responding. The consequences were two-fold; it led to an increase in the number of potential casualties and sowed further psychological fear.

Is this really far-fetched? Two years ago a young man sitting behind his desktop computer thousands of miles away in Toborg, Sweden, disabled portions of the Emergency 911 system in Southern Florida. Another example of a significant infrastructure disruption occurred in 1997, when a Massachusetts teenager was charged with disabling the Federal Airline Aviation control tower for six hours at Worcester Regional Airport.

It is only a matter of time before there is a convergence between those with hostile intent and techno-savvy, where the real bad guys exploit the real good stuff. As we contemplate methods of dealing with these threats it is important to remember that our national security community and law enforcement institutions were designed and established to protect our freedom, our civil liberties and our way of life. We expect the national law enforcement agencies to protect us from criminal elements within our borders. We expect the Defense Department and the Armed Forces to protect us from external threats. We expect the nation's intelligence agencies to provide insight into the intentions and capabilities of our adversaries and to provide advance early warning of threats to us.

It would be a mistake to place our national security and law enforcement institutions in a position where they would have to compromise our precious hard-won rights or infringe upon our privacy in order to protect us. The worst possible victory granted cyber attackers would be one that destroyed these values whereby we would become less open, less tolerant and less free.

Concomitantly, we must recognize the many benefits of information technology and understand that these benefits far outweigh any risks. Thus, our policies in response to threats of any kind must not stifle the engines of innovation that drive our economy and enhance our lives. We cannot afford to over react or put up too many "virtual" or "physical walls." If we do, the adversary wins by default because our way of life has been lost.

It is possible to ensure the security of our nation's critical infrastructures without compromising civil liberties and personal privacy or locking down the Internet. Throughout history, the first obligation of the state has been to protect its citizens. Today is no exception. Information technology, while providing us many comforts and conveniences has also created for us new kinds of vulnerabilities that can be exploited. These vulnerabilities must be addressed and balanced with the civil liberties we have worked so hard to earn as a nation. It makes no sense to trample on civil liberties in order to preserve them.

Too often, the debate is framed as if security and privacy are mutually exclusive. This is simply not true. It is wrong to think of the issue as "either" "or". We must rather think of the need to incorporate both. In order to preserve the twin goals of security and privacy, we must begin with the notion of a true partnership.

For a number of years many, myself included, have criticized the current Administration for being "long on nouns and short on verbs" - a lot of talk, not a lot of action - with respect to critical infrastructure protection and related policies. A concern I know you share Mr. Chairman, especially given your amendment to the 1996 Defense Authorization Act, wherein "the President

shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national information infrastructure against strategic attacks." Four years later, we have a 200-page document ("the Plan") that begins to address some of your concerns. To their credit, the President and his team have done some good work with the Critical Infrastructure Working Group (CIWG), Executive Order 13010, the President's Commission on Critical Infrastructure Protection (PCCIP), Presidential Decision Directive 62, and Presidential Decision Directive 63, albeit most of these initiatives do not adequately address high-end national security threats to our information infrastructures, including strategic information warfare.

Overall, I think the Plan does an excellent job identifying gaps and shortfalls within the Federal government, and charting an initial course of action to address them. My major concern is that it does not do enough.

We must be willing to commit real money to tackling the problem -- after all policy without resources is rhetoric. While the President's proposed budget for FY 01 is a good start, a vast majority of the resources have already been earmarked and allocated in previous budgets. I personally believe that more money should be devoted to government-wide programs (i.e. a more robust and complete PKI infrastructure) and measures aimed at prevention and protection. While there are no protective measures that are completely effective, the 80 percent solution will be sufficient to deter most attackers by increasing the risk of detection or failure. In essence, by raising the bar higher, we would then improve our "signal to noise" ratio and be better positioned to address the more significant threats. Moreover, only through leading by example can the government realistically hope for the private sector to commit the sort of resources expected of them.

There have also been concerns that the Plan was developed behind closed doors, and that public input was not solicited through the Federal Register and other means. Many individuals and organizations, including the Congress and the owners and operators of many of the critical infrastructures within industry, could have offered valuable counsel and prevented some of the adverse publicity surrounding the Plan last summer. Nevertheless, it is encouraging that the Administration seems amenable to accept input at this point, a process that needs to be enhanced and encouraged.

With respect to infrastructure assurance, we must continue to work toward and build upon a true national plan with full representation from industry and all interested parties. We need to forge a genuine partnership between the public and private sectors. The public actions of the Critical Infrastructure Assurance Office (CIAO) are very encouraging in this respect. Specifically, the recently announced Partnership for Critical Infrastructure Security, which has brought together approximately ninety leading corporations and various federal agencies to address the problems of infrastructure assurance, is a good example of a step in the right direction.

We also need a true national debate on infrastructure assurance and we need to re-think national security strategy accordingly. It can no longer be a case of the government leading and the private sector following. In other words, Silicon Valley and the Beltway, where the sandal meets the wingtip, must stand side by side and on equal footing in addressing these issues and formulating responses.

Philosopher and New York Yankee great, Yogi Berra, once said, "The future ain't what it used to be." The best way to predict the future is to help build it. We should not have to choose between security and privacy. With a lot of hard work, we can and must, have both.

Thank you for your time. I would be pleased to try to answer any questions you may have.