Cyber-Attack: The National Protection Plan and Its Privacy Implications
November 2000

Frank J. Cilluffo
Senior Policy Analyst/Deputy Director Global Organized Crime Project at the Center for Strategic and International Studies

Frank J. Cilluffo is a Senior Policy Analyst and Deputy Director of the Global Organized Crime Project at the Center for Strategic and International Studies, where he is also chairing two multi-agency committees on homeland defense. He has coauthored and edited several works, including *Global Organized Crime: The New Empire of Evil*; *Russian Organized Crime*; and *Cybercrime, Cyberterrorism, Cyberwarfare*. In addition, Mr. Cilluffo lectures regularly to government agencies, corporate groups, and universities and has testified before U.S. Congressional committees and Presidential, Defense, and Congressional commissions on matters of terrorism, information warfare, and national security policy. He is a World Economic Forum fellow, a Council on Foreign Relations term member, and a member of the Office of the Secretary of Defense's Highlands Forum.

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. From quality of life to national security, information technology's impact on society has been profound and touches everyone. 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 threats against our critical infrastructures, to 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 fail to understand these potential consequences, major disruptions of critical infrastructure—once the domain of science fiction—will become a reality for us all.

The "Love Bug" computer virus, which blitzed many of the world's e-mail networks in a matter of hours, is the latest glimpse into what such a future may have in store. The fastest-spreading and most destructive computer virus yet unleashed, the Love Bug caused billions of dollars of damage, with estimates reaching as high as $10 billion worldwide, according to Lloyd's of London. Few were spared its effects. A majority of Fortune 500 companies were impacted, and at least 14 US federal agencies were hit by the virus, which also managed to penetrate classified systems. While actual destruction of mission-critical applications was limited, work was disrupted for millions.

The Love Bug is not the first malady of its kind to spread electronically around the globe. The virus is only one of a growing list of incidents that have disrupted cyberspace. In February 2000, we experienced a spate of distributed denial-of-service attacks that temporarily halted business at electronic commerce titans such as Amazon.com, Yahoo! and E-Trade. Two years ago, a young man sitting behind his desktop computer many thousands of miles away in Toborg, Sweden, disabled portions of the emergency 911 system in southern Florida. In 1997, a Massachusetts teenager disabled the control tower at Worcester (MA) Regional Airport for six hours. And the list goes on.

We must recognize that in each of these events, the perpetrators were not virtuoso computer programmers with large sums of money and state-of-the-art technology at their disposal, but rather relatively unsophisticated young adults operating out of their bedrooms.

The tools needed to cause cyber-havoc have become more sophisticated, easier to use and more widespread, substantially lowering the bar and making it easier to mount a cyber-attack. Thousands of websites and Internet Relay Chat programs exist, offering hacker tools, techniques, and advice. In some cases, the hacker tools and software programs are so user friendly and automated that all one has to know is how to point and click a mouse.

Taken individually, each of these events had significant, though not devastating, consequences. We must, however, ask ourselves: If young adults have been able to sow such disruption already, what could a well-funded terrorist organization or foreign military or intelligence service do?

Would we be overwhelmed by a concerted cyber-attack that simultaneously disrupted emergency 911 systems, denied service to hundreds of e-commerce websites, and released viruses or other attacks against our critical national infrastructures?[1] Our highly complex and internetworked environment is based on insecure foundations. It is seldom understood that the Internet's predecessor, ARPANET, was never intended to be "secure."[2] 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 to the final report of the President's Commission on Critical Infrastructure Protection, by 2002, a worldwide population of approximately 19 million will have the skills to mount a cyber-attack.[3]

All of this interconnection leads to the origins of our problem. Modern societies depend on 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, 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.[4]

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 aspects 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 nation-states.[5] To date, the United States has no readily available means to discern which actor 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 appear to originate from halfway around the world. All of this occurs while law enforcement is forced to stop at jurisdictional boundaries defined by the physical world that 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"), at least ten countries possess offensive information warfare capabilities comparable to our own. Moreover, a 1996 General Accounting Office report indicates that approximately 120 nations have some form of computer attack capability.[6]. The reality of this potential threat was illustrated in an article in the *Liberation Army Daily*, the official newspaper of the Chinese People's Liberation Army, titled "Bringing Internet Warfare into the Military System Is of Equal Significance with Land, Sea, and Air Power."[7] In this article, the authors discuss Chinese preparations to carry out high-technology warfare over the Internet and advocate the creation, within the People's Liberation Army, of a fourth branch of the armed services devoted to information warfare.

While it may be unlikely that any nation will turn to a full-scale information warfare attack against the United States in the near future, there is evidence that some nations are engaged in sophisticated espionage campaigns (computer network exploitation) and are mapping critical nodes and assets by doing reconnaissance on our networks. These activities can be compared to the cyber-equivalent of intelligence preparation of the battlefield.

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, are relatively low in cost and risk, and still generate headline news. As a force multiplier, however, when used in concert with other more conventional means, cyber-warfare increases the lethality of the terrorist. For example, one scenario we devised at the Center for Strategic and International Studies involved a malcontent 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 twofold: an increase in the number of potential casualties and further psychological fear.

The denial-of-service attacks and Web page defacements carried out by pro-Israeli and pro-Palestinian groups against such sites as Hezbollah's Web page or Netvision, the Internet service provider hosting the Israeli Defense Forces Web page, offer yet another dimension to the Middle East conflict. While these tactics may not be cyberterrorism in the literal sense, they clearly are forms of terrorism *in cyberspace*.

It is only a matter of time before there is a convergence between those with hostile intent and people with 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 early warning of threats to us.

William Cohen, Secretary of Defense in the Clinton Administration, suggested that "we, as a democratic society, have yet to come to grips with the tension that exists between our constitutional protection of the right to privacy with the demand that we made on the need to protect us."[8]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 overreact 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 with 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 were mutually exclusive. This is simply not true. Rather, we must think of the need to incorporate both. To preserve the twin goals of security and privacy, we must begin with the notion of a true partnership.

Many, I included, have criticized the Clinton 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. Senator Jon Kyl's Amendment to the 1996 Defense Authorization Act reflects this belief as well, stating, "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."[9] Four years later, we have a 200-page document, "The President's National Plan for Information Systems Protection," that begins to address these concerns.

To their credit, the president and his team, spearheaded by Richard Clarke, did some good work with the Critical Infrastructure Working Group, Executive Order 13010, the President's Commission on Critical Infrastructure Protection, 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 president's plan does an excellent job of 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.

In my view, a comprehensive information assurance strategy requires a three-pronged approach centered on policy, technology, and people. Underpinning this triad must be education, training, and awareness, and superseding it must be leadership. Without leadership, the entire structure crumbles, because policy priorities are sustained only if they are supported by political will and the necessary resources. "The President's National Plan for Information Systems Protection" attempts to set the outline for much the same.

We must be willing to commit real money to tackling the problem—after all, policy without resources is merely rhetoric. While the president's proposed budget for fiscal year 2001 was a good start, a vast majority of the resources had already been earmarked and allocated in previous budgets. Compounding matters, Congress is primed to fund only half the new monies requested. More money should be devoted to governmentwide programs (for example, a more robust and complete public key infrastructure) and measures aimed at prevention and protection. Arguably, too much emphasis has been placed on catching the perpetrators after the crime, rather than keeping them out in the first place. While no protective measures 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, we would improve our "signal to noise" ratio and be better positioned to address the more significant threats.

Moreover, only through leading by example, by getting its own house in order, can the government realistically hope for the private sector to commit the sort of resources expected of it. This is essential because only part of the solution lies with government.

There have also been concerns that the president's 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 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 accepting 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 are very encouraging in this respect. Specifically, the Partnership for Critical Infrastructure Security brings together more than 100 leading corporations and various federal agencies to address the problems of infrastructure assurance.

We also need a true national debate on infrastructure assurance, and we need to rethink 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."[10] 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.

Click on an end note number to return to the article.

[1] Sam Nunn and Frank Cilluffo, "Cyberthreats: Eating at Our Security," *The Atlanta Journal-Constitution*, May 21, 2000

[2] See Michael Wines, "It's Clear Now: A System Can Be Too User-Friendly," *New York Times*, Nov. 13, 1998; see also Peter Grier, "In the Beginning There Was ARPANET," *Air Force Magazine*, Jan. 1, 1997.

[3] Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures," p. 5 (Oct. 1997) (available via the Internet at http://www.pccip.ncr.gov/reportindex.html).

[4] Frank Vizard, Waging War.com, "A Hacker Attack Against NATO Spawns a War in Cyberspace," *Popular Science*, July 1999, p. 80 (discussing the number of attacks on the Pentagon and clarifying that most are not serious). See also Ron Laurenzo, "Q & A," *Defense Week*, July 19, 1999, p. 8 (interview with Captain Jim Newman, USN, noting that there were approximately 12,000 attacks on the U.S. Navy each year, but that only one half of one percent were successful in that the outsider was able to get into the system, extract data, destroy data, deny access to data, manipulate data, or insert new data).

[5] An ankle-biter is "a person who aspires to be a hacker/cracker but has very limited knowledge or skills related to Automated Information Systems. Usually associated with young teens who collect and use simple malicious programs obtained from the Internet"—SANS Institute, "NSA Glossary of Terms Used in Security and Intrusion Detection" (http://www. sans.org/newlook/resources/glossary.htm). This is different from "hacking," which is defined as "unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network."

[6] General Accounting Office, “Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,” GAO/AIMD-96-84 (May 22, 1996) (http://www.access.gpo.gov/sudocs/aces/aces160.shtml).

[7] Bill Gertz, “China Plots Winning Role in Cyberspace: Military Paper Cites Need for ‘Paralyzing’ Internet Software,” *Washington Times*, Nov. 17, 1999, p. A1.

[8] “Cohen Sketches Future of Homeland Defense,” by Jim Garamone, American Forces Press Service, Oct. 6, 2000.

[9] National Defense Authorization Act for Fiscal Year 1996: Quote taken from Subtitle E, Section 1053 http://www.fas.org/spp/starwars/congress/1995_r/h104406.htm.

[10] Yogi’s World (http://sun-tzu.iwarp.com/baseball00a.html).