



Center for Strategic & International Studies
Washington, DC

Wired World: Cyber Security and the U.S. Economy

Testimony of Frank J. Cilluffo

Co-chairman, Cyber Threats Task Force Homeland Defense Project
Center for Strategic & International Studies

Before the Joint Economic Committee of the U.S. Congress

21 June 2001

Chairman Saxton, Chairman Reed, Senator Bennett, distinguished members of the committee, I appreciate the opportunity to submit to you today, for the record, my thoughts on U.S. cyber security policy and its implications for economic security. In holding hearings on this issue, the Committee should be commended for its foresight. For too long on the cyber front, we have been focused on the "beep and squeak" issues, to the neglect of the bigger picture, incorporating the economy and beyond. By seizing this opportunity to identify gaps and shortfalls in our current policies, we are taking a significant step forward: we are paving the way for the future by laying down the outlines of a solid course of action that will remedy existing shortcomings.

This hearing is all the more timely because a new National Plan relating to the cyber arena is scheduled to issue from the executive branch at year's end. Likewise, it seems that an Executive Order (EO) on the same subject, titled "Security in the Information Age," is near completion. This EO has grown legs and is currently being circulated for comment. And, in his first National Security Presidential Decision (NSPD 1), promulgated on March 5, 2001, President Bush emphasized that national security also depends on America's opportunity to prosper in the world economy. Indeed, cyber security lies at the core of our economic prosperity, which is our "nerve center" - and President Bush and his team should be congratulated for having taken a leading role on this front.

As both Congress and the Executive consider how best to proceed in this area, we should not be afraid to wipe the slate clean and review the matter with fresh eyes. To this end, we should ask: what has worked to date? What has not? What are the gaps and shortfalls in our current policies? Though it is crucial to conduct our review with a critical eye, it is equally important to adopt a balanced viewpoint - one that appreciates both how far we have come and how far we have to go.

Fortunately, centers of excellence do exist - and we should leverage and build on them. Only now, with the requisite amount of water under the proverbial bridge, have we amassed sufficient knowledge and experience to formulate the contours of a comprehensive cyber security strategy - that is, one that encompasses prevention, preparedness and incident response, vis-à-vis the public and private sectors, as well as the interface between them.

Such a strategy would generate synergies and result in the whole amounting to more than simply the sum of the parts (which is not presently the case). Such an approach would also offer enhanced protection for the "nerve center" that is the U.S. economy.

A Brief Snapshot

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. 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.

Unfortunately, our ability to network has far outpaced our ability to protect networks. Though the myth persists that the United States has not been invaded since 1812, invasion through cyberspace is now a daily occurrence. There is no shortage of examples of our vulnerability, based on past red team exercises. Likewise, demonstrated capabilities - fortunately, without truly nefarious intent - are also in evidence. Already, we have seen a young man in Sweden disable portions of the emergency 911 system in Southern Florida, and a Massachusetts teenager disable communications to a Federal Airline Aviation control tower.

Luckily, however, we have yet to see the coupling of capabilities and intent (aside from foreign intelligence collection and surveillance), where the really bad guys exploit the real good stuff and become more techno-savvy. But, while a window of opportunity remains for us, it will not stay open forever. It is only a matter of time before the convergence of bad guys and good stuff occurs. Clearly, 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.

Against this background, we need a true national debate on infrastructure assurance and we need to re-think national security strategy - and, by extension, economic security and our nation's security - 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.

Building a Business Case

Cyber security and its implications for economic security represent twenty-first century challenges. Twentieth century approaches and institutions simply will not work. Instead, we need new organizations, novel management practices and an array of new tools. Though this is not an area where government can go it alone, it can - and must - set a good example. In fact, only through leading by example can the government realistically hope for the private sector to commit the sort of effort - in time and resources - expected of them.

But, while government is eminently well suited to do certain things, others are best left to industry to do. Put another way, just as important as identifying what government should do, is identifying what it should not do. What follows below is an attempt to put flesh on these skeletal statements in so far as they relate to cyber security and its implications for economic security.

Before proceeding to focus on sector-specific (that is, public and private) strategies, however, I would like to lay out briefly a few general guiding principles. In particular, a solid approach to critical infrastructure protection and information assurance (CIPIA) must, in my view, be centered on three "prongs," namely: policy, technology and people. Underpinning this triadic structure must be education and awareness, and superceding it must be leadership. Without leadership, the entire structure crumbles because policy priorities are only sustained if they are supported by political will and the necessary resources.

1. Government: Leading by Example

The starting point for discussion here must surely be PDD 63. Promulgated in May 1998, this Directive established a structure to protect critical infrastructure. Among other things, PDD 63 created a National Infrastructure Protection Center (NIPC); a National Infrastructure Assurance Council (NIAC); and a Critical Infrastructure Assurance Office (CIAO). Unfortunately, this Directive has proved to be long on nouns and short on verbs. Put another way, planning is everything - plans are nothing: the time has come for implementation and execution.

But planning, implementation and execution are all complicated by the fact that the government is presently organized along vertical lines - even though cyber security constitutes a cross-cutting mission. Among other things, this makes it difficult to assure accountability. Against this background, we need to streamline and re-adjust the workings of our public sector, and coordinate its constituent components so as to increase efficiency, clarify responsibilities and heighten accountability - all the while bearing in mind that outreach to the private sector is equally critical.

Recommendations for action on the public sector side follow below. They are organized topically so as to reflect the preferred three-pronged approach to CIPIA mentioned above.

(i) *Policy*

Critical to the public sector effort is having, at its apex, a single individual endowed with the requisite powers and responsibilities to make the system work. To this end, we should appoint a senior government official with clout or "teeth" - that is, an Assistant to the President for CIPIA or a Deputy National Security Adviser within the National Security Council - whose efforts would be institutionally supported. This position would be confirmed by Congress and, among other things, would be empowered to issue directives regulating the security of federal agencies' information technology and systems; and conduct audits/inspections so as to ensure government-wide (federal) civilian agency accountability in the area of cyber security. In addition to formulating and overseeing, on an annual basis, a one-year plan containing specific milestones to be met by the government, this position would also be responsible for shepherding the interagency community to develop five-year plans and RDT&E efforts.

The foregoing proposal, with its centralizing features, is intended to streamline and replace the myriad of structures that currently exist. Notably, a similar motive apparently underlies the EO that is currently being formulated. There is a good chance that the EO will establish some sort of a Board, with a Chair, with an eye towards clarifying and delineating responsibilities in the area of cyber security, and heightening accountability.

Returning to my own proposed architecture, a central office, presided over by an Assistant to the President, could be tasked with crucial operational and administrative responsibilities. For instance, it could assemble an expert review team - in effect, a "red team" of 25 to 30 people possessing requisite technical skills - with an eye toward risk mitigation. And, in conjunction with the General Accounting Office, the red team could be tasked with testing for federal government agencies' (cyber-related) vulnerabilities and with identifying best practices. In fact, I would go so far as to suggest that there ought to be required, by law, an annual test of each agency's vulnerabilities and capabilities (with the latter assessing their ability to respond to events). Further, based on the results of the annual testing process, we could derive baselines that would be applicable across the board, so as to hold all agencies subject to the same standard of account.

(ii) *Technology*

By way of illustration, a central intrusion detection center - initially directed only towards federal government operations and systems - could serve a series of critical functions:

- First and foremost, such a center could provide the government with indications and warning (I&W) of intrusion and attack.
- Second, the center could, in conjunction with its principal function, create an "infocon" system (analogous to the "defcon" warning apparatus), which would spur the taking of additional precautionary measures in response to a warning of intrusion or attack.
- Third, the center could maintain the ability to deploy an emergency response team for incident management.

- And fourth, the center could regularly disseminate software patches of known vulnerabilities throughout the federal government in non-crisis situations.

(iii) *People*

In leading by example, however, it is crucial that the government pay heed not only to its own organizational structure but also to the human side of the equation. This is where education and training come in. Here, at least two key issues arise: the cultivation of technical expertise and capability, as well as the formulation of appropriate (if not best) management practices.

My own position on education and training is quite radical: we should establish an actual discipline, at the university level, in information assurance. This would involve the creation of an actual field of study (not just a degree program) that would bring together into a cohesive whole a variety of subject areas (such as electrical engineering, computer science and information security) that are currently dealt with in piecemeal fashion. And this is more than simply an idle recommendation. Indeed, it is a matter of concern that an exceedingly high percentage of students presently pursuing studies of this sort are foreign nationals. Together with universities and industry, government could provide the impetus for an initiative of the type described. The same trio of actors could even co-fund the endeavor, with the expectation that all three would ultimately benefit from bringing the project to fruition.

From the government's perspective in particular, the aim would be to attract the best and the brightest to public service for at least a portion of their careers. Unless we succeed in doing so, in the long run, our national security will suffer. Put another way, recruitment and retention are, for the public sector, issues as pressing as education and training. Further to this point, I would suggest that we introduce reward programs that would not only lay out a promotion path but also establish recognition mechanisms that would stand alone (separately from promotion *per se*). Relatedly, pay scales for those with relatively rare but highly prized skills should be revisited and adjusted upwards. (Though President Clinton's National Plan for Information Systems Protection did speak to training and recruitment, the Plan did not address squarely the challenge of retention within the public sector).

2. The Private Sector: A Crucial New Partner

Government can - and should - also provide specific incentives to the private sector to better protect its own systems. For instance, government could act as the catalyst for the establishment of industry-wide standards for information assurance in different business sectors, and could establish liability limits against disruption of service for companies using security "best practices." Equally, tax breaks or equivalent "credits" could be accorded to companies that use certified safety products and enforce specific types of security procedures. (The mechanism for certifying the safety and effectiveness of security products should be the consensus product of a private-sector dialogue that government should facilitate).

Government could also grant relief from specific provisions of antitrust laws to companies that share information related specifically to vulnerabilities or threats. Notably, the Freedom of Information Act (FOIA) has been a significant obstacle to public-private information sharing to date because companies run the risk of having sensitive or proprietary data compromised if it is revealed to the public, and fear damage to shareholder confidence if vulnerabilities are publicly acknowledged. Fortunately, FOIA-related obstacles are now being recognized and addressed, and Senator Bennett in particular should be commended for his leadership in this area.

Furthermore, government could provide extraordinary liability relief to the private sector in the case of cyberwarfare (similar to the indemnification authorities set up in the case of destruction of commercial assets through conventional warfare). Financial relief for digital disasters would have insurance companies insuring to a certain level, with government intervening in cases of massive outages or shutdowns. Likewise, a consortium of insurance, software and hardware companies could create a pool for reinsurance purposes.

Although quantifying risk in the cyber area is difficult because of the lack of experience and actuarial data, insurance companies should be encouraged to include in their portfolios limited liability indemnification policies against cyber disruption. Here, government should be the catalyst, not the enforcer, for the creation of parameters and standards.

In addition to "incentivizing" the private sector in the ways outlined above, government should seek to solidify partnerships between the public and private sectors. Already, under the auspices of the CIAO, the Partnership for Critical Infrastructure Security has brought together hundreds of leading corporations and various federal agencies to address the problems of infrastructure assurance. This is a good example of a step in the right direction - but we need to do more.

By way of illustration, we should try to improve public-private cooperation through information sharing on: vulnerabilities, warnings of ongoing attacks or threats, hacker modus operandi, and solutions and defenses to established threats and attacks. In doing so, we should try to learn from our experience with the National Infrastructure Protection Center (NIPC). Looking to the future, we should aim to leverage the NIPC's strengths and encourage it to focus on investigations. Recent criticism of the Center is to some extent unfair because the Center was tasked from the get-go with "mission impossible." In any case, both the NIPC and the FBI which houses it, should be encouraged to focus on core competencies. At the end of the day, the NIPC, as an initiative, represents a good start - but one that must be supplemented with more robust models.

Cross-sector cooperation on information sharing is especially important because each sector has its own comparative advantage: whereas government possesses the core insights on CIP from a national security perspective, the private sector possesses the core insights on information security management. With this in mind, government should continue to assist the private sector by interacting constructively with information sharing and analysis centers (ISACs), which are sector-specific associations on the industry side, and by continuing to facilitate cyber security discussions within these various sectors (including banking and finance, telecommunications, and information technology).

Key Issues and Challenges

The suggestions above are not exhaustive, of course. And, even if it were possible to cover the field, it must be conceded that no matter how concerted our efforts are, there will be failures, whether in the public or the private realm. For this reason, reconstitution (that is, the restoration of essential systems and services) is a matter that we cannot afford to ignore. Indeed, continuity of operations and government may be the key to deterrence: if we can restore our systems and provide business continuity in relatively short order following an attack, the incentive to engage in further attacks of the same sort in future should be diminished.

Our policies in response to threats of any kind, moreover, 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. Indeed, the worst possible victory granted cyber attackers would be one that compromised our precious, hard-won rights and values, leaving our society less open, less tolerant and less free. Put another way, it simply makes no sense to infringe upon civil liberties in order to preserve them.

In particular, some seem to think that privacy, security and electronic commerce are mutually exclusive. This is just not so. The "game" is not zero-sum: we can - **and** should - ensure privacy, security and e-commerce. Indeed, I would go so far as to say that you cannot have privacy without security, and without security, e-commerce can never flourish.

Plainly, the challenges that we face are great. But we, as a nation, are up to the task. At the end of the day, it all comes down to leadership -not only in government, but in the private sector and on the part of individuals, too. Critically, the president and Congress must demonstrate political will on this matter. But that alone will not be enough. We all share responsibility for this issue and we must all muster the will, and be prepared to contribute the resources, to deal with it.

In closing, I offer the comments above in the spirit of this hearing, that is, to determine the best course of action. For the past year, I have co-chaired with Arnaud de Borchgrave a Task Force on Cyber Threats, coordinated by Sharon Cardash, as part of the Homeland Defense Project at the Center for Strategic & International Studies. This is not to say that we (CSIS) have all the answers. To the contrary, our recommendations represent just one possible course of action among many - and it is up to you, Congress, to decide, together with the executive branch, precisely which course should be pursued.

Thank you for the opportunity to share my thoughts with you today. It is with sincere regret that I offer apologies for being unable to appear before you in person. If, however, you have any questions for me, I would be delighted to answer them either in writing or in person. I look forward to working with you in future.