Are We Headed for a "Cyber-9/11?": The American in Cyberstrategy[1]

By Benoît Gagnon[2]

Abstract

In the wake of September 11, the U.S. Superpower once again became a target. This time, the attack was carried out by means of the Internet. How effective is American cyberstrategy? Examining the hacking scene in the last couple of years, it is clear that it is not an adequate response to present – and future – cyberthreats. Therefore, it is fair to say that the United States has a national security problem rather than a cybersecurity problem and to conclude that as things stand at present the American government is steering the United States toward a cyber-9/11.

"You bring me 10 hackers and within 90 days I'll bring this country to its knees"
- Jim Settle, former head of the FBI

Although the terrorist attack on the World Trade Center seems to have caught many by surprise, we now know that the American government had long ago concluded that such a terrorist act could occur. However, for many reasons, the authorities did not take suitable measures to avert these types of aggression. It was well known that terrorists could use planes to assault American society, but the US government did not take the appropriate countermeasures to prevent an attack of this nature.

We can now conclude from those attacks that terrorist organizations were strong enough to undermine a powerful state like the United States, that American hegemony can be challenged -- in a violent manner. Again, all of this was known by U.S. security agencies long before the World Trade Center collapsed.

---

[1] Paper presented at the annual International Studies Association Convention - March 20, 2004

[2] The author is a researcher at the Raoul Dandurand Chair of Strategic and Diplomatic Studies and at the Center for United States Studies. He would like to thank all the members of the Chair for their support.

The online challenge

In the wake of September 11, the U.S. Superpower once again became a target. This time, the attack was carried out by means of the Internet. The Nimda (Admin spelled backward) cyberattack, which consisted of a blend of a virus[3] and a worm[4], spread through the Internet to infect more than 86,000 computers in less than an hour.[5] Although it was not aimed specifically at the United States information grid, the attack was extremely damaging by virtue of American society's great dependence on information technology.

Once before, in 2001, Code Red, a virulent worm, infected more than 150,000 computers in 14 hours.[6] On that occasion the target was the White House. The Code Red worm led to a Distributed Denial of Service (DDoS)[7] attack against the server that hosted the White House Website.

We can draw some parallels between the pre-9/11 physical security context and the current cybersecurity environment:

- In both situations, it was known that people were working to hurt the United States in one way or another;
- In both situations, the government possessed scenarios demonstrating that an attack directed against the United States could be successful and quite damaging[8];
- In both situations, the government did not enact the right measures to handle the threats.

These points are central to our argument. If the government seems to have failed in responding to the "new threat" of terrorism, the situation seems to be repeating itself with respect to the cyberthreat. As we will show, the current American cyberstrategy is not effective in face of the cyberthreat looming in the international system. The question arises: are we heading directly toward a cyber-9/11?

---

[3] A virus is a program or a piece of code that is loaded onto a computer without the user's knowledge and causes the system to react unpredictably. Unlike a worm (see note 3), a virus cannot infect other systems without human intervention.

[4] Worms are computer programs that replicate themselves and that may contain some functionalities that will disrupt the normal use of a computer system. A worm can spread itself automatically over the Internet from one computer to the other.

[5] Government of the United States, *The National Strategy to Secure Cyberspace*, White House, 2003, p. 6.

[6] *Ibid*.

[7] A DDoS attack is one in which many compromised computer systems attack a single target, thereby causing a denial of service for users of the targeted system. The overload of requests made on the target essentially forces it to shut down, with the result that legitimate users are denied service. For more information on DDoS, see: DDoS World, *DDoS World*, (page consulted February 10, 2004), [online], URL address: http://www.ddosworld.com/

[8] For a good overview of the potentially catastrophic effects of a successful cyberattack against a country, see: Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism*, McGraw-Hill, California, 2003, 273 p.

Cyberattacks: A real threat?

In most of the literature on infowar, cyberwar and cyberterrorism, the issue of whether cyberattacks constitute a genuine national threat is a recurrent theme. While there is no consensus on the subject[9], the studies tend to show that attacks carried out by and on computers can be a real risk for states that are massive users of information technology.

The growing threat of cyberattacks against the United States appears to have been confirmed by the exercise dubbed *Eligible Receiver*. This exercise, which took place in the United States, integrated the National Security Agency (NSA) and the Department of Defense (DoD): 35 agents of the NSA were sent around the world with a couple of thousand dollars; their mission was to attack the United States information grid with tools that they could acquire legally and on the Internet. The results were impressive. As one observer remarked:

> Very few people in the Pentagon knew that the attack would occur. Several days into the computer attack, very few people in the Pentagon knew the attack was going on. By the end of the week, a small group of unclassified hackers had control of numerous significant computer systems owned by the Department of Defense throughout the world.[10]

In fact, in less than two weeks, the 35 agents took control of the 911 systems and attacked 41,000 of the 100,000 Pentagon computers.[11] From that point on, the American government began to anticipate the many possible threats lurking in cyberspace.

There are two types of scenarios. First, there are those in which a disruptive attack on information technology systems is carried out, targeting the country's economic base. Many people studying the subject have warned the authorities that a hacker could easily shut down a significant portion of the American electrical grid.[12] This type of attack could engender large-scale economic losses, such as those witnessed after the power outages in the United States and

---

[9] For example, Martin C. Libicki, one of the specialists on the topic of infowar, is quite reluctant to say that cyberweapons are effective weapons. See Martin C. Libicki, "What is Information Warfare", in Thierry Gongora and Harald von Riekhoff (dir.), *Toward a Revolution in Military Affairs?: Defense and Security at the Dawn of the Twenty-First Century*, Greenwood Press, Westport, 2000, p. 77-86.

[10] Richard Clarke, *National Coordinator for Security, Infrastructure Protection, and Counterterrorism, National Security Council*, (site consulted February 10, 2004), [online], URL address: http://www.washingtoninstitute.org/pubs/lansdowne/clarke.htm

[11] James Adams, «Virtual Defense», *Foreign Affairs*, vol. 80, no. 3, May-June 2001, p. 98-112.

[12] See Jim Krane, *Electrical Grid Vulnerable to Hackers*, (page consulted February 20, 2004), [online], URL address: http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=44445

Canada in August 2003. In other scenarios, cyberattacks are liable to become a life threatening event.[13]

The American response to the threat

For all these reasons and many more that are too involved to explain here, in 1998, the American government, under the Clinton administration, decided to issue several directives to guide key players in the US cybersecurity sector. This guide, better known as Presidential Decision Directive (PDD) 63 on the protection of American Infrastructure, paved the way for the year 2000's *National Plan for Information Systems Protection 1.0* (NPISP).[14] This was the very first foray into cyberstrategy by the American Government. It was followed, three years later, by the Bush administration's vision of cybersecurity in the *National Strategy to secure Cyberspace* (NSSC).

Problems with American cyberstrategy

We can identify six major problems at the core of the NSSC. They are:

1. Timing;
2. A weak analysis of the strategic environment;
    a. A deficient identification of the threat vector;
    b. An inadequate evaluation of the evolving technological challenge;
    c. A failure to grasp the trends in cyberattacks;
3. An inability to identify major changes in the high technology market;
4. A failure to analyze major trends in the hacking world;
5. A failure to ensure that the strategy will work efficiently within the private sector, and;
6. A lack of understanding of the citizen's role in the protection of the entire information grid.

Timing

The first major problem with the NSSC is that it was late in coming. The first American cyberstrategy was developed under the Clinton administration in 2000. Considering the fast pace of technological change, waiting three years to rethink the cyberstrategy seems excessive. As Clinton's NPISP notes:

> "An Internet Year" is a term used to mean three calendar months. Information technology is evolving so quickly, that those programs and plans adopted a year ago will likely bear little relevance to the technologies available now. […] Therefore, a continuous process is needed for reviewing the new vulnerabilities,

[13] For example we could easily imagine a hacker breaking into a hospital database and changing all the blood types of the patients registered therein. This situation would quickly create havoc, making it impossible to perform blood transfusions.

[14] Government of the United States, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0, An Invitation to Dialogue*, (site consulted February 10, 2004), [online], URL address: http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

> the new protections, and standards and recommended practices as they become available.[15]

The three-year gap between the two documents resulted in an incoherent policy.

For example, a cursory comparison of the document produced under the Clinton administration and the one written under the Bush administration reveals a lack of continuity between the two visions. While the Clinton document discussed the Joint Task Force-Computer Network Defense (JTF-CND)[16] team's role in protecting the US information grid, the Bush document does not mention it.

The lack of continuity between the two policy documents is also apparent when we consider their similarities. For example, both documents address the importance of a strong public-private partnership. The problem is that in the NSSC, the discourse on public-private sector relations is almost identical to that in the NPISP. It is as though nothing happened in the intervening period. The Bush document adopts the same starting point as the Clinton document. This lack of linkage seems to be the result of the 12 Internet years that elapsed between the publication of the first and the second cyberstrategy. The public-private relationship issue was not taken up. Apparently, it was easier to begin again from scratch.

A weak analysis of the strategic environment

The second major problem that we can point to in the current American cyberstrategy is the inadequate analysis of the strategic environment. Every strategic document must briefly examine look the security environment to identify potential threats. However, the security survey done in the NSSC seems to be completely off track in light of contemporary cyberthreats.

A mistaken multilayered approach

The first problem that arises in the strategic survey of the NSSC relates to the "area of action": the Internet. If we take a look at the official text, we can see that the United States government conceives five levels where the cyberstrategy should apply:

1. The home user/small business;
2. Large enterprises;
3. Critical sectors/infrastructures;
4. National issues and vulnerabilities;
5. Global.[17]

---

[15] *Ibid*.

[16] In April 2, 2002, the JTF-CND was renamed the JTF-CNO (Joint Task Force-Computer Network Operations). The reason for the change was that the Pentagon added an offensive capability – Computer Network Attack (CNA) - to the unit.

[17] Government of the United States, *The National Strategy to Secure Cyberspace*, *op. cit.*, p. 7-8.

However, in spite of this, the document refers primarily to "national cyberspace" or "American cyberspace". This ambiguity in the cyberstrategy text makes the rest of the analysis vague and irrelevant. It is never altogether clear to which part of cyberspace the United States Government is referring.

Further, it should be noted that the NSSC diverges from the view dominant in the literature. While the cyberstrategy document identifies five levels of operation, the text on the subject divides the information grid into four layers, namely:

1. The Critical Information Infrastructure (CII);
2. The Defense Information Infrastructure (DII);
3. The National Information Infrastructure (NII);
4. The Global Information Infrastructure (GII).[18]

Therefore, when we look at the way the environment is treated in the NSSC strategic analysis, we find evidence of confusion. There is a lack of consistency in the arguments, and the established structural framework is not respected. Moreover, the analysis is at odds with the general consensus on the subject. In sum, it failed to pinpoint precisely how and where the cyberstrategy would be effective.

There is another important point to consider: all these infrastructures are not only potential targets, but are also potential threats. A cyberattack may target any of the infrastructures, and may come from any of them too. Again, the National Strategy to secure cyberspace does not take this fact into account and does not even refer to it.

Identifying the threat vector

An additional difficulty with the NSSC is the imprecise identification of the cyberthreats that represent a risk for the US government. For example, the classification of the cyberthreat vectors undertaken by the Clinton administration, although far from perfect, came closer to grasping the nature of the threat. As the NPISP notes:

> Some attacks are the equivalent of car "joy riders", committing a felony as a thrill. Others are committed for industrial espionage, theft, revenge-seeking vandalism, or extortions. Some may be committed for intelligence collection, reconnaissance, or creation of a future attack capability. The perpetrators range from juveniles to thieves, from organized crime groups to terrorists, potentially hostile militaries, and intelligence services.[19]

[18] Mark Henych, Stephen Holmes and Charles Mesloch, "Cyber Terrorism: An Examination of the Critical Issues", *Journal of Information Warfare*, vol. 2, no. 2, 2003, p. 8.
[19] Government of the United States, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0*, *op. cit.*, p. 2.

Clearly, although the classification of potential cyberthreat vectors is limited, it does include some important elements, and it may be considered a good starting point, especially for a first cyberstrategy.

The draft of the NSSC, which was published in September 2002, moved in the same direction and pushed the analysis further by providing a more convincing classification of cyberthreats to the United States. It states:

> They range from "script kiddies" who download malicious software from the Internet to carry out the equivalent of annoying graffiti attacks in cyberspace; to hackers who merely want to demonstrate their destructive skills; to trusted "insiders" who exploit their access to computer systems to cause damage; to criminal organizations that engage in fraud, extortion, and theft in cyberspace; and to terrorists and potential enemy nation states spying on us now, and developing plans that would enable them, in a future conflict, to damage our economy and weaken or control the physical and cyber systems the United States need to fight back.[20]

If the definition of threat vectors is clear in the draft, it is less so in the final report.

Ultimately, the identification of threat vectors in the official NSSC proved inadequate. The document refers rather vaguely to "[…] individuals, criminal cartels, terrorists, or nation states."[21] when discussing who may pose a threat to the United States.

Not only does this analysis of cyberthreats diverge from the thrust of the two preceding reports, it also departs from the tenor of most of the literature dealing with the subject. Usually, cyberthreat vectors are divided into eight categories[22]:

1. State sponsored cyberthreats[23];
2. Cyberterrorism[24];
3. Cybercriminal activities;
4. Pressure groups using technologies in a violent manner to convey their messages[25];

---

[20] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace Draft*, White House, 2002, p. 4.

[21] Government of the United States, *The National Strategy to Secure Cyberspace*, *op*. *cit*., p. 27.

[22] See Andy Jones, "A Methodology for the Assessment of the Capability of Threat Agents in an Information Environment", *Journal of Information Warfare*, *loc*. *cit*., p. 53.

[23] With the introduction of the National Security Presidential Directive 16 (NSPD-16) we now know that the United States is developing cyberwarfare capabilities. We know too that other countries, such as Russia, India, and China, are attempting to develop the same type of capabilities. See: Curtis M. Hellenbrand Jr., "Is Task Force Smith Rushing To An Electronic Pearl Harbor?", *Journal of Information Warfare*, *loc*. *cit*.

[24] On this question, see Limore Yagil, *Terroristes et Internet: la cyberguerre*, Trait d'union, Montréal 2002, 231 p.

[25] This is one of the many sources of hacktivism - a blend betweem activism and hacking - that exist in the international systems tight now. On this question, see John Arquilla, David Rondfelt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute, Santa Monica, 2001, 375 p. See also: Dorothy E. Denning, *Hacktivism: An Emerging*

5. Commercial groups using cyberspying techniques to obtain information about their competitors ;
6. Hackers;
7. Disgruntled employees[26]
8. "Curious Joe"[27] or users who surf the Web and cause unintentional damage to the NII. [28]

As we can see, the official document fails to correctly identify the threat vectors. It is also mute on the issue of how these vectors can prove weaker or stronger depending on the context. Again, an examination of the literature reveals that many variables modify the gravity of a potential threat. A partial list of these variables includes:

- Resources:
  - Equipment;
  - Facilities;
  - Personnel/time;
- Technology;
- Available software;
- Knowledge;
  - Education and training;
  - Books and manuals;
  - Methods.[29]

In sum, we have a situation in which the American cyberstrategy is based on a loose enumeration of threats, to which the government is attempting to respond.

Technological challenges

The third problem with the NSSC is its failure to consider the rapid technological developments taking place in the digital world. Nowhere in the NSSC document does it appear that the government is aware of the new technologies that will radically transform the information infrastructure in coming years.

Threat to Diplomacy, (page consulted February 18, 2004), [online], URL address: http://www.afsa.org/fsj/sept00/Denning.cfm

[26] The best example of this type of threat vector comes to us from Australia. In 1999, after a water treatment plant employee was fired, he vented his anger by hacking into the computer system of the company and reversing the pumping system. He caused hundreds of thousands of liters of raw sewage to be pumped into public waterways. See: Public Safety and Emergency Preparedness Canada, *The Former Minister of National Defence*, (page consulted February 15, 2004), [online], URL address: http://www.ocipep.gc.ca/whoweare/speeches/ae_hamilton_e.asp

[27] On this point, see: Yannick Chatelain and Loïck Roche, *Hackers! Le 5e pouvoir : qui sont les pirates de l'Internet?*, Maxima, Paris, 2002, 171 p.

[28] The best example of this is the story of the AT&T technician who crashed the Internet in 1990 when he changed three lines of code in a long-distance network system. See: Dan Verton, *op. cit.*, p. 9.

[29] Andy Jones, *loc. cit.*

A good example of this is the Wi-Fi (wireless) technology that is flooding the market right now. Within a few months, more and more people will be able to access the Internet without being physically wired to an Internet access point.

In information security terms, this means that a potential hacker would no longer need to be in a contained space to launch a cyberattack. He could move freely, using homemade and low-cost equipment[30], while directing his attack on the CII, the DII, the NII or the GII. It is thus clear that this wireless trend will complicate cyberattacks in the future, making them even tougher to investigate.[31]

As noted earlier, the NSSC does not speculate on technological trends. However, the situation becomes even more dramatic when we consider the government's inability to produce a cyberstrategy that can keep pace with the evolution of high technology.[32] It is not only that current American cyberstrategy fails to address the issue of technological evolution, but also that it will take a considerable amount of time to mount an effective defense.

Key trends in the hacking world

The fourth major problem evident in the NSSC is its incapacity to size up the major trends in the hacking community. As is clear from the history of hacking, there are trends that indicate where the majority of cyberattacks come from.

While the United States was the major source of computer attacks in the period from 1970 to 1980, this was no longer the case from the end of the 1980's to the middle of the 1990's. Eastern Europe became the source of most attacks. From the end of the 1990's until today, the majority of Internet attacks were launched from South America. Since the year 2000, however, a gradual shift has been taking place. More and more attacks are coming from the Middle-East and from South Asia.[33]

Such trends are completely neglected by the NSSC, even though an understanding of them could prove most useful in developing a coherent cyberstrategy. By failing to pay attention to emerging movements in the hacking world, the American government is likely to overlook new sources of potential threats. It is thus behaving almost as it did prior to the events of September 11, 2001.

---

[30] For example, we now know that it is possible to create a strong antenna using a used package of Pringles chips. On this topic see: Rob Flickenger, *Antenna on the Cheap (er, Chip)*, (page consulted February 28, 2004), [online], URL address: http://www.oreillynet.com/cs/weblog/view/wlg/448

[31] On this topic, see: Peter Judge, *Opportunities for Wi-Fi hackers on the increase*, (page consulted February 28, 2004), [online], URL address: http://www.computerweekly.com/Article127964.htm

[32] See the point above concerning timing.

[33] On this subject, see the statistics of the mi2g at this URL address: http://mi2g.com/ See also: Mark Higgins (ed.), *Riptech Internet Security Threat Report*, Riptech, Alexendria, 2002, 37 p.

Approach to the public-private partnership

The fifth problem with the NSSC is its muddled approach to handling the relationship between the public and the private sectors. While the NSSC claims that "Public-private engagement is a key component of [the] Strategy to secure cyberspace"[34], it is obvious that this partnership is not really being built.

In theory, the public-private partnership is supposed to be organized by the National Cyberspace Security Response System (NCSRS), which will be coordinated by the Department of Homeland Security (DHS).[35] But, in reality, the lack of legislation designed to push the private sector to adopt cybersecurity measures is an obstacle to real coordination between the different partners in this structure.

"Every American who can contribute to securing part of cyberspace is encouraged to do so"[36] states the NSSC. From this it is clear that the government is acting more like a cheerleader, encouraging private entities to adopt effective information security procedures without compelling them to do so.

Expecting the private sector to regulate itself in the field of cybersecurity is a dangerous gamble. The private sector usually aims to achieve three major goals:

1. Profit;
2. Customer satisfaction;
3. Innovation.

Therefore, even if "In general, the private sector is best equipped and structured to respond to an evolving cyberthreat"[37], computer security is usually low down on the priority list. In fact, until customers demand that businesses have a secure information network, it would be surprising if companies invested massively in that area.

Given that more than 80 percent of the critical infrastructures are in the hands of the private sector, it is legitimate to ask whether the CII and the NII are at risk.[38] Private leadership in most of the United States critical nodes cannot but pose a security risk to the American information grid. Moreover, most of the systems that manage the critical infrastructures are vulnerable because they have been designed that way.[39]

---

[34] Government of the United States, *The National Strategy to Secure Cyberspace*, *op. cit.*, p. ix.
[35] *Ibid*., p. 20.
[36] *Ibid*., p. xiii.
[37] *Ibid*., p. ix.
[38] This number varies from one document to another. Usually, it is between 80 and 85 per cent. See: George W. Bush, *The Department of Homeland Security*, White House, Washington, June 2002, p. 15.
[39] See Alan S. Brown, *SCADA vs. the hackers*, (page consulted February 29, 2004), [online], URL address: http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html

Not only can the private sector be a potential target, it can also hinder cybersecurity solutions. Too often, companies that are the target of cyberattacks are not aware of it, and do not inform the authorities concerned. This is usually the result of many variables. What follows is a partial list:

- The company may not have a cybersecurity team;
- The cybersecurity team may not be proficient enough to detect cyberattacks;
- There may be no year round 24/7 surveillance of the network, which means that the intrusion/attack/digital robbery may go undetected;
- The network administrator may not give his superior any information for fear of losing his job;
- The company that is attacked may be reluctant to provide any information about it for fear that stockholders will withdraw their investments;
- The attacked company may decline to report anything to the authorities because it is afraid of revealing vital information to a third party.

These are all potential obstacles to companies divulging cybersecurity problems. The result is that cyberaggressors can exploit vulnerabilities many times over before they are repaired. Thus private entities can easily become an impediment to an efficient cyberstrategy, which is the case at present. Again, these types of problems are neglected by the NSSC.

Growing dependency

The final issue related to public-private sector partnership is the growing dependency of the government on certain sectors of the computer world. The problem posed by Microsoft's quasi-monopolistic position in the operating system (OS) market is well known. But, there is also an increasing dependency on a number of the largest cybersecurity companies. This can cause some major setbacks.

For example, in January 2003, the SQL Slammer worm struck the Internet[40], infecting thousands of computers and causing more than one billion dollars in damage around the world.[41] The problem is that Symantec – one of the major players in the cybersecurity field – withheld information about SQL Slammer.

In other words, before the attack was out of control, the company knew that this worm existed.[42] Symantec only informed its own customers, who paid roughly

[40] Michael S. Mimoso, *Update: SQL worm slows Internet; some root DNS servers down*, (page consulted February 24, 2004), [online], URL address: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci876689,00.html
[41] Robert Lemos, *Counting the cost of Slammer*, (page consulted February 29, 2004), [online], URL address: http://news.com.com/2100-1001-982955.html?tag=fd_top
[42] Michelle Delio, *What Symantec Knew But Didn't Say*, (page consulted February 24, 2004), [online], URL address: http://www.wired.com/news/infostructure/0,1377,57676,00.html

$10,000 to have access to early warning. The majority of Internet users were not informed. The outcome was a worldwide infection that caused millions of dollars in damage and recovery.

Clearly, this type of dependency on the private sector is creating problems. Once again, the NSSC nowhere states that measures should be taken to minimize this excessive reliance on the private sector in the cybersecurity field.

Citizens, the NII and the GII

The final fault that can be ascribed to the NSSC is its management of the problem of individual responsibility versus cybersecurity. The cyberstrategy states that "All users of cyberspace have some responsibility, not just for their own security, but also for the overall health of cyberspace."[43] If "[…] the security of the entire infrastructure will depend on the security of each component […]"[44], then everybody should protect their computers to guard against:

1. Being attacked;
2. Serving as a ramp for an attack on another party.

Once again, this sounds good in theory, but in practice it is difficult to attain. The cost of good antivirus/firewall software is around $100. For many home users, this is too much to pay. Consequently, the network contains many potential vulnerabilities; like a Swiss cheese, the NII and the GII are "filled with holes". The NSSC seems to have ignored the well-known observation that a chain is as strong as its weakest link…

The efficacy of American cyberstrategy

The preceding arguments lead us to the core question of this text: how effective is American cyberstrategy? Taking a cursory look at the hacking scene in the last couple of years, it is clear that this cyberstrategy isn't the response to present – and future – cyberthreats. There are three factors which lead us to conclude that the cyberstrategy is not effective.

First, there is the continuous rise of cyberattacks. The statistics of the Computer Emergency Response Team Coordination Center (CERT/CC) show that, since 2000 -– the year in when the Clinton administration issued the first cyberstrategy –- the number of cyberattacks has been constantly increasing. Cyberattacks have risen by approximately 55 per cent each year. In 2003 alone, the year in which the NSSC was initiated, the number of attacks rose by about 60 per cent.[45]

[43] Government of the United States, *The National Strategy to Secure Cyberspace*, *op*. *cit*., p. 37.
[44] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace Draft*, *op*. *cit*., p. 9.
[45] See the CERT/CC, *CERT/CC Statistics 1988-2003*, (page consulted March 1, 2004), [online], URL address: http://www.cert.org/stats/cert_stats.html#incidents

Not only is the number of cyberattacks against the NII growing, but the number of attacks launched on the DII is also a matter of concern. "Since 1995, DoD systems have been regularly attacked, up to 250,000 times a year, and only about one of every 50 attacks is detected and reported."[46] These kinds of trends make it clear that current cyberstrategy is failing to reduce the number of cyberattacks that target the United States.

Second, the so called "public-private partnership", which has supposedly been in place with the NPISP since 2000, does not appear to be helping companies to reduce the number of cyberattacks they sustain or to limit financial losses due to hacking. A recent survey conducted by the Computer Security Institutes (CSI) reveals:

> […] that 90 percent of the survey's respondents had detected security breaches in the last 12 months and 74 percent of the respondents reported that they had suffered financial loses as a result of systems penetrations.[47]

It is evident, therefore, that current American cyberstrategy is incapable of providing the private sector with a framework for securing their information networks.

The third and last factor that demonstrates the deficiency of American cyberstrategy is the United States government's repeated failure of its own cybersecurity tests. In 2000 --- again, the year in which the first American cyberstrategy appeared, the US government got a "D" in computer security. In 2001, this grade dropped to a "D-minus".[48] In 2002, it was rated a total failure with an "F". Here is a list of the grades the GAO assigned to the agencies for 2002:

- B-minus: Social Security Administration;
- C-plus: Labor Department;
- C: Nuclear Regulatory Commission;
- D-plus: Commerce Department, NASA;
- D: Education Department, General Services Administration;
- D-minus: Environmental Protection Agency, National Science Foundation, Department of Health and Human Services;
- F: Department of Agriculture, Defense, Energy, Interior, Justice, State, Housing and Urban Development, Transportation, Treasury and Veterans' Administration. Also, United States Agency for International Development,

---

[46] Colin Robinson, *Military and Cyber-Defense: Reactions to the Threat*, (page consulted February 28, 2004), [online], URL address: http://www.cdi.org/terrorism/cyberdefense.cfm

[47] Mark Henych, Stephen Holmes and Charles Mesloch, *loc*. *cit*., p. 5.

[48] Washington Post, *Timeline: The U.S. Government and Cybersecurity*, (Page consulted March 1, 2004), [online], URL address: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true

Office of Personnel Management, Small Business Administration, and the Federal Emergency Management Agency.[49]

In 2003, the situation improved and the government got a "D" in cybersecurity. We should note, however, that this improvement was largely due to the good performance of the Nuclear Regulatory Commission, the National Science Foundation, the Social Security Administration, the Labor Department, and the Veterans Affairs Department in their cybersecurity management.[50]

Except for the Nuclear Regulatory Commission, these sectors are rather remote from US national security. By contrast, the DHS got an "F" in cybersecurity.[51] When we consider how many aspects of national security the DHS deals with (intelligence, police, etc.) it is legitimate to say that the United States has a national security problem rather than a cybersecurity problem.

The NSSC states that "The federal government will lead by example, giving cybersecurity appropriate attention and care, and encouraging others to do so."[52] Clearly, this is not being done very well. Once again, this is evidence of the total failure of American cyberstrategy to attain its objective: namely, to secure the US information grid.

Why such a failure?

The question we must ask ourselves in face of this issue is why the American government has not been able to build a working cyberstrategy? The government is well aware of the cyberthreats that confront the United States and is aware of the many harsh criticisms of its poorly-designed cyberstrategy. Why, then, does it pursue the current strategy as if it were reliable?

The first major reason we can point to in the United States government's failure to implement an effective cyberstrategy is that officials do not consider the issue important. Since 9/11, the American government has tried to conduct its war on terrorism. Being thus preoccupied, it appears to have relegated cyberthreats to the bottom of the priority list.

The second reason that might explain why the American government is missing the mark with its cyberstrategy is that it tends to operate with the concept of "risk management" in mind when dealing with threats. In effect, officials try to

---

[49] Washington Post, *U.S. Government Flunks Computer Security Tests*, (page consulted March 1, 2004), [online], URL address: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A9496-2002Nov19&notFound=true See also: Robert F. Robert F. Dacey, *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, General Accounting Office, 2002, 33 p.

[50] Diane Frank, *Government gets 'D' on security*, (page consulted March 1, 2004), [online] URL address: http://www.fcw.com/fcw/articles/2003/1208/web-grades-12-09-03.asp

[51] *Ibid*.

[52] Government of the United States, *The National Strategy to Secure Cyberspace*, *op. cit.*, p. 43.

implement the right measures to settle the major security problems at the lowest cost.

The perverse effect of this vision is that it leads to a false analysis of looming threats. The administrators are persuaded that since no cyberattack has been successful in destabilizing the United States, there is no need to be overly concerned about these kinds of threats. Instead, attention must be focused on terrorism which is, of course, a clear and present danger. As stated earlier, almost the same mindset predominated in the administration before the 9/11 events: we know that it could happen, but it never has, and so there is less risk in managing it than is true of many other security issues.

The third reason is the impossibility of ascertaining the precise scope and intensity of cyberthreats. In fact, there is still no consensus on what constitutes a cyberthreat. At this point, no cybercampaign aimed at the United States has caused more than economics damage. The principal reason is that:

> Most of the hackers who exploit […] vulnerabilities lack the political motivation, resources, technical capabilities, and malicious intent of terrorists groups or hostile nations. For this reason, most cyber security incidents to date have not inflicted the maximum possible damage on compromised systems, and they rarely, if ever, have injured or killed people.[53]

In other words, the ultimate consequences of this type of aggression are hard to conceive and assess, with the result that the threat is not really known or understood.

This state of affairs points to a lack of research and development on the subject:

> Much work is currently underway in the private sector to develop new virus detection software, firewalls, and the like. But commercial research is largely focused on existing threats and near-term profit making developments. What remains sorely needed is research that can address the mid- and long-term threats and develop secure, next-generation networks.[54]

It remains difficult to evaluate the requirements of a sound cyberstrategy when the nature of the threat is not clearly grasped.

The final reason that helps to explain the shortcomings of U.S. cyberstrategy is that most U.S. officials appear to be caught up in a Cold War logic when it comes to thinking about security. The Cold War involved the confrontation of two Superpowers (two states). In relation to cyberthreats, however, the United States not only faces other states, but also individuals, terrorist groups, and so on. Cold War logic cannot contend with the new realities of the post-Cold War and post-

[53] Michael A. Vatis, "Cyber Attacks : Protecting America's Security against Digital Threats", in Arnold M. Howitt and Robyn L. Pangi (ed.), *Countering Terrorism: Dimensions of Preparedness*, MIT Press, Cambridge, 2003, p. 248-249.
[54] *Ibid*., p. 247.

9/11 eras. Indeed, by relying on this logic in the area of cyberstrategy, the United States may very well be reproducing a way of thinking about interstate relations that is limited to situations in which clear boundaries exist – a way of thinking that is ill suited to the nature of the cyberspace environment.[55]

Conclusion

As we have seen, current American cyberstrategy is not capable of responding appropriately to cyberthreats directed at the United States. The analysis carried out by the current NSSC is incapable of scoping out the existing cyberstrategy environment and is too vague to be able to keep pace with what is happening in the GII at the present time.

Moreover, it is difficult to envision the positive effects of the cyberstrategy, given that ever since the government developed its first cyberstrategy, it has failed its cybersecurity tests, and, overall, the NII does not appear to be more secure. This would tend to confirm our thesis that American cyberstrategy is not effective in face of the international system's looming cyberthreats.

Clearly, this situation is generating deep discomfort within the government. The lack of interest in the matter on the part of senior White House authorities has created frustration among those individuals who have been working on the issue. The precipitous departure of Richard Clarke and Howard Schmidt as heads of the cybersecurity office is a signal that all is not well.

Moreover, Richard Clarke has made accusations against the US government and criticized its behavior in relation to matters of cybersecurity. As he told the press in April 2003, “I would hope that with cybersecurity we can do more to raise our defenses before we have a major disaster”.[56] Yet the US government does not seem to be taking this advice seriously and is continuing in the same direction it initiated with the NSSC.

As noted earlier, this situation is similar to the pre-September 11 strategic context. The government knows a threat exists; many experts are pointing out that there is a problem, yet the government seems unmoved to find the appropriate means to respond to it. As one observer commented:

> The airplane hijackings and terrorist attacks of September 11, 2001, occurred in spite of many previous GAO (General Accounting Office) reports, new media

---

[55] See David Grondin, *(Re)Writing the 'National Security State': How and Why Realists (Re)Built The(ir) Cold War*, Paper prepared for the International Studies Association (ISA) Conference in Montreal, Canada, March 17-20, 2004.

[56] Grant Gross, *Former Bush official blasts government cybersecurity*, (page consulted March 1, 2004), [online], URL address: http://www.infoworld.com/article/03/04/08/HNcyberbush_1.html

> reports and TV exposes on lax airport security and air passenger screening. Until September 11, 2001, the airports, airline industry, and the flying public did not take the need for adequate airport security and airplane screening seriously, because a catastrophe had not yet occurred.[57]

Therefore, it is safe to say that as things stand at present the American government is steering the United States toward a cyber-9/11. It is not responding appropriately to the issues at hand and the strategic plans it is implementing are inadequate to cope with a problem that was not correctly analyzed to begin with.

Of course, solutions are not altogether easy to find. One option might be to create an independent and permanent committee of specialists to work on the subject. The group's goals could include, among others:

- Updating the cyberstrategy at least once a year;
- Suggesting rules and standards that the government should adopt to regulate industry;
- Setting up a national computer protection program that would give home users access to a low-cost antivirus/firewall program.

However, at the moment, the most important action the government can take is to step up its level of concern about the problem. The current attitude of the Bush administration toward matters of cybersecurity will prove dangerous in the long run. If we know that there is a problem with cybersecurity, it is certain that the enemies of the United States know it as well; and they are likely to exploit this weakness to once again disrupt American society.

[57] Curtis M. Hellenbrand Jr., *loc*. *cit*.

Select Bibliography

Books

ARQUILLA, John, David Rondfelt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute, Santa Monica, 2001.

CHATELAIN, Yannick and Loïck ROCHE, *Hackers! Le 5e pouvoir : qui sont les pirates de l'Internet?*, Maxima, Paris, 2002.

DACEY, Robert F., *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, General Accounting Office, 2002.

GONGORA, Thierry and Harald von RIEKHOFF (dir.), *Toward a Revolution in Military Affairs?: Defense and Security at the Dawn of the Twenty-First Century*, Greenwood Press, Westport, 2000.

Higgins, Mark (ed.), *Riptech Internet Security Threat Report*, Riptech, Alexendria, 2002.

HOWITT, Arnold M. and Robyn L. PANGI (ed.), *Countering Terrorism: Dimensions of Preparedness*, MIT Press, Cambridge, 2003.

VERTON, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism*, McGraw-Hill, California, 2003.

YAGIL, Limore, *Terroristes et Internet: la cyberguerre*, Trait d'union, Montréal 2002.

Official documents

BUSH, George W., *The Department of Homeland Security*, White House, Washington, June 2002

CERT/CC, *CERT/CC Statistics 1988-2003*, (page consulted March 1, 2004), [online], URL address: http://www.cert.org/stats/cert_stats.html#incidents

Government of the United States, *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0, An Invitation to Dialogue*, (site consulted February 10, 2004), [online], URL address: http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

Government of the United States, *The National Strategy to Secure Cyberspace*, White House, 2003.

GRONDIN, David, *(Re)Writing the 'National Security State': How and Why Realists (Re)Built The(ir) Cold War***,** Paper prepared for the International Studies Association (ISA) Conference in Montreal, Canada, March 17-20, 2004.

Public Safety and Emergency Preparedness Canada, *The Former Minister of National Defence*, (page consulted February 15, 2004), [online], URL address: http://www.ocipep.gc.ca/whoweare/speeches/ae_hamilton_e.asp

The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace Draft*, White House, 2002

Articles

ADAMS, James, "Virtual Defense", *Foreign Affairs*, vol. 80, no. 3, May-June 2001, p. 98-112.

HELLENBRAND Jr., Curtis M., "Is Task Force Smith Rushing To An Electronic Pearl Harbor?", *Journal of Information Warfare*, vol. 2, no. 2, 2003, p. 43-50.

HENYCH, Mark, Stephen Holmes and Charles Mesloch, "Cyber Terrorism: An Examination of the Critical Issues", *Journal of Information Warfare*, vol. 2, no. 2, 2003, p. 1-14.

JONES, Andy, "A Methodology for the Assessment of the Capability of Threat Agents in an Information Environment", *Journal of Information Warfare*, vol. 2, no. 2, 2003, p. 51-71.

Internet sites

BROWN, Alan S., *SCADA vs. the hackers*, (page consulted February 29, 2004), [online], URL address: http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html

CLARKE, Richard, *National Coordinator for Security, Infrastructure Protection, and Counterterrorism, National Security Council*, (site consulted February 10, 2004), [online], URL address: http://www.washingtoninstitute.org/pubs/lansdowne/clarke.htm

DDoS World, *DDoS World*, (page consulted February 10, 2004), [online], URL address: http://www.ddosworld.com/

DELIO, Michelle, *What Symantec Knew But Didn't Say*, (page consulted February 24, 2004), [online], URL address: http://www.wired.com/news/infostructure/0,1377,57676,00.html

DENNING, Dorothy E., *Hacktivism: An Emerging Threat to Diplomacy*, (page consulted February 18, 2004), [online], URL address: http://www.afsa.org/fsj/sept00/Denning.cfm

FLICKENGER, Rob, *Antenna on the Cheap (er, Chip)*, (page consulted February 28, 2004), [online], URL address: http://www.oreillynet.com/cs/weblog/view/wlg/448

FRANK, Diane, *Government gets 'D' on security*, (page consulted March 1, 2004), [online] URL address: http://www.fcw.com/fcw/articles/2003/1208/web-grades-12-09-03.asp

GROSS, Grant, *Former Bush official blasts government cybersecurity*, (page consulted March 1, 2004), [online], URL address: http://www.infoworld.com/article/03/04/08/HNcyberbush_1.html

JUDGE, Peter, *Opportunities for Wi-Fi hackers on the increase*, (page consulted February 28, 2004), [online], URL address: http://www.computerweekly.com/Article127964.htm

Krane, Jim, *Electrical Grid Vulnerable to Hackers*, (page consulted February 20, 2004), [online], URL address: http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=44445

LEMOS, Robert, *Counting the cost of Slammer*, (page consulted February 29, 2004), [online], URL address: http://news.com.com/2100-1001-982955.html?tag=fd_top

MIMOSO, Michael S., *Update: SQL worm slows Internet; some root DNS servers down*, (page consulted February 24, 2004), [online], URL address: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci876689,00.html

ROBINSON, Colin, *Military and Cyber-Defense: Reactions to the Threat*, (page consulted February 28, 2004), [online], URL address: http://www.cdi.org/terrorism/cyberdefense.cfm

Washington Post, *Timeline: The U.S. Government and Cybersecurity*, (Page consulted March 1, 2004), [online], URL address: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50606-2002Jun26&notFound=true

Washington Post, *U.S. Government Flunks Computer Security Tests*, (page consulted March 1, 2004), [online], URL address: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A9496-2002Nov19&notFound=true