

## The Next Battlefield

### The Reality of Virtual Threats

From [\*Global Catastrophe\*](#), Vol. 28 (3) - Fall 2006

**Michael Vatis** is currently a partner in the law firm Steptoe & Johnson LLP. He served as Executive Director of the Markle Foundation Task Force on National Security in the Information Age. From 2001 to 2003, he was the Director of the Institute for Security Technology Studies at Dartmouth College.

In today's increasingly interconnected world, a person with a laptop computer can sit at a coffee shop in London and trade stocks listed on the New York Stock Exchange, transfer funds from a bank account in Zurich to an account in Tokyo, chat on an Internet phone call with a friend in Estonia, check in on his child's daycare center through a live video feed, upload a video clip of his brother's stand-up comedy performance onto YouTube, and place a bet with an online casino in Costa Rica. Such are the conveniences of today's communications technology.

But if that same person were more maliciously inclined, he might hack into the stock exchange and alter share price information to send a target company into a downward spiral, use a stolen identity to pilfer funds from a victim's savings account, use a pseudonymous email address and encryption technology to send secret information to his spy handler, or upload to a jihadi website a video of Osama Bin Laden calling for a new wave of attacks against the United States. The only constraints on his capacity to do harm are his level of technological sophistication, the defenses put in place by his intended targets, and governments' capabilities to learn about his activities and stop them.

### A New Weapon

A decade ago, when the World Wide Web was still in its infancy, the scenarios just posited would have been derided as alarmist. If it was a person from the information technology industry speaking, he would have been accused of scaring people into buying new security tools. If it was a policy wonk, he would have been accused of not understanding the robust and resilient nature of Internet technology. And if it was a government official, he would have been accused of searching for a new mission—or new reasons for government funding—in the post-Cold War world.

Today skepticism about the cyber threat is more difficult to find. Government agencies, companies, and individuals are all too aware of the harm that computer viruses and hackers can cause. The problem now is not so much recognizing vulnerability to computer-based threats as understanding just what those threats are and what should be

done to stop them. One year the main concern seems to be teenage hackers defacing websites or breaking into computer networks for the thrill of causing a disruption; the next year the primary concern is fast-spreading viruses that shut down corporate networks for a few hours or even days; and the next it is international criminal groups stealing and selling credit card and social security numbers.

While the public face of the cyber threat changes frequently, there is an abiding spectrum of threats that is far broader, and far more dangerous, than is typically appreciated. While citizens today are fearful of identity theft and the US government is focused on preventing a full-scale civil war in Iraq and avoiding another Hurricane Katrina catastrophe, the United States' current and potential adversaries—whether radical Islamic terrorists, Iran, or China—are looking for the weaknesses in the US information infrastructure and mapping out where and how they would mount a cyber attack.

## **Re-learning the Lessons of September 11**

The terrorist attacks of September 11, 2001, demonstrated all too clearly the vulnerability of the United States to foreign attack. Once comfortable with its physical distance from the ancient quarrels that plague the rest of the world, the United States became aware that its relatively open borders, democratic liberties, and modern technology could be turned against it to devastating effect. Since September 11, the US government has focused on measures to prevent similar attacks—strengthening airport security, hardening cockpit doors, and putting air marshals on commercial flights.

Far less attention has been devoted to other forms of attack, some of which could be even more destructive than the September 11 attacks. These include attacks using nuclear, radiological, chemical, and biological weapons. They also include physical attacks on soft targets such as subways and railroads, chemical plants, or hotels and office buildings. In addition, the United States remains highly vulnerable to cyber attacks against computer networks that are critical to its national and economic security.

Cyber attacks generally consist of directed intrusions into computer networks to steal or alter information or damage the system; malicious code, known as viruses or worms, that propagates from computer to computer and disrupts their functionality; or denial of service attacks that bombard networks with bogus communications so that they cannot function properly.

Using these methods, cyber attackers could target financial institutions, communication systems, energy infrastructures, government operations, hospitals, and many other entities that rely on computer networks for their basic operation. Cyber attacks are no longer a mere nuisance that concerns only computer geeks. Attackers could disrupt the basic engines of the US economy, affecting individuals across the country and national security as a whole. The international ripple effects of such a disruption would be serious and wide-ranging.

The growing complexity and interconnectedness of these infrastructure systems, and their reliance on computers, not only makes them more vulnerable to attack but also increases the potential scope of an attack's effects. An attack that disables electrical power or telecommunications, for instance, would have cascading effects on banks, hospitals, and government operations. While many organizations have developed redundant or alternative systems, such as power generators or back-up communications systems, many have not. Further, the alternative systems typically provide only limited capabilities.

The majority of critical infrastructures in the United States are owned by private industries. As a result, the US government alone cannot defend the infrastructures from attack but needs the cooperation of the private sector. A central question is how to obtain that cooperation and avoid the inevitable free-rider problem. The CEO of a bank, for example, may ensure that her bank takes steps to prevent the common sorts of cyber crime aimed at stealing funds from account holders. She might question, however, why she should pay for additional measures that might be necessary to prevent a catastrophic attack that could have effects that spread beyond her company to other financial institutions and other parts of the economy. This is particularly true if the bank's competitors, or service providers, are not taking such measures.

## **The Challenge of Cyber Attacks**

The global nature of the Internet and telecommunications networks means that cyber attacks can be launched from anywhere in the world, at low cost, and with incredible speed. With current technology, it is nearly impossible to predict in advance when an attack may begin. There is no longer the luxury of the 20-minute window from launch to landing of a nuclear-tipped intercontinental ballistic missile found in the Cold War. Cyber attacks therefore require swift responses and effective cooperation with international counterparts to detect and respond to an attack after it is underway.

Because cyber attacks are easy and cheap to carry out—requiring only a laptop and an Internet connection—the barrier to entry is low. That means almost anyone with a modicum of technological sophistication can carry out some form of attack—ranging from teenage hackers and virus writers to terrorist groups and nation-states. The capability of an attacker to cause damage depends mainly on his level of technological skill and the defenses implemented by his chosen target.

The motivations for attack can vary widely: attackers range from hackers bent on proving their skills to others in the hacking community, to criminals stealing credit card numbers, to extortion rings, to foreign intelligence services stealing military secrets, to terrorists or foreign armies wanting to cause widespread damage to the US economy and its capacity to project military power abroad.

The press and the general public have typically focused their attention on the most common, or at least the most visible, forms of cyber attacks. In the early and mid-1990s, that normally meant teenagers who broke into computers or defaced websites for “bragging rights” in the hacker community. In the late 1990s, virus writers unleashed

fast-spreading viruses that temporarily disrupted corporate networks and personal computers, earning front-page headlines. Today, the focus is on identity thieves, some of whom break into the computers of universities, merchants, and other entities to steal credit card numbers, bank account information, and other useful personal information.

While these types of crimes are serious, they pale in comparison to the attacks that terrorists or foreign nation states could execute.

## **Cyber Terrorism**

People often use the term “cyber terrorism” far too broadly, to refer to any sort of cyber attack, regardless of the motivation or identity of the attacker. In keeping with the US government’s general definition of terrorism, I define cyber terrorism more narrowly as computer-to-computer attacks intended to cause significant damage in order to coerce or intimidate a government or civilian population.

To date the United States has not seen significant instances of true cyber terrorism. Some people have taken the lack of precedent as proof that terrorists are not interested in such attacks and would prefer to continue engaging in bombings and other physical attacks that cause visceral fear and bloodshed. But that sort of thinking is similar to the pre-September 11 notion that terrorists would hijack airplanes only to hold the passengers hostage or fly to Cuba. The relevant question is not whether we have seen the method of attack before. The question is whether terrorists have the means and the motivation to use the method now or in the future. For cyber attacks, the answer to both is yes.

The means: terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. Sympathizers of terrorists, in only loosely organized efforts, have often called for and occasionally carried out attacks on websites or communications links of governments or entities. In 2002, the US Federal Bureau of Investigation (FBI) received reports that Al Qaeda agents had probed government websites that contain information about nuclear power plants and other critical infrastructure. The Washington Post also reported in 2002 that browser logs of suspected Al Qaeda operatives revealed that they spent significant amounts of time on websites featuring hacking tools and other programs that facilitate cyber attacks. The means to execute a cyber attack exist.

The motivation: while terrorists may prefer attacks that cause blood and gore, physical and cyber attacks are not mutually exclusive. Osama bin Laden has spoken about his desire to use advanced technology to attack the West and its economy. Other Al Qaeda members or sympathizers also have occasionally talked of their desire to engage in cyber attacks. Now that we see Al Qaeda morphing into a loose coalition of like-minded but disparate groups and individuals spread around the world, it would seem more likely that cells would launch a broader array of attacks, including cyber attacks.

It would appear, then, that a cyber terror attack is the other shoe that has not yet dropped. Given the frequency with which other types of damaging attacks take place, a cyber terror attack seems inevitable.

## **Cyber Espionage**

Foreign intelligence services have been using cyber tools as part of their information gathering and espionage tradecraft for at least 20 years. Between 1986 and 1989, for example, a ring of West German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, programs, and other information that they sold to the Soviet Union's KGB. And in the last few years, the US government has experienced widespread intrusions into government systems in which unclassified but sensitive research information was stolen. Although the US government has not confirmed that these intrusions were state-sponsored, the attacks were traced back to Russia and China, at least suggesting the possibility of foreign espionage.

Of course, the US government is unlikely to announce what it knows about foreign espionage, preferring to engage in counterintelligence efforts to trace the intrusions, learn about the intruder's methods and purpose, and contain the damage or plant misinformation. More worrisome is what the government does not know.

Given the weaknesses in US government agencies' defenses and their ability to detect sophisticated attacks, it would be naïve to believe that the US government is aware of everything that is happening in its information networks. If it takes months for an agency like the US Veterans Administration to know that it lost a laptop with personal data of active and retired military personnel, imagine how long a sophisticated intruder—who gains access to a network, disguises his location, and erases network logs and other indications of his activities—could escape notice inside a government computer system.

## **Cyber Warfare**

During a military conflict, foreign countries can also be expected to mount cyber attacks not only to steal information but also to damage or shut down critical infrastructure systems that underlie the civilian economy, the functioning of government agencies, and military operations. The majority of military communications—critical to command and control of US forces and to their logistical systems—rely on commercial networks. The United States' very ability to project force during a military conflict is, therefore, dependent upon an inherently vulnerable civilian infrastructure.

Foreign nations might also seek to alter information in order to spread propaganda or misinformation, in order to sow fear, sap public support for military action, or undermine confidence in information vital to the functioning of markets. They would, in short, attempt to accomplish by cyber means many of the same things militaries have always done.

Several foreign nations have already developed cyber warfare or “information warfare” doctrine, programs, and capabilities for use against each other and the United States or other nations. Russia and China are the clearest examples; other oft-cited candidates include France, Israel, India, and Pakistan. Media reports, though, quoting unspecified CIA sources, have claimed that as many as 100 nations may currently possess some cyber warfare capabilities, while the Defense Department’s Foreign Technology Assessment (FTA) for 2000 suggested that around 25 countries may now have the ability to carry out significant cyber warfare attacks. Knowing they cannot defeat the United States in a head-to-head military encounter, foreign nations see cyber attacks as a way to strike a vulnerability. In that sense, cyber warfare is the contemporary equivalent of guerilla warfare—only rather than fighting on their turf, the guerillas fight on their enemies’.

A country could engage in cyber attacks as an adjunct to more conventional forms of attack. The United States itself is reported to have used cyber attacks in the initial stages of the war in Iraq in order to degrade Iraqi command-and-control functions and possibly to shut down electrical power.

Because a cyber attack offers the potential for anonymity—or at least plausible deniability—a nation might also engage in a cyber attack during a situation short of open military conflict. A nation might do this to send a message about the potential costs of engaging in military action against it. Because it is easy to disguise the origin of a cyber attack, a country could also pretend that an attack is coming from a third country, either to avoid a possible retaliatory response by the target or to cause the target to attack the third country.

### **What Is To Be Done?**

The broad diversity of potential sources of attacks, US reliance on information systems that are inherently insecure, and the international dimensions of both cyber attacks and governmental responses raise a host of complicated policy questions. These include how best to improve the state of cyber security; what can be done to improve international cooperation on stemming cyber crime and preventing and responding to cyber terrorism; and whether an international treaty or other measures should be taken to prevent or contain cyber warfare.

At a bare minimum, the United States needs to improve the state of cyber security of its critical infrastructures so that it is less vulnerable to attack from any source. A key question, though, is what more the government can and should do to promote better cyber security. Since 9/11, cyber security has been significantly downgraded as a government priority. The Administration of US President George W. Bush has taken over a year to nominate Greg Garcia to fill the post of Assistant Secretary of Homeland Security. Further, no previous occupant of the post, or predecessor posts, lasted more than one year, apparently due to frustration over the lack of attention to or resources for the issue within the government. Without concerted leadership from Washington, it is unlikely that industry will take adequate measures, particularly to deal with the large-scale attacks that no individual company can prevent or defend against on its own.

This is not to say that cyber security has not improved. Software manufacturers have tried to reduce vulnerabilities in their products, and companies have attempted to improve their information security practices and procedures. Part of the motivation has been the sheer cost of dealing with viruses and intrusions. But part of it has also been the result of federal mandates, at least for the financial services and health industries. State laws require companies to notify affected persons when they suffer a breach that leads to the disclosure of personal information. These regulations have given more attention to the issue and have caused companies to increase security to avoid the need to make embarrassing notifications. Still, given the extent of cyber insecurity, much more needs to be done, including research and development of new security technologies and policies designed to promote greater security across all critical industries.

A second issue is improving international cooperation in preventing and responding to cyber attacks. Cyber attackers today can hop from computer to computer as they route their attack from the point of origin to the ultimate targets. A cyber investigation therefore typically involves multiple countries and requires tracing an evidentiary trail across international borders. This makes effective international cooperation essential to cyber crime investigations.

Some steps have already been taken to address this problem. Since the late 1990s, the US government has been urging other nations to strengthen their cyber investigative capacity and to pass domestic laws criminalizing computer viruses and intrusions. The FBI has also trained foreign counterparts to make them more effective partners in international cyber crime investigations. Recently, the US Senate ratified the Council of Europe Convention on Cybercrime, which binds all signatory nations to cooperate with one another and to ensure that they are able to investigate and prosecute cyber crimes effectively. But more must be done to enlarge the community of cooperation, such as including developing nations that are less equipped to deal with cyber crime and do not have a history of cooperation with the United States on criminal investigations.

Finally, the United States must consider whether an international treaty regarding cyber warfare is in its long-term interests. There is presently no treaty that bans or limits cyber warfare. To date, the United States has not been willing even to consider this issue, presumably because it wants to preserve its own option to engage in offensive cyber warfare and espionage. With the United States enjoying a technological edge, this stance is understandable. But it is clear that, as a technologically advanced nation incredibly reliant on information systems in its economy and civil society, the United States is also among the most vulnerable to cyber attack, with the most to lose. Because the United States does not have a monopoly on cyber power, it should seriously consider where its best interests lie in the long term.

### **Who Will Lead?**

The pace of technology continues to increase, while the US government seems less and less capable of dealing with complicated issues quickly. The prospect of the federal government dealing with these issues anytime soon—particularly with crises ongoing in

Iraq, North Korea, and Iran—is very small. But the United States must not repeat the mistake of waiting until a devastating attack before it takes cyber warfare seriously.

**Fatal error:** Call to undefined function: display\_ad() in  
**/home/harva5/public\_html/inc/footer.inc** on line **6**