**January 26, 2010**

**Cyberwar**

**In Digital Combat, U.S. Finds No Easy Deterrent**

**By JOHN MARKOFF, DAVID E. SANGER and THOM SHANKER**

This article was reported by John Markoff, David E. Sanger and Thom Shanker, and written by Mr. Sanger.

WASHINGTON — On a Monday morning earlier this month, top Pentagon leaders gathered to simulate how they would respond to a sophisticated cyberattack aimed at paralyzing the nation’s power grids, its communications systems or its financial networks.

The results were dispiriting. The enemy had all the advantages: stealth, anonymity and unpredictability. No one could pinpoint the country from which the attack came, so there was no effective way to deter further damage by threatening retaliation. What’s more, the military commanders noted that they even lacked the legal authority to respond — especially because it was never clear if the attack was an act of vandalism, an attempt at commercial theft or a state-sponsored effort to cripple the United States, perhaps as a prelude to a conventional war.

What some participants in the simulation knew — and others did not — was that a version of their nightmare had just played out in real life, not at the Pentagon where they were meeting, but in the far less formal war rooms at [Google Inc.](http://topics.nytimes.com/top/news/business/companies/google_inc/index.html?inline=nyt-org) Computers at Google and more than 30 other companies [had been penetrated](http://www.nytimes.com/2010/01/14/technology/14google.html), and Google’s software engineers quickly tracked the source of the attack to seven servers in Taiwan, with footprints back to the Chinese mainland.

After that, the trail disappeared into a cloud of angry Chinese government denials, and then an ugly exchange of accusations between Washington and Beijing. That continued Monday, with Chinese assertions that critics were trying to “denigrate China” and that the United States was pursuing “hegemonic domination” in cyberspace.

These recent events demonstrate how quickly the nation’s escalating cyberbattles have outpaced the rush to find a deterrent, something equivalent to the cold-war-era strategy of threatening nuclear retaliation.

So far, despite millions of dollars spent on studies, that quest has failed. Last week, Secretary of State [Hillary Rodham Clinton](http://topics.nytimes.com/top/reference/timestopics/people/c/hillary_rodham_clinton/index.html?inline=nyt-per) made the most comprehensive effort yet to warn potential adversaries that cyberattacks would not be ignored, drawing on the language of nuclear deterrence.

“States, terrorists and those who would act as their proxies must know that the United States will protect our networks,” she [declared in a speech](http://www.state.gov/secretary/rm/2010/01/135519.htm) on Thursday that drew an angry response from Beijing. “Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government and our civil society.”

But Mrs. Clinton did not say how the United States would respond, beyond suggesting that countries that knowingly permit cyberattacks to be launched from their territories would suffer damage to their reputations, and could be frozen out of the global economy.

There is, in fact, an intense debate inside and outside the government about what the United States can credibly threaten. One alternative could be a diplomatic démarche, or formal protest, like the one the State Department said was forthcoming, but was still not delivered, in the Google case. Economic retaliation and criminal prosecution are also possibilities.

Inside the [National Security Agency](http://www.nsa.gov/), which secretly scours overseas computer networks, officials have debated whether evidence of an imminent cyberattack on the United States would justify a pre-emptive American cyberattack — something the president would have to authorize. In an extreme case, like evidence that an adversary was about to launch an attack intended to shut down power stations across America, some officials argue that the right response might be a military strike.

“We are now in the phase that we found ourselves in during the early 1950s, after the Soviets got the bomb,” said Joseph Nye, a professor at the Kennedy School at Harvard. “It won’t have the same shape as nuclear deterrence, but what you heard Secretary Clinton doing was beginning to explain that we can create some high costs for attackers.”

Fighting Shadows

When the Pentagon summoned its top regional commanders from around the globe for meetings and a dinner with [President Obama](http://topics.nytimes.com/top/reference/timestopics/people/o/barack_obama/index.html?inline=nyt-per) on Jan. 11, the war game prepared for them had nothing to do with Afghanistan, Iraq or Yemen. Instead, it was the simulated cyberattack — a battle unlike any they had engaged in.

Participants in the war game emerged with a worrisome realization. Because the Internet has blurred the line between military and civilian targets, an adversary can cripple a country — say, freeze its credit markets — without ever taking aim at a government installation or a military network, meaning that the Defense Department’s advanced capabilities may not be brought to bear short of a presidential order.

“The fact of the matter,” said one senior intelligence official, “is that unless Google had told us about the attack on it and other companies, we probably never would have seen it. When you think about that, it’s really scary.”

William J. Lynn III, the deputy defense secretary, who oversaw the simulation, said in an interview after the exercise that America’s concepts for protecting computer networks reminded him of one of defensive warfare’s great failures, the [Maginot Line](http://europeanhistory.about.com/library/weekly/aa070601a.htm) of pre-World War II France.

Mr. Lynn, one of the Pentagon’s top strategists for computer network operations, argues that the billions spent on defensive shields surrounding America’s banks, businesses and military installations provide a similarly illusory sense of security.

“A fortress mentality will not work in cyber,” he said. “We cannot retreat behind a Maginot Line of firewalls. We must also keep maneuvering. If we stand still for a minute, our adversaries will overtake us.”

The Pentagon simulation and the nearly simultaneous real-world attacks on Google and more than 30 other companies show that those firewalls are falling fast. But if it is obvious that the government cannot afford to do nothing about such breaches, it is also clear that the old principles of retaliation — you bomb Los Angeles, we’ll destroy Moscow — just do not translate.

“We are looking beyond just the pure military might as the solution to every deterrence problem,” said Gen. Kevin P. Chilton, in charge of the military’s [Strategic Command](http://www.stratcom.mil/), which defends military computer networks. “There are other elements of national power that can be brought to bear. You could deter a country with some economic moves, for example.”

But first you would have to figure out who was behind the attack.

Even Google’s engineers could not track, with absolute certainty, the attackers who appeared to be trying to steal their source code and, perhaps, insert a “Trojan horse” — a backdoor entryway to attack — in Google’s search engines. Chinese officials have denied their government was involved, and said nothing about American demands that it investigate. China’s denials, American officials say, are one reason that President Obama has said nothing in public about the attacks — a notable silence, given that he has made cybersecurity a central part of national security strategy.

“You have to be quite careful about attributions and accusations,” said a senior administration official deeply involved in dealing with the Chinese incident with Google. The official was authorized by the Obama administration to talk about its strategy, with the condition that he would not be named.

“It’s the nature of these attacks that the [forensics](http://topics.nytimes.com/top/reference/timestopics/subjects/f/forensic_science/index.html?inline=nyt-classifier) are difficult,” the official added. “The perpetrator can mask their involvement, or disguise it as another country’s.” Those are known as “false flag” attacks, and American officials worry about being fooled by a dissident group, or a criminal gang, into retaliating against the wrong country.

Nonetheless, the White House said in a statement that “deterrence has been a fundamental part of the administration’s cybersecurity efforts from the start,” citing work in the past year to protect networks and “international engagement to influence the behavior of potential adversaries.”

Left unsaid is whether the Obama administration has decided whether it would ever threaten retaliatory cyberattacks or military attacks after a major cyberattack on American targets. The senior administration official provided by the White House, asked about Mr. Obama’s thinking on the issue, said: “Like most operational things like this, the less said, the better.” But he added, “there are authorities to deal with these attacks residing in many places, and ultimately, of course, with the president.”

Others are less convinced. “The U.S. is widely recognized to have pre-eminent offensive cybercapabilities, but it obtains little or no deterrent effect from this,” said James A. Lewis, director of the [Center for Strategic and International Studies](http://csis.org/) program on technology and public policy.

In its final years, the Bush administration started a highly classified effort, led by Melissa Hathaway, to build the foundations of a national cyberdeterrence strategy. “We didn’t even come close,” she said in a recent interview. Her hope had been to recreate [Project Solarium](http://www.eisenhowerinstitute.org/about/living_history/solarium_for_today.dot), which President [Dwight D. Eisenhower](http://topics.nytimes.com/top/reference/timestopics/people/e/dwight_david_eisenhower/index.html?inline=nyt-per) began in the sunroom of the White House in 1953, to come up with new ways of thinking about the nuclear threats then facing the country. “There was a lot of good work done, but it lacked the rigor of the original Solarium Project. They didn’t produce what you need to do decision making.”

Ms. Hathaway was asked to stay on to run Mr. Obama’s early review. Yet when [the unclassified version of its report](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) was published in the spring, there was little mention of deterrence. She left the administration when she was not chosen as the White House cybersecurity coordinator. After a delay of seven months, that post is now filled: Howard A. Schmidt, a veteran computer specialist, [reported for work last week](http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator), just as the government was sorting through the lessons of the Google attack and calculating its chances of halting a more serious one in the future.

Government-Corporate Divide

In nuclear deterrence, both the Americans and the Soviets knew it was all or nothing: the Cuban missile crisis was resolved out of fear of catastrophic escalation. But in cyberattacks, the damage can range from the minor to the catastrophic, from slowing computer searches to bringing down a country’s cellphone networks, neutralizing its spy satellites, or crashing its electrical grid or its air traffic control systems. It is difficult to know if small attacks could escalate into bigger ones.

So part of the problem is to calibrate a response to the severity of the attack.

The government has responded to the escalating cyberattacks by ordering up new strategies and a new United States Cyber Command. The office of Defense Secretary [Robert M. Gates](http://topics.nytimes.com/top/reference/timestopics/people/g/robert_m_gates/index.html?inline=nyt-per) — whose unclassified e-mail system was hacked in 2007 — is developing a “framework document” that would describe the threat and potential responses, and perhaps the beginnings of a deterrence strategy to parallel the one used in the nuclear world.

The new Cyber Command, if approved by Congress, would be run by Lt. Gen. Keith B. Alexander, head of the [National Security Agency](http://topics.nytimes.com/top/reference/timestopics/organizations/n/national_security_agency/index.html?inline=nyt-org). Since the agency spies on the computer systems of foreign governments and terrorist groups, General Alexander would, in effect, be in charge of both finding and, if so ordered, neutralizing cyberattacks in the making.

But many in the military, led by General Chilton of the Strategic Command and Gen. James E. Cartwright, the vice chairman of the [Joint Chiefs of Staff](http://topics.nytimes.com/top/reference/timestopics/organizations/j/joint_chiefs_of_staff/index.html?inline=nyt-org), have been urging the United States to think more broadly about ways to deter attacks by threatening a country’s economic well-being or its reputation.

Mrs. Clinton went down that road in her speech on Thursday, describing how a country that cracked down on Internet freedom or harbored groups that conduct cyberattacks could be ostracized. But though sanctions might work against a small country, few companies are likely to shun a market the size of China, or Russia, because they disapprove of how those governments control cyberspace or use cyberweapons.

That is what makes the Google-China standoff so fascinating. Google broke the silence that usually surrounds cyberattacks; most American banks or companies do not want to admit their computer systems were pierced. Google has said it will stop censoring searches conducted by Chinese, even if that means being thrown out of China. The threat alone is an attempt at deterrence: Google’s executives are essentially betting that Beijing will back down, lift censorship of searches and crack down on the torrent of cyberattacks that pour out of China every day. If not, millions of young Chinese will be deprived of the Google search engine, and be left to the ones controlled by the Chinese government.

An Obama administration official who has been dealing with the Chinese mused recently, “You could argue that Google came up with a potential deterrent for the Chinese before we did.”