China's Cyber-Militia

CHINESE HACKERS POSE A CLEAR AND PRESENT DANGER TO U.S. GOVERNMENT AND PRIVATE-SECTOR COMPUTER NETWORKS AND MAY BE RESPONSIBLE FOR TWO MAJOR U.S. POWER BLACKOUTS.

by Shane Harris

Sat. May 31, 2008

Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast, according to U.S. government officials and computer-security experts.

One prominent expert told *National Journal* he believes that China's People's Liberation Army played a role in the power outages. Tim Bennett, the former president of the Cyber Security Industry Alliance, a leading trade group, said that U.S. intelligence officials have told him that the PLA in 2003 gained access to a network that controlled electric power systems serving the northeastern United States. The intelligence officials said that forensic analysis had confirmed the source, Bennett said. "They said that, with confidence, it had been traced back to the PLA." These officials believe that the intrusion may have precipitated the largest blackout in North American history, which occurred in August of that year. A 9,300-square-mile area, touching Michigan, Ohio, New York, and parts of Canada, lost power; an estimated 50 million people were affected.

Officially, the blackout was attributed to a variety of factors, none of which involved foreign intervention. Investigators blamed "overgrown trees" that came into contact with strained high-voltage lines near facilities in Ohio owned by FirstEnergy Corp. More than 100 power plants were shut down during the cascading failure. A computer virus, then in wide circulation, disrupted the communications lines that utility companies use to manage the power grid, and this exacerbated the problem. The blackout prompted President Bush to address the nation the day it happened. Power was mostly restored within 24 hours.

There has never been an official U.S. government assertion of Chinese involvement in the outage, but intelligence and other government officials contacted for this story did not explicitly rule out a Chinese role. One security analyst in the private sector with close ties to the intelligence community said that some senior intelligence officials believe that China played a role in the 2003 blackout that is still not fully understood.

Bennett, whose former trade association includes some of the nation's largest computer-security companies and who has testified before Congress on the vulnerability of information networks, also said that a blackout in February, which affected 3 million customers in South Florida, was precipitated by a cyber-hacker. That outage cut off electricity along Florida's east coast, from Daytona Beach to Monroe County, and affected eight power-generating stations. Bennett said that the chief executive officer of a security firm that belonged to Bennett's trade group told him that federal officials had hired the CEO's company to investigate the blackout for evidence of a network intrusion, and to "reverse engineer" the incident to see if China had played a role.

Bennett, who now works as a private consultant, said he decided to speak publicly about these incidents to point out that security for the nation's critical electronic infrastructures remains intolerably weak and to emphasize that government and company officials haven't sufficiently acknowledged these vulnerabilities.

The Florida Blackout

A second information-security expert independently corroborated Bennett's account of the Florida blackout. According to this individual, who cited sources with direct knowledge of the investigation, a Chinese PLA hacker attempting to map Florida Power & Light's computer infrastructure apparently made a mistake. "The hacker was probably supposed to be mapping the system for his bosses and just got carried away and had a 'what happens if I pull on this' moment." The hacker triggered a cascade effect, shutting down large portions of the Florida power grid, the security expert said. "I suspect, as the system went down, the PLA hacker said something like, 'Oops, my bad,' in Chinese."

The power company has blamed "human error" for the incident, specifically an engineer who improperly disabled safety backups while working on a faulty switch. But federal officials are still investigating the matter and have not issued a final report, a spokeswoman for the Federal Energy Regulatory Commission said. The industry source, who conducts security research for government and corporate clients, said that hackers in China have devoted considerable time and resources to mapping the technology infrastructure of other U.S. companies. That assertion has been backed up by the current vice chairman of the Joint Chiefs of Staff, who said last year that Chinese sources are probing U.S. government and commercial networks.

Asked whether Washington knew of hacker involvement in the two blackouts, Joel Brenner, the government's senior counterintelligence official, told *National Journal*, "I can't comment on that." But he added, "It's certainly possible that sort of thing could happen. The kinds of network exploitation one does to explore a network and map it and learn one's way around it has to be done whether you are going to … steal information, bring [the network] down, or corrupt it.… The possible consequences of this behavior are profound."

Brenner, who works for Director of National Intelligence Mike McConnell, looks for vulnerabilities in the government's information networks. He pointed to China as a source of attacks against U.S. interests. "Some [attacks], we have high confidence, are coming from government-sponsored sites," Brenner said. "The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It's a kind of cyber-militia.… It's coming in volumes that are just staggering."

The Central Intelligence Agency's chief cyber-security officer, Tom Donahue, said that hackers had breached the computer systems of utility companies outside the United States and that they had even demanded ransom. Donahue spoke at a January gathering in New Orleans of security executives from government agencies and some of the nation's largest utility and energy companies. He said he suspected that some of the hackers had inside knowledge of the utility systems and that in at least one case, an intrusion caused a power outage that affected multiple cities. The CIA didn't know who launched the attacks or why, Donahue said, "but all involved intrusions through the Internet."

Donahue's public remarks, which were unprecedented at the time, prompted questions about whether power plants in the United States had been hacked. Many computer-security experts, including Bennett, believe that his admission about foreign incidents was intended to warn American companies that if intrusions hadn't already happened stateside, they certainly could. A CIA spokesman at the time said that Donahue's comments were "designed to highlight to the audience the challenges posed by potential cyber intrusions." The CIA declined *National Journal*'s request to interview Donahue.

Cyber-Espionage

In addition to disruptive attacks on networks, officials are worried about the Chinese using long-established computer-hacking techniques to steal sensitive information from government agencies and U.S. corporations.

Brenner, the U.S. counterintelligence chief, said he knows of “a large American company” whose strategic information was obtained by its Chinese counterparts in advance of a business negotiation. As Brenner recounted the story, “The delegation gets to China and realizes, ‘These guys on the other side of the table know every bottom line on every significant negotiating point.’ They had to have got this by hacking into [the company's] systems.”

Bennett told a similar story about a large, well-known American company. (Both he and Brenner declined to provide the names of the companies.) According to Bennett, the Chinese based their starting points for negotiation on the Americans’ end points.

Two sources also alleged that the hacking extends to high-level administration officials.

During a trip to Beijing in December 2007, spyware programs designed to clandestinely remove information from personal computers and other electronic equipment were discovered on devices used by Commerce Secretary Carlos Gutierrez and possibly other members of a U.S. trade delegation, according to a computer-security expert with firsthand knowledge of the spyware used. Gutierrez was in China with the Joint Commission on Commerce and Trade, a high-level delegation that includes the U.S. trade representative and that meets with Chinese officials to discuss such matters as intellectual-property rights, market access, and consumer product safety. According to the computer-security expert, the spyware programs were designed to open communications channels to an outside system, and to download the contents of the infected devices at regular intervals. The source said that the computer codes were identical to those found in the laptop computers and other devices of several senior executives of U.S. corporations who also had their electronics “slurped” while on business in China. The source said he believes, based on conversations with U.S. officials, that the Gutierrez compromise was a source of considerable concern in the Bush administration. Another source with knowledge of the incident corroborated the computer-security expert’s account.

National Journal had a series of conversations with Rich Mills, a Commerce Department spokesman. Asked whether spyware or other malicious software code was found on any electronic devices used by Gutierrez or people traveling with him in China in December 2007, Mills said he “could not confirm or deny” the computer-security expert’s allegations. “I cannot comment on specific [information-technology] issues, but the Department of Commerce is actively working to safeguard sensitive information.” Mills added that the source had provided some inaccurate information, but he did not address the veracity of the source’s claim that the delegation was electronically compromised.

“China is indeed a counterintelligence threat, and specifically a cyber-counterintelligence threat,” said Brenner, who served for four years as inspector general of the National Security Agency, the intelligence organization that electronically steals other countries’ secrets. Brenner said that the American company’s experience “is an example of how hard the Chinese will work at this, and how much more seriously the American corporate sector has to take the information-security issue.” He called economic espionage a national security risk and said that it makes little difference to a foreign power whether it steals sensitive information from a government-operated computer or from one owned by a contractor. “If you travel abroad and are the director of research or the chief executive of a large company, you’re a target,” he said.

“Cyber-networks are the new frontier of counterintelligence,” Brenner emphasized. “If you can steal information or disrupt an organization by attacking its networks remotely, why go to the trouble of running a spy?”

Stephen Spoonamore, CEO of Cybrinth, a cyber-security firm that works for government and corporate clients, said that Chinese hackers attempt to map the IT networks of his clients on a daily basis. He said that executives from three *Fortune* 500 companies, all clients, had document-stealing code planted in their computers while traveling in China, the same fate that befell Gutierrez.

Spoonamore challenged U.S. officials to be more forthcoming about the breaches that have occurred on their systems. “By not talking openly about this, they are making a truly dangerous national security problem worse,” Spoonamore said. “Secrecy in this matter benefits no one. Our nation’s intellectual capital, industrial secrets, and economic security are under daily and withering attack. The oceans that surround us are no protection from sophisticated hackers, working at the speed of light on behalf of nation-states and mafias. We must cease denying the scope, scale, and risks of the issue. I, and a growing number of my peers believe our nation is in grave and growing danger.”

A Growing Threat

Brenner said that Chinese hackers are “very good and getting better all the time.… What makes the Chinese stand out is the pervasive and relentless nature of the attacks that are coming from China.”

The issue has caught Congress’s attention. Rep. Jim Langevin, D-R.I., who chairs the Homeland Security panel’s Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, said that his staff has examined a range of hacker networks, from criminal syndicates to nationally supported groups. “China has been a primary concern,” he said. The deepest penetrations into U.S. systems have been traced back to sources within China, Langevin noted.

(At a hearing last week, Langevin said that the private sector, which owns the vast majority of U.S. information networks, including those that operate power plants, dams, and other critical infrastructure, had taken a “halfhearted approach” to improving security. He cited a new report by the Government Accountability Office, which found that the Tennessee Valley Authority, the nation’s largest power generator, “has not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures.” Langevin said that the TVA “risks a disruption of its operations as the result of a cyber-incident, which could impact its customers,” and he expressed “little confidence that industry is taking the appropriate actions.”)

The Chinese make little distinction between hackers who work for the government and those who undertake cyber-adventures on its behalf. “There’s a huge pool of Chinese individuals, students, academics, unemployed, whatever it may be, who are, at minimum, not discouraged from trying this out,” said Rodger Baker, a senior China analyst for Stratfor, a private intelligence firm. So-called patriotic-hacker groups have launched attacks from inside China, usually aimed at people they think have offended the country or pose a threat to its strategic interests. At a minimum the Chinese government has done little to shut down these groups, which are typically composed of technologically skilled and highly nationalistic young men. Officially, Chinese military and diplomatic officials say they have no policy of attacking other governments’ systems.

“This has been a growing wave in recent years,” Brenner said, attributing China’s cyber-tactics to its global economic and political ambitions. “The Chinese are out to develop a modern economy and society in one generation.… There is much about their determination that is admirable. But they’re also willing to steal a lot of proprietary information to do it, and that’s not admirable. And we’ve got to stop it as best we can.”

High-profile penetrations of government systems have been occurring for several years. In 2007, an unidentified hacker broke into the e-mail system for Defense Secretary Robert Gates’s office, and the Pentagon shut down about 1,500 computers in response. But officials said that the intrusion caused no harm. In 2006, a State Department employee opened an e-mail containing a Trojan horse, a program designed to install itself on a host machine to give a hacker covert access. As a result, officials cut off Internet access to the department’s East Asia and Pacific region, but the department suffered no long-term problems.

The Homeland Security Department, which is responsible for protecting civilian computer systems, suffered nearly 850 attacks over a two-year period beginning in 2005, officials have said. In one instance,

they found that a program designed to steal passwords had been installed on two of the department's network servers. In these and other incidents, there is considerable debate about whether the intruders stole truly valuable information that could compromise U.S. strategy or ongoing operations.

"The penetrations we've seen are on unclassified systems, which are obviously less protected than classified systems," Brenner said.

Private Sector Foot-Dragging

There is little indication that cyber-intrusions, however menacing, have severely impaired government operations for very long. So why are so many officials increasingly sounding the alarm about network attacks, Chinese hacking and espionage, and the advent of cyberwar?

Part of the answer lies in officials' most recent appraisals of the cyber-threat. They cite evidence that attacks are increasing in volume and appear engineered more to cause real harm than sporadic inconvenience. Without naming China, Robert Jamison, the top cyber-security official at DHS, told reporters at a March briefing, "We're concerned that the intrusions are more frequent, and they're more targeted, and they're more sophisticated."

"In terms of breaches within government systems, it's something that has happened quite a bit over the last six, seven years," says Shannon Kellogg, the director of information-security policy for EMC Corp., which owns RSA, a top cyber-security research firm. "But the scale of these types of breaches and attacks seems to have increased substantially."

Government officials are more concerned now than in recent years about the private sector's inability, or unwillingness, to stop these pervasive attacks. When Donahue, the CIA cyber-security officer, warned the gathering in New Orleans about foreign hackings of power plants, some saw it as a direct challenge to American companies.

"Donahue wouldn't have said it publicly if he didn't think the threat was very large and that companies needed to fix things right now," Alan Paller, the highly regarded director of research at the SANS Institute, told *The Washington Post* at the time. (SANS, a cyber-security research and education group, sponsored the January meeting in New Orleans.) Another security expert noted that in the previous 18 months, there had been "a huge increase in focused attacks on our national infrastructure networks … and they have been coming from outside the United States."

In comments posted on *Wired* magazine's *Danger Room* blog, which is trafficked by many techno-elites who are skeptical of the administration's more boisterous public warnings, Donahue's remarks about power plants drew support. Michael Tanji, a former intelligence officer with the Defense Intelligence Agency, said that the comments weren't part of a government plot to hype the threat. "Having worked with [Donahue] on these and related issues in the past, I regret to inform conspiracy theorists that he is virulently allergic to hyperbole," Tanji said. "I've long been a skeptic of claims about being able to shut down the world from the Net.… But after today, I'm starting to come around to the idea that the ignorance or intransigence of utility system owners just might merit a more robust response than has been undertaken to date."

Tanji's remarks pointed to one of the most nettlesome realities of cyber-security policy. Because most of the infrastructure in the United States is privately owned, the government finds it exceptionally difficult to compel utility operators to better monitor their systems. The FBI and DHS have established formal groups where business operators can disclose their known vulnerabilities privately. (Companies fear that public exposure will decrease shareholder confidence or incite more hackings.) But membership in these organizations isn't compulsory. Furthermore, many of the systems that utility operators use were designed by others. Intelligence officials now worry that software developed overseas poses another

layer of risk because malicious codes or backdoors can be embedded in the software at its creation. U.S. officials have singled out software manufacturers in emerging markets such as, not surprisingly, China.

Military Response

The intelligence community's and private sector's vocal warnings and dire suspicions of Chinese hackers join a chorus of concern emanating from the Defense Department in recent months. In the most recent annual report on China's military power, the Defense Department declared publicly for the first time that attacks against government and commercial computer networks in 2007 appear to have emanated from China. "Numerous computer networks around the world, including those owned by the U.S. government, were subject to intrusions that appear to have originated within" the People's Republic of China. Although not claiming that the attacks were conducted by the Chinese government, or officially endorsed, the declaration built upon the previous year's warning that the People's Liberation Army is "building capabilities for information warfare" for possible use in "pre-emptive attacks."

The military is not waiting for China, or any other nation or hacker group, to strike a lethal cyber-blow. In March, Air Force Gen. Kevin Chilton, the chief of U.S. Strategic Command, said that the Pentagon has its own cyberwar plans. "Our challenge is to define, shape, develop, deliver, and sustain a cyber-force second to none," Chilton told the Senate Armed Services Committee. He asked appropriators for an "increased emphasis" on the Defense Department's cyber-capabilities to help train personnel to "conduct network warfare."

The Air Force is in the process of setting up a Cyberspace Command, headed by a two-star general and comprising about 160 individuals assigned to a handful of bases. As *Wired* noted in a recent profile, Cyberspace Command "is dedicated to the proposition that the next war will be fought in the electromagnetic spectrum and that computers are military weapons." The Air Force has launched a TV ad campaign to drum up support for the new command, and to call attention to cyberwar. "You used to need an army to wage a war," a narrator in the TV spot declares. "Now all you need is an Internet connection."

> "It's a kind of cyber-militia.... It's coming in volumes that are just staggering." ***--Joel Brenner***

Defense and intelligence officials have been surprised by China's cyber-advances, according to the U.S-China Economic and Security Review Commission. In November, the commission reported that "Chinese military strategists have embraced … cyberattacks" as a weapon in their military arsenal. Gen. James Cartwright, the former head of U.S. Strategic Command and now the vice chairman of the Joint Chiefs, told the commission that China was engaged in cyber-reconnaissance, probing computer networks of U.S. agencies and corporations. He was particularly concerned about China's ability to conduct "denial-of-service" attacks, which overwhelm a computer system with massive amounts of automatically generated message traffic. Cartwright provocatively asserted that the consequences of a cyberattack "could, in fact, be in the magnitude of a weapon of mass destruction."

A former CIA official cast the cyber-threat in a similarly dire terms. "We are currently in a cyberwar, and war is going on today," Andrew Palowitch, who's now a consultant to U.S. Strategic Command, told an audience at Georgetown University in November. STRATCOM, headquartered at Offutt Air Force Base in Nebraska, oversees the Defense Department's Joint Task Force-Global Network Operations, which defends military systems against cyber-attack. Palowitch cited statistics, provided by Cartwright, that 37,000 reported breaches of government and private systems occured in fiscal 2007. The Defense Department experienced almost 80,000 computer attacks, he said. Some of these assaults "reduced" the military's "operational capabilities," Palowitch noted.

Presidential Attention

President Bush has personally devoted more high-level attention to the cyberattack issue in the last year or so than he did in the first six years of his tenure combined. Many security experts are surprised that the administration is only now moving to take dramatic measures to improve the security of government networks, because some Cabinet-level and White House officials have been warning about the threat for years to just about anyone who will listen.

Until McConnell, the national intelligence director, personally drove the point home to Bush in an Oval Office meeting in 2006, there was little top-level support for a comprehensive government cyber-security plan. “They ignored it,” one former senior administration official said flatly. “McConnell has the president’s ear.”

McConnell, a former director of the National Security Agency, whose main job is to intercept foreign communications intelligence but which is also responsible for protecting U.S. classified information and systems, takes the computer-security issue as seriously as his counter-terrorism mission. After McConnell left the NSA, in 1996, he took over the intelligence practice at Booz Allen Hamilton, where he again turned to security problems, particularly within the nation’s financial infrastructure. Working with officials from the New York Stock Exchange, McConnell developed a report for the government on network vulnerabilities; he has said that it was so revealing, the administration decided to classify it.

Lawrence Wright of *The New Yorker* reported earlier this year that McConnell told Bush during the 2006 Oval Office meeting, “If the 9/11 perpetrators had focused on a single U.S. bank through cyberattack and it had been successful, it would have had an order-of-magnitude greater impact on the U.S. economy.” According to Wright, the president was disturbed, and then asked Treasury Secretary Henry Paulson Jr., who was at the meeting, if McConnell was correct; Paulson assured the president that he was.

Brenner confirmed Wright’s account as “a true story.” And separately, a former senior administration official told *National Journal* of another dimension. In that meeting, McConnell also told the president that White House communications systems could be targeted for attack just as other U.S. government systems had been targeted. The intelligence chief was telling the president, “If the capability to exploit a communications device exists, we have to assume that our enemies either have it, or are trying to develop it,” the former official said.

This meeting compelled the White House to craft an executive order laying out a broad and ambitious plan to shore up government-network defenses. Known internally as “the cyber-initiative,” it was formally issued in January. The details remain classified, but it has been reported that the order authorizes the National Security Agency to monitor federal computer networks. It also requires that the government dramatically scale back the number of points at which federal networks connect to the public Internet. The Office of Management and Budget has directed agencies to limit the total number of Internet “points of presence” to 50 by June.

Limiting connection points is analogous to pulling up drawbridges in order to defend the government’s cyber-infrastructure. Security experts interviewed for this story said that it shows how little the government can do, at least for now, to ward off intrusions if the first line of defense is to “unplug.”

Mixed Reactions

Under the president’s cyber-initiative, the Homeland Security Department will be responsible for monitoring government agencies apart from the Defense Department. In March, Homeland Security Secretary Michael Chertoff told *National Journal* that the first step is “to survey all the points” of presence. “We have no final number yet.”

“The agencies’ networks have grown very haphazardly. No one really knows where [the connections to the Internet] are,” said Bruce McConnell, who was the chief of information technology and policy in the Office of Management and Budget. He left government in 2000. “Trying to catalogue where things are so you could turn them off is a daunting task in and of itself,” said McConnell, who is not related to the intelligence chief.

Bush’s cyber-initiative has received mixed reviews. Generally, cyber-experts favor a comprehensive approach, and they are relieved that the issue finally has the president’s full attention. But some question how the program is being implemented—under a cloak of secrecy and with a heavy reliance on the intelligence community.

“Our nation’s intellectual capital, industrial secrets, and economic security are under daily and withering attack.” ***--Stephen Spoonamore***

The sharpest criticisms are directed at the NSA, an intelligence agency whose traditional mandate is to collect information coming from outside the United States; it has no customary role monitoring networks inside the country, although this has changed in the years following the 9/11 attacks. It’s not clear just how far the government’s monitoring of computer networks will extend into the private sector and precisely what role the NSA will play tracking networks inside the United States, but lawmakers have already raised concerns that the cyber-initiative will creep into domestic intelligence-gathering. The same kinds of technologies that are used to monitor networks for viruses and other malicious threats could be used to track domestic communications. On May 2, DHS’s top overseers sent a letter to Chertoff questioning “the secrecy of the project.” Sens. Joe Lieberman, ID-Conn., and Susan Collins, R-Maine, the chairman and ranking member of the Homeland Security and Governmental Affairs Committee, respectively, noted that the department had requested an additional $83 million for its National Cyber Security Division; DHS had already been allocated $115 million for the cyber-initiative in the 2008 omnibus appropriations bill. “This would be a nearly $200 million increase, tripling the amount of money spent on cyber-security in DHS since 2007,” the senators wrote. The full cost of implementing the president’s cyber-initiative is estimated to be $30 *billion*. The entire 2009 budget request for the Homeland Security Department is about $50 billion.

Marc Sachs, who was the director for communication infrastructure protection in the White House Office of Cyberspace Security in 2002, praised the administration for taking a bold initial step. But he said that the level of attention is 10 years overdue. Sachs noted that in 1998, President Clinton issued a directive that set ambitious infrastructure-protection goals. “I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber-systems,” Clinton wrote.

Without pointing to particular policies, Brenner, the counterintelligence chief, said, “We need to take these policy declarations that we’ve had for 10 years and turn them into practical reality.” He said the job of securing cyberspace is hardly as simple as “put two padlocks on the door…. This is an incredibly open and porous and, in many cases, wireless system. Controlling cyber-security is like controlling the air flow in a large, segmented building complex in a noxious neighborhood. You cannot be sure you are keeping all the noxious stuff out. What you’ve got to say is, gee, in the infirmary, we’ve really got to deal differently than we do in the lobby.”

False Accusations?

Given the political fallout that could stem from a proven Chinese attack on power plants or theft of government secrets—not to mention the pressure to launch some sort of military response—skeptics have asked whether the Chinese really are behind so many high-profile incidents.

Brenner affirmed the widely held view that it's technologically difficult to attribute the exact source of any cyberattack and that the government needs better technologies to do so. But despite his assurances that the government has indeed sourced cyber-intrusions to China, others urge caution.

"We want to find a natural enemy, so we're looking everywhere," Sachs said. He noted that some hackers launch their attacks through computers based in other countries, and that China is an easy mask. "I think all of us should remember that not everything you see online is truthful."

Another former administration official echoed those sentiments. "I think it's a little bit naive to suggest that everything that says it comes from China comes from China," said Amit Yoran, the first director of DHS's National Cyber Security Division, who left the post in 2004.

But there is little to no doubt, including among skeptics, that China is vigorously pursuing offensive cyber-capabilities. Military analysts say that the Chinese know their armed forces cannot match America's in a head-on confrontation, and they realize their nuclear arsenal pales in comparison. These imbalances have forced Chinese military planners to adopt what the Pentagon calls "asymmetric" techniques—tactics that aim at a foe's vulnerabilities—in order to counter, or at least deter, U.S. military power.

"There has been much writing on information warfare among China's military thinkers, who indicate a strong conceptual understanding of its methods and uses," according to the Pentagon's annual report on China's military power. The report stated that "there is no evidence of a formal Chinese … doctrine" but noted that the People's Liberation Army has "established information-warfare units to develop viruses to attack enemy computer systems and networks."

U.S. military officials see cyber-warfare as one arrow in a quiver of asymmetric techniques to disrupt an enemy's command-and-control systems. The Chinese strategy, according to this line of thinking, is not to defeat U.S. military forces but to make it harder for them to operate.

China's military history has been defined by asymmetric warfare, said Harry Harding, an expert on Chinese domestic politics and U.S.-China relations, who teaches at George Washington University's Elliott School of International Affairs. Cyber-warfare is just one of the more recent tactics. If the U.S. government tries to protect its systems, the Chinese will simply attack the private sector; he cited the financial services industry as an obvious target. "I have no doubt that China is doing this," Harding said.

Bennett, the former head of the Cyber Security Industry Alliance, said that if China has penetrated power plants and the power grid, it serves as a show of force to the United States and is likely meant to deter any U.S. military intervention on behalf of Taiwan. He noted that the Florida blackout occurred only a few days after the Navy shot down a failing U.S. satellite with a missile designed to intercept inbound ballistic missiles. A year earlier, the Chinese had downed one of their own satellites in orbit. The Bush administration has pursued ballistic missile defense systems, and Taiwan has sought that technology from the United States.

Cyberwar

The Chinese are not alone, of course, in their pursuit of cyber-warfare. The Air Force is setting up the Cyberspace Command, the 10th command in the service's history.

"The next kind of warfare will be asymmetric warfare," Gen. William Lord, the provisional commander, said during a roundtable discussion at the Council of Foreign Relations in March. "Who is going to take on

the United States Army, Marine Corps, U.S. Air Force, and U.S. Navy as probably the most powerful force on the face of the planet?"

Lord didn't limit his remarks to China. He said that cyber-criminals and other "bad guys" were as much a concern for the military. He also pointed to a massive cyberattack launched last year against computers in Estonia, in which Russian hackers—perhaps operating at Moscow's behest—tried to take down the country's systems in retaliation for Estonia's decision to move a statue commemorating fallen Soviet troops, a statue that Russians living in Estonia love but that native-born Estonians don't. The attack has been billed as the first "cyberwar" because of the overwhelming electronic force brought to bear on the tiny country of 1.3 million people.

"I had an opportunity to speak with the minister of defense from Estonia," Lord said. "He was attacked by 1 million computers."

The Estonia attack probably shook nerves more than it caused long-term damage. But it served as a potent example of how determined, coordinated hackers could gang up on a foreign government. It has also created profound policy questions about what qualifies as war in cyberspace.

"The problem with this kind of warfare," Lord said, "is determining who is the enemy, what is their intent, and where are they, and then what can you do about it?"

Brenner, the senior U.S. counterintelligence official, said, "Another country knows that if it starts taking out our satellites, that would be an act of war." But "if they were to take out certain parts of our infrastructure, electronically, that could be regarded as an act of war," he said. "It's not my job to say that."

NATO officials are reluctantly struggling with that question, too. At a ministerial meeting last June, Defense Secretary Gates asked the allied members to consider defining cyberattacks in the context of traditional warfare. Cyberwar is still abstract, and there are no international conventions that govern military conduct on a digital battlefield.

"The U.S. government doesn't really have a policy on the use of these techniques," said Michael Vatis, a former director of the FBI's National Infrastructure Protection Center. "The closest analogy is to covert actions," he said, meaning spy operations undertaken by intelligence agencies against foreign governments. "They take place, and people have strong suspicions about [who's responsible]. But as long as they're not able to prove it, there's very little that they can do about it. And so there's often not as much outrage expressed."

Staff Correspondent Bruce Stokes contributed to this article. The author can be reached at sharris@nationaljournal.com

-
-