washingtonpost.com

U.S. Fears Al Qaeda Cyber Attacks

By Barton Gellman
Washington Post Staff Writer
Wednesday, June 26, 2002; 6:00 PM

Late last fall, Detective Chris Hsiung of the Mountain View, Calif., police department began investigating a suspicious pattern of surveillance against Silicon Valley computers. From the Middle East and South Asia, unknown browsers were exploring the digital systems used to manage Bay Area utilities and government offices. Hsiung, a specialist in high-technology crime, alerted the FBI's San Francisco computer intrusion squad.

Working with experts at the Lawrence Livermore National Laboratory, the FBI traced back trails of a broader reconnaissance. A forensic summary of the investigation, prepared in the Defense Department, said the bureau found "multiple casings of sites" nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities.

Some of the probes suggested planning for a conventional attack, U.S. officials said. But others homed in on a class of digital device that allows remote control of services such as fire dispatch and machinery such as pipelines. More information about those devices – and how to program them – turned up on al Qaeda computers seized this year, according to law enforcement and national security officials.

Unsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshhold of using the Internet as a direct instrument of bloodshed. The new threat bears little resemblance to familiar financial disruptions by hackers responsible for viruses and worms. It comes instead at the meeting points between computers and the physical structures they control.

By disabling or taking command of floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, U.S. analysts believe an intruder could use virtual tools to destroy real-world lives and property. They surmise, with limited evidence, that al Qaeda aims to employ those techniques in synchrony with "kinetic weapons" such as explosives.

"The event I fear most is a physical attack in conjunction with a successful cyber attack on the responders' 911 system or on the power grid," Ronald Dick, director of the FBI's National Infrastructure Protection Center, told a closed gathering of corporate security executives hosted by Infraguard in Niagara Falls on June 12.

In an interview, Dick said those additions to a conventional al Qaeda attack might mean that "the first responders couldn't get there . . . and water didn't flow, hospitals didn't have power. Is that an unreasonable scenario? Not in this world. And that keeps me awake at night."

'Bad Ones and Zeros'

Regarded until recently as remote, the risks of cyberterrorism now command urgent White House attention. Discovery of one acute vulnerability – in a data transmission standard known as ASN.1, short for Abstract Syntax Notification – rushed government experts to the Oval Office on Feb. 7 to brief President Bush. The security flaw, according to subsequent written assessment by the FBI, could have been exploited to bring down telephone networks and halt "all control information exchanged between ground and aircraft flight control systems."

Officials said Osama bin Laden's operatives have nothing like the proficiency in information war of the most sophisticated nation-states. But al Qaeda is now judged to be considerably more capable than analysts believed a year ago. And its intentions are unrelentingly aimed at inflicting catastrophic harm.

One al Qaeda laptop found in Afghanistan, sources said, had made multiple visits to a French site run by the Societe» Anonyme, or Anonymous Society. The site offers a two-volume online "Sabotage Handbook" with sections on tools of the trade, planning a hit, switchgear and instrumentation, anti-surveillance methods and advanced techniques. In Islamic chat rooms, other computers linked to al Qaeda had access to "cracking" tools used to search out networked computers, scan for security flaws and exploit them to gain entry – or full command.

Most significantly, perhaps, U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Qaeda operators spent time on sites that offer software and programming instructions for the digital

switches that run power, water, transport and communications grids. In some interrogations, the most recent of which was reported to policymakers last week, al Qaeda prisoners have described intentions, in general terms, to use those tools.

Specialized digital devices are used by the millions as the brains of American "critical infrastructure" – a term defined by federal directive to mean industrial sectors that are "essential to the minimum operations of the economy and government."

The devices are called distributed control systems, or DCS, and supervisory control and data acquisition, or SCADA, systems. The simplest ones collect measurements, throw railway switches, close circuit-breakers or adjust valves in the pipes that carry water, oil and gas. More complicated versions sift incoming data, govern multiple devices and cover a broader area.

What is new and dangerous is that most of these devices are now being connected to the Internet – some of them, according to classified "Red Team" intrusion exercises, in ways that their owners do not suspect.

Because the digital controls were not designed with public access in mind, they typically lack even rudimentary security, with fewer safeguards than the purchase of flowers online.

Until recently, said director John Tritak of the Commerce Department's Critical Infrastructure Assurance Office, many government and corporate officials regarded hackers mainly as a menace to their email.

"There's this view that the problems of cyberspace originate, reside and remain in cyberspace," Tritak said. "Bad ones and zeros hurt good ones and zeros, and it sort of stays there. . . . The point we're making is that increasingly we are relying on 21st century technology and information networks to run physical assets." Digital controls are so pervasive, he said, that terrorists might use them to wreak damage on a scale that otherwise would "not be available except through a very systematic and comprehensive physical attack."

'Mapping Our Vulnerabilities'

The 13 agencies and offices of the U.S. intelligence community have not reached consensus on the scale or imminence of this threat, according to participants in and close observers of the discussion. The Defense Department, which concentrates on information war with nation-states, is most skeptical of al Qaeda's interest and prowess in cyberspace.

"DCS and SCADA systems might be accessible to bits and bytes," Assistant Secretary of Defense John P. Stenbit said in an interview. But al Qaeda prefers simple, reliable plans and would not allow the success of a large-scale attack "to be dependent on some sophisticated, tricky cyber thing to work."

"We're thinking more in physical terms – biological agents, isotopes in explosions, other analogies to the fully loaded airplane," he said. "That's more what I'm worried about. When I think of cyber I think of it as ancillary to one of those."

White House and FBI analysts, as well as officials in the Energy and Commerce departments with more direct responsibility for the civilian infrastructure, describe the threat in more robust terms.

"We were underestimating the amount of attention [al Qaeda was] paying to the Internet," said Roger Cressey, a long-time counterterrorist official who became chief of staff of the President's Critical Infrastructure Protection Board in October. "Now we know they see it as a potential attack vehicle. Al Qaeda spent more time mapping our vulnerabilities in cyberspace than we previously thought. An attack is a question of when, not if."

Ron Ross, who heads a new "information assurance" partnership between the National Security Agency and the National Institute of Standards and Technology, reminded the Infraguard delegates in Niagara Falls that air traffic controllers brought down every commercial plane in the air on Sept. 11. "If there had been a cyber attack at the same time that prevented them from doing that," he said, "the magnitude of the event could have been much greater."

"It's not science fiction," Ross said in an interview. "A cyberattack can be launched with fairly limited resources."

U.S. intelligence agencies have upgraded their warnings about al Qaeda's use of cyberspace. Just over a year ago, a National Intelligence Estimate on the threat to U.S. information systems gave prominence to China, Russia and other nation-states. It judged al Qaeda operatives as "less developed in their network capabilities" than many individual hackers and "likely to pose only a limited cyber threat," according to an authoritative description of its contents.

In February, the CIA issued a revised Directorate of Intelligence Memorandum. According to officials who read it, the new

memo said al Qaeda had "far more interest" in cyberterrorism than previously believed and contemplated use of hackers for hire to speed acquisition of capabilities.

"I don't think they are capable of bringing a major segment of this country to its knees using cyber attack alone," said an official representing the current consensus, but "they would be able to conduct an integrated attack using a combination of physical and cyber resources and get an amplification of consequences."

Counterterrorist analysts have known for years that al Qaeda prepares for attacks with elaborate "targeting packages" of photographs and notes. But in January U.S. forces in Kabul found something new.

A computer seized at an al Qaeda office contained models of a dam, made with structural architecture and engineering software, that enabled the planners to simulate its catastrophic failure. Bush administration officials, who discussed the find, declined to say whether they had identified a specific dam as target.

The FBI reported that the computer had been running Microstran, an advanced tool for analyzing steel and concrete structures; Autocad 2000, which manipulates technical drawings in two or three dimensions; and software "used to identify and classify soils," which would assist in predicting the course of a wall of water surging downstream.

To destroy a dam physically would require "tons of explosives," Assistant Attorney General Michael Chertoff said a year ago. To breach it from cyberspace is not out of the question. In 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that runs Arizona's Roosevelt Dam. He did not know or care, but federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates.

Roosevelt Dam holds back as much as 1.5 million acre-feet of water, or 489 trillion gallons. That volume would theoretically cover the city of Phoenix, down river, to a height of five feet. In practice that could not happen. Before it reached the Arizona capital, the rampant Salt River would spend most of itself in a flood plain encompassing the cities of Mesa and Tempe – with a combined population of nearly a million.

'Could Have Done Anything'

In Queensland, Australia, on April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment along Australia's Sunshine Coast.

Boden's arrest solved a mystery that had plagued the Maroochy Shire wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and the manicured grounds of the Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency said "marine life died, the creek water turned black and the stench was unbearable for residents." Until Boden's capture – during his 46th successful intrusion – the utility's managers did not know why.

Specialists in cyber terrorism have studied Boden's case because it is the only one known in which someone used a digital control system deliberately to wreak harm. Details of Boden's intrusion, not disclosed before, show how easily Boden broke in – and how restrained he was with his power.

Boden had quit his job at Hunter Watertech, the supplier of Maroochy Shire's remote control and telemetry equipment. Evidence at trial suggested he was angling for a consulting contract to solve the problems he caused.

To sabotage the system he set the software on his laptop to identify itself as "pumping station 4," then suppressed all alarms. Paul Chisholm, Hunter Watertech's CEO, said in an interview last week that Boden "was the central control system" during his intrusions, with unlimited command of 300 SCADA nodes governing sewage and drinking water alike. "He could have done anything he liked to the fresh water," Chisholm said.

Like thousands of utilities around the world, Maroochy Shire allowed technicians operating remotely to manipulate its digital controls. Boden learned how to use those controls as an insider, but the software he used conforms to international standards and manuals are available on the web. He faced virtually no obstacles to breaking in.

Nearly identical systems run oil and gas utilities and many manufacturing plants. But their most dangerous use is in the generation, transmission and distribution of electrical power, because electricity has no substitute and every other key infrastructure depends on it.

Massoud Amin, a mathematician directing new security efforts in the industry, described the North American power grid as "the most complex machine ever built." At an April 2 conference hosted by the Commerce Department, participants

said, government and industry scientists agreed that they have no idea how the grid would respond to an actual cyberattack.

What they do know is that "Red Teams" of mock intruders from the Energy Department's four national laboratories have devised what one government document listed as "eight scenarios for SCADA attack on an electrical power grid" – and all of them work. Eighteen such exercises have been conducted to date against large regional utilities, and Richard A. Clarke, President Bush's cybersecurity adviser, said the intruders "have always, always succeeded."

Joseph M. Weiss of KEMA Consulting, a leading expert in control system security, reported at two recent industry conferences that intruders were "able to assemble a detailed map" of each system and "intercepted and changed" SCADA commands without detection.

"What the labs do is look at simple, easy things I can do to get in" with tools commonly available on the Internet, Weiss said in an interview. "In most of these cases they are not using anything that a hacker couldn't have access to."

Bush has launched a top-priority research program at the Livermore, Sandia and Los Alamos labs to improve safeguards in the estimated three million SCADA systems in use. But many of the systems rely on instantaneous response and cannot tolerate authentication delays. And the devices now deployed lack the memory and bandwidth to use techniques such as "integrity checks" that are standard elsewhere.

In a book-length Electricity Infrastructure Security Assessment, the industry concluded on Jan. 7 that "it may not be possible to provide sufficient security when using the Internet for power system control." Power companies, it said, will probably have to build a parallel private network for themselves.

'Where Their Crown Jewels Are'

The U.S. government may never have fought a war with so little power in the battlefield. That became clear again on Feb. 7, when Clarke and his vice-chairman at the critical infrastructure board, Howard A. Schmidt, arrived in the Oval Office.

They told the president that researchers in Finland had identified a serious security hole in the Internet's standard language for routing data through switches. A government threat team found implications – for air traffic control and civilian and military phone links, among others – that were more serious still.

"We've got troops on the ground in Afghanistan and we've got communication systems that we all depend on that, at that time, were vulnerable," Schmidt recalled.

Bush ordered the Pentagon and key federal agencies to patch their systems. But most of the vulnerable networks were not government-owned. Since Feb. 12 "those who have the fix in their power are in the private sector," Schmidt said. Asked about progress, he said: "I don't know that we'd ever get to 100 percent."

Frustrated at the pace of repairs, Clarke traveled to San Jose on Feb. 19 and accused industry leaders of spending more on coffee than information security. "You will be hacked," he told them. "What's more, you deserve to be hacked."

Tritak, at the Commerce Department, appealed to patriotism. Speaking of al Qaeda, he said: "When you've got people who are saying, 'We're coming after your economy,' everyone has a responsibility to do their bit to safeguard against it."

New public-private partnerships are helping, but the government case remains a tough sell. Even among banks and brokerages, considered the most security-conscious major industry, Alan Paller, director of research at the SANS Institute in Bethesda, said "substantially none of them" tell government when their systems are attacked. Sources said the government did not learn crucial details about September's Nimda worm, which caused an estimated $530 million in damages to some 300,000 computers, until the stricken companies began firing their security executives.

Experts said public companies worry about loss of customer confidence and legal liability to shareholders or security vendors when they report flaws.

The FBI is having even less success with its "key asset initiative," an attempt to identify the most dangerous points of vulnerability in 5,700 companies deemed essential to national security.

"What we really want to drill down to, eventually, is not the companies but the actual things themselves, the actual switches . . . that are vital to [a firm's] continued operations," Dick said. He acknowledged a rocky start: "For them to tell us where their crown jewels are is not reasonable until you've built up trust."

Michehl R. Gent, president of the North American Electric Reliability Council, said last month it will not happen. "We're not going to build such a list. . . . We have no confidence that the government can keep that a secret."

For fear of terrorist infiltration, Clarke's critical infrastructure board and Tom Ridge's homeland security office are now exploring whether private companies will consider telling government the names of employees with access to sensitive sites.

"Obviously the ability to check intelligence records from the terrorist standpoint would be the goal," Dick said.

There is no precedent for that. The FBI screens bank employees, but has no statutory authority in other industries. Using classified intelligence databases, such as the Visa Viper list of suspected terrorists, would mean the results could not be shared with the employers. Bobby Gillham, manager of global security at oil giant Conoco, said he doubts his industry will go along with that.

"You have Privacy Act concerns," he said in an interivew. "And just to get feedback that there's nothing here, or there's something here but we can't share it with you, doesn't do us a lot of good. Most of our companies would not [remove an employee] in a frivolous way, on a wink."

Exasperated by companies seeking proof that they are targets, Clarke has stopped talking about threats at all.

"It doesn't matter whether it's al Qaeda or a nation-state or the teenage kid up the street," he said. "Who does the damage to you is far less important than the fact that damage can be done. You've got to focus on your vulnerability . . . and not wait for the FBI to tell you that al Qaeda has you in its sights."

Staff researcher Robert Thomason contributed to this report.

© 2002 The Washington Post Company