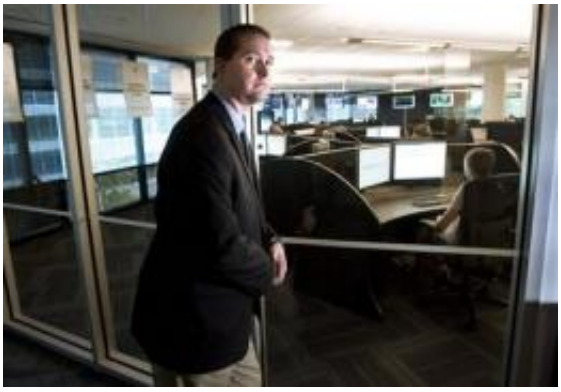
US largely ruling out NKorea in 2009 cyberattacks

July 3 2010, By LOLITA C. BALDOR , Associated Press Writer



Don Jackson, director of intelligence at SecureWorks is pictured outside the security operations center of his company which manages security information systems for corporations world wide, Friday July 2, 2010, in Atlanta. Analysts at the company worked on the investigation into last year's cyber attack that took down websites in the U.S. and South Korea. (AP Photo/John Amis)

(AP) -- U.S. officials have largely ruled out North Korea as the origin of a computer attack last July that took down U.S. and South Korean government websites, according to cybersecurity experts.

But authorities are not much closer than they were a year ago to knowing exactly who did it - and why.

In the days after the fast-moving, widespread attack, analysis pointed to North Korea as the likely starting point because code used in the attack

included Korean language and other indicators. Experts now say there is no conclusive evidence that North Korea, or any other nation, orchestrated it.

The crippling strikes, known as "denial of service" attacks, did not compromise security or breach any sensitive data or critical systems. Officials and experts say the agencies are better prepared today. But they acknowledge that many government and business sites remain vulnerable to similar intrusions.

The incidents underscore the increasing threats posed by computer-based attacks, and how they can disrupt service as well as inflame political tensions.

Pinpointing the culprits for such attacks is difficult or even impossible, officials say. Some suggest the July 4 weekend attacks a year ago may have been designed as a political broadside.

These officials point suspicions at South Koreans, possibly activists, who are concerned about the threat from North Korea and would be looking to ramp up antagonism toward their neighbor. Several experts familiar with the investigation spoke on condition of anonymity because the results are not final.

According to U.S. officials and private computer analysts, the attacks were largely restricted to vandalizing the public Web pages of about a half dozen federal agencies, including the Treasury Department and the Federal Trade Commission. About three dozen other sites were targeted, including some private companies and a number of South Korean government sites, which reportedly had the most damage.

While the questions of who did it and why are unanswered, many investigators and experts now do not consider it a critical case.

"It's about as frightening as someone driving around the block blowing their horn a lot," said James Lewis, cybersecurity expert and a senior fellow at the Center for Strategic and International Studies. "A lot of people could have done it, and it doesn't leave a lot of clues to their identity."

To Don Jackson, director of threat intelligence for Atlanta-based SecureWorks, a computer security consulting company, "it's a dead end as far as who did it. I don't think we've ever gone past that."

Those responsible, he said, "pulled it off so well, managed it so well - this was someone who has experience at running these types of attacks."

Jackson, whose company was among several private firms that studied the codes after the attack, said one possibility is that hackers in South Korea were the culprits.

South Korean sources had a mission and may have "wanted someone blamed for it," said Jackson. "It would further the point that North Korea has elite squads" of hackers targeting Seoul.

South Korean officials have pointed to North Korea as the suspected assailant, and experts agree that it is within the North's abilities to wage cyberattacks. More recently, however, a government-run website in South Korea was hit with a similar - although smaller - denial of service attack that officials said was traced to China.

"There are a number of national intelligence agencies who are creating cybercapabilities. It's a natural area of exploration," said retired Gen. Wesley Clark. "I wouldn't underestimate North Korea's potential in this space."

Denial of service attacks, Lewis said, don't leave detailed forensic clues

that a more directed intrusion, such as an effort to breach a sensitive government program, might leave.

Still, officials worry that even a large, well executed attack against critical controlling computer servers could interrupt service if directed at a power company or utility. A strike could disrupt financial markets if directed at Wall Street or hinder travel if aimed at transportation sectors.

Those systems tend to be more heavily protected. But an attack against a bank's website could prevent customers from having online access to their accounts and prevent them from paying bills. Such attacks can prove lucrative as an extortion tool, when hackers take down popular gambling sites and demand payment to end the disruption.

Despite the lack of a clear culprit, there are things investigators do know about last year's denial of service attack.

The malicious computer code was distributed through nine main control servers in four countries. It fanned out to infect about 60,000 computers around the world. Those computers - likely on the desktops of innocent victims - were linked together in what is called a botnet, and they flooded government websites with traffic, knocking them offline or slowing them down over the Independence Day holiday weekend.

Altogether, 43 sites were targeted, and the size of the attack suggested it required several people to carry it out. While some Treasury, FTC and State Department sites were slowed or shut down by the software attack, others such as the White House and Department of Homeland Security were able to fend it off with little disruption.

Other targets included Nasdaq and New York Stock Exchange, Voice of America, U.S. Postal Service, and Amazon and Yahoo.

Government officials and analysts say there has been some improvements in dealing with future strikes. Private contractors, such as the web hosting giant Akamai, has a redundant system that will move government sites to other servers if one is seeing an unusual or massive flow of traffic.

Agencies are now better prepared.

But, Jackson said, "as far as any better capability in tracking down actors or in attributing attacks to any individual or group, I don't know that we're any further along. I would seriously doubt it."

More information: Department of Homeland Security: http://www.dhs.gov/index.shtm
SecureWorks: http://www.secureworks.com/