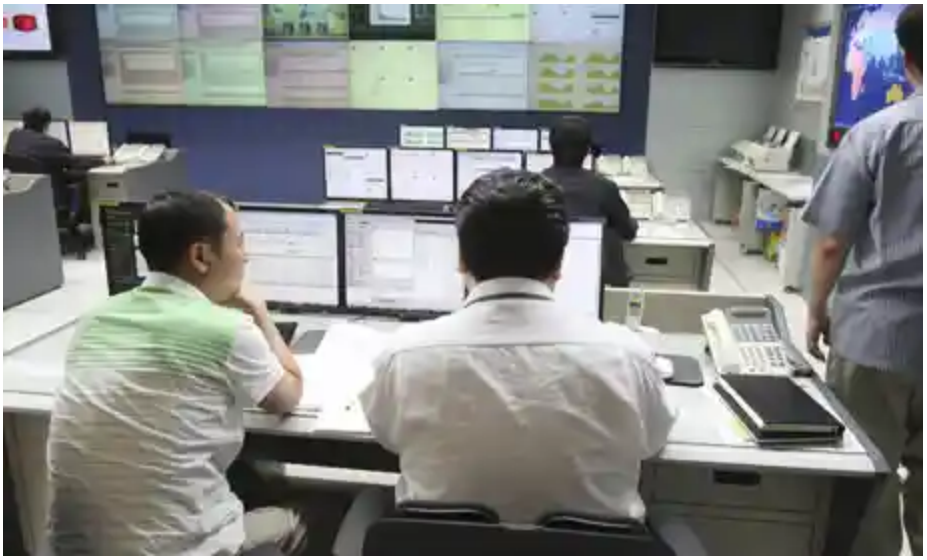
Cyber attackers target South Korea and US

theguardian.com/world/2009/jul/08/south-korea-cyber-attack

Matthew Weaver July 8, 2009

This article is more than **12 years old**
This article is more than 12 years old

South Korea sees presidential and bank websites paralysed as Pentagon and White House succeed in deflecting barrage



Staff at the Korea Internet Security Centre in Seoul. Photograph: Ahn Young-joon/AP
Staff at the Korea Internet Security Centre in Seoul. Photograph: Ahn Young-joon/AP

North Korean hackers are suspected of launching a cyber-attack on some of the most important government offices in the US and South Korea in recent days, including the White House, the Pentagon, the New York Stock Exchange and the presidential Blue House in Seoul.

The attack took out some of South Korea's most important websites, including those of the Blue House, the defence ministry, the national assembly, Shinhan bank, Korea Exchange bank and the top internet portal Naver.

Ahn Jeong-eun, a spokeswoman for Korea Information Security Agency, said the websites of 11 organisations had either gone down or had access problems.

The Associated Press reported that the White House, Pentagon and New York Stock Exchange were also targeted, but apparently deflected the electronic barrage. South Korea's Yonhap news agency said military intelligence officers were looking into the possibility that the attack may have been carried out by North Korean hackers and pro-North Korea forces in the South.

It resembles an attack that began last Saturday on government websites in the US, including some that are responsible for fighting cyber-crime.

John Bumgarner, director of research at the US Cyber Consequences Unit, said: "There's been a lot chatter recently about cyber-war. The North Koreans may have felt they were not getting enough attention launching missiles so they moved into another potential warfare – cyber. It's a form of sabre rattling. But the big question is, did the North Koreans launch it themselves or did someone do it for them?"

Yang Moo-jin, a professor at Seoul's University of North Korean Studies, said he doubted whether the North had the capability to knock down the websites.

But Hong Hyun-ik, an analyst at the Sejong Institute thinktank, said the attack could have been carried out by either North Korea or China, saying he "heard North Korea has been working hard to hack into" South Korean networks.

South Korea's National Intelligence Service told a group of politicians today that it believes that North Korea or its sympathisers were behind the attacks, a source at the meeting told Associated Press.

The agency refused to comment, but it confirmed it was working with US authorities to investigate the attack. It said it believed the attack was thoroughly prepared and committed "at the level of a certain organisation or state".

The attacks appeared to be linked to problems on the US sites, although investigators were still unsure who was behind them, Ahn said.

In the US, the treasury department, secret service, Federal Trade Commission and transport department websites were all down at varying points over the 4 July holiday weekend. Some of the sites were still experiencing problems last night.

The website of the Washington Post was also affected. Its computer security writer Brian Krebs blamed "malicious software" that ordered infected PCs to repeatedly visit targeted websites. A large proportion of the PCs involved were located in South Korea, he reported.

An initial investigation in South Korea found that many personal computers were infected with a virus ordering them to visit official websites in South Korea and the US at the same time, the Korean information agency official Shin Hwa-su said.

The US homeland security department confirmed that officials had received reports of "malicious web activity" and said they were investigating. Two government officials confirmed that the treasury and secret service sites had been brought down, and said the agencies were working with their internet service provider to resolve the problem.

Ben Rushlo, director of internet technologies at the website monitoring company Keynote Systems, called it a "massive outage".

Denial of service attacks against websites are not uncommon, and are usually caused when sites are deluged with internet traffic to take them offline. Documenting cyber-attacks against government sites is difficult, and depends heavily on how agencies characterise an incident and how successful or damaging it is.