'World's leading bank robbers': North Korea's hacker army

May 26 2021, by Sunghee Hwang

North Korea's cyber-programme dates back to at least the mid-1990s, when Kim Jong Il, father of the current leader Kim Jong Un reportedly said "all wars in future years will be computer wars"

Nuclear-armed North Korea is advancing on the front lines of cyberwarfare, analysts say, stealing billions of dollars and presenting a clearer and more present danger than its banned weapons programmes.

Pyongyang is under multiple international sanctions over its atomic bomb and ballistic missile programmes, which have seen rapid progress under North Korean leader Kim Jong Un.

But while the world's diplomatic focus has been on its nuclear ambitions, the North has been quietly and steadily building up its cyber capabilities, and analysts say its army of thousands of well-trained hackers are proving to be just as dangerous.

"North Korea's nuclear and military programmes are long-term threats, but its cyber threats are immediate, realistic threats," said Oh Il-seok, a researcher at the Institute for National Security Strategy in Seoul.

Pyongyang's cyberwarfare abilities first came to global prominence in 2014 when it was accused of hacking into Sony Pictures Entertainment as revenge for "The Interview", a satirical film that mocked leader Kim.

The attack resulted in the posting of several unreleased movies online as well as a vast trove of confidential documents.

Since then the North has been blamed for a number of high-profile cyberattacks, including a $81 million heist from the Bangladesh Central Bank as well as the 2017 WannaCry global ransomware attack, which infected some 300,000 computers in 150 nations.

Pyongyang has denied any involvement, describing US allegations over WannaCry as "absurd" and a foreign ministry spokesman declaring: "We have nothing to do with cyberattacks."

Pyongyang's cyberwarfare abilities first came to global prominence in 2014 when it was accused of hacking into Sony Pictures Entertainment as revenge for "The Interview", a satirical film that mocked leader Kim.

But the US Justice Department in February indicted three North Koreans on charges of "participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks".

In its 2021 Annual Threat Assessment Report, Washington acknowledged that Pyongyang "probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks" across the United States.

The North's cyber programme "poses a growing espionage, theft, and

attack threat," said the document from the Office of the Director of National Intelligence.

It accused Pyongyang of stealing hundreds of millions of dollars from financial institutions and cryptocurrency exchanges, "probably to fund government priorities, such as its nuclear and missile programs".

'The best defence'

North Korea's cyber-programme dates back to at least the mid-1990s, when then-leader Kim Jong Il reportedly said "all wars in future years will be computer wars".

Today Pyongyang's 6,000-strong cyberwarfare unit, known as Bureau 121, operates from several countries including Belarus, China, India, Malaysia and Russia, according to a US military report published in July 2020.

Scott Jarkoff of cybersecurity firm CrowdStrike rates them highly: "They are extremely sophisticated, dedicated, and capable of conducting advanced attacks."

North Korea has been blamed for a number of high-profile cyberattacks, including a $81 million heist from the Bangladesh Central Bank as well as the 2017 WannaCry global ransomware attack, which infected some 300,000 computers in 150 nations.

Bureau 121 recruits are trained in different coding languages and operating systems at special establishments such as Mirim University, said former student Jang Se-yul, who defected in 2007.

Now known as the University of Automation, it takes in only 100 students a year from among the North's highest-scoring schoolchildren.

"We were taught that we had to be prepared against America's cyberwarfare capabilities," Jang told AFP.

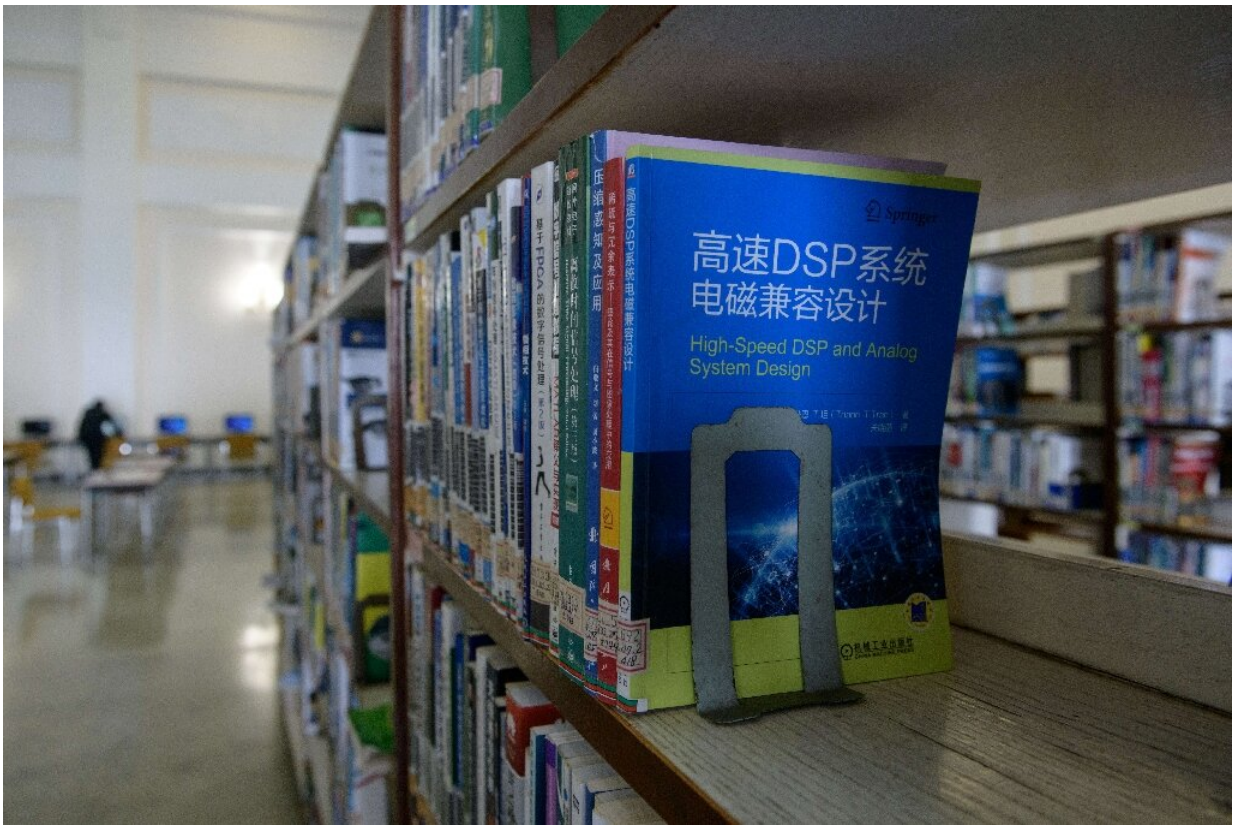
"Ultimately, we were taught that we had to develop our own hacking programmes since attacking the enemy's operating system is the best defence."

Cyberwarfare is particularly appealing for small, poor countries like the North that are "outgunned in terms of equipment such as planes, tanks and other modern weapons systems", said Stimson Center researcher Martyn Williams.

"Hacking just requires a computer and Internet connection."

Keyboards over guns

Most state-sponsored hacking groups are mainly used for espionage purposes, but experts say North Korea is unusual in also deploying its cyber capabilities for financial gain.



Most state-sponsored hacking groups are mainly used for espionage purposes, but experts say North Korea is unusual in also deploying its cyber capabilities for financial gain.

Pyongyang has blockaded itself to protect against the coronavirus pandemic, adding to the pressure on its economy, and has for years sought to earn foreign currency by multiple means.

And Williams added: "Stealing it is a lot faster and potentially more lucrative than doing business, especially if you have skilled hackers."

The February US indictment accused the three North Koreans of stealing more than $1.3 billion worth of money and cryptocurrency from financial institutions and companies.

When it was issued Assistant Attorney General John Demers called North Korea's operatives "the world's leading bank robbers", adding they were "using keyboards rather than guns, stealing digital wallets of cryptocurrency instead of sacks of cash".

The rise of cryptocurrencies such as Bitcoin have presented hackers globally with a whole new range of increasingly lucrative targets.

In addition, said Jarkoff, their decentralised networks were a particular bonus for the North, offering a way to circumvent financial sanctions.

"This allows North Korea to easily launder money back into the country, outside the control of the global banking system," he said.

"Cryptocurrency is attractive because it is uncontrolled, borderless, and relatively anonymous."

Citation: 'World's leading bank robbers': North Korea's hacker army (2021, May 26) retrieved 10 April 2024 from https://techxplore.com/news/2021-05-world-bank-robbers-north-korea.html