CO23001 | The Cyber Threat from Pyongyang

Nah Liang Tuang

05 January 2023

SYNOPSIS

Poverty-stricken North Korea spends a lot of its national resources on the military, including cyber, capabilities. Its cyber units, especially Bureau 121, are assumed to possess sophisticated cyber espionage capabilities, operating systems, and intrusion software; and the expertise to create highly destructive malware deliverable online to networked computers, or to standalone systems autonomous of the internet. Military and national security planners must implement relevant threat mitigation measures in the face of Pyongyang's cyber offensives.

Source: Freepik

COMMENTARY

North Korea's numerous missile tests in 2022, amid fears that it could also test a nuclear device, amounted to a well-worn strategy designed to put pressure on the US, South Korea, and Japan. However, it is inconceivable that Pyongyang would actually launch ballistic missiles at any of these countries as this would invite massive retaliation from the US and its allies. North Korea is more likely to continue with its cyber operations, which have been disruptive. The international community ought to be on guard against the actions of its cyber units, including the elite Bureau 121.

Refocusing on the Cyber Threat

For a nation where few have access to computers of any kind, and internet access is prohibited, North Korea or the Democratic People's Republic of Korea (DPRK) maintains a well-resourced, talented and highly trained cyber unit in the form of Bureau 121. This unit also operates from DPRK-friendly states like Belarus, China, India and Russia in order to circumvent North Korea's poor IT infrastructure and to mask the source of its online offensives.

From what is publicly known, in retaliation for the 2014 release of the movie, "*The Interview*", which was about the fictional assassination of Kim Jong-un, Bureau 121 or associated cyber operatives were thought to be responsible for the online theft of commercially damaging confidential information belonging to Sony Pictures Entertainment. Additionally, malware was used to erase Sony's vital operating systems.

Another cyber-attack by Pyongyang was the 2016 online infiltration of the Central Bank of Bangladesh, which resulted in US$81 million of Bangladesh's sovereign funds being illicitly withdrawn from their Federal Reserve Bank of New York account. Of this, only US$18 million was recovered.

But beyond commercial sabotage and grand theft, North Korean cyber-attacks can jeopardise national security and cause massive damage. The following section provides three possible scenarios in which such attacks can take place and for which countermeasures would be advisable.

Possible Cyber-attack Scenarios

The first scenario begins with the identification of key personnel from the military industrial complexes or government defence establishments of adversary states, who are deemed to be corrupt, susceptible to corruption or have compromising weaknesses. Pyongyang's cyber agents then employ purpose-built search engines to conduct exhaustive reconnaissance of the targeted organisation's system portals, which are in contact with the internet. Those managed by vulnerable software are then subjected to intrusion attacks by dedicated operating systems optimised to exploit such vulnerabilities.

Once entry into targeted networks is made, Bureau 121 then proceeds to steal non-encrypted data. A greater danger lies in its use of the organisational databases to locate the accounts of susceptible individuals, whose passwords can be derived from the victims' background details using software applications. Thereafter, these victims can be framed by the planting of fake evidence alleging corruption, or be bribed in various ways, or blackmailed into performing nationally detrimental activities such as providing de-encrypted secrets. Such cyber espionage is insidious as it quietly undermines the targeted state's security apparatus from within.

In the second scenario, the vulnerabilities created in the first scenario could be exploited to inflict greater harm. If compromised victims can be manipulated, motivated, or coerced into inserting a malware-infected data storage device into the standalone systems of vital infrastructure like water purification facilities, road traffic management systems, and rail transportation control systems, the results could be disastrous.

For government departments or large firms whose computer networks are linked to their employee's emails, the risk of malware infection is even greater. In such cases, the hackers can employ "spear phishing" attacks where small groups of individuals within these entities, identified via intrusion-based database reconnaissance, are investigated using available information sources. Emails can then be sent bearing malware infected attachments, which when opened, would spread malware into the network.

Beyond the physical catastrophes that could result from a malware-induced collapse of the aforementioned essential public services, public confidence in the authorities could also be affected. For instance, if “spear phishing” implanted malware resulted in incorrect pension payments and overstated tax bills nation-wide, there would be much public anger. During an election year, such vulnerabilities would allow the Kim regime to interfere in the domestic politics of targeted countries.

The third scenario is surgical and nefarious. After a successful network intrusion, the cyber operatives could seek out the personnel records of significant foreign officials strongly opposed to Pyongyang. The objectives would be to uncover the residential addresses of such persons, along with their vehicle licence plate numbers, and any other downloadable non-encrypted professional details. As with “spear phishing”, internet-based research will collect available information about the target’s private life to derive a holistic individual dossier, which can assist in creating an invitation to a fictitious event.

When the fake invitation is accepted, the espionage agents will then plant a remotely activated GPS spoofing device on the victim’s car. Since the fictitious event will be held in an unfamiliar location, the victim will probably rely on GPS for navigation wherein the spoofing device would be activated. This device will replace the real GPS map with one that will lead the victim to a location where he or she would be kidnapped or dispatched. The technology to undertake this is available.

These scenarios could apply to any nation with a sufficiently developed IT infrastructure. In the case of North Korea, concerns about its nuclear weapons programme should not cause us to overlook the threat of its cyber capabilities. How then should we deal with the threat?

Constant Vigilance and Preventive Measures

At the operational level, IT security technicians need to ensure that online infiltration filters like firewalls are constantly updated, networks frequently screened for malware, security software kept current, and data encryption protocols enforced, amongst other essential measures. Relevant authorities need to mandate that cyber security procedures be followed not only by government organisations and the defence industry, but also by all national security contractors.

Employees and IT users at all levels and in all security and defence related entities need to be taught network security and cyber hygiene, with annual recertification tests. Secure use of the internet and email including password setting, guarding against “spear phishing”, etc., need to be taught.

As for protecting standalone systems from physical malware infiltration, the recommendations include hardware surveillance like monitoring of equipment to detect abnormalities, and automatic shutdown to prevent damage from sabotage. Additionally, a precaution against compromised staff wilfully infecting the system is malware screening of all data storage devices, and regulated access to industrial networks guarded by biometric scans and security cameras.

Regarding abduction and/or assassination facilitated by GPS spoofing, preventive avoidance involves greater attention to personal security. Specifically, senior personnel should be advised that they are at risk from hostile intelligence agencies and to exercise caution when accepting invitations. When travelling to unfamiliar destinations, they ought to preview what the venue and its vicinity look like at street level using reliable e-platforms or be accompanied by other staff members.

Finally, cyber defence cooperation ought to be coordinated at the regional level, with friendly countries sharing intelligence about new malware, attack methodologies, target emphasis or other useful information about hostile cyber agencies.

Notwithstanding the headline grabbing potential of the DPRK's missile and nuclear programmes, it bears emphasising that the North Korean cyber threat is ever present, which necessitates sustained vigilance and defensive efforts.

About the Author

Nah Liang Tuang, PhD, is a Research Fellow at the Institute of Defence and Strategic Studies (IDSS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. His research interests include nuclear weapons politics, North Korean affairs, and the role of nationalism in the defence of small states.

Categories:

Last updated on 05/01/2023