The Incredible Rise of DPRK’s Cyber Warfare

blog.cybureau.org/the-incredible-rise-of-dprks-cyber-warfare/

Aahir Das

DPRK holds mass parade for Foundation Day (*Source: China Daily*)

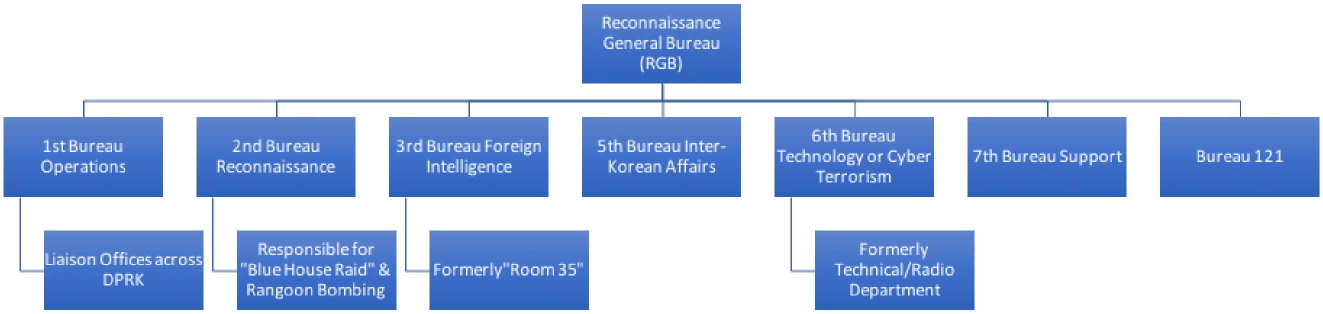
The military doctrine of the Democratic People’s Republic of Korea relies heavily on deliberate deception and denial operations. Their cyber capabilities despite the banning of any internet services all over the state, apart from their native intranet “Kwangmyong”, has been said to be rather longitudinal; it has gained notoriety for its past hacking activities, most remarkably the attacks against Sony Pictures Entertainment in 2014 and the Bangladesh bank heist in 2016, cryptocurrency and bank heists, and ransomware attacks. Of course, there is no way to cross-reference or verify whether its deliberate dissemination or accurate information. So, relying on any open-source information can result in an echo chamber effect of establishing them as evidential facts.

North Korea's existing political and military strategies can help provide context for understanding its cyber strategy. Traditionally, they have relied on a system of asymmetrical and irregular combination of warfare to sidestep the conventional military deadlock in the peninsula. Cyber capabilities would provide for a risk-minimized means of exploiting USA and ROK vulnerabilities at a low intensity. During peacetime, this can allow them to upset the status quo by using cost-effective strategies to target USA and ROK command control, computers, intelligence, surveillance and reconnaissance (C4ISR) in support of their "quick war, quick end" strategy.

Since the 1990s, the DPRK has come a long way in terms of cyber warfare, when the computer infrastructure was rudimentary at best. Kim Jong-il recognized the value of cyber capabilities back then, which gave North Korea ample time to recruit and train human resources and invest in institutions to develop and sustain the country's assets in cyberspace.DPRK's priorities in the realm of information and communications technology (ICT) are embedded in the leadership's national strategy, which is essentially composed of two main parts: national security and economic development. It is no different from any other state, except that the type of regime, division of the two Koreas, and its external environment presents several threats and challenges that affect its cyber posture.

North Korea, whose government is the only one on earth known to conduct nakedly criminal hacking for monetary gain, has run schemes in some hundred and fifty nations. Illustration by Anuj Shrestha.

When in 2009, the US National Intelligence Estimate dismissed North Korea, noting it would take years to develop them into a meaningful threat. Yet right around that time, that same year, North Korea reportedly unified all of its intelligence and internal security services and brought them under the direct control of the National Defense Commission to cement the control of current North Korean leader Kim Jong-un. It merged intelligence organizations and its various cyber units such as Bureau 121 into the Reconnaissance General Bureau (RGB). It later became their primary foreign intelligence service, and headquarters for cyber operations. In 2013, the RGB reportedly also established Unit 180, tasked with hacking international financial institutions to extract foreign currency in support of North Korea's nuclear and ballistic missile programs. It would also install malicious backdoors in software development businesses in Japan and China. Over the years, the focus of Unit 180 shifted toward targeting cryptocurrency exchanges while Bureau 121 has expanded its cyber operations beyond South Korea by attacking foreign infrastructure elsewhere.


Reconnaissance General Bureau (RGB)
1st Bureau Operations
2nd Bureau Reconnaissance
3rd Bureau Foreign Intelligence
5th Bureau Inter-Korean Affairs
6th Bureau Technology or Cyber Terrorism
7th Bureau Support
Bureau 121
Liaison Offices across DPRK
Responsible for "Blue House Raid" & Rangoon Bombing
Formerly"Room 35"
Formerly Technical/Radio Department

The RGB chain

North Korea’s cyber operations reflect at least three distinct characteristics. First, North Korea’s cyber units and hacker groups have shown considerable diversity in terms of their capabilities and experience. The line between low-end and high-end North Korean cyberspace operations has frequently been blurred. North Korea can employ non-state actors as surrogates, utilise low-cost, off-the-shelf tools that are freely available and exploit known techniques such as denial of service attacks.

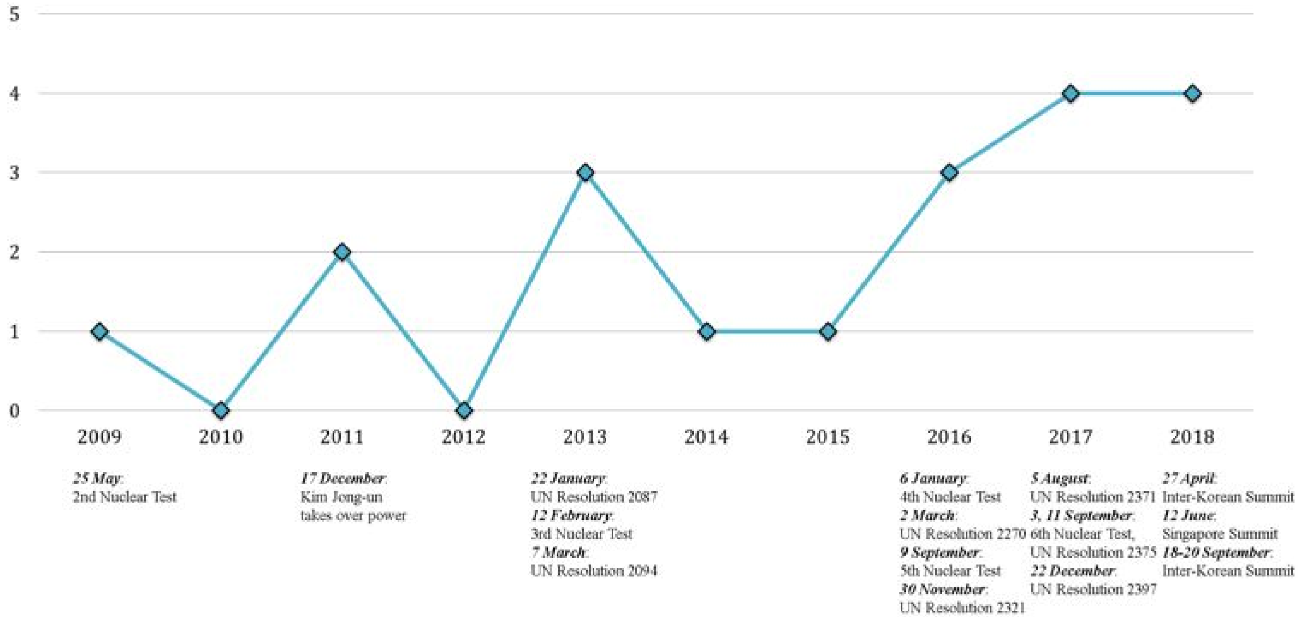
Second, North Korea has gradually demonstrated a resolve for cyber-escalation, targeting the critical infrastructure of other nation-states as well as private corporations and banks for varying political motivations. Increasingly, it also aims to achieve illicit financial gain by bypassing international sanctions and generating foreign currency.

Third, the essential ‘dialectics of North Korea’s cyberspace’ is asymmetric. Its internet infrastructure is isolated from global networks, with the country’s entire internet traffic channelled through only two providers — China’s Unicom and Russia’s TransTeleCom. The country is largely unplugged from the global internet and is ringfenced by China’s ‘Great Firewall’.

Source: VTech Solution Inc.

North Korean hacker groups have therefore been widely dispersed places elsewhere, such as China, Russia, Southeast Asia, and even Europe, acting independently or mutually supporting each other based on their specific cyber missions.

Thus, it is safe to say that the cyber operations carried out by North Korea are *not ad hoc, isolated incidents.* They are the accumulation of carefully planned efforts under the direction of preexisting organizations that directly support the country's national strategy. Knowing which organizations do this, is extremely crucial because they do not have a published cyber doctrine. The Reconnaissance General Bureau and General Staff Department of the Korean People's Army generally control most of North Korea's known cyber capabilities ranging from peacetime provocations to wartime disruptive operations.



The Evolution of North Korean Cyber Threats. *Source: The Asian Institute for Policy Studies*

North Korea has spearheaded fraudulent cyber operations to circumvent sanctions, gaining access to the international financial system and illegally forcing the transfer of funds from financial institutions, SWIFT banking networks, and cryptocurrency exchanges worldwide. At the same time, North Korea also has been able to protect its critical infrastructure from potential reprisals, limiting its access, dependencies, and vulnerabilities on the internet and communication networks by relying instead primarily on China's internet infrastructure. This has been augmented only recently with a second internet link to Russian networks, and dispersion of its hackers to select countries worldwide, including India, Nepal, Kenya, Mozambique, and Indonesia.

Consequently, North Korea's 21st-century cyber operations have essentially become weapons of mass effectiveness working alongside the weapons of mass destruction in its nuclear arsenal, together composing a unified asymmetric political strategy designed to pressure the United States and the wider international community to recognize as legitimate Supreme Leader Kim Jong-Un's interpretation of North Korea's sovereignty and security. Lately, Kim Jong Un has quietly built a 7,000-man cyber army that gives North Korea an edge nuclear weapons does not.

As Kim reportedly declared in 2013, "cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."

תגובות

תגובות