Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations

Mandiant believes that North Korea's cyber capability supports both long-standing and immediate political and national security priorities, as well as financial goals. We assess most of North Korea's cyber operations, including espionage, destructive operations, and financial crimes, are primarily conducted by elements within the Reconnaissance General Bureau. Meanwhile, the Ministry of State Security and United Front Department's missions appear to play limited roles in North Korea's cyber program. Open-source reporting often uses the *Lazarus Group* title as an umbrella term referring to numerous North Korean cyber operators, however, understanding the different institutions within this secretive hermit nation and how they continue to evolve and share resources aids organizations in proactively defending from these types of threats. Mandiant judges North Korea's intelligence apparatus possesses the flexibility and resilience to create cyber units based on the needs of the country. Additionally overlaps in infrastructure, malware, and tactics, techniques and procedures indicate there are shared resources amongst their cyber operations.

Figure 1 is an assessed cyber organizational chart derived from various OSINT, targeting patterns, malware usage, and defector reporting that shines some light onto a seeming change taking place within the North Korean cyber ranks.

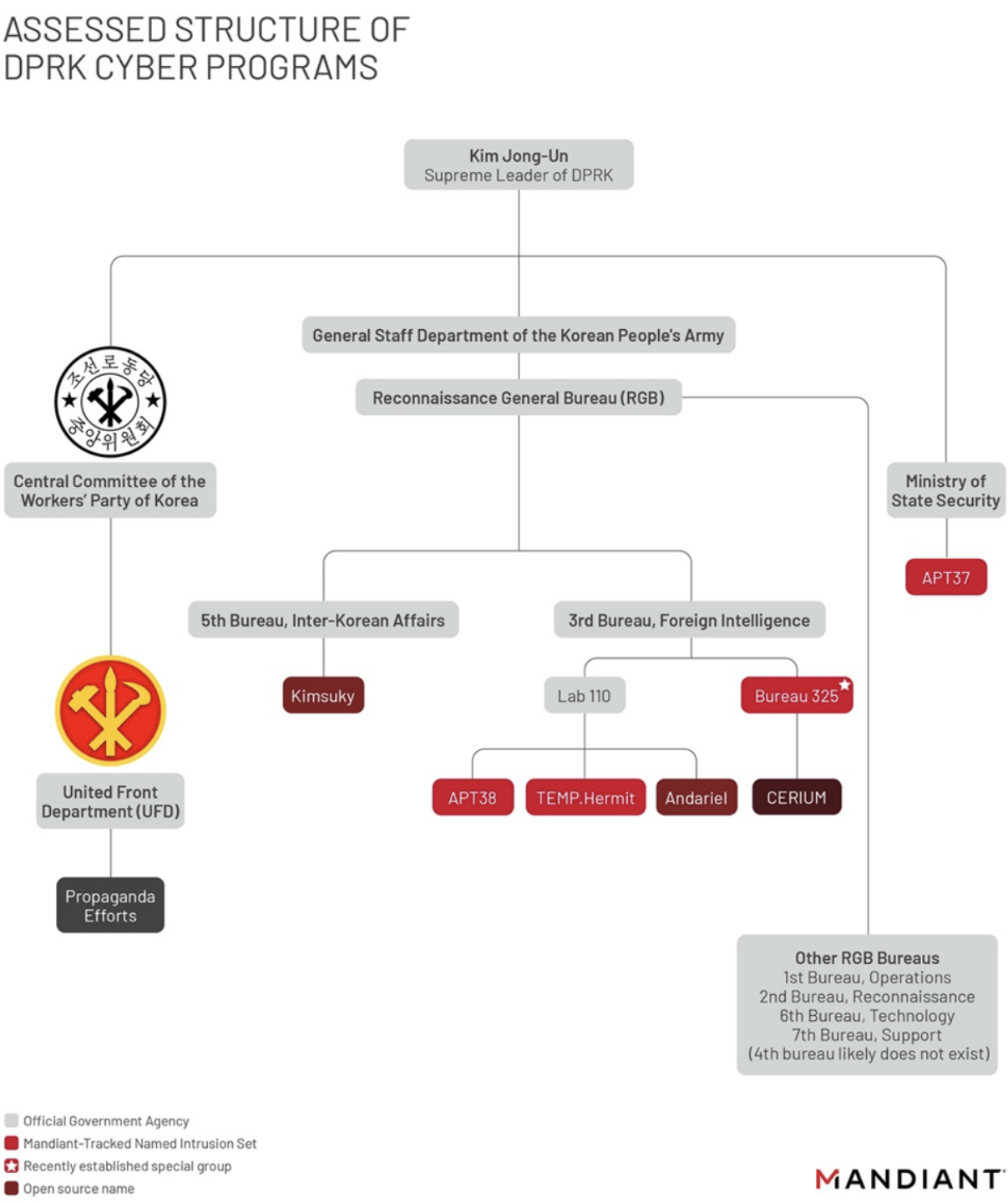

Figure 1: Assessed cyber structure of DPRK cyber programs

United Front Department

UFD is an organization sponsored by the Central Committee of the Workers' Party of Korea. Although it is comprised of operating groups that may not correspond to well-known “cyber actors”, the organization's overall effort centers around disseminating pro-regime propaganda targeting South Korea, likely to undermine their primary geopolitical rival. The UFD typically leverages online information operations, including an "army of cyber trolls," to promote pro-DPRK political narratives on web forums as well as conventional propaganda efforts, such as leaflets and radio broadcasts targeting their southern neighbor.

In a two-year span, these “cyber trolls” allegedly hijacked South Korean users accounts online and posted an estimated 68k propaganda items in web forums and various comment sections in an attempt to

amplify the regimes' message in South Korea. This organization's end goal is the establishment of pro-North Korean groups within South Korea

Ministry of State Security

The MSS is the DRPK's primary counterintelligence service which operates as an autonomous part of the government and is primarily tasked with domestic counterespionage and overseas counterintelligence activities. APT37's previous campaigns targeting foreign joint venture partners as well as threat activity against defectors, defector support agencies, and humanitarian organizations indicate APT37's activities most likely align with the agenda of MSS.

- **APT37**'s assessed primary mission is covert intelligence gathering in support of DPRK's strategic military, political, and economic interests. A lack of recent, significant activity from this actor matched with an uptick in similar targeting from units within the "Kimsuky" actor-set may indicate a shift or consolidation within North Korea's cyber leadership.

Reconnaissance General Bureau: An Overview

The RGB is the North Korea's primary foreign intelligence service, responsible for intelligence collection and clandestine operations. It is believed to be comprised of six bureaus:

- 1st Bureau: Operations
- 2nd Bureau: Reconnaissance
- 3rd Bureau: Foreign Intelligence
- 5th Bureau: Inter-Korean Affairs
- 6th Bureau: Technology
- 7th Bureau: Support

Notably, a 4th bureau does not exist likely because the number "4" is considered taboo.

While cyber efforts are a portion of the organization's overall operations, the 3rd Bureau (Foreign Intelligence) and 5th Bureau (Inter-Korean Affairs) appear to hold the "meat and potatoes" of North Korea's cyber program.

Reconnaissance General Bureau: 3rd Bureau

Lab 110…the focal point for the Lazarus Group Umbrella

TEMP.Hermit, APT38, and Andariel are likely subordinate to Lab 110. Lab 110 is likely an expanded and reorganized version of "Bureau 121," often noted as North Korea's primary hacking unit. Lab 110 contains some elements that are most closely aligned with the organization, publicly reported as "Lazarus Group." Open-source reporting often uses the Lazarus Group title as an umbrella term, referring to numerous clusters that we track separately. Although TEMP.Hermit is most frequently aligned with *Lazarus Group* reporting, often times, researchers and open sources lump all three of these actor sets – and sometimes even all of the North Korean APTs – merely as "*Lazarus Group*".

- **TEMP.Hermit** is an actor that has been around since at least 2013. Their operations since that time are representative of Pyongyang's efforts to collect strategic intelligence to benefit North Korean interests. This actor targets government, defense, telecommunications, and financial institutions worldwide and the term "*Lazarus Group*" refers most often to this cluster of activities.
- **APT38** is a financially motivated group sponsored by North Korea, known for significant financial compromises and its use of destructive malware against financial institutions. The group has been attributed to sophisticated compromises targeting Interbank Fund Transfer Systems to steal millions of dollars at a time across multiple countries worldwide.
- **Andariel** focuses its operations on foreign businesses, government agencies, financial services infrastructure, private corporations, and businesses, as well as the defense industry. The group also conducts cyber crime likely as an extra source of income to the government as we observed in signature malware activity by this actor; however, targeting of military and government personnel appear to be the primary focus.
- **Bureau 325** was publicly announced in January 2021, when the structure of the RGB likely shifted in response to the coronavirus (COVID-19) pandemic. The new unit appeared to take on primarily conducting intelligence gathering operations against COVID-19 research and manufacturing organizations. Defector reporting also stated that in January 2021, the unit was not fully operational. Overtime, we have observed sharing of efforts and "non-COVID-19" type of activities, indicating this actor may be nearing the milestone that defector reporting states, "...*the group will soon begin 'full-scale' operations*". This newly formed Bureau 325 houses the DPRK COVID-19-focused unit and corresponds to activities tracked in the open source as "CERIUM". We suspect that individuals from several previously tracked clusters – including TEMP.Hermit, and Kimsuky – were also drafted to Bureau 325 to respond to high-priority operations from DPRK leadership.
    - Over time, we began to see this organization shift from "strictly COVID-19" efforts to the targeting of defectors, defense and governments, bloggers, media, cryptocurrency services, and financial institutions. This increase in responsibilities indicates the group has quickly gained the confidence of DPRK's senior leadership and likely gained prominence. Defenders will continue to see Bureau 325's fingerprints on more campaigns in the wild.

Reconnaissance General Bureau: 5th Bureau

There are overlaps that indicate cyber elements of the UFD share interests regarding issues on the Korean peninsula and share targeting overlaps with APT37; however, these extra elements appear to be supplemental to the 5th Bureau's overall mandate.

- **Kimsuky** is an actor often conflated in OSINT that conducts targeted campaigns to collect strategic intelligence on geopolitical events and negotiations affecting the DPRK's interests. The actor primarily targets organizations in the U.S. and South Korea, including individuals working within the government, military, manufacturing, academic, and think tank organizations that possess subject matter expertise in defense and security, particularly nuclear security and nonproliferation policy. This threat actor's activities include collecting financial, personal, and client data specifically from academic, manufacturing, and national security industries in South Korea. The most likely reason is for the purpose of setting up further infrastructure for cyber espionage operations, leveraging personas for phishing campaigns, or carrying out identity theft and fraud.

Conclusion

The country's espionage operations are believed to be reflective of the regime's immediate concerns and priorities, which is likely currently focused on acquiring financial resources through crypto heists, targeting of media, news, and political entities, information on foreign relations and nuclear information, and a slight decline in the once spiked stealing of COVID-19 vaccine research. Information collected in these campaigns will possibly be used to develop or produce internal items and strategies, as in vaccines, mitigations to bypass sanctions, funding for the country’s weapons programs, and so on. Additional information continues to be collected to determine the extent to which these groups operate and streamline their operations. Being able to see though the intentional fog left by North Korean leadership, and able to identify targeting patterns that align to physical units allows for a proactive defense against these cyber operators. This effort is critical in a country where little is known to the outside world and defector reporting supplemented with cyber operations can help.