Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Loose Cobras:

DPRK regime succession and uncertain control over offensive cyber capabilities

MAY 2020

JD WORK

EXECUTIVE SUMMARY

- The world does not yet know if Kim Jong Un is incapacitated, or dead, as has been rumoured in April 2020. However, any potential transition of leadership raises concern over control of strategic weapons – including offensive cyber capabilities commonly referred to as HIDDEN COBRA.

- If the DPRK succession does not occur smoothly, multiple scenarios may be considered where HIDDEN COBRA threat activity may result in new intrusion or attack against critical infrastructure targets. These include potential action on pre-planned contingency plans for retaliation in the event of conflict arising out of miscommunication or other mistakes, attempts to acquire new illicit revenue to cover the ever-rising costs of ensuring loyalty to a new successor, or incidents driven competition and opportunism in the disorder inherent to contested transition where no heir has yet clearly emerged.

- The opaqueness of the regime is likely to be aggravated by crisis, limiting opportunities to observe prospective regime threat activity and provide further warning across these scenarios.

Unconfirmed rumors surfaced in mid April 2020 regarding the potential incapacitation of North Korean leader Kim Jong Un, leading to speculation about the ramifications of a sudden transition of leadership in Pyongyang. These rumors have once again raised serious concerns over the stability of the Democratic People's Republic of Korea's (DPRK) control of strategic weapons, including nuclear and ballistic missiles.[1] Any regime succession scenario in an autocracy involves the potential for a contested transition with different factions competing for ultimate authority from differing bases of power, influence, and resources. Control of strategic weapons becomes a key prize in such struggles, leading to longstanding nightmares of potential "loose nukes" no longer fully under the authority of a unitary government. Political power contests are particularly risky within the North Korean system, as it remains both famously opaque and notoriously prone to political violence and personal retribution. These worries are familiar to the international affairs community from multiple earlier crisis moments.[2] A prospective change of leadership in Pyongyang also uniquely takes place as a family affair, within a political dynasty built around the perceived legitimacy of the Kim bloodline.

In particular, the international community's fears surrounding a North Korean transition of power are compounded by its questions about control of offensive cyber operations capabilities. In the case of intrusion sets, or malign offensive cyber actors attributed to the DPRK, known commonly under the umbrella term HIDDEN COBRA, the risk of unanticipated actions triggered by a transition crisis are magnified by these groups' high operational tempo and their varied selection of targets, both unrestrained by any sense of international norms.[3] Efforts to understand DPRK-attributed threat activity groups face many challenges limiting the ability to gather information. To date, intelligence efforts focus primarily on observed technical artifacts and operational patterns, paying less attention to the operators behind the keyboard, or to the organizational structures in which these operators work. However, it remains notoriously difficult to gather facts and information regarding the situation on the ground in Pyongyang, let alone from within the compound at Wonsan where Kim allegedly sheltered from the ongoing coronavirus pandemic. Yet even without a full picture, the international community may still consider a number of potential scenarios upon the death of Kim Jong Un, whether at this moment, or at some unknown point in the future.

DEAD HAND SCENARIO

The first scenario of immediate concern is that of Dead Hand control. This involves the pre-delegation of authorities to automatically execute cyber attacks in the wake of the death or incapacitation of DPRK leadership. The Dead Hand command and control architecture for offensive cyber operations has been contemplated for almost a decade among multiple adversaries. In this system, loss of positive direction from national leadership triggers immediate pre-planned strikes against the United States and its allies. HIDDEN COBRA sustains routine, recurring intrusion accesses within multiple financial, energy, transportation, defense and government, media, and telecom networks—many of which have remained active for extended periods of months before detection and remediation.[4] These accesses may be leveraged to generate prompt destructive effects.

Dead Hand control is modeled on early nuclear warfighting concepts including the reported Russian system Perimeter, which issued attack orders to the strategic rocket force and other nuclear warfighting components, automatically triggered by disruption of communications with national command authorities. The Russian system was intended to assure second strike retaliation in the event of successful surprise attack resulting in leadership incapacitation. Multiple actors have adapted these nuclear concepts in offensive cyber operations, initially as a measure to harden botnet command and control in the face of law enforcement and security takedowns.[5] Given the degree to which command and control of the North Korean state has been centralized to Kim Jong Un, and to a wider extent to the Kim bloodline, it remains unclear how military and intelligence services may respond to the sudden loss of their leader, or even disruption in the flow of routine orders. Such responses may include action on any standing pre-delegation of authority to initiate offensive strikes. The

1 Economist Intelligence Unit, "North Korea politics: Reports of leader's illness stoke regime stability concerns," April 22, 2020.

2 Bruce W. Bennett and Jennifer Lind, "The Collapse of North Korea: Military Missions and Requirements," *International Security*, 36:2 (2011), 84-119, http://www.belfercenter.org/sites/default/files/files/publication/Collapse_of_North_Korea.pdf; Bruce Cummings, "The Kims' Three Bodies: Communism and Dynastic Succession in North Korea," *Current History* 111:746 (2012), 216-222, http://www.currenthistory.com/Article.php?ID=990.

3 For summary of the HIDDEN COBRA intrusion set, see Departments of State, the Treasury, and Homeland Security, and Federal Bureau of Investigation. "Guidance on the North Korean Cyber Threat," 15 April 2020, https://www.us-cert.gov/ncas/alerts/aa20-106a.

4 "Critical Infrastructure Threat Actor Spotlight: TEMP.Hermit," *FireEye*, October 24, 2018.

5 David Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and its Dangerous Legacy*, (New York: Knopf Doubleday, 2009); iSIGHT Partners, "Potential 'Dead Hand' C&C Architecture Suggested by Adversary Adaptation Following Failed Botnet Takedown Attempt," February 2011; JD Work, *Autonomy & Conflict Management in Offensive & Defensive Cyber Engagement*, (Nashville, Tennessee: IWCon, April 2016).

Source: Pixabay

potential for catastrophic escalation of otherwise "normal" frictions under such conditions has been considered in terms of a nuclear crisis, and such concerns are equally valid in the case of offensive cybersecurity operations.[6]

This scenario raises particular dangers where a pre-programmed strike from DPRK may involve out-of-theater retaliation capabilities, staged to provide assured second-strike offensive cyber options in the event of conflict on the Korean Peninsula. Components assigned to carry out these strikes may potentially include at least some subset of DPRK threat activity groups known variously as APT37, REAPER, Scarcruft, Group123, and Richochet Chollima, based on industry reporting suggesting broader global presence and round-the-clock operations cycles.[7] While these elements have likely been assigned other primary missions, a contingency role cannot be ruled out.

DPRK's ability to maintain its presence abroad has been substantially degraded in recent years by international diplomatic pressure and continuing sanctions that have disrupted cover companies and associated intelligence service basing options. This pressure has likely also degraded DPRK's ability to sustain offensive cyber teams in a number of countries. However, even a small number of surviving threat activity groups would be sufficient to initiate pre-planned offensive operations. This is especially true where reconnaissance, initial access footholds, and construction of tailored payloads have been previously built up over time within the headquarters components of the Korean People's Army (KPA) Reconnaissance General Bureau.

North Korean-attributed intrusion operations targeting the United States and its allies' critical infrastructure have been observed corresponding during earlier periods of heightened conflict risk. Beyond well-known financial sector intrusions, DPRK has targeted electrical and other energy sectors in actions which have encompassed attempted compromise of US utilities in September 2017, as well successful intrusions against global nuclear energy generation targets on multiple occasions, including incidents ongoing through early 2019.[8] Such networks almost certainly remain ongoing targets of interest and would be priorities for destructive effects in a Dead Hand tasking model.

The dangers of a Dead Hand scenario resulting in prompt destructive cyber actions are greatest in the initial hours or days of a transition crisis. This is especially true where even outer circles of North Korean elites may not be fully aware of developments pertaining to Kim Jong Un's health, given the regime's tendency to limit information deemed threatening to the image of the Kim family. The tight restrictions on news of Kim Jong Il's death in 2011 offers a likely precedent. A lack of formal transition planning, due to the unexpected nature of Kim Jong Un's rumored health concerns, only exacerbates this uncertain and reactionary atmosphere. The fears and speculation of elites outside of the family circle may therefore supplant verifiable information. As a result, a small number of intermediate leadership elements may in fact execute retaliation scenarios for which authorities had been pre-delegated by the younger Kim. Execution of offensive cyber operations may be driven by orders arising from miscalculation, or worse yet, middle management failure to countermand standing orders triggered by some misunderstood version of events.

---

6 Jeffrey Lewis, *The 2020 Commission Report on the North Korean Nuclear Attacks Against the United States*, (Boston: Houghton Mifflin Harcourt, 2018).

7 "APT37 (Reaper): North Korean Cyber Espionage Group Expands Its Focus and Capabilities," *FireEye*, last updated February 20, 2018. https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf; "RICOCHET CHOLLIMA: Campaigns Spanning 2016 to 2018," *CrowdStrike*, April 4, 2018; Marie Baezner, "Cyber disruption and cybercrime: Democratic People's Republic of Korea," *ETH Zurich*, June 2018, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314511/Cyber-Reports-2018-03.pdf.

8 "DPRK Actors Target Korea Hydro and Nuclear Power Co with MBR Wiping Malware," *CrowdStrike*, December 2014.; "In Wake of Escalating Tensions Between DPRK and U.S., DPRK Destructive Attacks Remain a Concern," *CrowdStrike*, April 20, 2017; Cyber Conflict Documentation Project, "JUCHE PHOENIX: Considering potential DPRK destructive campaigns against US critical infrastructure networks," October 2017; "LEADLIFT Activity May Have Impacted India's Kudankulam Nuclear Power Plant," *FireEye*, October 29, 2019; "LEADLIFT Infection at Kudankulam Nuclear Power Plant Likely Espionage Driven, Compromise Occurred Prior To March 2019," *FireEye*, November 1, 2019; "Technical Analysis of KKNPP Tailored LEADLIFT Malware," *FireEye*, November 27, 2019.

Since the most recent rumors regarding Kim Jong Un's health have stretched over multiple days (and perhaps even weeks), the immediacy of this retaliation scenario is somewhat diminished. However, the prospect of such action may take on a new dimension depending on the timing and manner in which the party is directed to acknowledge Kim Jong Un's death or serious health complications, should they need to do so. This consideration is compounded by risks arising from the potential irregularities inherent in any scenario other than a smooth transition. North Korea's offensive cyber cells deployed around the world may be expected to be isolated from key internal information flows, particularly through informal channels, and therefore the officers responsible for key tactical decisions are likely poorly informed. As a result, it is possible that they may react to conflicting narratives or even deliberate disinformation emanating from Pyongyang. The risks of such misinformed aggressive actions become magnified should DPRK attempt to place blame for Kim Jong Un's passing on the usual external enemies highlighted in their propaganda.

KINGMAKER SCENARIO

Cyber operations previously played a linchpin role in Kim Jong Un's ascension to power. The line of succession to follow Kim Jong Il remained profoundly unclear throughout the '00s. While a familial dynasty was considered the most likely outcome, Kim Jong Un's then youth and lack of leadership experience did not suggest he would emerge as the favored son.[9] However, he was reported to have been deeply involved in early cyberattacks in July 2009 against the US and Republic of Korea (ROK) governments, as well as global military and financial sector targets.[10] These attacks were followed in March 2010 by the cyberattack on the ROK corvette Cheonan, in which Kim Jong Jun was allegedly personally involved.[11] Kim Jong Un was rewarded in October 2010 with a four star general rank, having ably demonstrated his ability to engage and manage the Korean People's Army and Reconnaissance General Bureau.[12]

Offensive cyber operations continued to underpin the consolidation of Kim Jong Un's control of the regime after Kim Jong Il's death. This required cementing the support of key military and intelligence factions, and eliminating potential rivals.[13] Ongoing attacks against South Korean targets, including media companies, demonstrated his ideological commitment. Successful breaches of banking networks, continued cryptocurrency mining, and other online theft campaigns created a steady flow of illicit revenue to support the young leader's efforts to buy personal loyalties and direct funding elsewhere in the North Korean regime.[14]

Control of these capabilities, reportedly managed in part through the consolidated Korean Worker's Party (KWP) function known informally as Office 39, may thus serve as kingmaker for Kim Jong Un's successor, whether through direct institutional authority or backroom political support. This sprawling enterprise, allegedly run much like an ongoing racketeering conspiracy, manages global front companies, smuggling networks, and money laundering exchanges. Office 39's prior director, Jang Song-thaek, was one of Kim Jong Un's most important early mentors. In return for that support, Kim Jong Un offered him political redemption. Jang finally fell from favor following his failure to respond effectively to tightening sanctions, leading to his execution in late 2013 and the exile of his wife Kim Kyong-hui, who would not reappear until January 2020.[15] Jang would be one of the highest profile victims of what became a major government purge, resulting in the

9 "North Korea: Succession is regime's weakness," in *Oxford Analytica* (November 2005); "North Korea: Succession process risks failing," in Oxford Analytica (June 2009); David W. Shin, "North Korea's Post-Totalitarian State: The Rise of the Suryong (Supreme Leader) and the Transfer of Charismatic Leadership," *American Intelligence Journal*, 33:1 (2016): 31-48, https://www.jstor.org/stable/26202164.

10 JD Work, "Clouded ice: Examining cyber intelligence assessments of the Independence Day 2009 cyber attack," (limited distribution paper for closed cyber operations study group, September 2010).

11 Jae-Cheon Lim, "North Korea's Hereditary Succession: Comparing Two Key Transitions in the DPRK," Asian Survey, 52:3 (2012), 550-570, https://as.ucpress.edu/content/52/3/550; Bruce E. Bechtol, *The Last Days of Kim Jong-il: The North Korean Threat in a Changing Era*, (University of Nebraska Pres, 2013).

12 Sebastien Falletti, "Kim Jong-Il's Son Promoted to General," Jane's Defence Weekly (October 6, 2010); Sebastien Falletti, Duncan Lennox, Ted Parsons, "Pyongyang Shows Off Hardware and New Heir," Jane's Defence Weekly (October 20, 2010).

13 Reuben F. Johnson, "North Korean Charm Offensive Suggests Kim Consolidating Position," Jane's Defence Weekly (June 4 2014); James Hardy and Sebastian Falletti, "Seoul urges vigilance after Chang execution," Jane's Defence Weekly (December 18, 2013); "Pyongyang's new master spies," *Intelligence Online*, January 14, 2015, https://bit.ly/2zwoQmt; Economist Intelligence Unit, "North Korea politics: High-profile executions raise questions about stability," May 22, 2015.

14 Soo Kim, "Luxury Goods in North Korea: Tangible and Symbolic Importance to the Kim Jong-un Regime," *On Korea Academic Paper Series, Korea Economic Institute of America* (2014), http://keia.org/sites/default/files/publications/2013_luxury_goods_in_north_korea.pdf; "North Korea, Iran, and Other Isolated Regimes May Increasingly Use Cyber Crime Capabilities," *FireEye*, (May 18, 2017); "Baselining North Korean Cyber Capabilities," *CrowdStrike*, (August 3, 2017); "Threats to Cryptocurrencies," *FireEye*, (August 10, 2017); "Office 39: North Korea's Money Maker," *CrowdStrike*, (December 5, 2017); "Organizational Overview of Bureau 121: The Suspected DPRK Cryptocurrency Miner," *CrowdStrike*, (February 26, 2018); "Country Profile: North Korea," *FireEye*, (March 8, 2018).

15 Ju-min Park and Jack Kim, "Handsome accordion player is North Korea's kingmaker," *Reuters*, December 23, 2011, https://www.reuters.com/article/us-korea-north-jang/handsome-accordion-player-is-north-koreas-kingmaker-idUSTRE7BM0BA20111223; Choe Sang-Hun, "Kim's Aunt Re-emerges After Six Years," *New York Times*, January 27, 2020, https://www.nytimes.com/2020/01/25/world/asia/north-korea-kim-jong-un-aunt.html

reported murder of hundreds. This in turn led to the defection of other key Office 39 staff and disruption to Kim Jong Un's illicit fundraising.[16]

It is no coincidence that one of the key inner circle figures in prospective line of succession is Kim Jong Un's younger sister Kim Yo-Jong, who reportedly took Kim Kyong-hui's position in the Politburo. She had studied at Kim Il-sung University, an institution reportedly involved in cryptocurrency mining operations for the regime. More importantly, by some accounts Yo-Jong is also married to Choe Song, the current director of Office 39 and son of KWP Secretary Choe Ryong-hae. [17]

While Kim Yo-Jong's role in advancing her brother's interests abroad has had mixed results, and led to uncertainty about her status and relative prominence, her ties to critical revenue streams offer a powerful advantage in any transition scenario. Yo-Jong's place in the current uncertain period is also unique in that she has continued to speak for her brother, assuming an important role of responsibility during Kim Jong Un's reported incapacitation, though detailed timing remains unclear.[18] Evidence of her ideological stance and policy preferences, to the extent that these may be discerned while her brother has been in power, suggest she would sustain the country's current strategic direction.[19] Such continuity would presumably incentivize the support of key regime power centers including both Office 39 and the Reconnaissance General Bureau.[20] Even if she does not assume the highest seat in government, her support—or her elimination—will be critical to the ultimate victor.[21]

ROGUE FACTION SCENARIO

As with any strategically significant capability, a scenario exists where a dissident faction takes advantage of the disorder inherent to transition periods to pursue external attacks for its own objectives. The risks for rogue command of offensive cyber capabilities are likely more pronounced than comparative nuclear command and control scenarios, due to the degree of decentralized control over cyber actors as opposed to the centralization of launch authorities for nuclear release. The degree of personal control exercised by the North Korean Supreme Leader over ballistic missile systems and associated nuclear warheads is more likely to preclude origination of falsified orders, or misguided action on such orders in case of irregularities.[22] However, this is an unproven hypothesis that may be tested in a transition crisis. While nuclear assurance is a relatively more mature problem for multiple military organizations, the newer issues associated with offensive cyber approval and direction are as yet understudied.[23] These process matters are further complicated by the unconventional, and frequently non-military, nature of key cyber threat activity groups. How such already murky concerns then play out in the opaque HIDDEN COBRA organizational structure remains a mystery. Likewise, the reaction of these entities under the stress of a transition crisis remains nearly impossible to predict.

However, offensive cyber action against ROK, US, or other global targets driven by factional competition within the North Korean government is unlikely to become a reality without internal pressures in which success of an operation would advantage a given faction. The most plausible circumstances

16 Baik Sungwon, "High-level North Korean Official Defected After Watching Executions," *Voice of America*, June 28, 2017, https://www.voanews.com/east-asia-pacific/executions-brutal-purges-prompted-high-level-north-korean-official-defect

17 CrowdStrike, "Kim Il Sung University: Where DPRK Student Hackers Mine Monero Cryptocurrency," March 8, 2018.

18 Sarah Kim, "Pyongyang refutes Trump's claim of correspondence from Kim," JoongAng Ilbo, April 21, 2020.

19 "Kim Yo Jong, sister of Kim Jong Un, lashes out at "foolish" South Korea," Korean Central News Agency, March 3, 2020, https://www.nknews.org/2020/03/kim-yo-jong-sister-of-kim-jong-un-lashes-out-at-foolish-south-korea/; "WPK Central Committee plenary session sets forth head-on offensive policy," Pyongyang Times, January 4, 2020, http://www.pyongyangtimes.com.kp/?bbs=32633.

20 Hannah Cotillon, "Government stability and policy direction continuity likely despite North Korean leader's probable ill health," IHS Global Insight, April 23, 2020.

21 Anna Fifield, "Kim's Real Secret Weapons," Telegraph, July 13, 2019, https://www.pressreader.com/uk/the-daily-telegraph-telegraph-magazine/20190713/281513637715951

22 Jordan Seng,"Less is more: Command and control advantages of minor nuclear states," Security Studies 6:4 (1997), 50-92, https://doi.org/10.1080/09636419708429322; Vipin Narang and Ankit Panda, "Command And Control In North Korea: What A Nuclear Launch Might Look Like," *War on the Rocks*, September 15, 2017. https://warontherocks.com/2017/09/command-and-control-in-north-korea-what-a-nuclear-launch-might-look-like/; Vipin Narang and Ankit Panda, "Thinking Through Nuclear Command and Control in North Korea," *The Diplomat*, September 16, 2017, https://thediplomat.com/2017/09/thinking-through-nuclear-command-and-control-in-north-korea/; Daniel Wertz, Matthew Mcgrath, and Scott LaFoy, "North Korea's Nuclear Weapons Program," National Committee on North Korea, April 2018, https://www.ncnk.org/resources/publications/DPRK-Nuclear-Weapons-Issue-Brief.pdf; Giles David Arceneaux, "Beyond the Rubicon: Command and Control in Regional Nuclear Powers," Syracuse University, August 2019, https://surface.syr.edu/cgi/viewcontent.cgi?article=2081&context=etd.

23 Adam S. Morgan and Steve W. Stone, "Command and Control for Cyberspace Operations - A Call for Research," *Military Cyber Affairs* 4:1 (2019), https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1051&context=mca.

leading to such a scenario would involve a contested transition where no heir has yet clearly emerged. The uncertainties of a fight for leadership, especially over an extended crisis duration, may be seen among KWP and KPA elites as inviting external intervention by other parties. Such interventions may include unwanted Chinese influence, or even prospective US-ROK mobilization or Japanese response. Such eventualities may occur in any circumstance as a contingency measure for enhanced crisis readiness. An aspiring successor and their supporters may therefore believe that destructive cyberattacks could offer a low-risk option to push back against possible intervention from foreign governments, with less potential to trigger international response than kinetic campaigns or use of strategic capabilities.

Attacks against the key resources supporting political rivals competing for the most senior leadership roles in the event of a sudden political vacuum may also appear as a variation on this scenario. In North Korea's narrowly constrained technology ecosystem, the potential efficacy of these options is somewhat reduced. However, the available cyber capabilities function best when aimed at key groups and assets rather than broad disruption. The regime is critically dependent on a number of external financing mechanisms, driven by illicit relationships and continuing criminal enterprise, that serve to reduce the impact of international sanctions. These units are likely targets in the event one faction may seek to deny their value to a competitor. The threat activity groups would be a tempting target in their own right for both kinetic or virtual action by any faction that would seek to undermine competitors' support.

In the event that transition devolves and the overbearing scrutiny of central KWP elites wavers, there is also a likelihood that individual leaders or even mid-level operators may seek to realize their own ambitions. A succession crisis could present an opportunity that comes but once in several generations, allowing political players the chance to acquire personal wealth and a potential exit from the nightmare that is service to the North Korean regime. A number of prior defections have occurred with less favourable prospects than those provided by a sudden transition, including by key individuals involved in handling of illicit funds.[24] In this climate, offensive capabilities may thus be bent to personal ends.

Cyber capabilities remain a new and largely untested element in significant succession disputes. Despite the fact that rogue action by factional elements in control of other strategic assets has remained a longstanding concern in other crisis events, custodial security safeguards for offensive cyber arsenals has received little consideration to date.[25] Some prior evidence exists to suggest that cyber capabilities may feature prominently in future contested leadership transitions within authoritarian regimes. Indications of action by factional elements observed during the prior unexplained absence of Russian President Vladimir Putin provide one such example.[26] During the Syrian civil war, the contested control and ultimate loss of key Syrian signals intelligence facilities, including critical bilateral liaison operations capabilities, provides a second analogy.[27] However, the North Korean case is substantially unique due to the centrality of cyber espionage and theft to the regime's ongoing survival.

IMPLICATIONS AND OUTLOOK

DPRK offensive cyber operations activity remains a prestige program for the regime, though its importance may have been somewhat overlooked to date by external observers. This program is made up of a number of key functions that enable Hidden Cobra threat activities, including vulnerability discovery, malware implant development, targeting and access operations, effects actions on objective, financial theft operations, and influence operations. The generation of these capabilities and employment roles appear to be split, and in some cases duplicated, across competing organizations, including KWP offices, DPRK Ministry of State Security directorates, and KPA components. The offensive cyber operations capability lacks much of the physical footprint, associated pattern of life, and other geospatial signatures of strategic and undersea warfare programs. Its intangible nature has limited more widespread

24 Anna Fifield, "He ran North Korea's secret moneymaking operation. Now he lives in Virginia," *Washington Post*, July 13, 2017 - https://www.washingtonpost.com/world/asia_pacific/he-ran-north-koreas-secret-money-making-operation-now-he-lives-in-virginia/2017/07/12/4cb9a590-6584-11e7-94ab-5b1f0ff459df_story.html

25 Ashton B. Carter, "Reducing the Nuclear Dangers from the Former Soviet Union," *Arms Control Today*, 22:1 (1992), https://www.jstor.org/stable/23624671; Gregory F. Giles, "Safeguarding the Undeclared Nuclear Arsenals," *The Washington Quarterly*, 16:2 (1993), 173-186, https://doi.org/10.1080/01636609309443403; Steven E. Miller, "The Case against a Ukrainian Nuclear Deterrent," *Foreign Affairs* 71:3 (1993), 67-80, https://www.foreignaffairs.com/articles/ukraine/1993-06-01/case-against-ukrainian-nuclear-deterrent; Kenneth Sewell, Clint Richmond, *Red Star Rogue* (New York: Simon & Schuster, 2005); Kenneth N. Luongo, Naeem Salik, "Building Confidence in Pakistan's Nuclear Security," *Arms Control Today* 37:10 (2007), https://www.armscontrol.org/act/2007-12/features/building-confidence-pakistan%E2%80%99s-nuclear-security; Jane's Intelligence Review, "Deadly stockpile - Syria's chemical weapons capabilities," February 28, 2014.

26 Cyber Conflict Documentation Project, "Russia: Cyber attack potentially linked to rumored coup d'etat," March 2015.

27 Oryx, "Captured Russian Spy Facility Reveals the Extent of Russian Aid to the Assad Regime," *Bellingcat*, October 6, 2014, https://www.bellingcat.com/news/mena/2014/10/06/captured-russian-spy-facility-reveals-the-extent-of-russian-aid-to-the-assad-regime-2/.

analysis using commercial overhead imagery and the associated open source collection, tracking, and modeling methodologies increasingly familiar to the international affairs community.

Yet these cyber capabilities offer the regime clandestine means for accumulating illicit wealth, projecting power to hold regional and great power adversaries at risk, and sustaining North Korea's Juche ideology of self-reliance that appears increasingly built upon economic and military espionage. Any challenger wishing to assume the legacy forged by Mount Paektu (at least as the regime's mythmaking would so style), must prove themselves equal to the task of mastering this portfolio of cyber capabilities and to command the compliance, if not the respect, of the leaders that shape the organizations involved in the conduct of these operations. The prospect of infighting, cooperation, or opportunism among these key figures will determine in no small part the shape of North Korea's post-Kim Jong Un future, now or in years to come.[28]

The apparent centrality of Kim Yo-Jong in the succession question may well also drive additional actions by DPRK's cyber groups, intended to demonstrate loyalty, capability, and effectiveness. Potential near-term courses of action favor leveraging existing Hidden Cobra infrastructure and access for rapid action, including further theft from cryptocurrency exchanges, international banking institutions, and other financial sector targets. Observers should also anticipate accelerated intrusion attempts to drive new revenue opportunities, as any successor will require the funds directed through Office 39 to cover the ever-rising costs of ensuring loyalty.

Despite the cyber domain's importance to the regime for purposes of clandestine espionage, attack, and finance, it remains an open question what proportion of these capabilities will remain under control of the Politburo and Kim Jong Un's successor in the event of contested transition. Uncoordinated use of offensive cyber capabilities at levels below the national command echelon may be contemplated under multiple scenarios with potential disruptive or destructive effects across a variety of targets. While some scenarios may suggest confusion and disruption of routine processes leading to operational pauses and degraded effectiveness, these outcomes appear more likely in cases where a strong unitary leadership continues and the operators and planners merely await guidance, preparing to prove themselves to the new successor. Without expectations of a clean succession, there are strong incentives to execute new operations aggressively in pursuit of different beliefs regarding personal and positional benefit. Additionally, red-on-red engagements between competing factions controlling differing cyberattack arsenals and infrastructure may surface, where various Hidden Cobra subset operators leverage insider knowledge and access to hunt and degrade sources of power contributing to rivals' base of support. These fights over staging and delivery mechanisms, foothold, implant command and control, exfiltration infrastructure, and effects triggers may very well play out across the compromised systems and networks of uninvolved third-party victims previously targeted by North Korean military and intelligence services, and threaten unanticipated collateral damage.

Limited information from within the North Korean regime may be further restricted by instability, distrust, and internal crackdowns that may collectively deny what limited channels of information remain available to the international community. This will limit opportunities to observe specific threats and deny options to validate the credibility and veracity of what few indications may surface. Coupled with the disruption of routine interactions, movement restrictions, and economic contraction due to the ongoing coronavirus pandemic, any prolonged leadership transition could well pose the most severe intelligence and policy challenges of a decade which has already defied even the most fevered imagination in just its opening months.

JD Work serves as the Bren Chair for Cyber Conflict and Security at Marine Corps University, and as a non-resident senior fellow with the Atlantic Council's Cyber Statecraft Initiative in the Scowcroft Center for Security and Strategy. He holds additional affiliations with the School of International and Public Affairs at Columbia University, the Elliot School of International Affairs at George Washington University, and as a senior adviser to the Cyberspace Solarium Commission. He can be found on Twitter @HostileSpectrum. The views and opinions expressed here are those of the author(s) and do not necessarily reflect the official policy or position of any agency of the US government or other organization.

28 Adam Cathcart, "Pyongyang Machiavelli: All of Kim's Men," *The Diplomat*, April 17, 2013, https://thediplomat.com/2013/04/pyongyang-machiavelli-all-of-kims-men/.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org