APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CYBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT

Marc R. DeVore / Sangho Lee

Marc R. DeVore is a lecturer of the International Relations at the University of St. Andrews (United Kingdom). He completed his Ph.D. from Massachusetts Institute of Technology (MIT) and conducted researches in France, Switzerland and Italy. His research interests include security studies, comparative political economy, American foreign policy, religion and terrorism, civil-military relations and cyber warfare. He was a national security advisor for the government of CAR (Central African Republic) and Guinea-Bissau.

Sangho Lee is a Professor of Political Science and Diplomacy at Daejeon University, South Korea. He completed his Ph.D. in War Studies at King's College London. While in London, he worked as a research associate at the Centre for Defence Studies (CDS) and joined the Sejong Institute as a research fellow before moving to Daejeon University. Professor Lee's primary research interests are national security, military strategy and operations, cyber war and security, and weapon systems. He was the Assistant Administrator of the ROK Navy Development Committee and the Chairman of the Korea Cyber Peace and Security Forum, in addition to holding a number of advisory posts with the government and private sector entities.

Abstract

APT(Advanced Persistent Threats)s are the most sophisticated form of cyber weapon that exists. APTs are reshaping the balance of military capabilities in unpredictable and disruptive ways. Unlike simpler attacks, such as distributed denial of service (DDoS) operations, APTs are customized and designed to the systems they are to infiltrate. Therefore, states, rather than hacktivists or terrorists, are the only entities likely to possess the necessary resources and expertise to develop APTs. Prominent international examples of APTs include the American/Israeli Stuxnet worm and Flame virus employed to disrupt Iranian Uranium enrichment capability and China's Shady Rat operation designed to steal data from foreign defense contractors. The increasing use of APTs is potentially destabilizing for the international system especially in East Asia, where the distribution of cyber attack capabilities and vulnerabilities is highly asymmetric. China and North Korea are both important cyber powers and they are extremely active. China leads the world in terms of the number of hostile cyber incidents attributed to it. They are two of the most capable and likely actors to use cyber capabilities during a conflict and have strong incentives to employ APT to cripple, for example, the United States ability to respond to a crisis in the Taiwan Straits and/or Korean peninsula. One of the most potentially destabilizing characteristics of APTs is their offensive nature that incentivizes states to start a war rather than temporize during international crises situations. APTs are highly capable weapon of surprise but are limited by its short-term, single-use nature of their impact. All of this creates acute incentives for a state in possession of superior cyber weapons to attack while its capability exists. APTs are reshaping the balance of military capabilities in unpredictable and disruptive ways as cyber weapons are undeniably an increasingly important component of states' military power.

Key words: APT(Advanced Persistent Threats), Stuxnet, Cyber attack, China and A2AD , North Korea' cyber capability

INTRODUCTION

Few technological developments can potentially shape the international balance of power than the emergence of cyber weapons. Cyber operations enabled Russia to interfere in the United States' 2016 elections, China to steal blueprints for the United States' F-35

fighter, and the United States to disrupt Iran's nuclear program. This increasing prominence of cyber operations has given rise to a debate between cyber "optimists" who argue that states are more likely to practice restraint than fully exploit their capabilities and "pessimists" who view cyber warfare's facility as destabilizing the international order. In this article we will examine the possible applications of one particular form of cyber weapon—advanced persistent threats (APT). Our analysis of inherent APT characteristics leads us to steer a mid- course between cyber "optimists" and "pessimists" since APTs exacerbate the risk of pre-emption in the midst of crises by running the risk of escalation from minor cyber incidents to full-scale cyber war.

APTs are the most sophisticated form of cyber weapon that exists. Unlike simpler attacks, such as distributed denial of service (DDoS) operations, APTs are customized and designed to the systems they are to infiltrate. The need for customization means that APT developers need access to precise technical intelligence on the systems they intend to attack and sizeable numbers of software developers. As a consequence, states, rather than hacktivists or terrorists, are the only entities likely to possess the resources and expertise to develop APTs.[1]

The long time frames needed to develop and implement APTs, meanwhile, demand that they be integrated into long-term foreign and military strategies. Indeed, some APTs have been detected remaining concealed for up to 205 days or even 2,982 days.[2] The costs for developing individual APT also vary, from $10,000 to $100 million, depending on their sophistication, meaning that the most complex APTs bear price tags equivalent to individual major con-

---

[1] Brandon Valeriano and Ryan Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015), 164-87.

[2] M-Trends@ 2015: A View from the Front Lines, p.1.

ventional weapons systems.[3]

Prominent international examples of APTs include the American/Israeli Stuxnet worm and Flame virus employed to disrupt Iranian Uranium enrichment capability and China's Shady Rat operation designed to steal data from foreign defense contractors. South Korea itself has been subjected to several APTs, including the 2011 Nonghyup Bank Hack, the IceFog espionage campaign initiated in 2011, the 3 March 2013 attacks, and the Kimsuky anti-think tank campaign.[4] While APTs have thus far been used in peacetime for either sabotage or espionage purposes, their real potential lies in their ability to disrupt or subvert major electronic systems, such as power grids or military communications.

To assess APT's likely impact on the international system we first examine the arguments that cyber "pessimists" pose about how cyber capabilities are allegedly rendering international conflict more likely and then assess whether these apply to APTs. Although we find that the "attribution problems" and "cyber escalation" are less acute for APT than less sophisticated cyber weapons, we argue that APTs create incentives for pre-emption during international crises. We then examine two scenarios—China/United States and North Korea / South Korea—to illustrate this use of APTs in crisis scenarios. To preview our conclusions, policymakers and security professionals must take APT seriously because the timely use of APT could temporarily shift the military balance in the midst of a crisis and also incentivize states to engage in attack rather than temporize.

---

[3] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times* (16 February 2014) available at: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451 (consulted 4 March 2017).

[4] *Malware Analysis* (Soon Chun Hyang University Industry-Academic Cooperation Foundation, 2014), p.12.

THE APT *PROBLÉMATIQUE*

Anticipating new technologies' impact on warfare is always a fraught process. Such is particularly the case with cyber weapons, where the novelty of the tools and the medium has led to widespread disagreement. To assess APTs' likely impact on warfare we will analyze three arguments for why cyber weapons are a destabilizing element, namely that they are alleged to be un-attributable, prone to escalation and favor the offensive. We find that, regardless of whether the arguments apply to simpler cyber warfare techniques, attribution problems and risks of cyber escalation are minimal with respect to APT. The third hypothesis, that APTs incentivize more offensive military operations, including preemptive and preventative attacks, is much more plausible.

Perhaps no aspect of cyber warfare has attracted more attention that the so-called attribution problem. The attribution problem is an alleged product of the fact that cyber attacks do not occur in physical space and that cyber attackers can therefore route malware via servers in uninvolved countries to cloak their actions under a veil of anonymity. This problem led authors such as Richard Clarke and Robert Knake to envisage a dystopian future where the United States economy is destroyed and large numbers of people killed in a cyber attack where the attacker's identity remains entirely unknown.[5]

While attribution may be problematic for less sophisticated and capital intensive cyber operations, such as DDoS attacks and the employment of commercially available malware, attribution is much less problematic for APT. One reason for this is APTs' sophistication and capital intensiveness. In other words, the number of potential attackers, and thus the attribution problem, is limited due to the

---

[5] Richard Clarke and Robert Knake, *Cyber War* (New York: Ecco 2010), 33-68.

fact that only a limited number of states can develop APT. APTs' capital and labor costs, meanwhile, incentivize states to use them only against their geopolitical rivals. Consequently, the number of potential perpetrators for any APT attack can easily be reduced to one or two by posing the question of *cui bono*.

Cyber attribution, finally, has empirically proven simpler than oftentimes asserted. Since APT developers need intensive training and work in teams, they generally develop coding patterns that are forensically detectable after an attack. This simplifies the task of attributing specific attacks to states. Such, was the case in several North Korean attacks, where malware coders employed *Hangul*, and Russia's manipulation of the 2016 US election, where FSB and GRU hackers reused computer code their organizations had previously employed. Thus, although the problem of attribution has been raised frequently, no major cyber attack to date actually remains un-attributable.[6]

In addition to the attribution problem being minimal with APT, unwanted escalation is equally unlikely. Certain experts argue that low-level cyber intrusions, such as espionage or DDoS attacks, will escalate into states crippling one another's critical infrastructure with APTs.[7] Such fears of escalation, however, are both analytically unlikely and empirically unjustified in light of the current evidence.

APTs' cost and impact means that policymakers rightfully regard them as qualitatively different from simpler forms of cyber attack. They are therefore no more likely to respond to irritating DDoS attacks or data thefts with anti-infrastructure APTs than states are to respond to physical espionage or harassment with air strikes. Brandon Valeriano and Ryan Maness, indeed, demonstrate

---

[6] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Attacks* 38:1-2, 4-37.

[7] Timothy Junio, "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate," *Journal of Strategic Studies* 36/1 (2013), 125-33.

that empirically states respond to low level acts of cyber aggression in a restrained manner and a norm of "cyber restraint" may indeed be emerging.[8]

If cyber pessimists' predictions about the attribution problem and escalation are unlikely to be realized in the area of APTs, then we must address the cyber pessimists' final hypothesis; cyber warfare is destabilizing because it incentivizes offensive operations.

APTS AND OFFENSIVE ADVANTAGES

A detailed analysis of APTs' inherent characteristics reveals, regrettably, that they do indeed incentivize attacks in conjunction with aggressive conventional military actions. Three factors contribute to APTs' offensiveness: 1) their single-use nature, 2) the short-term nature of their impact, and 3) their capacity for surprising opponents.

One factor that compels states to reserve sophisticated APTs for major military operations lies in their single-use nature. The most sophisticated APTs rely on weakness detected in an opponent's computing infrastructure, including the so-called zero-day vulnerabilities, which are software weaknesses that are unknown to their creators, yet exploitable by hackers. The Stuxnet worm, for example, relied on four distinct zero-day vulnerabilities.[9]

The act of using an APT offensively for the first time enables defending states and cyber security firms to expeditiously fix the vulnerabilities that the APT exploited. APTs are thus best conceived as single-use weapons in disputes amongst well-resourced states. To

---

[8] Valeriano and Maness.

[9] Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, 36/1 (2013), 120-124.

make matters worse, using APTs reveals their underlying code, enabling adversaries to re-employ elements in crafting their own malware. This form of cyber blowback was evident in Iran's reemployment of elements of the Stuxnet code in their own APT, Shamoon, which they used to attack financial services in Saudi Arabia.[10]

In sum, employing an APT and thereby revealing its characteristics enables opponents to both develop means of neutralizing that APT and re-employ elements of its code in crafting their own attacks. This single-use nature of complex APT incentivizes states to reserve their best cyber weapons for use in conjunction with conventional military operations.

While APTs' single-use nature drives states to reserve their use for warfare or crisis situations, their short term impacts incentivize states to use them in support of high tempo operations. Most analysts regard infrastructure and communications as the two military-relevant targets most vulnerable to APT because these systems possess multiple vulnerable nodes and are difficult to isolate from the internet.[11] Attacking such targets, including civilian transportation infrastructure, can hobble a state's military operations by hindering military units' ability to deploy and degrading their communications systems. Cyber defenders can, however, circumvent or fix vulnerabilities if given the necessary time. Such APTs therefore are most effective when combined with conventional plans that aim to swiftly achieve a military objective.

Finally, the very purpose of APTs is to surprise the adversary. APT developers must identify vulnerable information systems in peacetime that will be critical to military operations if they are to impact future battlefields. If an adversary knew of an APT's pres-

---

[10] François-Bernard Huyghe et al., Gagner les Cyberconflits: au-delà du technique (Paris: Economica, 2015), 109-10.

[11] Chee-Wooi Ten et al., "Cyber-Vulnerability of Power Grid Monitoring and Control Systems," *Power Infrastructure Cybersecurity Laboratory* (Ames, Iowa: Iowa State, n.d.).

ence within their computer infrastructure they would rapidly patch vulnerabilities and develop other means of mitigating the damage. APT developers must therefore move by stealth, identifying zero day events, collecting intelligence on their targets and potentially employing human operatives to infiltrate their malware into the targeted systems.

APTs designed to disable command-and-control systems and disrupt infrastructure are therefore, by definition, weapons of surprise.[12] Warning opponents of their existence or gradually escalating their employment are therefore antithetical to the nature of the technologies in question. APTs will therefore likely be employed in a massive scale at the onset of a conflict, rather than being brandished to deter a potential conflict or employed incrementally. This, in turn, will render crises more prone to escalation. As Thomas Schelling predicted, "If surprise carries an advantage, it is worthwhile to avert it by striking first. Fear that the other may be about to strike in the mistaken belief that we are about to strike gives us a motive for striking."[13]

In short, APTs incentivize offensive warfare whenever inter-state relations cross the threshold into open conflict. States reserve their most potent cyber weapons for such scenarios because employing them for lesser goals compromises their code and invites cyber blowback. APTs' utility for attacking transportation and command-and-control systems meanwhile favors their use in conjunction with high tempo operations, rather than more gradual ones. Finally, APTs, by their very nature, favor surprise attacks.

---

[12] Huyghe, 132-35.

[13] Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard UP, 1960).

CASE SELECTION

The remainder of this article demonstrates our central argument that APTs are most likely to be employed in a massive fashion in conjunction with conventional military operations. To this end, we examine the hypothetical conflict scenarios: 1) Chinese APT employment to cripple the United States ability to respond to a crisis in the Taiwan Straits, and 2) North Korean APT attacks on the Republic of Korea during a crisis. These cases have been selected based on two criteria: their importance and the quality of data on their likely operations.

Firstly, China and North Korea are both important cyber powers. Valeriano's and Maness' cyber capability ranking assesses China as possessing the world's second best offensive capabilities and North Korea as the world's sixth most significant (military) cyber power overall.[14] These states are also extremely active. China leads the world in terms of the number of hostile cyber incidents attributed to it. North Korea, meanwhile, ranks fourth according to the same scale.[15] China and North Korea are, in other words, two of the most capable and likely actors to use cyber capabilities during a conflict.

In addition to being formidable cyber powers, China and North Korea are states that have strong incentives to use their capabilities because their offensive capabilities are not matched by concomitant cyber vulnerabilities. North Korea's absence of a modern network economy, or indeed any civilian connectivity to the broader internet, renders cyber attacks on North Korea a nugatory prospect. Although less pronounced, China's requirement for internet access to pass through Chinese routers, which are monitored by Chinese internet

[14] Valeriano and Maness, 25.

[15] Ibid, 90.

police, renders China comparatively resistant to cyber attacks.[16]

Besides being potent cyber actors, China and North Korea are, secondly, also states whose cyber activities are amply documented. The governments of the United States and Republic of Korea have put in considerable efforts to document Chinese and North Korean cyber activities. Cyber security firms and think tanks have contributed to other pertinent studies on this matter. This enables us to build realistic scenarios about how these states will likely design their APT attacks for use in wartime.

CRISIS IN THE TAIWAN STRAITS

Few states possess cyber capabilities equivalent to China's and none has arguably proven so willing to use those capabilities more than China. Since 2010, Mandiant, Fire Eye, Kaspersky and other organizations specializing in international security identified China as the origin of a substantial number of APT intrusions.[17] Mandiant, indeed, identified China in 2013 as the world's principle source of APTs.[18] China's People's Liberation Army (PLA) maintains its own sizable cyber force. The PLA's 2nd Bureau runs cyberwarfare units, including the Unit 69138, whose activities have attracted considerable international attention.[19]

The PLA also operates through proxies, such as the groups that employed APT-30 against Southeast Asia countries and hacked biometric data from 5.6 million US government employees.[20] The United States consistently protests against this activity and Presi-

---

[16] Ibid.

[17] The defector's personal information cannot be shown, due to threat of exposure.

[18] MANDIANT. APT1, Exposing One of China's Cyber Espionage Units (2013.02).

[19] Ibid.

[20] 'APT30 and the Mechanics of a Long-running Cyber Espionage Operation' (2015.04).

dent Barack Obama brought up the topic in his bilateral meetings with China's President Xi Jinping.[21]

China's peacetime cyber activities have enabled it to amass considerable data on vulnerabilities in the United States' information infrastructure. As already mentioned, a hack attributed to China obtained biometric data on 5.6 million US federal employees.[22] China likewise used a spear-phishing attack, employing a malware-infected Microsoft Exel file, to collect internal network manager information from EMC Corporation's Security Division. The SecureID certificate information that was extracted was then used to hack Lockheed Martin, stealing data on the F-35 fighter aircraft.[23]

Operations such as these demonstrate that China is both capable of infiltrating sensitive American systems and also suggest that China has gathered the preliminary information needed to implant APTs in critical US systems for use in wartime. China supplements the data it has collected with cyber espionage with decades of more conventional intelligence gathering on the United States' military presence in the Asia-Pacific Region. Thus, China has employed its hitherto low-intensity APT activities to lay the groundwork for disruptive attacks in the event of a war. Experts and unclassified reports, indeed, assume that Chinese malicious code has created "back doors" and "trap doors" in critical American systems, and also implanted "logic bombs" that they will activate during a conflict.[24] China's focused research and development on hacking advanced rootkits and the Basic Input / Output System (BIOS) has furthermore prepared it well to exploit these weaknesses.

Chinese doctrine emphasizes that the PLA will use its cyber

---

[21] "U.S. Government 5,6 million civil servants' fingerprint information have been leaked in a hacking attack. Information authorities suspect a connection with China."

[22] 'APT30 and the Mechanics of a Long-running Cyber Espionage Operation' (2015.04).

[23] Chinese Capabilities for Computer Network Operations and Cyber Espionage (2013.03).

[24] Northrop Grumman Corp, Field Report p 34.

capabilities against the United States as an integral portion of its Anti-Access Area Denial (A2AD) doctrine, which is designed to prevent American military forces from effectively intervening in an East Asian conflict. Since 2012, American experts and policymakers have anticipated that cyber A2AD operations would disrupt and delay American operations by targeting the complex sequence or activities, which partly rely on civilian infrastructure, required for the United States to rush adequate forces to the theater of conflict.

A conflict in the Taiwan Strait is both the most likely and suitable theater for China to employ offensive cyber operations in this way. Taiwan's political status, which precludes a permanent American military presence, renders America's contribution to Taiwan's defense highly contingent on its ability to rapidly deploy forces. Since a peacetime deployment to Taiwan would be highly provocative, American forces would moreover need to rush to the island and its bases in the region (Guam, Japan and Korea) once combat is imminent.

The PLA will also most likely have sufficient lead-time to activate its anti-American APT due to the likely ways a hypothetical Taiwan Straits crisis would develop. Historically, crises over Taiwan have been sparked by clear events with predictable time scales. The 1958 Crisis, for example, was sparked by China's ultimatum over Quemoy and Matsu, while the 1995 Crisis evolved in step with Taiwan's elections, which a nationalist party was slated to win. A future Straits crisis would also likely evolve in a similar manner, triggered by an ultimatum, referendum or election. This would enable the PLA to prepare its APT operations several weeks in advance of the onset of conventional military operations.

China will likely exploit this warning period when the United States cannot yet politically deploy forces, to initiate cyber operations. PLA cyber units would begin aggressively by penetrating into Pentagon contractors' networks and insufficiently secured armed forces networks exploiting vulnerabilities and passwords that they

have already obtained. The Department of Defense's (DoD) NIPRNET would be a target of particular attention as this network is less secure than United States military networks, yet constitutes the primary platform wherein the DoD interacts with contractors.[25] Including NIPRNET, 90% of the United States military's interactions with contractors occurred over commercial networks and unclassified DoD networks.

China would step up with these operations as the conflict escalates, activating more destructive malware to disrupt the flow of ammunition and supplies to the theater of conflict. It would do this by attempting to disable for router traffic, or 'BACK REV', and Basic Input / Output Systems (BIOS).[26]

PLA cyber attack efforts would focus on other critical, yet vulnerable systems. Aerial refueling constitutes a primary example of such a system. The United States' military response to a crisis in East Asia will depend heavily on its aerial refueling capabilities. At present, the United States possesses over 400 airborne refueling tankers and leverages this fleet and its ability to coordinate them to swiftly strike targets at great distances and rapidly deploy forces to crisis environments. Aerial refueling, moreover, plays a critical role in American efforts to mitigate the danger of Chinese conventional missile strikes on American airbases. Refueling will enable American aircraft to operate from a wider-array of dispersed facilities and deploy to bases further from the area of conflict.

PLA cyber attacks will likely disrupt this critical capacity, significantly undermining the United States' war-making effort. American aerial refueling depends on a web-based application, the Air Refueling Management System (ARMS), through which aerial refueling requests are received, prioritized and executed. ARMS data is

[25] https://en.wikipedia.org/wiki/NIPRNet.

[26] Northrop Grumman Corp, Field Report p 34.

reportedly transmitted via the internet. Such a distributed system, with many nodes and connected units, is inherently vulnerable to Chinese infiltration. Chinese cyber warriors are doubtless aware of this state of affairs and ARMS' internet-based structure is nearly impossible to defend with total confidence.

Spear-phishing and keystrike logging programs will (or have) likely exposed ARMS' IP address and operating system password. Other techniques, such as SQL injection and cross-site scripting, can also be applied.[27] While PLA hackers can employ an array of techniques to access ARMS, only one must succeed in order for them to remotely upload CnC malware. Corrupting or disabling ARMS during a crisis will cripple the United States' ability to respond to a crisis or conflict.

In sum, Chinese APT capabilities can incentivize China to preemptively strike in the event of a crisis, such as could occur in the Taiwan Straits. Even though many crucial American systems are air-gapped and therefore resistant to cyber attacks, certain critical systems are nonetheless tied to the internet. ARMS and NIPRNET are two such cases of crucial systems that can be remotely accessed. Attacking two systems such as these will impede the United States' ability to respond to a fast tempo crisis, potentially meaning the difference between strategic success and failure.

CONFLICT ON THE KOREAN PENINSULA

No other state possesses cyberwar capabilities that are highly disproportionate to the overall condition of the state than North Korea. North Korean strategists understood the potentials of cyber weapons relatively sooner than other countries and began investing

---

[27] Northrop Grumman Corp, Field Report p 34-36.

in them. Today, North Korean cyber warfare forces are estimated to be around6,000 personnel, including 2,000 hackers. These cyber forces are divided amongst four organizations: the General Reconnaissance Department (GRD), the International Liasion Department, the United Front Department and the Central Party Examination Department.[28]

Since their foundation, North Korean cyber forces have focused on identifying and preparing to exploit the Republic of Korea's (ROK) cyber vulnerabilities. The GRD-associated Institute 110 has therefore conducted cyber espionage operations against ROK military and strategic targets. Amongst the North's exploits have been the 2013 hacking of the ROK's military tactics and command-and-control tactics. Cyber operatives, at this point, compromised critical systems, including the Aegis air defense systems' source codes, details of the ROK's joint tactical data links and technical parameters for identification friend-or-foe (IFF) equipment.[29] North Korean hackers succeeded, even more impressively, in hacking the ROK military's cyber command in 2016. These operations demonstrate both the North Korean hackers' ability to penetrate ROK systems and suggest that they thereby collected information of further vulnerabilities susceptible to damage by APTs.

North Korean sizeable human intelligence assets in the Republic of Korea raise the likelihood of substantial synergies with its burgeoning cyber forces. Human agents and unwitting accomplices indeed offer North Korea substantial opportunities for obtaining security information for hacking secure networks and infiltrating USB sticks into air-gapped networks.

North Korea is likely leveraging this capacity to develop and im-

---

[28] Seong Kyu Ahn, Asan Column, *Cyber Cancer – can we prepare for APT(Advanced Persistent Threat).* (2015.08.05)

[29] Joongang Ilbo, 2015.09.10, 'Aegis, KF-16 joint operations and core secrets were hacked. http://news.joins.com/article/18631228

plant APT attacks that it would activate in the event of a war. North Korean cyber warriors will likely begin preparing their wartime APT operations in four distinct ways.

First, one weak point in the ROK's military cyber infrastructure that the North is likely to pursue in peacetime is the outside contractors upon which the armed forces depend. The ROK's armed forces, particularly the air force, depend on regular software updates and changes that contractors provide over supposedly secure USB sticks. North Korean intelligence services will likely attempt to infiltrate these software supply chains and thereby insert infected USBs into the air forces' supply chain. If successful, they can embed malware in critical systems, such as the ROK's air defense network.

Second, North Korean cyber forces will - also likely employ "shellshock" attacks to seize control over selected web servers in the ROK. North Korean cyber warriors can then embed an "exploit kit" into the captured website and modify its source code (e.g. Angler, Orange, CK VIP, etc.) and the URL's tag (e.g. iframe, script, etc.).

Third, North Korea is likely to use "watering hole" infiltration tactics whereby North Korean cyber forces will seek to identify and then infect websites that ROK armed forces and critical infrastructure providers will likely connect to. This technique will enable North Korea to implant malware on systems that they cannot directly penetrate and will function even vis-à-vis ROK targets that are schooled to avoid phishing attacks.

Finally, North Korean intelligence may install "logic bombs" on critical ROK systems should they anticipate a crisis in inter-Korean relations. Logic bombs are fragments of malicious code programmed to initiate themselves once certain conditions are met, such as the arrival of a date or time. The North Korean cyber force will seek to implant such logic bombs should the state's leadership plan a provocation that might escalate into war (i.e. by conducting an atmospheric nuclear test, provoking battle over the Northern Limit Line, or announcing an ultimatum). Logic bombs are partic-

ularly potent because they can disable air-gapped systems on cue provided that North Korean intelligence manages to infect a laptop that will be connected with the targeted system or dupe a human agent into inserting an infected USB stick.

North Korea's cyber forces thus have ample scope for preparing wartime APT attacks in peacetime. Indeed, it can prepare its future cyber battle by; targeting vulnerable contractors, initiating "shellshock" attacks, exploiting "watering holes" and implanting logic bombs. North Korea's ability to conduct such preparatory operations is greatly enhanced by their leaders' ability to pick the time and location of their military provocations, and their comparative invulnerability to cyber counter attacks.[30]

North Korea will therefore probably be well prepared to launch substantial cyber attacks on the ROK provided that it chooses a crisis' timing in advance. Under these circumstances, they stand to benefit from a cascade of devastating APT attacks that will disable key ROK systems at the precise time when the conflict breaks out.

One particularly tempting target will be the ROK's Army Tactical Command Information System (ATCIS). The ATCIS is a C4I (command, control, communications, computers and intelligence) network designed to automatically combine data from tactical military units and share them in real time. ATCIS has been critical to ROK military doctrine since 2008 and is projected to continually evolve with new hardware and software upgrades being added to the system until at least 2020.[31]

While ATCIS may indeed improve the ROK armed forces' efficiency, it has also been criticized for reducing subordinate commanders' initiative and introducing increased complexity to the armed forces command structure. These factors, detracting from

[30] Valeriano and Maness, 25.

[31] 2013, IT professionals develop implementation plans for the digital battlefield.

the ROK Army's ability to tactically implement mission command, will have a downright catastrophic effect if North Korea disables or corrupts the ATCIS system. Research indeed suggests that ATCIS is remarkably unsecure for such a critical system.[32] Certain experts venture so far as to suggest that a worm-type attack that exploits zero-day vulnerabilities can completely incapacitate ATCIS in a very short time.[33]

Even if North Korea failed to develop an APT capable of disabling ATCIS in it's entirely, it could attack ATCIS in other ways or portions of the system that are more vulnerable than the network as a whole. Three particular aspects of ATCIS will be particularly tempting to an attacker; the anti-artillery Kairos DBMS subsystem, ATCIS' window-based operating systems, and the increasing connectivity between ATCIS and the Korean Joint Command and Control System (KJCSS).

One component of the ATCIS that may be particularly susceptible is the Kairos DBMS, which was added to ATCIS comparatively recently to improve anti-artillery warfare. North Korea's artillery poses a sizeable and growing threat to the ROK. This threat has grown even as the North's other conventional capabilities declined. Within this context, the North Korean leadership's threat to transform Seoul into a "sea of fire" achieved concrete form with the construction of 500 hardened artillery sites (HARTS) within 5kms of the DMZ and the deployment of more unsheltered artillery within that zone in 2010-11.[34]

---

[32] 2008, field automation information system operational measures carried out research for the future SNW (Incorporated 21st Century Military Institute).

[33] 2008 conducted Study on Simulation-based Army Tactical Information Systems worm damage assessment.

[34] Joseph Bermudez, *The Armed Forces of North Korea* (London: I.B. Tauris, 2001), 165-66; and Joseph Bermudez, "M-1978 and M-1989 170mm Self-Propelled Guns, Part II," *KPA Journal* 2/7 (2011), 1-8.

Kairos DBMS achieves this objective by rapidly processing data on enemy artillery units and connecting that data to ROK assets capable of shooting back. Kairos accomplishes this by retaining frequently accessed data in each node's random access memory (RAM), thereby avoiding the data processing delays that occur when database information is recorded on discs.[35] Kairos is exceedingly vulnerable because of this reliance on RAM since APTs can increasingly recombine malicious code in RAM memory and therefore are not bound by the need to infect file systems.[36] Kairos' many nodes facilitate North Korea's task by enabling them to inject the APT simultaneously and the malicious code can then manipulate data within the system.[37]

Another ATCIS weakness that can be exploited lies in its protocols for distributing information throughout the military command structure. ATCIS therefore, in principle, enables commanders at every echelon to quickly apprehend battlefield developments and coordinate their responses to them. Commanders at the platoon level carry individual PDAs while divisional commanders are equipped with laptops that enable access to ATCIS.

These systems, however, all employ windows-based operating systems and the nodes in each major unit (i.e. army corps) are connected to one another. Furthermore, PDAs and laptops contain a pre-prepared disc image so that a unit's systems can rapidly be reset following exercises and command post exercises. These systems' characteristics—windows-based operating systems and high levels of connectivity—render it easy for North Korean cyber warriors to infect a units' nodes with malicious RAT(Remotely Activated Trojan)s. This would enable North Korean forces to extract the location, strategy and tactics of ROK military units in real time.

---

[35] www.realtimetech.co.kr/mil4/ (Real Time Tech: Kairos RDBMS).

[36] 2014, The Inception Framework (Blue Coat)

[37] 2014, The Inception Framework (Blue Coat)

North Korean attackers can also potentially take advantage of the growing connectivity between ATCIS and the armed forces' higher echelons and join Korean Joint Command and Control System (KJCSS) to disrupt ROK military operations to an even greater extent. While units that employ ATCIS can seamlessly coordinate their activities, it actually became more difficult for those units to cooperate with units and functions that were not connected to the network when ATCIS was initially rolled out.[38] The ROK's Defense Ministry addressed this problem in ATCIS' second-phase performance improvement program, which increasingly tied ATCIS to the web and introduced greater connectivity with KJCSS.

This performance improvement enhanced interoperability among the ROK's different command and control systems. Experts have, however, identified numerous weaknesses in the system's increasingly complex architecture. Attackers can, for example, infect an ever greater number of system components via each infected laptop or access the network in SPIDER through any certified ATCIS device. North Korea cyber warriors can potentially also mount a variety of attacks (SQL injection, XSS, Remote-code injection, weak section management attack, HeartBleed, etc.) to remotely control a node and access the network. Furthermore, by manipulating the ATCIS database in peacetime, North Korean cyber warriors can induce wartime chaos via KJCCS because the two systems will synchronize in wartime.

North Korea can, in sum, employ a combination of logic bombs and attacks on ATCIS to substantially degrade the ROK's ability to respond to a crisis or fight a war. The need to set specific date or activation criteria will likely oblige North Korean cyber warriors to coordinate their logic bombs with their leadership's broader foreign and military crises. The regime will, in other words, prepare cyber

---

[38] 2008, Field Automation Information System Operational Measures Carried Out Research for the Future SNW (Incorporated 21st Century Military Institute).

attacks in advance to coincide with the crises and provocations that are premeditated by its leadership.

CONCLUSION

As we demonstrated, APT capabilities are changing the international distribution of power and the prospects for crisis stability. These two East Asian cases indeed suggest that APTs are potentially highly destabilizing.

In a prospective Taiwan Straits Crisis, China's offensive cyber capabilities can potentially negate the United States' overall military superiority. Such is the case even though the United States also possesses significant offensive cyber capabilities that likely equal or exceed Chinese capabilities. The reason for this is that the United States' need to deploy forces at greater distances and reliance upon allies renders American forces asymmetrically sensitive to disruption by cyber assault. Within this context, lower-security American systems such as NIPRNET and ARMS may prove the Achilles heel.

A prospective crisis on the Korean peninsula reveals similar asymmetries. Within this context, the ROK's dependence on digitized command-and-control systems such as ATCIS and KJCCS, and its reliance on civilian infrastructure to mobilize reservists, provides opportunities for North Korean cyber forces to disrupt ROK military operations. The ROK's efforts to leverage technology to enhance military effectiveness have, thus, created weaknesses North Korea is targeting. North Korea's less sophisticated forces possess no equivalent vulnerabilities that the ROK can exploit.

While APTs can potentially change the course of a conflict or crisis, they also create incentives for crises to escalate into war. There are three reasons for this that lie in the weapons' intrinsic characteristics, namely: 1) their greater utility for attacking than ei-

ther deterring or coercing, 2) the inflexible nature of certain tactics, such as logic bombs, and 3) the short-lived nature of the advantages that certain cyber weapons will confer, which creates ephemeral windows-of-opportunity for revising the international status quo.

Cyber weapons are undeniably increasingly important components of states' military power. States cannot, however, wield cyber weapons to coerce or deter in the same way as they do with more conventional weapons. Whereas states can conduct military exercises and launch missiles to communicate their military power and resolve to potential opponents, they cannot display their cyber power in a similar manner. Demonstrating an APT will reveal its code and therefore enable defenders to neutralize the threat before it can be used. APTs are therefore weapons that are much useful as offensive means than at achieving states' military objectives through means short of war.

Certain APTs, such as logic bombs, have the added drawback in that they oblige the attacker to decide ahead of time when it will activate. This, in effect, drives governments to script crises well in advance. Furthermore, if a potential cyber attacker has infected key systems with logic bombs programmed to activate at a specific time, the states' government will have an added incentive to cross the threshold into war at that time.

Finally, states that possess superior cyber weapons will have an incentive to fight now rather than later. Whereas most conventional weapons systems, such as tanks and warships, have life spans of decades, cyber weapons exploit particular software and hardware systems, and rely on undetected vulnerabilities. These characteristics mean that cyber weapons have comparatively short life spans. If not used, they naturally expire as the designated target updates software and fixes vulnerabilities. All of this creates acute incentives for a state that possesses superior cyber weapons to attack while capability exists.

APTs are, in sum, reshaping the balance of military capabilities

in unpredictable and disruptive ways. The very nature of these weapons, furthermore, incentivizes states to attack, rather than temporize, during international crises. Nowhere are these trends more potentially destabilizing for the international system than in East Asia, where the distribution of cyber attack capabilities and vulnerabilities is highly asymmetric. Korean experts and policy-makers should integrate this phenomenon as they manage future crises involving North Korea, China and the United States.

REFERENCE

Ahn, Seong Kyu, Asan Column, *Cyber Cancer – can we prepare for APT(Advanced Persistent Threat).* 2015.08.05.

Bermudez, Joseph. "M-1978 and M-1989 170mm Self-Propelled Guns, Part II," *KPA Journal* 2/7 (2011)

Bermudez, Joseph. *The Armed Forces of North Korea* (London: I.B. Tauris, 2001)

Clarke, Richard and Knake, Rober. *Cyber War.* New York: Ecco, 2010.

Gilbert, David. "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times* (16 February 2014) available at: http://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451 (consulted 4 March 2017).

Huyghe, François-Bernard et al., Gagner les Cyberconflits: au-delà du technique (Paris: Economica, 2015), 109-10.

Junio, Timothy. "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate," *Journal of Strategic Studies* 36/1 (2013), 125-33.

Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, 36/1 (2013), 120-124.

Rid, Thomas and Buchanan, Ben. "Attributing Cyber Attacks," *Journal of Strategic Attacks* 38:1-37.

Schelling, Thomas. *The Strategy of Conflict.* Cambridge, MA: Harvard UP, 1960.

Ten, Chee-Wooi et al., "Cyber-Vulnerability of Power Grid Monitoring and Control Systems," *Power Infrastructure Cybersecurity Laboratory* (Ames, Iowa: Iowa State, n.d.).

Valeriano, Brandon and Maness, Rayn. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System.* Oxford: Oxford

University Press, 2015.
2008 conducted Study on Simulation-based Army Tactical Information Systems worm damage assessment.
'APT30 and the Mechanics of a Long-running Cyber Espionage Operation' (2015.04).
Chinese Capabilities for Computer Network Operations and Cyber Espionage (2013.03).
Field automation information system operational measures carried out research for the future SNW (Incorporated 21st Century Military Institute), 2008.
IT professionals develop implementation plans for the digital battlefield. 2013,
Joongang Ilbo, 2015.09.10, 'Aegis, KF-16 joint operations and core secrets were hacked.
M-Trends@ 2015: A View from the Front Lines, p.1.
MANDIANT. APT1, Exposing One of China's Cyber Espionage Units (2013.02).
Northrop Grumman Corp, Field Report p 34.
Malware Analysis (Soon Chun Hyang University Industry-Academic Cooperation Foundation, 2014)
"U.S. Government 5,6 million civil servants' fingerprint information have been leaked in a hacking attack. Information authorities suspect a connection with China."
The defector's personal information cannot be shown, due to threat of exposure.
The Inception Framework (Blue Coat), 2014.
www.realtimetech.co.kr/mil4/ (Real Time Tech: Kairos RDBMS).
http://news.joins.com/article/18631228
https://en.wikipedia.org/wiki/NIPRNet.