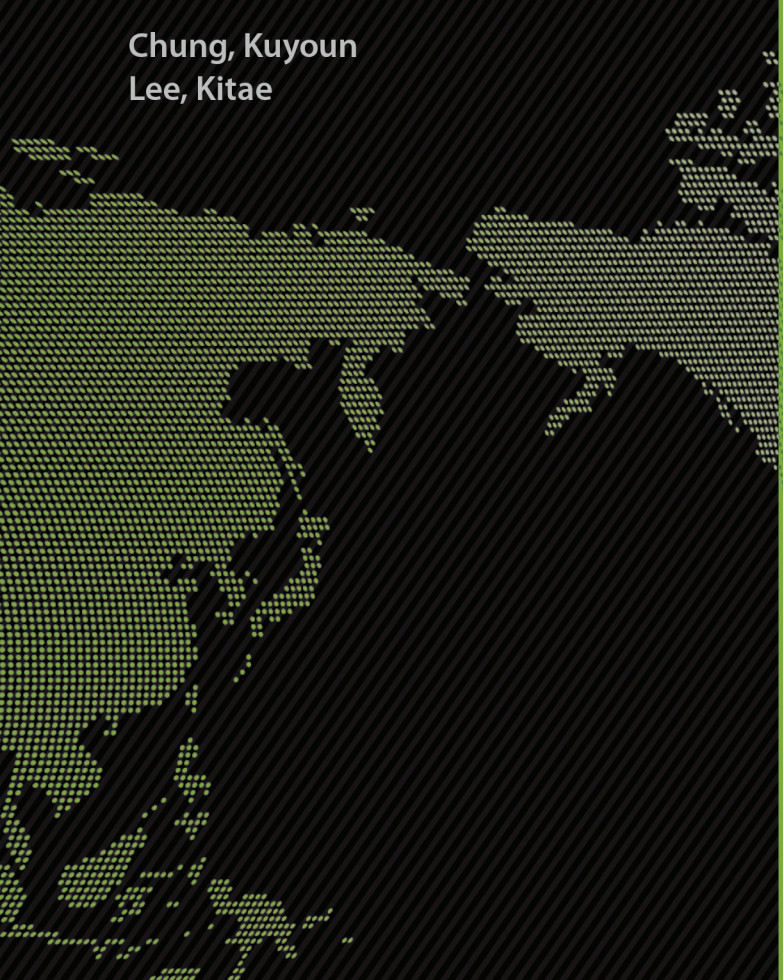
Study Series 2017-03

Advancement of Science and Technology and North Korea's Asymmetric Threat :

Rise of Cyber Warfare and Unmanned Aerial Vehicle

Chung, Kuyoun
Lee, Kitae



Korea Institute for National Unification

Study Series 2017-03

Advancement of Science and Technology and North Korea's Asymmetric Threat :
Rise of Cyber Warfare and Unmanned Aerial Vehicle

Chung, Kuyoun
Lee, Kitae

Korea Institute for National Unification

Advancement of Science and Technology and North Korea's Asymmetric Threat
: Rise of Cyber Warfare and Unmanned Aerial Vehicle

Printed	August 2017
Published	August 2017
Published by	Korea Institute for National Unification (KINU)
Publisher	President, Korea Institute for National Unification
Editor	External Cooperation Team, Division of Planning and Coordination
Registration number	No.2-2361 (April 23, 1997)
Address	217 Banpo-daero(Banpo-dong), Seocho-gu, Seoul 06578, Korea
Telephone	(82-2) 2023-8208
Fax	(82-2) 2023-8298
Homepage	http://www.kinu.or.kr
Design/Print	Handesigncorporation Co. Ltd (82-2) 2269-9917
ISBN	ISBN 978-89-8479-880-9 93340 : Not for sale 340.911-KDC6 / 320.9519-DDC23 CIP2017021494

CONTENTS

Korea Institute for National Unification

1. Introduction

1. Introduction

Recently, North Korea has attempted new forms of provocation through cyber warfare and unmanned aerial technology. For example, North Korea's hacking of United States Sony Pictures raised international awareness concerning North Korea's new forms of asymmetric threat, and particularly over its capacity and tactics on cyber terrorism. Chairman of the State Affairs Commission Kim Jong-un allegedly claimed cyber warfare to be an "all-purpose sword," along with nuclear weapons and missiles. Already, North Korea has established cyber-headquarters and seven hacking sub-organizations under the military and the Workers Party of Korea (WPK), with estimated 1,700 people. In addition, there are about 10 hacking-support organizations with roughly 6,000 manpower involved.

Meanwhile, North Korea's unmanned aerial vehicles (UAV) have provided another cause of urgency for South Korea to come up with countermeasures against North Korea's UAV-based provocation and infiltration. Since the discovery of North Korean UAV, which crashed in South Korea's Baengnyeong Island, Paju, and Samcheok in 2014, there has been increasing interest in the state of North Korea's UAV technical development and plans for usage. Even though the North's technological standard falls behind that of the US or other developed countries, it has been improving its

technical capacity by acquiring UAV manufactured in the US, China, and Russia. Given the globally-expanding drone market and the rapid advancement of relevant technology, it is necessary for the Republic of Korea (ROK) to assess the technological development of North Korea's UAV as well as its measures of usage, and seek ways to respond to these developments.

To that end, this research analyzes North Korea's newly emerging asymmetric threats that have come about as a result of advanced scientific technology, with a special focus on cyber warfare and UAV infiltration. Given the specialization of research fields among North Korea and military experts, an incomplete assessment of the newly emerging threat brought forward by North Korea's scientific and technological development makes for a timely and pressing research topic. Moreover, as the construction of knowledge-based strong state was proclaimed at the Seventh Congress of WPK in 2016, asymmetrical threat based on North Korea's scientific and technological development is expected to expand in both quantitative and qualitative terms. In this regard, a discussion of North Korea's cyber warfare and UAV technology newly sought under the Kim Jong-un era is viewed as a timely task. And based on findings of such discussion, a comprehensive assessment should be carried out on the distribution and capacity of North Korea's asymmetrical threat.

The aim of this research is to identify new military threats posed by North Korea in the context of newly emerging forms of warfare and the expansion of battlefield attributed to the development of science and technology. Therefore, rather than focusing on

previously identified cases of North Korea's asymmetrical threat, such as nuclear weapon, missile, long-range guns, and special operation forces, this research will focus on the cases of cyber-attacks and UAV.

The objective of this research is three-fold. First, it will look into the characteristics of South and North Korea's asymmetric power structures, through which it will analyze the level and status of North Korea's asymmetric threat. Second, regarding North Korea's asymmetric power, this research will focus on reviewing cyber warfare, UAV, and North North Korea's strategies in using them and assess South Korea's countermeasure ability. Third, it will forecast the influence of threat posed by asymmetric power on inter-Korean military and non-military relations, and discuss its implications on South Korea's policies toward the North and inter-Korean relations.

Korea Institute for National Unification

2. Strategic Asymmetry and North Korea's Asymmetric Threat

2. Strategic Asymmetry and North Korea's Asymmetric Threat

This section will discuss the concept of asymmetry and examine its characteristics based on not only physical military assets but also non-military assets. With such examination, it will look into characteristics of positive and negative asymmetry developing between the two Koreas.

To begin, in general, asymmetry indicates the difference used to gain a strategic advantage over an adversary in a situation of conflict.[1] The exact difference and the effects of inclusion of such difference in wartime strategy determine how various forms of asymmetry is categorized, leading to a gradual expansion of its conceptual framework. Furthermore, discussions of asymmetry have been dominantly led driven by the US, which has maintained military supremacy since the end of the Cold War.

More specifically, strategic asymmetry refers to the thoughts and actions to use and maximize one's advantage or exploit the weakness of the opponent so that one can obtain freedom of movement or attain the initiative in relations to the other party in

1) Steven Metz and Douglas V. Johnson II, Asymmetry and US Military Strategy: Definition, Background, and Strategic Concepts (Carlisle, Pennsylvania: Strategic Studies Institute, U.S. Army War College, 2001), p. 1.

fields of military security or state security. The strategic asymmetry is a two-directional concept which manifests in the relations of states in a conflict situation. It includes both positive asymmetries where one's state superiority imposes a threat to the other state and negative asymmetry where the other state's superiority imposes a threat to one's state.[2)]

Forms of strategic asymmetry are not just limited to traditional military factors such as a weapon system or the physical scale of military force, but include non-military factors that can indirectly influence conflict situations between states, such as science and technology, social system, and normative factors. In this regard, strategic asymmetry can be broadly categorized into five types.[3)]

First, there exists an asymmetry of method. This refers to using different operational concepts or tactical doctrines from those used by the enemy. Guerrilla warfare during the Vietnam War is one example. A more recent example is given by the US Military, who conducts operations with its mobile infantry by deploying a method of vertical envelopment with the use of airborne troops instead of dispatching infantry or striking an air assault.

Second, there is an asymmetry of technology. Historically, technological asymmetry occurs between developed and developing states. This is mainly because developing nations lack the capacity and time to receive the technology possessed by developed states.

---

2) Stephen Blank, Rethinking Asymmetric Threats (Carlisle, Pennsylvania: Strategic Studies Institute, US Army War College, 2003), pp. 1-2.

3) Mets and Johnson II, pp. 9-12.

Third, there is an asymmetry between the will to protect one's survival and the one to secure vital interests. If an adversary had relatively greater will to protect one's survival and interests, the adversary will be willing to bear greater costs or attain the objective even by breaking the generally prohibited moral or legal rules. For example, ethnic cleansing, genocide, human shield, and terrorism that have frequently occurred in civil wars since the end of the Cold War can be put in this category and be defined as normative asymmetry. While such normative asymmetry can help a state acquire initiative in a conflict situation for the short term, it has often been self-defeating in the longer term.

Fourth, there is an asymmetry in organizations. For instance, the network organization of a non-state enemy demonstrated by ISIL exemplifies organizational asymmetry where such organization and the traditional military organizations with the inherent hierarchy are different in terms of their internal dynamic and operational concepts.

Fifth, there is asymmetry in patience, which is a matter of how to predict the war-time horizon. For instance, the US prefers winning a war within a short period of time. It is attributed to the fact that the US Congress and constituents tend not to favor long-term engagement in a war that does not have vital national interest. It is also because if the US – with its security commitment on a global scale - is engaged in a protracted conflict in a particular region, it could trigger an adversary provocation in a different region, thereby weakening US military commitment and actual resource supply.

Meanwhile, the concept of asymmetry and its existing researches have been the subject of criticism as to whether they are valid as a tool of analysis due to its extensively comprehensive and multi-faceted nature, as well as the asymmetric nature of war itself. Although it is true that the concept of asymmetry has become more inclusive, the threats that were categorized as asymmetric in the past have since been neutralized thanks to the developments in science and technology, making the concept even more flexible. In fact, the US has begun to use the term 'hybrid threat' instead of the asymmetric threat in its 2010 Quadrennial Defense Review Report.

The existing researches on the origins of North Korea's strategic asymmetry point out the overlapping influence of Soviet Union's modern warfare strategy, Chinese People's War strategy, and the experiences of anti-Japanese guerrilla warfare, Chinese Civil War, and the Korean War. In particular, Chinese influence and Kim Il-sung's personal experience of unconventional warfare during anti-Japanese guerrilla movement have morphed into North Korea's particular form of asymmetry. A recent research criticizes the influence of North Korea's strategic culture. According to this study, while North Korea acknowledges that it has a siege mentality in its fight against imperial threat, thereby wreaking havoc on people's lives, its worldview is full of declarative propositions of why 'Joseon victory' is inevitably grounded in Marxist-Leninist rule of historical development.[4)]

A research suggests that the source of North Korea's asymmetric

4) Hwang, Il-do, *The DNA of North Korea's Military Strategy Seen through Nuclear Weapons, Long-range Artillery, and the Northern Limit Line* (Seoul: Planet Media, 2013), pp.36-39. (in Korean, unofficial translation of title)

threat lies in North Korea's defeat in the Korean War and its limitations in exercising symmetric countermeasure against ROK-US joint military power.[5] Chronic food shortages and diplomatic isolation and economic crisis as a result of sanctions have made the introduction of a new weapons system difficult. Therefore, rather than strengthening conventional power, North Korea has managed to identify South Korea's negative asymmetry and focused on developing asymmetric strategies in areas where it can impose a strategic superiority in military defense even with limited investment.

Inter-Korean military power structure demonstrates asymmetry in four areas.[6] First, the overall asymmetry shown in military power structure between the two Koreas is attributed to a confrontation between quantitative and qualitative asymmetry. In North Korea's case, it possesses roughly 1,190,000 troops, 3,900 tanks, 13,600 field artillery and multiple rocket launchers, 420 combat ships, and 820 combat planes, among other conventional forces, showing quantitative asymmetric superiority. Meanwhile, South Korea has about half the number of troops and tanks but carries qualitative superiority over North Korea's forces.

Second, North Korea's possession of various weapons of mass

---

5) Bae, Dal-hyung, "Direction for Development of Structure Centering around Cyber Warfare and Cyber-Psychological Warfare in the View-Point of Asymmetric Threats and 4th Generation of War," *Strategic Studies*, Vol.22, No.1 (2015): 141-172. (in Korean)

6) Park, Sung-young, "The Maritime Asymmetric Forces of North Korea and the Maritime Security of South Korea: Features of Threats and South Korea's Strategic Responses," Journal of Political Science and Communication, Vol.14, No.2 (2011): 105-130. (in Korean)

destruction poses a problem of asymmetric deterrence. In particular, the physical force of destruction and public fear of nuclear and biochemical weapons are significantly different from those posed by conventional deterrence.

Third, the degree of mutual exposure to asymmetrical threat and subsequent social ramifications are asymmetric between the two Koreas. For instance, recent North Korea's GPS radio disturbance imposed on South Korea is a representative case of an asymmetric threat as a result of South Korea's weakness. Another example of asymmetric threat decided by the degree of mutual exposure to the threat is North Korea's long-range gun. In particular, given that most of South Korea's political, economic, and cultural functions are concentrated in the central city of Seoul and the metropolitan area, the existence of threat itself imposes significant confusion and has far reaching effects regardless of whether there will be an actual attack or not.

Lastly, asymmetricity can be found in the different systems of the two Koreas. For instance, North Korea wields strong control over its society whereas South Korea, a liberal democratic state, enjoys a considerable amount of freedom so that the public opinion can even influence national defense policy. However, such flexibility can act as a weakness in the process of policy decision-making, whereas North Korea's strong control over its people can act as an asymmetric superiority.

Korea Institute for National Unification

3. Cyber Threat and Inter-Korean Relations

3. Cyber Threat and Inter-Korean Relations

North Korea's efforts to establish cyber power strategies, establish relevant units, and focus on developing cyber offense technology date back to around 1995. Chairman of the Central Military Commission Kim Jong-il commented after the 2003 Iraqi War, "the war of the 20th century was a war of oil and bullets, but the war of the 21st century is of intelligence" and emphasized the importance of strengthening cyber warfare ability.

In fact, North Korea has been inviting computer experts from the Soviet Union since the early 1980s, demonstrating its interest in cyber warfare. In 1986, North Korea established the Mirim College (now known as Kim Il Political Military University) in Pyongyang and since then has annually nurtured about 100 cyber experts. Every year, ten of the best graduates are selected and dispatched to the General Bureau of Reconnaissance of the Ministry of the People's Armed Forces. They are assigned to conduct cyber terrorism activities, such as searching the internet, hacking, and developing a malignant code. A cyber task force was established in the Korean Workers' Party (KWP) Operations Department in 1996, and was integrated into the General Bureau of Reconnaissance of the Ministry of the People's Armed Forces as a result of organizational restructuring in 2009.

At present, there are about 6,000 regular cyber warriors in North Korea, who are engaged in cyber-attacks against South Korea's core facilities such as nuclear plants, railway, and subway.[7] The organization carrying out cyber-attacks and cyber terrorism against South Korea is an elite, well-trained group, called Bureau 121 of the General Bureau of Reconnaissance. In addition to Bureau 121, there are various other expert groups such as Unit 204, and General Investigation Unit of the United Front Department in the Central Party.[8] Among them, Bureau 121 has about 300 agents. Although its headquarter is in Pyongyang, operations have been carried out from various foreign offices, including China, that have been set up since 2001. Main tasks include infiltrating the network of military-relevant organizations, stealing secret resources, and disseminating virus when necessary. Until 2009, agents in Bureau 121 mostly carried out terror attacks using DDoS or worm virus attacks. However, since 2013, their hacking attacks have become more aggressive, such as physically damaging or incapacitating an adversary's computer and network system.

Lab 110 in the Reconnaissance Technical Unit under the General Bureau of Reconnaissance is credited to leading cyber-attacks on military and strategic organizations and is involved in hacking and developing malignant codes. Because North Korea uses Assembler, C language, and other programming languages with low level of

---

7) Lim, Jong-in, "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The Quarterly Journal of Defense Policy Studies*, Vol.29, No.4 (2013). (in Korean)

8) Hong, Sung-pyo, "The Means of Offense, Acceleration, and Intellectualization of North Korea's Cyber Attacks," *The Unified Korea*, 2011 April. (in Korean, unofficial translation of title)

complexity, they have been able to develop internet hacking programs in a very short period of time.

Meanwhile, Unit 204, under the General Staff Department (GSD) is a cyber-psychological warfare unit and consists of about 100 agents. It is tasked with manipulating public opinion in foreign states. Specifically, its agents carry out a psychological warfare both on the internet and mobile phones, including South Korea's public websites, blogs, social network services, etc., praise North Korea, and disseminate false information for the purpose of triggering dissatisfaction with South Korea's policies.

The Command Automation Bureau is another sub-unit under the GSD. The Command Automation Bureau consists of virus experts (hackers) and staff members, and their main task is to develop hacking programs and train hackers specialized in cyber welfare. Unit 31 in the Automation Department consists of 50 to 60 officers and develops hacking programs. Unit 32, like Unit 31, is tasked with developing military-related programs. Unit 51 consists of 60 to 70 officers and develops communications programs for command control.

These experts make up the Reconnaissance Technical Unit, initially selected from the Command Automation Bureau, Pyongyang Command Automation University, Kim Chaek University of Technology, Pyongyang Computer Technology University, etc. Among them, Pyongyang Command Automation University has about 700 students, 500 to 600 staff members, and nurtures about 10 virus expert agents, 10 technical agents, and 80 general computer agents every year.

According to a recent report by the Korean Central News Agency, North Korea held a conference of reconnaissance affairs by military officers on June 18, 2015, who were in charge of carrying out espionage and cyber warfare against South Korea and foreign states, suggesting that North Korea will strive to enhance its foreign espionage and cyber strategic abilities in the future.[9] Moreover, in order to develop various cyber infiltration methods targeted at South Korea and the US, it had carried out the cyber terrorism competition for three months from July 2015. The anti-South Korea espionage department, a core sub-unit of the General Bureau of Reconnaissance, not to mention cyber espionage units in computer universities, participated in the conference.

North Korea sees cyber space as a strategically important new battlefield, and actively utilizes cyber power as a form of strategically asymmetric power. This is because a cyber-attack is relatively cost efficient in terms of manpower, and it creates large ripple effects owing to its ease of use and fast dissemination. Moreover, its anonymity and clandestine nature make adversarial sanctions and retaliation difficult.

North Korea's recent trend of enhancing its cyber power can be explained with six military perspectives. First, compared to establishing conventional power, cyber power has a low establishment and maintenance cost. Second, cyber power can be used in times of peace. Third, because cyber power can hide aggressive action under the cloak of anonymity, it is significantly suitable for North Korea's strategy toward South Korea. Fourth,

9) *Chosun Central News Agency*, June 18, 2015.

cyber power has strong asymmetry. Fifth, due to its open nature, cyber space is inherently vulnerable in terms of security. Sixth, South Korea's cyber space is relatively untouched by governmental power.[10)]

The objective of North Korea's cyber power is to create chaos in the South Korean society, freeze state functions, obstruct a military operation in war-time situations, and enhance regime propaganda and promotion. In particular, the US sees the ROK-US alliance as the main objective of North Korea's cyber-attacks. The US Department of Defense reported that North Korea's July 2009 DDoS attack was aimed at identifying how many zombie PCs were needed to disconnect the internet connection between South Korea and the US.

In fact, North Korea has always carried out cyber-attacks within one or two months following a nuclear test or long-range missile launch, and released a threatening statement in defiance against the international community's sanctions, implying a potential terrorist attack. North Korea's chain of actions normally follows the following order: 1) nuclear or missile provocation; 2) warning of provoking South Korea by issuing a party-level declaration; and 3) cyber terrorism.

Meanwhile, North Korea's cyber strategic ability is far from clear. While many point to the strengthening of asymmetric offense capability centered on the General Bureau of Reconnaissance under

10) Kim, Heung-kwang, "The Reasons Behind the Dramatic Increase in the General Bureau of Reconnaissance's Cyber Force," *The Unified Korea*, 2011 June. (in Korean, unofficial translation of title)

the Ministry of the People's Armed Forces, there is a lack of information on the status of their tactical ability.

Recent cases of cyber threats on South Korea are the following. The Korean government reported on March 17, 2015 that North Korea had carried out a cyber-attack on South Korea's nuclear plant operator in December 2014. In addition to that, there is a possibility that North Korea might have carried out a massive-scale cyber-attack on Seoul Metro in July 2014. The number of cyber-attacks reported is as follows: 184,378 cases in 2013; 370,713 cases in 2014; and 350,188 cases as of September 2015. In March 2013, major media outlets and financial institutions were under massive-scale cyber-attacks. North Korea's cyber-attacks have brought about relatively new but severe security problems.

Cyber-attacks on South Korea stared to begin in earnest on 2009. In July 2009, the South Korean government organizations and banks were attacked by hackers on a massive scale and became unable to access their websites, in an incident referred to as the 7.7 DDoS attack. Although there was no evidence to suggest that internal information had been extorted, major Korean and US websites such as the Blue House, Parliament, and the White House were affected for about 70 hours. 1,400 computers were damaged from a computer virus with the massive amount of synchronous accesses causing servers to become saturated. South Korea's National Intelligence Service stated that given the systematic and meticulous nature of the attack, it is probable that it was not an individual's doing but that organizations or military of the North regime had been involved.

North Korea's cyber-attacks are not only carried out against the South Korean society in general but also its military. The Korean military confirmed that North Korea had tapped 33 of 80 wireless networks used by the Korean army base during the 2004 Ulchi Focus Lens training period. In July 2006, military personnel commented that North Korea's cyber unit - Bureau 121 - had hacked into Korea's Ministry of National Defense and the US Department of Defense, causing great damage to South Korea.

In 2004, South Korea's Ministry of National Defense confirmed 26 websites either managed directly by North Korean authorities or through North Korea-friendly organizations, which publicize the North Korean regime and facilitate political propaganda. The Ministry stated that these sites are used by North Korea to issue directions to North Korean spies operating in foreign states.

According to the Ministry of National Defense, there were 28million hacking cases targeting the military in 2008. The number rose to 34million cases in 2009 and over 76million cases in the first half of 2010. The Cyber threat posed to the military is increasingly becoming a grave concern with up to 1,700 military secrets leaked to North Korea through hacking.

After North Korea's fourth nuclear test in January 2016, hundreds of smart phones owned by key personnel in South Korea's foreign policy and security circles were hacked between the end of February and early March. The attacks were carried out by an organization assumed to be a North Korean hacking group. Among them, 20 percent of the attacks were launched in the form of a uniform resource locator (URL) sent via text message, leading the

user to click on the link, after which a malignant code was implanted. The malignant code recorded telephone conversations, extorted the recorded file, hacked into text messages, phone records, and telephone numbers.

North Korea's targeting of key personnel in the Korean government's foreign policy and security circles appears to be aimed at assessing the Korean government's response to North Korea's fourth nuclear test and long-range missile test, and at making preparations to launch a cyber-attack on key organizations. Furthermore, by hacking smart phones, the phone numbers of key personnel were leaked, raising the possibility of North Korea's further attacks using smart phones. In that way, North Korea has expanded its forms of cyber-attacks, moving from its numerous DDoS attacks, targeting servers and computers to targeting mobile phones.

In addition, North Korea has also carried out cyber-attacks on the US. Last December, the US Federal Bureau of Investigation (FBI) reported that there was sufficient evidence to conclude that North Korea was responsible for a series of attacks that had occurred from November to December 2014 on Sony Pictures entertainment, a US-based motion picture distribution company. The National Security Council reported that North Korea had successfully infiltrated the computer network long before these cyber-attacks were carried out.

Korea Institute for National Unification

4. Unmanned Aerial Vehicles and Inter-Korean Relations

4. Unmanned Aerial Vehicles and Inter-Korean Relations

To understand the asymmetric threat posed by North Korea's UAV, it is necessary to assess the two Korea's military power structure and UAV's operational strategy and objective. North Korea's mere possession of UAV cannot be said to constitute an asymmetric threat. This is because South Korea's military also operates reconnaissance UAV at the battalion level. Moreover, states with advanced UAV, such as South Korea and the US, possess UAV technology on a par with piloted combat planes. When considering stealth functions and types of UAV loading system, a significant asymmetry can be formed between countries who possess such technology and those who do not. In fact, given the current state of UAV in the two Koreas, South Korea's UAV can be viewed as posing an asymmetric threat to North Korea.

Nevertheless, given the rapid speed of cost reduction and UAV-related technological development, North Korea's UAV can indeed be considered as an asymmetric threat. In recent years, high-cost electronic components and materials that were previously used only in special fields, such as GPS, gyro sensor, acceleration sensor, and capacity battery, have become more accessible. As a result, various components used in UAV are mounted on to low-cost hobby drones. Consequently, anyone can

easily use hobby or commercial drones, and its widespread use has continued to cut the cost of production. UAVs are no longer simply limited to military purposes; its scope has expanded to commercial purposes, and relevant technology or components can be easily bought and sold through the internet. In fact, UAV sent from North Korea into South Korean territory contain commercial engines, fuselage, and camera, and appeared to be easily assemblable from components bought from Japan or China, or the internet. In other words, development of military UAV has become possible due to the easy access to the private UAV market.

To date, North Korea has not attempted military provocation using UAV. Therefore, what is mounted onto the UAV payload will determine the asymmetric threat. For instance, one can postulate the mounting of weapons of mass destruction onto the payload. It is entirely probable for North Korea to mount chemical weapons or biological weapons onto a UAV to carry out terrorist or military attacks. However, South Korea cannot mount any kind of weapons of mass destruction onto a UAV, as it is a party to Chemical Weapons Convention (CWC) or Biological Weapons Convention (BWC). In this respect, North Korea's use of UAV could pose an asymmetric threat. Although the payload depends on the performance of the UAV, the payload on a commercial UAV is generally 10kg. Given the inverse proportion between the scope of operation and payload, the payload must be reduced to increase the scope of operation. Biological weapons such as anthrax can incur considerable damage with just a few dozen or hundred grams and is thus can be spread easily from a UAV. The symptoms or damages appear long after having been infected with anthrax due

to the long incubation period. Thus, it would be difficult to prove North Korea's role in the attack.

Second, UAV can be an asymmetric threat if used as a means for home-grown terrorism.[11] For instance, it is possible to imagine a situation of terror attacks where a UAV collides with a plane. Thus, one can postulate flying a UAV directly into a plane to bring it down. By situating a small drone near a private or military plane's take-off and landing sites, the drone can be sucked into the plane's engine or directly crash against the plane to cause massive-scale damage. In the case of small drones used in commercial drone races, not only can they fly over 10km at the speed of 100km, but also can be operated with a camera mounted on top. It is entirely plausible for the drone to take off on the outskirts of an airport and incur damages on a plane moving at slow speeds in the process of take-off or landing. The lithium polymer battery used for propulsion power explodes upon clash. Thus, not only will it amplify the intended damage, but also will be able to cause chaos without making it clear it was their doing.

Another possible scenario is to paralyze strategic networks. Carbon fibre can be dropped from the air onto power plants or substations to cause a black out. Carbon fibres are very thin and easy to mount on a small drone. They can be dropped from a low altitude in relative ease, making it possible to cause multiple black outs at the same time. What is important is that North Korea's UAV does not need to be sent from North Korean territory to wage a terror attack

11) Song, Seong-jong, Kil, Byong-ok, "A Study on the Historical Development of Military UAVs and Their Strategic Implications," *Military*, Vol.98 (2015), pp.263-398. (in Korean)

against South Korea. Home-grown terrorist organizations or individuals in South Korean society can directly operate these UAVs, or North Korea can make use of networks to directly operate them.

Third, North Korea can carry out a simultaneous massive-scale strategic attack; China is allegedly known to possess this strategy. The strategy dictates that to make up for its inferior air force, North Korea acquires UAVs in large number that can be produced at low cost, and at the initial stages of war "simultaneously introduces swarms of commercial drones followed by attack drones in massive numbers."[12] If a war breaks out after North Korea sends mass UAVs to South Korea and makes it appear as though South Korea initiated an invasion, North Korea will be able to avoid the responsibility of initiating a war. In addition, there is a chance that after a war is declared, North Korea could send mass UAVs to South Korea to blow up at a radar base or command the group in order to wipe out South Korea's counter attack at the initial stages of war.

For instance, not only do UAVs pose asymmetric threat as military means, they also possess asymmetry from a terrorism perspective. It is thus a form of power that is inherently uncertain. Moreover, given the fast evolution of science and technology along with the advanced UAVs, the asymmetric threat is expected to grow in various ways.

---

12) Jason Koebler, "Report: Chinese Drone 'Swarms' designed to attack American Aircraft carriers," *US News and World Report*, March 14, 2013

North Korea's UAVs appear to be directly operated by the General Bureau of Reconnaissance of the Ministry of the People's Armed Forces. As is well known, the General Bureau of Reconnaissance is tasked with infiltrating South Korea and collecting intelligence. It is an organization suspected of being responsible for the sinking of the Cheonan and shelling of Yeonpyeong Island, and carrying out cyber-attacks on Korean broadcasting stations, public organizations, and financial institutions. Given these facts, it is doubtful that North Korea's UAVs are simply aimed at information gathering, surveillance, and reconnaissance.

The currently-available information illustrates that the power and level of North Korea's UAVs are only limited to information gathering, surveillance, and reconnaissance. Most recently UAVs were discovered at Kangwon province and the north-western islands in 2014. Compared to international UAV standards, those discovered were considerably crude with the ability to carry only a 400g-900g grenade. The mounted engine and intelligence gathering camera have been assessed to be of a 1980s quality. However, these assessments are based on the UAVs that have entered South Korean airspace and those that crashed in South Korean territory; it is difficult to state the actual level of technology in North Korea's UAVs.

North Korea's interest in developing UAVs is estimated to have started in the early 1960s and 1970s. It is claimed that such interest was borne out of the presence of the United States Forces Korea (USFK)'s UAVs in South Korea. Although North Korea did not initially possess UAV production capability, it was able to

develop its own UAVs through import from other nations.

It is known that North Korea procured its first D-4 UAV (ASN-104) from China between 1997 and 1998, and that it began to develop and produce its own UAVs in the early 1990s. It is estimated that North Korean UAV Banghyun I and Banghyun II are these initial UAVs. The length of the Banghyun is 3.23m with an operation radius of 50km, and is estimated to be able to carry out reconnaissance operation for two hours at a 3,000m altitude. In terms of its technical standard, it has been analyzed that the Banghyun can carry 20kg-25kg bombs, and attack a target at a maximum speed of 162km. It has been claimed that the Banghyun has already been placed at the front lines troops in North Korea. In August 2010, North Korea fired 100 artillery shells into the Northern Limit Line (NLL) and used the Banghyun to reconnoiter the region surrounding Baengnyeong Island and Yeonpyeong Island.

It has been estimated that since then North Korea acquired ten short-range reconnaissance UAV Pchela-1T and VR-3 from Russia around 1997-1998. The operation radius for these UAVs are 60km to 90km. They are able to carry out reconnaissance operation for about two hours, but no evidence to date suggests that they were manufactured for offensive purposes.

Moreover, North Korea has procured the Streaker MQM-107D, a US target drone, from Syria, and allegedly enlarged it and mounted a jet engine so that it can run at 925km per hour. Furthermore, it has been claimed that North Korea has remodeled the UAV to mount a small bomb so that it can carry out a self-destructive

attack at a target from a distance of 600km to 800km. In March 2014, North Korea has in fact carried out an anti-missile training on replicated drone of the Streaker target drone (MQM-107D). Such UAV development suggests that North Korea possesses about 1,000 UAVs of various purposes ranging from small-sized to offensive purposes. Recently, it has been revealed that North Korea is building a communications relay station that can operate UAVs in the region surrounding the military demarcation line. It appears that the purpose is to expand its range of operation and obtain real-time surveillance information of South Korea's military situation by communicating with UAV from various relay stations.

The backdrop of North Korea's UAV development is analyzed to be rooted in the international community's increasingly widespread use of UAVs. In terms of security-motivated cases, the existing security theory, in which states confronted with security threats are likely to pursue new military and scientific technology, can be applied to North Korea. In fact, not only the US with its military and technical superiority, but also developing states on the opposite side of the spectrum are purchasing UAVs for security purposes. Bangladesh, Vietnam, and the Philippines have all purchased tactical UAVs from the US and it has been analyzed that these will be used for national security and surveillance of national borders. These states are at the inferior status in terms of naval and air power, and are unable to increase its military budget and thus will inevitably come to depend on technical progress, such as UAVs. Similarly, it has been assessed that China's UAV policy has aimed at offsetting its relative weakness in naval and air power vis-a-vis the US. It has been further predicted that China's speed of

technological development will soon reach that of the US and other UAV manufacturing states. In addition to such external security issues, states experiencing domestic political turmoil are also allegedly purchasing UAVs. Well known cases of UAV usage in counterinsurgency campaigns demonstrate this point. This also applies to the case of North Korea. Compared to South Korea, North Korea is significantly inferior in terms of air power. Furthermore, the lack of military satellites hinders information gathering, surveillance, and reconnaissance activities. Thus, it can be assessed that North Korea is focused on developing its UAVs as to offset these weaknesses.

Second, North Korea must have taken into consideration the symbolic significance of commanding UAV. UAV is a product of materials, energy technology, automation, advanced sensor, controlled airspace, and other various advanced technology. Moreover, UAV technology is continuously being developed and when transferred into civilian UAV, its industrial usage can be expanded into various fields. In this context, the development of UAV does not simply provide asymmetric military superiority, but can also be considered the result of Kim Jong-un's proposed construction of 'knowledge-based' strong state. Therefore, the development of UAV is a way to demonstrate the excellence of the North Korean regime to the international community. In other words, it is an instrument, through which North Korea can acquire not only prestige as indicated by international political theory, but also regime legitimacy. Furthermore, given North Korea's economic state, UAV is a very cost-effective weapons system to obtain prestige and at the same time it is an opportunity to

promote and sell North Korea's new weapons to developing states.

The objective behind North Korea's UAV development is currently moving from information gathering, surveillance, and reconnaissance to offensive purposes. In 2014, Kim Jong-un told military commanders to establish "measures to scientifically reconnoiter enemy situation" and "strengthen enemy reconnaissance activities using various UAVs." In this context, the main objective of UAVs appears to carry out reconnaissance activities. In August 2015, in the midst of a confrontational phase in inter-Korean relations following the wooden-box mine provocation on August 3, North Korea carried out a series of UAV infiltrations five times into South Korean territory. It was reported that the UAVs collected information in areas up to 3km below the military demarcation line before returning to North Korea.

However, North Korea's intent to develop offensive UAVs has been revealed long before. The image of a UAV being shot down by a ground-to-air missile was captured in North Korea's Central Television late 2011. North Korea also revealed a self-manufactured UAV during a military parade at the 100th birthday of Kim Il-sung in April 2012. At a military parade of the 60th anniversary of armistice in 2013, North Korea released self-destructive UAVs.

Furthermore, on July 14, 2016, a North Korean TV program broadcasting Kim Jong-un's field guidance at a military science and technology institute showed a camera-mounted small UAV of less than one meter in size. Compared to the 3m UAV that crashed in Baengnyeong Island in 2014, the new model's size was reduced by a third. In this context, some have suggested that North Korea has

already succeeded in miniaturization and is now engaged in mass production and actual battle preparation.

Korea Institute for National Unification

5. Conclusion and Proposal

5. Conclusion and Proposal

This paper has explained how North Korea's asymmetric threat is embedded in its military strategy toward South Korea through the attributes of the North Korean regime. In addition to North Korea's strategic culture, the asymmetry in power structure between the two Koreas, and the increasingly shrinking of its military economy due to recent economic crises have functioned as factors that can accelerate North Korea's asymmetric threat.

Furthermore, North Korea's asymmetric threat not only has increased with the development in science and technology, but also witnessed the increasing factors, by which asymmetric threat can be imposed in an international environment of enhanced technology proliferation. In particular, the possibility of low-intensity conflict stirring on the Korean Peninsula increases the chances of North Korea carrying out an asymmetric threat-based provocation. It should be noted that within North Korea, the cutting-edge policies officalized in the Kim Jong-il regime has led to the establishment of strategies of science and technology development. Ultimately, this is not only likely to diversify North Korea's asymmetric threat but also boost its intensity.

The cyber threat and asymmetric threat emerging from UAV infiltration analyzed in this paper are forms of the threat that are

receiving newfound attention in the context of science and technology development. In particular, cyber threats have even been called the 'fifth domain of war,' demonstrating its new form of asymmetric threat, and North Korea has already carried out a series of cyber-attacks on South Korea and the US. Although North Korea's UAVs have thus far been operated for reconnaissance and surveillance purposes, rapid developments in UAV technology in the international community have also advanced North Korea's UAV-related resources.

Meanwhile, South Korea's counter-response to asymmetric threats takes place case-by-case, without a theoretical foundation of the occurrence and developmental paths of respective asymmetric threats. The need to prepare against asymmetric threats has long been emphasized in South Korea, but the talk of the asymmetric threat continued to this date demonstrates that there is still a lack of preparation.

Furthermore, there is a lack of contemplation on the fundamental causes behind North Korea's asymmetric threat-based provocation and low-intensity conflict, as well as a comprehensive response at the North Korean policy level.

To this end, the following preparations need to be taken at the government level. To begin, in terms of cyber threats, there is a need for mid-to-long term planning at the state level regarding North Korea's cyber threats. The incumbent government prepares for cyber terrorism through the National Cyber Security Centre of the National Intelligence Service. At the Defense Ministry level, there has been much focus on protecting information on national

defense by, for example, establishing the Cyber Command in 2010. Although it is related to the integration of a state cyber security management agency, which will be mentioned next, cyber threats imposed by North Korea need to be addressed at the state level, with government and defense strategies established from a mid-to-long term perspective. To this end, a priority list of policies concerning North Korea's cyber threat should be established, and other measures such as expanding state budget for cyber threat countermeasures, need to be taken to strengthen state capacity for cyber security.

Second, there is a need for a state cyber security management agency. In order to efficiently respond to North Korea's cyber threats, relevant legislations need to be streamlined. These legislations include the Framework Act on the Promotion of National Information System, Act on the Promotion of Information and Communications Network Utilization and Information Protection, and the national cyber security management regulations. Furthermore, the integration of a state cyber security management agency, a control tower, is required according to the streamlined legislation. This control tower will allow establishing a cooperative system and sharing information among ministries, and manage cyber threats dealing with international cooperation and coordinative system amongst allies.

Third, it is necessary to secure experts to counter North Korea's cyber threats. The government needs to provide strong legal and systematic measures to acquire experts who can be in charge of cyber security at state and public institutions. Based on the

understanding that countering North Korea's cyber threat is a core means of defending national security, the government needs to increase interests and budget to attract the most gifted candidates. Particularly at the military level, steps need to be taken to nurture cyber experts into cyber-warfare specialists or through a substitutional military service system, who can be tasked with the future cyber warfare.

Fourth, cyber cooperation should be pursued with the US, Australia, and Japan. Recently, the US requested cyber cooperation to its traditional allies to strengthen its cyber capabilities, but South Korea did not actively respond due to its consideration for ROK-Sino relations. In contrast, Japan and Australia actively took part in cyber cooperation with the US. In particular, Japan established a cyber defense corp in 2014, and the Guidelines for US-Japan Defense Cooperation revised in April 2015 have expanded alliance cooperation to cover domains of cyberspace, and reflected budget concerning US-Japan cooperation in cyber security.

South Korea's lack of military cooperative relations to prepare for North Korea's cyber threat creates a need to establish cooperative relations with the US and Japan in the cyber security sphere, and particularly institutions on cyber security need to be further strengthened for the ROK-US alliance.

Meanwhile, at the government level, responses concerning UAV infiltration should include the following. To begin, there is an urgent need to enact laws that meet the needs of UAV technological development and commercialization. In particular,

UAV-related terrorist attacks can be carried out not only by North Korean UAV infiltrating South Korea, but also through home-grown terrorist organizations within South Korea. With this in mind, legislations on UAV operation and control need to be urgently drafted to respond to the illegal use of UAV and potential terrorism.

Second, the government will need to integrate the air traffic control system. This is because the commercialization of UAV has increased the threat of military UAVs or attractors crashing into an unidentified commercial UAV. For instance, it may be meaningful to add a UAV location detector function into the helicopter traffic control system that is being promoted by the ROK Joint Chiefs of Staff.

Third, cooperation at the ROK-US alliance level needs to be strengthened in order to respond to North Korean UAV infiltration. The US Department of Defense proposed its "third offset strategy" envisioning comprehensive countermeasures that could neutralize various forms of asymmetric threat. The US offset-strategy in the Asia-Pacific region involves an innovative weapons system that could neutralize even China's anti-access/area-denial strategy. Also, the US automated weapons system and electronic weapons' development constitute a core element of such strategy. This will enable South Korea to jointly respond to North Korea's UAV threat while during times of peace, the ROK-US alliance can cooperate and respond to North Korea's provocations to further strengthen the alliance.

Meanwhile, given that asymmetric threats pose a military threat,

military measures at the government level is most urgent. However, there is also a need to manage the asymmetry from a non-military perspective, particularly given the characteristic of the Korean system. Moreover, a special attention is needed to South Korea's security industry that is extremely vulnerable to democratic political system with free press, and rapid developments in network, and science and technology. This will ultimately lead to public and private sector cooperation.

Public and private sector cooperation on cyber threats can include the following. First, it is necessary to strengthen cooperation with the press and the media. North Korea's cyber threat carries additional ripple effects at a psychological level. Therefore, the government needs to improve relations and communications with the media. Therefore, friendly relations with the various media and news outlets not only lead to a stable government but also are directly related to national security. To date, North Korea has capitalized on South Korean news outlets that are sympathetic to them, and has also attempted psychological warfare on the internet to manipulate facts and control South Korean public's perception. Recently, North Korea has been able to influence public perception and subsequently manipulate the media through the use of social network services (SNS) by spreading and spamming replies. Therefore, given that North Korea is using psychological warfare in cyberspace as a tool to influence the perception and consciousness of the people and distort information, thus becoming likely to trigger domestic division, the South Korean government needs to pursue active communications with the press and the media to provide countermeasures and enhance cooperation against North Korea's

psychological warfare in cyberspace.

Second, above all, in order to respond to cyber threats, citizens need to be encouraged to actively cooperate and participate. Although a government-led response is primarily important, active participation is crucial not only at the individual level, but also at the national security level, given the intricate links that every citizen has between their everyday lives and cyberspace. To this end, the government should actively carry out promotion and education by publishing booklets, etc. to raise awareness of both individuals and businesses on cyber security. In particular, the government needs to seek methods to encourage people to participate in cyber security through protecting personal information.

Third, it is necessary to establish the public-private-military joint cyber defense system where the press, media, central and local governments, and private companies can all come together. Strategy based on the government and military is important for security in cyberspace; however, a comprehensive and integrated perspective on cyber security grounded on public consent and support is also as important.

In order to respond to UAV infiltration, the Ministry of Land, Infrastructure and Transport recently released "legislation roadmap for private unmanned aerial vehicles," and between 2014 and 2015 had promoted legislation and pursued studies on definition, categorization, certification, and aircraft operation, relating to UAV. Their plan for 2016-2018 is to promote legislation and studies concerning security, airspace, and aviation safety act, among others. In addition, they are currently operating a public-private joint task

force with the objective of jointly managing manned and unmanned aerial vehicles in state airspace. Public-private cooperation is very important when the threat of UAV infiltration is real. In particular, a UAV safety control committee led by public-private-military participants is imperative. For instance, the public-private-military consultative body that oversees the helicopter traffic control system promoted by the ROK Joint Chiefs of Staff should include UAV as to enable a multifaceted discussion on UAV safety control by all public-private-military participants. This group should consist of various participants from the Ministry of Defense, Joint Chiefs of Staff, Aviation Operations Command, Ministry of Land, Infrastructure and Transport, and representatives from the UAV industry as well as other relevant experts. This will enable a vibrant discussion based on different perspectives held by the public-private-military participants concerning the threat imbedded in UAV's rapidly developing science and technology, thereby alleviating the asymmetric threat imposed by UAVs.