Rachael M. Rudolf:

STRATEGIC CONTAINMENT: TRIANGULATING NORTH KOREA'S ASYMMETRIC PROVOCATIONS WITH A MULTILATERAL ELECTRONIC AND CYBER WARFARE CONTAINMENT STRATEGY

ABSTRACT: *North Korea's asymmetric provocations complicate the security environment, thereby preventing the employment of alternative forms of conflict transformation and peacebuilding operations to facilitate peace and stability on the Korean Peninsula. Strategically containing those provocations by employing electronic and cyberwarfare capabilities may provide the opening needed to introduce a new, concerted, multilateral, multipronged strategic approach to transform the conflict dynamics, stabilize the regional and domestic environment, and facilitate peace. Part one of this article provides readers with a general overview of electronic warfare (EW), cyber warfare (CW), cyberspace (CS), the electromagnetic spectrum (EMS), electromagnetic pulse (EMP) weapons, and North Korea's capabilities. Part two utilizes the information provided in part one to make the argument as to why a strategic EW/CW containment doctrine is needed, and outlines some of its parameters. Part three concludes that a EW/CW containment doctrine can only be one pillar of a new, concerted, multilateral, multipronged strategic approach to bringing lasting peace to the Korean Peninsula.*

KEYWORDS: *North Korea, South Korea, United States, China, Electronic Warfare, Cyber Warfare, Electromagnetic Pulse Weapons, containment, Asia-Pacific, Security*

INTRODUCTION

North Korea's asymmetric provocations increase tensions within the Asia-Pacific region and prevent discussion on the employment of alternative forms of conflict transformation and peacebuilding operations to facilitate peace and stability on the Korean Peninsula. Two specific provocations this year have been the missile launches and the cyber-attacks. North Korea's advancing missile technology development, the potential for it to launch an intercontinental ballistic missile with a nuclear warhead capable of reaching the territory of the U.S., and missile defense to prevent such an attack, however, have been of utmost concern to the United States.[1] Largely ignored and, arguably, of more immediate concern to the region is North Korea's ability to use electromagnetic pulse (EMP) weapons[2] and the

[1] Mason, K. "Can the U.S. defend itself from a missile attack from North Korea?". *The Financial Times*, 30 June 2017. https://www.ft.com/content/3e2a5a24-5d41-11e7-9bc8-8055f264aa8b, Accessed on 1 July 2017.

[2] Graham, W. R. "North Korea Nuclear EMP Attack: An Existential Threat". 38 North. 2 June 2017. http://www.38north.org/2017/06/wgraham060217/, Accessed on 1 July 2017.

unpreparedness of the surrounding countries for their use in a future war. The present situation on the Korean Peninsula, therefore, is untenable.

Past policies employed by the U.S.[3] and a doctrine of strategic coercion, as advocated by the Trump administration,[4] are unlikely to produce positive results in the present situation. The U.S., South Korea, Japan, China, or Russia alone cannot contain North Korea and its intentional asymmetric provocations. It would, however, be possible for certain strategically significant state actors, such as the United States, Japan, China, and Russia, just to name a few, to contain North Korea through a strategic doctrine of electronic and cyber warfare containment, while other strategically significant state and non-state actors simultaneously worked on transforming the conflict environment and facilitating the conditions for domestic and regional stability so that the main conflict actors can work toward a peaceful resolution of the North Korean issue. A concerted, multipronged, strategic approach is warranted to bring about lasting peace on the Korean Peninsula.

The remainder of the article is structured as follows: Part one provides readers with a general overview of electronic warfare (EW), cyber warfare (CW), cyberspace (CS), the electromagnetic spectrum (EMS), electromagnetic pulse (EMP) weapons, and North Korea's capabilities. The general information provided on EW, CW, CS, the EMS, and EMP weapons were derived from a combination of sources ranging from the U.S. Army's newly released manual on Cyberspace and Electronic Warfare Operations,[5] the U.S. Joint Chiefs of Staff's Joint Publications on Electronic Warfare[6] and Cyberspace Operations,[7] and expert studies.[8] Information on North Korea's capabilities was derived from open-sources, expert studies,

[3] Chanlett, E., Rinehart, I. E. and Nikitin, M. D. "North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation". Congressional Research Report. 2016. 1–28. https://fas.org/sgp/crs/nuke/R41259.pdf, Accessed on 29 June 2017.

[4] Lall, R. R. "America favors strategic coercion over Pyongyang". The National. 19 April 2017. Opinion. http://www.thenational.ae/opinion/comment/america-favours-strategic-coercion-over-pyongyang, Accessed on 29 June 2017.

[5] U.S. Army. *FM 3-12: Cyberspace and Electronic Warfare Operations.* Headquarters: U.S. Department of the Army. 2017. https://fas.org/irp/doddir/army/fm3-12.pdf, Accessed on 29 June 2017.

[6] U.S. Joint Chiefs of Staff. *Joint Publication 3-13.1: Electronic Warfare*, 2007. https://fas.org/irp/doddir/dod/jp3-13-1.pdf, Accessed on 29 June 2017.

[7] U.S. Joint Chiefs of Staff. *Joint Publication 3-12R: Cyber Operations*, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, Accessed on 29 June 2017.

[8] See: Miller, C. R. "Electromagnetic Pulse Threats in 2010". *Center for Strategy and Technology*: *Air War College, Air University.* 2010. 383–410. http://www.au.af.mil/au/awc/awcgate/cst/bugs_ch12.pdf, Accessed on 29 June 2017. Poisel, R. *Information Warfare and Electronic Warfare Systems.* Norwood, MA: Artech House, 2013. Scobell, A. and Sanford, J.M. *North Korea's Military Threat: Pyongyang's Conventional Forces of Mass Destruction, and Ballistic Missiles.* U.S. Army War College: Strategic Studies Institute, 2007. https://ssi.armywarcollege.edu/pdffiles/PUB771.pdf, Accessed 29 June 2017. Vass, S. "Defense against electromagnetic pulse weapons". *AARMS*, 3/3. 2004. 443–457. http://www.zmne.hu/aarms/docs/Volume3/Issue3/pdf/13vass.pdf, Accessed on 29 June 2017. Wilson, C. "High Altitude Electromagnetic Pulse (HEMP) and High-Power Microwave (HPM) Devices: Threat Assessments". *CRS Report for Congress*, 2008. 1–16. https://www.wired.com/images_blogs/dangerroom/files/Ebomb.pdf. Accessed on 29 June 2017.

and industry reports.[9] Part two utilizes the information provided in section one to make the argument as to why a strategic EW/CW containment doctrine is necessary, and outlines some of its parameters. It should be noted that this article is intentionally designed to be brief and exploratory in nature. Finally, part three concludes that an EW/CW containment doctrine can only be one pillars of a new concerted, multilateral, multipronged strategic approach to bringing lasting peace to the Korean Peninsula.

AN OVERVIEW OF EW, CW, CYBERSPACE, THE EMS, AND EMP WEAPONS AND NORTH KOREA'S CAPABILITIES

EW and CW are not new to 21st century warfare. What is new, however, is their simultaneous integration into overarching hybrid warfare strategies and operational plans by state and non-state actors. Hybrid warfare can be characterized by a unique set of physical and psychological, kinetic and non-kinetic threats, employed by both state and non-state actors to meet their aims.[10] North Korea's relationship to non-state actors involved in irregular warfare across the globe and its level of knowledge of EW and CW have raised security concerns for future stability within the Asia-Pacific region. A basic shared understanding of EW, CW, Cyberspace, EMS, and EMP weapons and North Korea's capabilities are, therefore, necessary.

Understanding the concepts: EW, CW, cyberspace, the EMS, and EMP weapons

EW is understood to be the use of military action to gain superiority in cyberspace and over the EMS by synchronizing operations, attacks, support, and protection across a network through the use of electromagnetic and directed energy in an area of operations, which encompasses the military and civilian information, communication, and technology

[9] See: Berkofsky, A. "North Korea's Military-What Do They Have, What do they Want?." *Instituto Per Gli Studi Di Politica Internazionale* 161. 2013. http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_161_2013_0.pdf, Accessed on 29 June 2017. Bermudez, J. S. "Chapter 13: SIGINT, EW, and EIW in the Korean People's Army: An Overview of Development and Organization". In Mansouroyv, A. (ed), *Bytes and Bullets: Information Technology Revolution and National Security.* Honolulu: Asia-Pacific Center for Security Studies, 2005. 234–275. http://apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf, Accessed on 29 June 2017. Chanlett, E. et al. "North Korea: U.S. Relations…". "HP Security Briefing Episode 16: Profiling an enigma: The mystery of North Korea's cyber threat landscape". HP Security Research. 2014. https://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf, Accessed on 29 June 2017. Jun, J., LaFoy, S. and Sohn, E. *North Korea's Cyber Operations: Strategies and Responses.* Center for Strategic and Intelligence Studies. Lanham, MD: Rowman and Littlefield, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf, Accessed on 29 June 2017. Mansourov, A. "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance". *Korea Economic Institute of America: Academic Paper Series*, 2014. 1–17. http://www.keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf, Accessed on 29 June 2017.

[10] Hoffman, F. G. "Hybrid Warfare and Challenges". *Joint Forces Quarterly* 52/1. 2009. 34–39.

infrastructures.[11] Superiority is understood as the degree to which an actor can manage the EMS to engage in either offensive or defensive operations.[12] Offensive and defensive operations include electronic attacks, electronic protection, and electronic support.[13] Electronic attacks are the use of radiofrequency weapons, lasers or particle beams that use either electromagnetic or directed energy against electronic equipment to prevent or reduce the use of the EMS. Deception, intrusion, jamming, probing, and pulse are the most common types of electromagnetic attack actions. Electronic protection include actions undertaken to prevent jamming, such as frequency hopping; to protect equipment through hardening, masking, emission control, or resisting an attack; and, to destroy the jamming capabilities of an adversary with anti-radiation missiles.[14] Electronic support actions include collecting intelligence on non-communications electromagnetic radiations; detecting, locating, identifying, and evaluating electromagnetic threats; and, protecting the EMS and networks in an operational area from an adversary's acquisition of information of value. EW operations and actions are separate from yet complimentary to CW operations.

CW is understood to be the use of cyber capabilities in cyberspace to carry out offensive and defensive operations and actions to attain superiority in an information environment.[15] Cyber capabilities refer to devices, computer programs, and techniques used to create cyber effects. Cyberspace is a "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers."[16] Cyber actions include the defense and protection of information networks through cyberattacks and cyber security; and the detection of threats through intelligence, surveillance, and reconnaissance. Cyberspace superiority is attained when an actor has a degree of dominance that either prohibits or restricts an adversary from interfering with an operation or warfare capabilities.[17] The informational dimension connects cyberspace to the EMS.

The EMS is the transport medium connecting cyberspace operations and electronic warfare operations.[18] It is defined as the range of frequencies of electromagnetic radiation.[19] The management of the EMS is, therefore, critical to effectively employ capabilities and conduct

[11] U.S. Army, FM 3-12: Cyberspace and Electronic Warfare Operations; Poisel. *Information Warfare and Electronic Warfare System;* U.S. Joint Chiefs of Staff. *Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations*, 2012. http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf, Accessed on 30 June 2017. U.S. Joint Chiefs of Staff. *Joint Publication 3-13.1: Electronic Warfare*; U.S. Army. *FMI 6-02.70 (FM 24-2): Army Electromagnetic Spectrum Management Operations.* Headquarters: U.S. Department of the Army. 2006. https://fas.org/irp/doddir/army/fmi6-02-70.pdf, Accessed on 27 June 2017.

[12] U.S. Army, FM 3-12: Cyberspace and Electronic Warfare Operations.

[13] U.S. Joint Chiefs of Staff. *Joint Publication 6-01.*

[14] Anderson, R. J. *Security Engineering.* Chichester, UK: John Wiley & Sons Ltd., 2001, 560.; U.S. Army, *FM 3-12: Cyberspace and Electronic Warfare Operations.* 1–29.

[15] U.S. Army, *FM 3-12: Cyberspace and Electronic Warfare Operations;* U.S. Joint Chiefs of Staff. *Joint Publication 3-12R: Cyber Operations.*

[16] U.S. Army, *FM 3-12: Cyberspace and Electronic Warfare Operations.* 1–2; U.S. Joint Chiefs of Staff. *Joint Publication 3-12R: Cyber Operations.*

[17] U.S. Army, *FM 3-12: Cyberspace and Electronic Warfare Operations.* 1–3.

[18] U.S. Army, *FM 3-12: Cyberspace and Electronic Warfare Operations.*

[19] U.S. Army. *FM 3-38: Cyber Electromagnetic Activities.* Headquarters: U.S. Department of the Army. 2014. https://fas.org/irp/doddir/army/fm3-38.pdf, Accessed on 29 June 2017. U.S. Joint Chiefs of Staff. *Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations.*

operations. Activities undertaken to manage the EMS include frequency assignment, host nation coordination, and establishment of policies for planning, management, and execution of operations. Spectrum management is critical for the use of EMP weapons, particularly because of their impact on both civilian and military infrastructures.

EMP is "an instantaneous, intense energy field that can overload or disrupt at a distance numerous electrical systems and high technology microcircuits, which are especially sensitive to power surges."[20] Two of the most common weaponized forms of EMP are HEMP and HPM. HEMP is a High-altitude Electro-Magnetic Pulse that is released into the atmosphere through the power and radiation of a nuclear explosion for the purpose of damaging, disrupting, or destroying electronic equipment and communication systems. Its actual impact, however, depends on the design of the nuclear device, the altitude of the burst, and the degree of hardening of the equipment and systems operating both in civilian and military infrastructures. HPM is an instantaneous High-Powered Microwave electromagnetic energy pulse. It is created through special electronic equipment that transforms a chemical reaction or explosion into microwaves, which are damaging to electronic equipment and systems near the blast. Although the blast of a HPM device is smaller and more direct, it is more difficult to harden against; thus, civilian and military equipment and systems are more susceptible to damage, disruption, or destruction. In any future war on the Korean Peninsula, North Korea is likely to use EMP weapons. HPM devices have the potential to alter the ground dynamics of any invasion—either by the North into the South or the South into the North.

North Korea's capabilities

EW and CW have long been central to North Korea's asymmetric military capabilities. In the 20th century, Kim Jong Il said that EW is the "key to victory in modern warfare,"[21] while Kim Jung Un highlighted the significance and power of CW in the 21st century.[22] Unlike many countries who considered EW and CW as separate yet complimentary forms of warfare in the 20th century, North Korea adopted an approach in 1990 that coupled EW, CW and Information Warfare, which it called Electronic Warfare and Electronic Intelligence Warfare (EW/EIW). For the sake of consistency, EW/CW will continue to be used for EW/EIW. Today, North Korea's EW/CW operational understanding is similar to the understanding of cyberspace and electronic warfare operations articulated in the U.S. Army's 2017 Field Manual on Cyberspace and Electronic Warfare Operations. Its capabilities, however, do not parallel those of the U.S. Armed Forces.

North Korea's EW/CW developments can be broken down into four periods of time — WWII-1960s, the 1960s-1980s, the 1990s, and the 2000s.[23] In the first period, SIGINT, EW, and EIW were introduced in North Korea by the former Soviet Union in WWII. SIGINT was used in the Korean War. In the second period, education and curriculum development were introduced in North Korea's civilian and military schools and universities; military personnel received specialized training in EW and SIGINT by the former Soviet Union and China; and, a small number of mainframe computers were acquired. By the end of the period, North Korea's military schools and universities had specialized EW/SIGINT curricula, which

[20] Wilson. "High Altitude Electromagnetic …". 1.
[21] Bermudez. "Chapter 13: SIGINT …". 5.
[22] Mansourov. "North Korea's Cyber Warfare…". 1.
[23] Bermudez. "Chapter 13: SIGINT …". 5.

were taught by those who had been trained in the 1960s and 1970s. Schools were no longer that reliant on Chinese and Eastern European foreign instructors. In the third period there were five key developments. First, the military underwent some organizational changes; all branches, however minor, began incorporating EW/SIGINT capabilities and focusing R&D on weaponizing EW/CW. Second, new educational curricula were introduced across the civilian and military schools and universities for computer software and hardware development. Third, the Korean Computer Center was established to cultivate computer program and software development among civilians. Fourth, technological cooperation was facilitated between Korean R&D institutes and developing countries for importing computer software and hardware. Fifth, the communication and information infrastructures were updated and enlarged. By the end of the period (it is significant to note), all branches of the Korean Armed Forces had training in and focused on R&D to further develop each branch's informational, technological, and operational EW/CW capabilities; an Electronics Industry Ministry was created; and significant infrastructural developments were made to lay the foundation for the cyberspace developments in the last period. Cyberspace, CW, and the missile program were focused on in the last period.

In conclusion, North Korea's EW/CW capabilities may not be comparable to those of the U.S. armed forces but its knowledge appears to be far more advanced than what some expected. Poor information, communication, and technological infrastructural developments remain the largest stumbling blocks. Despite the challenges, its capabilities are likely to advance in the years to come, particularly as its main adversaries' civil and military information and technological dependencies grow. Imagine the chaos that would ensue with the use of a HEMP weapon in the region or the use of HPM devices in any ground war with the South. While military equipment and communication systems among the surrounding countries' armed forces are likely to withstand a potential HEMP attack (depending of course on the altitude and degree of hardening), civilian infrastructures would not be as resistant. Similarly, in a ground invasion, the use of HPM in South Korea would create social and economic chaos; thus, creating a factor not *per se* taken into consideration when assessing threats for strategy and operation plan design. North Korea has consistently strategized in terms of contemporary asymmetric warfare, while its adversaries continue to largely think in terms of and approach it with ideas rooted in conventional warfare capabilities. An asymmetric, strategic approach is needed most at the present to contain North Korea's asymmetric provocations.

STRATEGIC CONTAINMENT OF NORTH KOREA'S ASYMMETIC PROVOCATION

North Korea's asymmetric provocations are perceived to be a threat to regional stability and international security, and a surgical strike, war, or regime change are not viable coercive policy options for the region or its actors. A coercive option that has not per se been tried is a multilateral containment strategy designed to use EW/CW capabilities over a sustained period, while other non-coercive measures are employed. The aim of such a strategy would be to contain North Korea's asymmetric provocative operations through disruption and/or limiting the effects of its actions.24 The immediate asymmetric provocations of concern

[24] For example, during the Aramco cyberattack, Saudi Arabia shut down parts of the grid from which the computer network systems operated to contain the attack. Rudolph was living in Saudi Arabia at the time of the attack.

are its missile launches and cyberattacks. It would have to be multilateral because of the nature of the EMS and North Korea's information and communication networks; its history of changing the locations of where missiles are launched and use of frequency-hopping; and finally, its running of cyber operations from countries in the Asia-Pacific, and the Middle Eastern regions, as well as using IP addresses from countries in South America and global non-state actors to launch cyberattacks.

The nature of the EMS grid and EW/CW operations to be undertaken in a containment strategy would determine which actors are strategically significant. Despite the global positioning of the U.S. D.O.D Information Network and the nature of the South Korean and Japanese military networks, the U.S., South Korea, and Japan cannot sustain an EW/CW containment strategy on their own. Other regional actors, such as China, Russia, Iran, and Thailand (to name just four) would be strategically significant. North Korea is heavily dependent on China for its ICT infrastructure. Moreover, some cyber-attacks conducted by North Korean operatives originate in China and use Chinese software. A sustained EW/CW containment strategy is not possible, in our humble opinion, without China's participation. Russia, then the Soviet Union, provided much of the technological training and equipment in use. The participation of both in such a strategy might also mitigate some of the present regional tensions over the U.S. positioning of the Terminal High-Altitude Area Defense (THAAD) system in South Korea.[25] Iran has aided North Korea with its missile development program. Thailand's Loxley Pacific has a history of working with North Korea on high-tech projects and a connection to the Star Venture Company. The Star Venture Company is responsible for North Korea's connection to the Internet. In addition to state actors, global state and non-state actors would also have to be considered and an assessment of their impact on containment operations conducted because of the relations they maintain with North Korea. The most notable non-state actor that has relations with North Korea and Iran, an EW/CW capability, and a global network is Hezbollah. Other insurgent and militant actors involved in arms trafficking, and non-insurgent actors involved in transnational organized crime who have significant political relations with licit actors in Africa, Asia, and Central and South America would be relevant not *per se* for actual EW/CW containment but for understanding potential asymmetric countermeasures by North Korea and its non-state allies.

Given the relevance of multiple sets of actors to the running of EW/CW containment operations, spectrum management would be extremely important yet also difficult. Spectrum management is defined as "the planning, coordinating, and managing the use of the electromagnetic spectrum through operational, engineering, and administrative procedures."[26] The U.S. Army's Cyber Electromagnetic Activities manual and the U.S. Joint Chiefs of Staff's Joint Electromagnetic Management Operations manual highlight the difficulty in planning and executing spectrum management operations involving international state and non-actors.[27] Differences in policies and training, difficulties in system integration and information sharing, language and terminology barriers, and security restrictions preventing full disclosure are cited as specific hindrances. Within the context of North Korea, U.S. coordination with Japan and South Korea do not raise any red flags but coordination with other strategic actors

[25] They both oppose its positioning in South Korea because of the potential impact on their own military equipment and radar systems.

[26] U.S. Army. *FMI 6-02.70 (FM 24-2): Army Electromagnetic Spectrum Management Operations.* 1-1.

[27] U.S. Army. *FM 3-38: Cyber Electromagnetic Activities;* U.S. Joint Chiefs of Staff. *Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations.*

such as China and Russia do. One can just imagine the national security debates in the U.S. over cooperating with them. Yet, it is coordination such and with China more specifically, which is necessary to make a sustained EW/CW containment strategy designed to curtail North Korea's cyber activities and missile launches a reality. The present situation is untenable and U.S. approaches thus far tried and proposed have had limited success. Perhaps then it is time for us to think and act with a hybrid warfare mindset when playing on a multilateral, multidimensional networked game board.

CONCLUSION: STRATEGIC CONTAINEMENT–EW/CW CONTAINMENT ONLY A PILLAR OF A MULTIPRONGED APPROACH

North Korea will continue developing its missile and nuclear programs while employing an asymmetric strategy and engaging in asymmetric provocations. Strategic containment doctrine employing EW/CW capabilities to triangulate and contain North Korea's asymmetric provocations is not sufficient alone. A multilateral and multipronged hybrid approach is needed, which incorporates both state and non-state actors and balances the symmetrical and asymmetric capabilities of the main actors so that a win-win solution can be attained. Past approaches tend to neglect the role of non-state actors. The non-state actors in mind are not the typical civil society actors, as they have long played a role in endeavors to implement non-coercive policies. It is rather those who have yet to be assessed and factored into the equation are the strategically significant, illicit actors which are central to North Korea's economic and political alliances and economic activities, and the state actors who are connected to and have relations with the global illicit and black economies. Transnational organized crime, criminal syndicates, and gangs in Asia, Africa, Europe, Central and South America, and the Middle East are relevant for thinking of alternative ways to contain North Korea's provocative asymmetric actions. A traditional multilateral approach will never work with a non-traditional, non-conformist state actor. We need to think creatively and outside of the box when developing a new, multilateral, multipronged hybrid approach to North Korea, particularly if the world is keen on facilitating stability on the Korean Peninsula.

BIBLIOGRAPHY

Alioto, S. "We're Not Blowing Up North Korean Rockets. The Red Chinese Are". *Santa Monica Observer*, 10 May 2017. News. http://www.smobserved.com/story/2017/04/29/news/were-not-blowing-up-north-korean-rockets-the-red-chinese-are/2856.html, Accessed on 29 June 2017.

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 2nd Edition. Chichester, UK: John Wiley & Sons Ltd., 2001. http://www.cl.cam.ac.uk/~rja14/book.html, Accessed on 29 June 2017.

Berkofsky, A. "North Korea's Military-What Do They Have, What do they Want?". Instituto Per Gli Studi Di Politica Internazionale. 161. 2013. http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_161_2013_0.pdf, Accessed on 29 June 2017.

Bermudez, J. S. "Chapter 13: SIGINT, EW, and EIW in the Korean People's Army: An Overview of Development and Organization". In Mansourov, A. *Bytes and Bullets: Information Technology Revolution and National Security.* Honolulu: Asia-Pacific Center for Security Studies, 2005. 234–275. http://apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf, Accessed on 29 June 2017.

Chanlett, E., Rinehart, I. E. and Nikitin, M. D. "North Korea: U.S. Relations, Nuclear Diplomacy, and Internal Situation". Congressional Research Report. 2016. 1–28. https://fas.org/sgp/crs/nuke/R41259.pdf, Accessed on 29 June 2017.

Graham, W. R. "North Korea Nuclear EMP Attack: An Existential Threat". 38 North. 2 June 2017. http://www.38north.org/2017/06/wgraham060217/, Accessed on 1 July 2017.

Hoffman, F. G. "Hybrid Warfare and Challenges". *Joint Forces Quarterly.* 52/1. 2009. 34-39.

"HP Security Briefing Episode 16: Profiling an enigma: The mystery of North Korea's cyber threat landscape". HP Security Research. 2014. https://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf, Accessed on 29 June 2017.

Jun, J., LaFoy, S. and Sohn, E. *North Korea's Cyber Operations: Strategies and Responses.* Center for Strategic and Intelligence Studies. Lanham, MD: Rowman and Littlefield, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf, Accessed on 29 June 2017.

Lall, R. R. "America favors strategic coercion over Pyongyang". The National. 19 April 2017. Opinion. http://www.thenational.ae/opinion/comment/america-favours-strategic-coercion-over-pyongyang, Accessed on 29 June 2017.

Mansourov, A. "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance". *Korea Economic Institute of America: Academic Paper Series*, 2014. 1–17. http://www.keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf, Accessed on 29 June 2017.

Mason, K. "Can the U.S. defend itself from a missile attack from North Korea?". *The Financial Times*, 30 June 2017. https://www.ft.com/content/3e2a5a24-5d41-11e7-9bc8-8055f264aa8b, Accessed on 1 July 2017.

McGrath, M. and Wertz, D. "North Korea's Ballistic Missile Program". *The National Committee on North Korea: Issue Brief*, 2015. 1–14. http://www.ncnk.org/resources/publications/Missile_Issue_Brief.pdf, Accessed on 29 June 2017.

Miller, C. R. "Electromagnetic Pulse Threats in 2010". Center for Strategy and Technology: Air War College, Air University. 2010. 383–410. http://www.au.af.mil/au/awc/awcgate/cst/bugs_ch12.pdf, Accessed on 29 June 2017.

Poisel, R. *Information Warfare and Electronic Warfare Systems.* Norwood, MA: Artech House, 2013.

Robinson, J. "North Korea could be preparing an EMP strike on the U.S. with two satellites already orbiting above America, expert warns". Daily Mail. 8 May 2017. News. http://www.dailymail.co.uk/news/article-4484760/North-Korea-preparing-EMP-strike-US.html, Accessed on 29 June 2017.

Ryall, J., Smith, N. and Millward, D. "North Korea's unsuccessful missile launch 'may have been thwarted by US cyber-attack'". *The Telegraph*, 16 April 2017. News. http://www.telegraph.co.uk/news/2017/04/16/north-korea-makes-unsuccessful-missile-launch-day-massive-show/, Accessed on 29 June 2017.

Scobell, A. and Sanford, J. M. *North Korea's Military Threat: Pyongyang's Conventional Forces of Mass Destruction, and Ballistic Missiles.* U.S. Army War College: Strategic Studies Institute, 2007. https://ssi.armywarcollege.edu/pdffiles/PUB771.pdf, Accessed 29 June 2017.

Vass, S. "Defense against electromagnetic pulse weapons". *AARMS* 3/3. 2004. 443–457. http://www.zmne.hu/aarms/docs/Volume3/Issue3/pdf/13vass.pdf, Accessed on 29 June 2017.

U.S. Army. *FM 3-12: Cyberspace and Electronic Warfare Operations.* Headquarters: U.S. Department of the Army. 2017. https://fas.org/irp/doddir/army/fm3-12.pdf, Accessed on 29 June 2017.

U.S. Army. *FM 3-38: Cyber Electromagnetic Activities.* Headquarters: U.S. Department of the Army. 2014. https://fas.org/irp/doddir/army/fm3-38.pdf, Accessed on 29 June 2017.

U.S. Army. *FMI 6-02.70 (FM 24-2): Army Electromagnetic Spectrum Management Operations.* Headquarters: U.S. Department of the Army. 2006. https://fas.org/irp/doddir/army/fmi6-02-70.pdf, Accessed on 27 June 2017.

U.S. Joint Chiefs of Staff. *Joint Publication 3-13.1: Electronic Warfare*, 2007. https://fas.org/irp/doddir/dod/jp3-13-1.pdf, Accessed on 29 June 2017.

U.S. Joint Chiefs of Staff. *Joint Publication 3-12R: Cyber Operations*, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf, Accessed on 29 June 2017.

U.S. Joint Chiefs of Staff. *Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations*, 2012. http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf, Accessed on 30 June 2017

Wilson, C. "High Altitude Electromagnetic Pulse (HEMP) and High-Power Microwave (HPM) Devices: Threat Assessments". *CRS Report for Congress*, 2008. 1–16. https://www.wired.com/images_blogs/dangerroom/files/Ebomb.pdf, Accessed on 29 June 2017.