Research Report

BRUCE W. BENNETT, KANG CHOI, GREGORY S. JONES, DU-HYEOGN CHA, JIYOUNG PARK, SCOTT W. HAROLD, MYONG-HYUN GO, YUN KANG

Characterizing the Risks of North Korean Chemical and Biological Weapons, Electromagnetic Pulse, and Cyber Threats

RAND CORPORATION

THE ASAN INSTITUTE for POLICY STUDIES

Characterizing the Risks of North Korean Chemical and Biological Weapons, Electromagnetic Pulse, and Cyber Threats

BRUCE W. BENNETT, KANG CHOI, GREGORY S. JONES, DU-HYEOGN CHA, JIYOUNG PARK, SCOTT W. HAROLD, MYONG-HYUN GO, YUN KANG

Sponsored by the Asan Institute

RAND NATIONAL SECURITY RESEARCH DIVISION

THE ASAN INSTITUTE for POLICY STUDIES

For more information on this publication, visit **www.rand.org/t/RRA2026-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.
© 2022 RAND Corporation
RAND® is a registered trademark.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-0981-2

Cover: Rick Penn-Kraus (design); Gwengoat/Getty Images/iStockphoto (map); amphotora/Getty Images (test tube); FedotovAnatoly/Getty Images/iStockphoto (gas mask); Kesu01/Getty Images/iStockphoto (explosion); weerapatkiatdumrong/Getty Images/iStockphoto (hacking).

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

About This Report

In this report, we describe a combined research effort from the RAND Corporation and the Asan Institute for Policy Studies focused on the North Korean chemical and biological weapon, electromagnetic pulse, and cyber threats. It is a follow-on to a report on the North Korean nuclear weapon threat issued in 2021.[1] Because North Korea denies most information on its capabilities in these areas, we estimate the North's apparent capabilities based only upon open information. We note that these capabilities serve the key North Korean objectives. We describe how these capabilities might be employed to serve the North Korean objectives, and the impacts that employment might have. We then propose actions that the Republic of Korea (ROK) and the United States can take to deter and, if necessary, counter these uses. As such, we intend to provide policymakers, including national-level military and civilian leadership, with possible courses of action to counter these North Korean threats along with open information they can use to explain their policy choices to the general population. In addition, we intend to provide information on these North Korean threats to general civil society stakeholders and influencers.

RAND National Security Research Division

This research was sponsored by the Asan Institute for Policy Studies and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Asan Institute Collaboration

The Asan Institute is an independent, nonpartisan ROK think tank dedicated to undertaking policy-relevant research to foster domestic, regional, and international environments conducive to peace and stability on the Korean Peninsula. RAND and Asan analysts have collaborated on many conferences and other Korean security activities over the years.

Chapters 2–6 of this report were each initially drafted by one RAND analyst and one Asan analyst.

---

[1] Bruce W. Bennett, Kang Choi, Myong-Hyun Go, Bruce E. Bechtol, Jr., Jiyoung Park, Bruce Klingner, and Du-Hyeogn Cha, *Countering the Risks of North Korean Nuclear Weapons*, Santa Monica, Calif.: RAND Corporation, PE-A1015-1, 2021.

Acknowledgments

We appreciate the formal substantive reviews performed by Jan Osburg of RAND and Bruce Bechtol of Angelo State University. We also appreciate comments from Christian Curriden (RAND), Ryu Jae-seung (ROK Army), Yoo Seong Ok (former president, Institute for National Security Strategy), Cheon Myeong Guk (active-duty officer assigned to the Korea Institute for Defense Analyses), Lee Sang Min (active-duty officer assigned to the Korea Institute for Defense Analyses), Jang Gyu Hyun (research professor at the Korea University School of Cybersecurity), Park Ki Cheol (ROK Army), Jang Yoon Jung (ROK Army), and Kim Jin Sun (ROK Army).

Summary

In 2021, the RAND Corporation and the Asan Institute produced a report on "Countering the Risks of North Korean Nuclear Weapons."[1] Nuclear weapons are but one type of weapon of mass destruction (WMD). The other types are chemical, biological, and electromagnetic pulse (EMP) weapons, referred to herein as other WMD (OWMD). This report is a follow-on joint effort that characterizes the North Korean OWMD and cyber threats.

Issue

The North Korean regime perceived decades ago that it needed to field powerful military weapons to secure the survival of the regime and to position it to dominate the Republic of Korea (ROK, or South Korea) and impose unification on the ROK. Initially denied access to nuclear weapons by the Soviet Union, North Korea pursued chemical and biological weapons. More recently, it has also pursued EMP and cyber capabilities. But in the last two decades, North Korea has acquired significant nuclear weapon capabilities, as described in our 2021 report.

Despite fielding many nuclear weapons, North Korea retains OWMD capabilities and is actively using its cyber capabilities. How does the North use these weapons to affect the peacetime and prepare for a major war with the ROK that could differ significantly from a conflict with just conventional weapons that is normally expected? We have sought to describe these activities based on open literature, while recognizing the serious uncertainties in each of these areas because of North Korean information denial. We also propose options that the ROK-U.S. could take to defend themselves against these weapons. We ultimately hope that stronger ROK-U.S. defenses will help deter North Korean aggression.

Approach

This report compiles information on North Korean OWMD and cyber capabilities from a wide range of open sources. The authors then employ their military expertise, knowledge of North Korea, and the history of North Korean OWMD and cyber usage to identify how these capabilities are and could be used in peacetime and to postulate how they might be used in crises or wartime. The basic theory of deterrence is presented with an explanation of how the ROK-U.S. could use that theory to support deterrence of North Korean attacks. Simple estimates of the potential areas affected by OWMD and the population densities in the ROK were used to estimate potential civilian casualties caused by OWMD employment, while the effects on facilities and equipment were drawn from various sources. The authors then compiled options for countering these threats, adding some innovative proposals of their own.

[1] Bennett et al., 2021.

Key Findings

Our examination of the North Korean OWMD and cyber threats led us to conclude the following:

- North Korea has apparently amassed a substantial inventory of chemical weapons (reportedly 2,500 to 5,000 tons), but an unknown quantity of biological weapons. It likely has sufficient nuclear weapons to execute nuclear EMP attacks, but an unknown capability to execute conventional EMP attacks. North Korea has created a *very active* cyber hacker force, though its ability to penetrate cyber defenses around key ROK-U.S. infrastructure is not known (but they likely have some successes over time).
- North Korea primarily uses its nuclear weapons rather than OWMD for peacetime deterrence, coercion, and influence. North Korea has apparently avoided employment of OWMD except for reportedly testing chemical and biological weapons on people and carrying out some assassinations with chemical weapons. North Korea's peacetime restraint has probably been due to its fear of a retaliation that could jeopardize regime survival.
- North Korea has actively employed its cyber capabilities in peacetime to collect information, steal money, and cause damage (e.g., the Sony Pictures hack).
- North Korean provocations in peacetime have many purposes, but internally, a key purpose is demonstrating North Korean regime empowerment to counteract the regime's many failings. Externally, Kim Jong-un seeks to demonstrate North Korean superiority over the ROK,[2] as well as his claim that North Korea is a peer of the United States.
- North Korea seeks to exercise influence over South Korea as well as the United States through provocations. North Korean peacetime provocations pose a risk of escalation to war, which could include WMD use. And North Korean provocations such as missile and nuclear weapon tests also facilitate the growth in the North Korean WMD threats—something the ROK-U.S. want to prevent.
- North Korea may in the future more aggressively employ its OWMD and cyber capabilities in peacetime, anticipating that its nuclear "shadow" would deter many ROK-U.S. responses.
- In wartime, North Korea would likely employ all of its WMD and cyber capabilities, including nuclear weapons, hoping to win the conflict and avoid suffering regime destruction. These weapons would substantially transform the nature of a major war in Korea and cause immense damage to ROK-U.S. military capabilities and civil society. Failure to adequately prepare for such a conflict could be a disaster for the ROK-U.S.

Recommendations

Based on the available open information, we therefore recommend the following lines of effort:

---

[2] Kim Yo-jong, the North Korean leader's sister, has said: "We will not fire even a single bullet or shell towards South Korea. It is because we do not regard it as a match for our armed forces" (Siladitya Ray, "Kim Jong-Un's Powerful Sister Threatens Nuclear Elimination of South Korea's Military After Pre-Emptive Strike Warning," *Forbes*, April 5, 2022).

- **Countering limited OWMD/cyberattacks.** To deter any North Korean limited employment of OWMD and cyber capabilities, the ROK-U.S. need to enhance their ability to detect and attribute North Korean attacks. North Korea needs to understand that even limited WMD attacks would constitute an act of war and be hard to distinguish from precursor attacks before a major invasion. If the ROK-U.S. judge that a major war is actually starting, they would be fully justified in launching an early conventional counterforce response to eliminate North Korean missiles and nuclear weapons, in an effort to blunt the expected subsequent North Korean main attack that the regime has said it would use to eliminate the ROK military forces in a single strike.[3]
- **Countering major OWMD/cyberattacks.** ROK-U.S. military planning needs to assume that a North Korean invasion of the ROK would include the employment of nuclear weapons, OWMD, and major cyberattacks. They need to develop the strategy and capabilities for such a conflict, including surveillance and warning approaches, counterforce operations, active defenses, passive defenses, recovery and reconstitution, and civil defense. The ROK-U.S. governments and the Combined Forces Command (CFC) may have done these things, but if not, they should. A "strategic deterrence and warfighting group"[4] could recommend the strategy and capabilities needed to enhance deterrence against the North's threats and to defeat it if deterrence fails. The ROK-U.S. CFC should build a war plan consistent with the proposed strategy, and the ROK-U.S. governments should fund the capability enhancements needed to implement the strategy and war plan.
- **Deterring conflict.** The ROK-U.S. should seek to deter all North Korean provocations. This recommendation goes beyond provocations involving OWMD and cyberattacks because of the escalatory nature of any confrontation with North Korea and because the North's perceived "nuclear shadow" may increase North Korean willingness to escalate to OWMD use. The ROK-U.S. need to convey to North Korea the costs it will pay for any provocations. For example, this strategy could respond to the North's ballistic-missile tests that the ROK-U.S. have been allowing with a flood of outside information into the North about ROK society and culture (which Kim Jong-un considers a "vicious cancer"[5]). The ROK-U.S. could also consider publicly revealing Chinese and other violations of the United Nations (UN) Security Council sanctions against North Korea. And they could threaten to interdict and seize North Korean ships carrying cargos such as coal that violate UN Security Council sanctions, disrupting North Korean access to the hard currency that supports its military programs.
- **Counter claims of hostility.** The ROK-U.S. could undermine the Kim family regime's justification for escalation of peninsula confrontations by asserting and demonstrating that the ROK-U.S. are not hostile toward North Korea. This can be done in part by actively

[3] This description draws on Kim Yo-jong's wording in Thomas Maresca, "N. Korea Warns of Nuclear Response to South If Attacked: 'Total Destruction and Ruin,'" United Press International, April 5, 2022.

[4] This would be a group familiar with integrated conventional and nuclear warfighting, probably best practiced last in Europe in the 1980s. They could advise senior ROK-U.S. military leaders on the potential impact of North Korean nuclear weapon, OWMD, and cyber employment and U.S. nuclear weapon responses in a future conflict and assist the responsible authorities in developing appropriate strategies and military plans.

[5] Choe Sang-Hun, "Kim Jong-Un Calls K-Pop a 'Vicious Cancer' in the New Culture War," *New York Times*, June 10, 2021.

rebutting North Korean misinformation on ROK-U.S. hostility. In addition, the ROK-U.S. could take the initiative on negotiations by unilaterally implementing a "carrot and stick" strategy, avoiding North Korea's refusal to negotiate. The ROK-U.S. could propose an initial warm-up offer to the North, including some Pfizer and Moderna coronavirus disease (COVID) vaccines, academic opportunities for young North Koreans, and seeking UN agreement to relax some of the textile-related export sanctions. In exchange, the ROK-U.S. could seek inspection of the reported Kangson uranium enrichment facility and the KN-23 ballistic missile. If North Korea refuses, many North Korean elites would likely be upset by Kim's refusal (one "stick"). A second stick could be the ROK-U.S. tightening the economic sanctions on North Korea by interdicting and seizing North Korean ships involved in illicit ship-to-ship transfers (perhaps putting pressure on China to join in the interdictions).

- **Breaking the negotiation impasse.** North Korea has made it appear to many inside the North and outside that the onus for resolving U.S./North Korean problems is on the United States. By making reasonable and even generous proposals to the North, the United States may be able to break the North's negotiation impasse and shift the onus to the North if it refuses proposed ROK-U.S. agreements.

Contents

About This Report iii
Summary v
Tables xii

Chapter 1. Introduction 1
Methodology 2
North Korean Objectives and the North's Strategy 3
North Korean Use of Asymmetric Means 6
What Must the Republic of Korea and the United States Do to Counter These Threats? 6
Organization of This Report 7
Chapter 2. The North Korean Chemical Weapon Threat 8
Background of North Korean Chemical Weapon Threats 8
Overview of the North Korean Chemical Weapon Capabilities 9
The Types, Effects, and Persistence of North Korean Chemical Weapons 9
Quantity of North Korean Chemical Weapons 11
Chemical Weapon Delivery 12
What Impact Might Chemical Weapon Use Have? 14
Potential North Korean Use of Chemical Weapons 15
How North Korea Might Use Chemical Weapons for Limited Attacks in Peacetime 16
North Korean Chemical Weapons Proliferation 16
How North Korea Might Use Chemical Weapons for Major Attacks and War 17
Potential Republic of Korea and United States Counters to North Korean Chemical Weapons 19
Left of Launch 19
Active Defenses 21
Passive Defenses 22
Consequence Management 23
Retaliation and Cost Imposing 24
Combining Defenses and Retaliation to Achieve Deterrence 25
Chapter 3. North Korean Biological Weapons Threat 26
Background on Biological Weapons 26
North Korean Biological Weapons Threat 27
Anthrax 29
Korean Hemorrhagic Fever 32
Possible North Korean Uses of Biological Weapons 34
Peacetime 34
Wartime 35

Potential Republic of Korea and United States Counters to North Korean Biological Weapons 39
Left of Launch 39
Active Defenses 39
Passive Defenses and Consequence Management 40
Retaliation and Cost Imposing 43
Combining Defenses and Retaliation to Achieve Deterrence 43
Chapter 4. The North Korean Electromagnetic Pulse Threat 45
An Electromagnetic Pulse Overview 45
North Korean Nuclear Forces 46
Potential North Korean Nuclear Electromagnetic Pulse Attacks 47
Nuclear Electromagnetic Pulse Attacks on the Republic of Korea 47
Nuclear Electromagnetic Pulse Attacks on the United States 48
North Korea's Nonnuclear Electromagnetic Pulse Capabilities 50
Potential Republic of Korea and United States Counters to North Korean Electromagnetic Pulse Attacks 51
Chapter 5. The Threat of North Korean Cyber Capabilities 55
Overview of the North Korean Cyber Threat 57
The Character and Quantity of North Korean Cyber 58
What Cyber Capabilities Would North Korea Likely Use? 59
Potential North Korean Uses of Cyber for Strategic Effects in Peacetime 62
How Might North Korea Use Cyber for Coercive and Warfighting Purposes? 63
What Impact Might North Korean Cyberattacks Have? 65
Potential Republic of Korea and United States Responses to North Korean Employment of Cyber 66
Negotiations 66
Defensive Responses 67
Offensive Responses 68
Third-Country Involvement 70
Conclusion 70
Chapter 6. Characterizing and Countering North Korean Combined Weapons of Mass Destruction and Cyber Employment 71
Projecting North Korean Weapons of Mass Destruction and Cyber Employment 72
What Can North Korea Do with Its Other Weapons of Mass Destruction and Cyber Capabilities? 72
Achieving Synergistic Effects 73
Would North Korea Be Willing to Employ Its Other Weapons of Mass Destruction and Cyber Capabilities? 74
North Korean Peacetime Uses of Other Weapons of Mass Destruction and Cyber Capabilities 75
North Korean Uses of Other Weapons of Mass Destruction and Cyber Capabilities in Crisis or Limited Conflict 79

North Korean Uses of Other Weapons of Mass Destruction and Cyber Capabilities in Major War 80
North Korean Preparations for Major War 80
North Korean Execution of a Major War 82
Regime Survival After a North Korean Invasion of the Republic of Korea Is Stopped 84
Seeking to Counter Chinese Intervention 85
Proposed Republic of Korea and United States Responses 85
Peacetime Responses 86
A "Carrot and Stick" Strategy 90
Wartime Responses 91
Conclusions 93

Appendix. Technical Description of Nuclear Electromagnetic Pulse 94
Abbreviations 97
Bibliography 99

Tables

Table 2.1. Likely North Korean Chemical Weapons 10
Table 2.2. Possible Delivery Means for North Korean Chemical Weapons 13
Table 2.3. Possible Effects of Chemical, Biological, and Nuclear Weapons 14
Table 3.1. Characteristics of Some Potential North Korean Biological Weapons 29
Table 3.2. Managing Possible North Korean Biological Warfare Agents 42
Table 4.1. Characteristics, Conditions of Use, and Damage Patterns of Nuclear and Nonnuclear Electromagnetic Pulse Weapons 52
Table 6.1. North Korean Peacetime and Crisis Employment of Other Weapons of Mass Destruction and Cyber Weapons 77

Chapter 1. Introduction

North Korea is transforming its threats in Northeast Asia, seriously pursuing weapons of mass destruction (WMD) and sophisticated cyber capabilities. The biggest transformation is with the developing North Korean nuclear weapon threat, which is substantially changing the security environment, especially on the Korean peninsula. In April 2021, the RAND Corporation and the Asan Institute for Policy Studies released a study on *Countering the Risks of North Korean Nuclear Weapons*" to address this transformation.[1] But North Korea continues to pursue other WMD (OWMD), including chemical and biological weapons (CW and BW) and electromagnetic pulse (EMP) weapons, which also pose a serious threat to regional security. In addition, the North Korean cyber threat has been significantly expanding and actively exploited by the North, imposing large costs in Northeast Asia and beyond.

The Asan Institute therefore asked RAND to cooperate in this follow-on study to examine the North Korean OWMD and cyber threats and how to counter them. The authors of this report describe the nature of these threats, how North Korea will or might use them, and what the Republic of Korea (ROK) and the United States can do to counter these threats. This introduction addresses the methodology used in this report. It then describes the apparent North Korean national objectives that motivate its pursuit of these capabilities. It also considers the roles of WMD and cyber operations in achieving these objectives and the limits the North has applied or might apply to such roles because of ROK-U.S. deterrence and North Korean restraint. It concludes with an outline of the chapters of this report.

While North Korea has generally been careful in using its OWMD capabilities in peacetime, the North Korean nuclear weapon development may reduce that caution, an effect referred to as a "nuclear shadow."[2] That is, North Korea may discount ROK-U.S. threats to retaliate against the North's peacetime aggression because it knows that the ROK-U.S. will seek to avoid escalation that could eventually result in nuclear weapon use. After all, the ROK-U.S. have historically shown considerable caution in retaliating against North Korean provocations, including the North's limited attacks, fearing escalation.[3] An adversary's "nuclear shadow" is perceived to embolden that country to be more aggressive with conventional attacks because that country's threat of nuclear escalation will discourage serious retaliation by a victim.

---

[1] Bennett et al., 2021.

[2] Madison A. Estes, *Prevailing Under the Nuclear Shadow*, Arlington, Va.: Center for Naval Analyses, September 2020.

[3] Tania Branigan and Ewen MacAskill, "North Korea: A Deadly Attack, a Counter-Strike—Now Koreans Hold Their Breath," *The Diplomat*, November 23, 2010.

Methodology

This report is a combined effort of the RAND Corporation and the Asan Institute. Chapters 2 through 6 were each drafted by one RAND expert and one Asan expert. This approach allowed the authors to include key open information from both U.S. and ROK sources. Bruce Bennett of RAND and Kang Choi of Asan took the overall lead, with Dr. Bennett coordinating the effort, integrating the chapters, and preparing this chapter and the front matter.

The authors draw from and summarize their threat assessments and policy analyses experiences in these areas, updating this expertise to the current Korean peninsula circumstances. It draws on the authors' substantial examination of Korean security and WMD. Over decades, the authors have monitored the open literature on the North Korean objectives and its WMD and cyber threats and have developed their own perspectives, based in part on discussions with hundreds of senior U.S. and ROK officials and experts on North Korea; dozens of experts on North Korean WMD and cyber threats; and dozens of officials and experts from China, Japan, and Russia, as well as dozens of senior North Korean escapees. The authors have performed many analyses of North Korea and its WMD and cyber threats;[4] they have also directed dozens of wargames on these subjects and participated in many more dozens.[5] This experience has also allowed them to draw connections between North Korean culture and its WMD efforts,[6] providing a unique perspective on these threats and what can be done about them.

The authors identify how North Korea could plausibly use it WMD and cyber threats. Using their knowledge of military operations in Korea, the authors examined ways that the North's WMD and cyber threats could be used to accomplish North Korean objectives, especially in areas where North Korean conventional capabilities would otherwise be lacking in either

---

[4] In addition to the RAND/Asan 2021 report, see, for example, Bruce W. Bennett and Darren Wheeler, *Chemical Challenge Level Analysis for Special Operations*, Santa Monica, Calif.: RAND Corporation, TR-791, 2010; Bruce W. Bennett, *Preparing for the Possibility of a North Korean Collapse*, Santa Monica, Calif.: RAND Corporation, RR-331-SRF, 2013b, especially Chapter 6; Bruce W. Bennett, *The Challenge of North Korean Biological Weapons*, Santa Monica, Calif.: RAND Corporation, CT-401, 2013a; Cha Du Hyeogn, "Kim Jong Un's Policy Plans in the Revision of the KWP Rules: Continued Goal of Communizing South Korea, Enhancing Political Power, and Internal Solidarity," Asan Institute, August 10, 2021; Choi Kang, Shin Beomchul, and Kang Jae-Kwang, "The Shifting Environment in Northeast Asia and Our Responses," Asan Institute, September 2019; Go Myong-Hyun, "Moon's North Korea Policy: Reengaging North Korea to Regain Strategic Initiative," Asan Institute, June 28, 2017; Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2015; and Brian G. Chow, Gregory S. Jones, Irving Lachow, John Stillion, Dean A. Wilkening, Howell Yee, et al., *Air Force Operations in a Chemical and Biological Environment*, Santa Monica, Calif.: RAND Corporation, DB-189/1-AF, 1998.

[5] Many of these wargames involved U.S. and/or ROK military experts on the different kinds of WMD, pressing them to consider how serious the effects of WMD would be and what could be done to counter those effects.

[6] For example, Kim Il-sung, the grandfather of the current North Korean leader, perceived that he was a special forces officer in his operations against Japan in World War II. He therefore built a military that has the largest cadre of special forces personnel in the world. He recognized that chemical and biological weapons could uniquely empower special forces teams, giving a cultural rationale especially for biological weapons that many current military analysts discount. For example, Kim Il-sung "told the Korean Workers Party that it would be 'effective to produce poison gas and germ weapons for use in combat.'" International Crisis Group, "North Korea's Chemical and Biological Weapons Programs," Asia Report No. 167, Brussels, June 18, 2009, pp. 5–6.

peacetime or wartime operations. Several tools were then used to assess the potential impact of these uses, including online damage assessment procedures and previously prepared simple rules of thumb. For example, some estimates of potential casualties are based on the area that could suffer lethal or casualty-causing exposure from the different types of WMD, given perceived human vulnerability. That area was then applied to the population density around likely targets. Appropriate counters to North Korean WMD use are estimated from the various North Korean capabilities and vulnerabilities and then used to identify and evaluate the means for countering the North Korean capabilities and exploiting the North's vulnerabilities. Some of these counters have been used for decades when various countries recognized their utilities (e.g., air base dispersal), while others are creative and new to this report (e.g., the proposed package of "carrots and sticks" for negotiating with North Korea).

This report uses only open information (which includes information from North Korean escapees) on the North Korean OWMD and cyber threats, as well as on North Korean objectives and strategies. The ROK and U.S. governments likely have better information in these areas. But no one, even Kim Jong-un, has complete information on these subjects and can predict exactly how these threats would be used, especially given the Kim regime's efforts to deny information in these areas. Instead, these areas involve substantial uncertainty. A renowned former RAND scholar, Roberta Wohlstetter, wrote: "We have to accept the fact of uncertainty and learn to live with it. No magic, in code or otherwise, will provide certainty. Our plans must work without it."[7]

The objective of this report is thus to provide the broader national security community with a basic sense of the North Korean OWMD and cyber threats—there are few experts across all four of these threats. How serious could these threats be, and what might the ROK-U.S. do about them, recognizing the uncertainties? Part of this recognition needs to include what can be done to manage the uncertainties. In particular, what can the ROK-U.S. do to deter or moderate North Korean use of its OWMD and cyber threats? Potential options will be discussed in Chapters 2 through 5 for each of these threats and then brought together in Chapter 6 to address the overall OWMD and cyber threats. Ultimately, government leaders need to take whatever further information they have available, either as that information develops or from sensitive sources, for selecting from the options described herein and potentially others to develop the ROK-U.S. government strategies for countering these threats.

North Korean Objectives and the North's Strategy

There is broad agreement that the most important North Korean regime objective is regime survival and sustained control of the North Korean state.[8] Kim Jong-un seems to understand that if his regime does not survive in control of the North, he and his family are unlikely to

[7] Richard Berstein, "Intelligence Has Its Limitations," *New York Times*, January 13, 2010.

[8] In an earlier report, RAND and the Asan Institute described their observations on North Korean objectives and strategy. See Bennett et al., 2021.

survive. Kim has chosen selective brutality and suppression as his key means for achieving this objective.[9] Kim faces internal instability because he has more often failed than succeeded as a national leader and has not been able to provide the food and consumer goods that the North Korean people have needed and wanted. Kim has emphasized his few successes, such as the development of nuclear weapons and his summit meetings with then-President Donald Trump, which have allowed him to claim that he is a powerful and successful leader,[10] and that he has made North Korea a near-peer of the United States.[11] He has also emphasized North Korean self-reliance as a means of demonstrating his accomplishments. Meanwhile, he strives to deny the North Korean people information on the ROK, because he fears that the North Korean people find a free and affluent ROK attractive as an alternative to the North Korean government. For example, Kim Jong-un recently described ROK culture and K-pop in particular as "a 'vicious cancer' corrupting young North Koreans' 'attire, hairstyles, speeches, behaviors.' His state media has warned that if left unchecked, it would make North Korea 'crumble like a damp wall.'"[12] Kim seeks to eliminate such influences because of the threat they pose.[13]

There is less agreement in the community relative to the other North Korean objectives. That said, we find that Kim Jong-il's final instructions to Kim Jong-un, reportedly written in October 2011 (two months before Kim Jong-il's death), provide a clear perspective on the North's other key objectives:

- "We must unify Korea. The unification of the peninsula is the ultimate goal of our family.
- "Unification through war has no meaning. If war were to occur, such an event will set us back several hundred years. Even if we win the war, we would leave nothing for our future generation, therefore you must carry out this wish of the Suryeong and unify the Koreas peacefully.
- "In order to do this, we must kick out the Americans from South Korea and we must overcome China's political and economic interjections in our domestic affairs.

---

[9] Kim appears to realize that brutal suppression of all dissent would affect far too many North Koreans, and thus he selectively imposes his punishments, depending upon the examples, to deflect others from the behaviors he fears. See, for example, Lee Chae Un, "N. Korean Middle School Student Sentenced to 14 Years of Forced Labor for Watching S. Korean Film," *DailyNK*, December 1, 2021.

[10] North Korea's state-run "Korean Central Television (KCTV) typically releases a documentary each year reviewing Kim's previous 12 months of activities and praising him for fixing problems." Colin Zwirko, "Kim Jong Un's Body 'Withered' as He 'Suffered' for the People, State TV Says," *NKNews*, February 1, 2022.

[11] Speaking of its demands for denuclearization negotiations, North Korea has reiterated its "longstanding insistence that it would engage Washington only if it is treated like an equal as a nuclear power." Choe Sang-Hun, "North Korea, Seeking 'Equal Footing,' Rejects Preconditions for U.S. Talks," *New York Times*, March 3, 2018.

[12] Choe, 2021.

[13] Jiro Ishimaru, "Inside N. Korea: Maximum Punishment Under the 'Korean Wave Suppression Act' Is Death . . . Still, K-Pop Is Popular," *Rimjin-Gang*, May 19, 2021.

- "Although China is currently our closest partner nation, it is also a country that we should be most wary of in the future. Historically, China has been the country that has made us the most miserable."[14]

We thus believe that North Korea's other two key objectives are coercing the ROK to accept, without war, unification of the Korean Peninsula under North Korean control and to thwart domination by the United States and China.[15] The North Korean strategy for achieving both of these objectives includes ending the ROK-U.S. alliance and getting the United States to remove its forces from the Korean Peninsula. After the U.S. decoupling, North Korea would likely seek a form of confederation with the ROK in which the North would be able to keep its borders closed as much as possible to ROK influence but could secure ROK funding of North Korean development, arguing that it is as a mutual interest with the ROK.[16] Any broader unification or conquest of the ROK would almost certainly lead to a flood of information from the ROK into North Korea, jeopardizing the North Korean regime. North Korea would likely use its military power as a means for coercing the desired financial support from the ROK. Even today, roughly a plurality of South Koreans view North Korea as being militarily superior to the ROK.[17] If the ROK-U.S. alliance were terminated, the ROK may well desire to placate North Korean demands due to ROK fears of North Korean military superiority. If the ROK were to provide significant funding to the North, Kim could provide for his people, continue building his military capabilities, and appear powerful, thereby probably strengthening the survivability of his regime.

But instability in North Korea could force Kim to change his strategy. If internal threats from parts of the North Korean military that imperil his regime develop, Kim Jong-un could execute a "diversionary war," in which he orders the North Korean military to invade the ROK, hoping to avoid it attacking the regime. Kim would be desperate to win such a war.

---

[14] See North Korea Strategic Information Center, "Full Text of Kim Jong-il's Will," translated by Diana Myers, *You Korea News*, November 23, 2012. Some are skeptical of this "will," which came from a single source. But the outside world was lucky to get this copy and is unlikely to get a confirming copy from someone else. The importance of these instructions is reflected in numerous media articles describing them, though these are mainly in Korean. In English, see, for example, Jeong Yong-soo, "Kim Jong-il's Final Orders: Build More Weapons," *JoongAng Ilbo*, January 29, 2013.

[15] Some experts believe that North Korea has abandoned North-controlled unification as an objective because of the view that only through conquest of the ROK could that happen. They believe that the ROK-U.S. alliance can defeat any North Korean invasion. North Korean control of unification is a very difficult proposition. We believe that Kim Jong-un would find an invasion of the ROK a flawed strategy because it would involve a destructive war and because it would open the North to a flood of outside information. Nevertheless, at least as of 2000, North Korean officials described this as their objective. See Joseph S. Bermudez, Jr., "The Democratic People's Republic of Korea and Unconventional Weapons," in Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, eds., *Planning the Unthinkable*, Ithaca, N.Y.: Cornell University Press, 2000, p. 183. By 2021, the Korean Workers Party had changed its rules to reflect its objective of having a more peaceful dominance of the ROK. See Lee Je-hun, "N. Korea No Longer Pursues Unification Through Revolution in S. Korea," *Hankyoreh,* June 1, 2021.

[16] Bruce W. Bennett, *Alternative Paths to Korean Unification*, Santa Monica, Calif.: RAND Corporation, RR-2808-KOF, 2018.

[17] Sang Sin Lee, Tae-un Min, Kwang-il Yoon, Bon-sang Koo, and Peter Gries, "KINU Unification Survey 2020: Press Briefing," Korea Institute of National Unification, June 26, 2020.

In addition, U.S. or Chinese dominance of the peninsula could undercut regime survival. Kim needs to be sufficiently powerful to periodically defy China and the United States.[18]

North Korean Use of Asymmetric Means

Kim Jong-un's interest in WMD is consistent with his father's further reported direction: "The continuous development and procurement of nuclear weapons, long-range ballistic missiles, and chemical and biological weapons is the only way to preserve peace on the Korean Peninsula, and you must take this mission seriously and never lose sight of it."[19] These North Korea WMD capabilities, plus related delivery means and cyber capabilities, have given the North means to achieve some of its objectives in peacetime and perhaps in wartime.

North Korean WMD and cyber capabilities have a wide range of uses in peacetime. The North's primary use of WMD is deterring ROK-U.S. military intervention in the North. But Kim Jong-un also uses these weapons to demonstrate his empowerment, especially for his elites and other North Koreans, but also for outside audiences. The North uses mainly its nuclear weapons for these purposes, though historically the Kim family appears to have used CW and BW for deterrence before it had fielded nuclear weapons. And in the last decade or so, Kim has used his cyber capabilities to collect intelligence and help finance his government, in particular seeking hard currency, which United Nations (UN) and U.S. sanctions have largely denied him.

In wartime, Kim Jong-un probably knows that he would lose if he invaded the ROK with only conventional forces. He has therefore sought asymmetric means—WMD and cyber capabilities—to give him a chance of achieving a victory. He might be able to use these same forces to defeat a ROK-U.S. invasion if he fails to deter such an eventuality, however unlikely that is. But would the United States allow North Korea to use CW, BW, and nuclear weapons (to include EMP attacks) without escalating to a nuclear weapon retaliation? Kim Jong-un may hope so. As discussed in Chapters 2 through 5 and especially Chapter 6, the North's OWMD and cyber threats require the ROK-U.S. to make major enhancements to their deterrence and war planning to avoid or minimize potentially catastrophic effects in a war, regardless of whether North Korea uses nuclear weapons.

What Must the Republic of Korea and the United States Do to Counter These Threats?

The ROK-U.S. do not want to suffer North Korean OWMD and cyberattacks. Several years ago, then–U.S. Army Chief of Staff, General Mark Milley, explained that "'what we want is to deter. Nobody wants to have any of these wars with near peer competitors, high grade powers.

---

[18] See, for example, Andrei Lankov and Peter Ward, "No, You're The Puppet: Why North Korea Isn't a Chinese Satellite," *NKNews*, May 14, 2020.

[19] North Korea Strategic Information Center, 2012.

And the only thing more expensive than deterrence, is actually fighting a war. And the only thing more expensive than fighting a war, is fighting one and losing one.'"[20] The ROK-U.S. need to have sufficient military and related capabilities to convince North Korea that it cannot "win" even a limited war using OWMD and cyber capabilities. It is hoped that having these needed military capabilities will deter North Korea from using its OWMD and cyber capabilities, and that deterrence is what the ROK-U.S. should seek.

Organization of This Report

In the remainder of this report, we examine four different kinds of North Korean asymmetric threats and how these could be applied in combination with the North Korean nuclear threat addressed in our previous report. The North Korean CW threat is examined in Chapter 2. Chapter 3 addresses the North Korean BW threat. Chemical and biological weapons are asymmetric because the ROK-U.S. has renounced these weapons as an active participant in the Chemical Weapons Convention and the Biological and Toxin Weapons Convention. Chapter 4 examines the North Korean EMP threat, which is in part asymmetric because North Korea is nowhere near as vulnerable to EMP as the ROK-U.S. The North Korean cyber threat, presented in Chapter 5, is also significantly asymmetric because of the relatively lower vulnerability of North Korea, which has isolated much of its electronic system and internet. The combination of these threats plus the North Korean nuclear weapon threat are addressed in Chapter 6, which focuses on how North Korea would likely use its WMD and cyber capabilities in peacetime, crises, and major war on the Korean Peninsula.

[20] Office of Senator James M. Inhofe, "ICYMI: Inhofe Requests Honest Assessment from Military Leaders on State of Readiness," press release, September 16, 2016.

Chapter 2. The North Korean Chemical Weapon Threat[1]

"Chemical warfare agents (CWAs) are highly toxic chemicals that have been used in modern military conflicts dating back to the First World War."[2] After widespread use in World War I, the world has seen much more selective use of CW. Nevertheless, the danger of these weapons has motivated all but four countries to renounce them by entering into the Chemical Weapons Convention (CWC) multilateral treaty.[3] Unfortunately, North Korea is one of those four holdouts. While North Korea claims that it does not possess CW, the reality appears to be quite the opposite.

This chapter examines the apparent North Korean CW program, the risks it poses to its neighbors, and the current ROK-U.S. abilities to reduce those risks. The risks of North Korean CW use in a major war appear to be considerable. Unfortunately, the ROK-U.S. do not appear to be adequately prepared to counter or deter such North Korean CW use. In this chapter, we examine CW use without linkage to the use of other WMD. In Chapter 6, we consider in more detail how North Korea would likely employ CW and what the ROK-U.S. can do to counter it.

Background of North Korean Chemical Weapon Threats

North Korea turned to developing CW soon after the Korean War. "In 1954 the Soviet Union and China transferred certain special technologies as well as chemical agents and means of protection against them captured from the Japanese and Kuomintang during World War II to the Korean People's Army [KPA]. . . . In 1964 the DPRK [Democratic People's Republic of Korea] concluded a contract with Japan for deliveries of agricultural chemicals. Under their guise, components came into the country initially for synthesis of tabun and mustard gas, and later chlorine and phosphorus-containing organic compounds were imported."[4] "In 1961, Kim Il-sung issued a 'declaration for chemicalisation' that was aimed at developing an independent chemical industry, with dual civilian and military use."[5]

---

[1] This chapter was prepared by Bruce Bennett and Choi Kang.

[2] Steven Pike, "What Are the Most Common Types of Chemical Warfare Agent (CWA)?" Luton, UK: Argon, 2019.

[3] The other three countries are Egypt, Israel, and South Sudan. See Paul F. Walker, "Presentation to the 22nd CWC Conference of States Parties," the 22nd CWC Conference of States Parties, Organization for the Prohibition of Chemical Weapons, November 27, 2017.

[4] Federation of American Scientists, "North Korea: Chemical Weapons Program," Washington, D.C.: 1998.

[5] International Crisis Group, 2009, p. 5.

Still, it was not until roughly 1980 that North Korea began major shifts that favored chemical warfare.[6] During the 1960s and 1970s, much of North Korea's focus in its military development program was on conventional forces, and in particular the fielding of armored ground forces. But in the early 1980s, many of the armored vehicles that North Korea produced were no longer armored personnel carriers, but rather self-propelled artillery, suitable for the delivery of CW. In November 1980, Kim Il-sung told the Korean Workers Party that it would be "effective to produce poison gas and germ weapons for use in combat."[7] By the late 1980s, the North Korean CW production capability had matured, allowing the North to produce large quantities of diverse CW and delivery systems.[8]

Overview of the North Korean Chemical Weapon Capabilities

This section provides a basic description of the CWA that North Korea produces, the likely quantities of North Korean CWA, and the systems that would be used to deliver those CWA.

The Types, Effects, and Persistence of North Korean Chemical Weapons

There are five types of CWA usually referred to in the community: (1) choking agents that disrupt breathing, (2) blood agents that block blood cells from using oxygen, (3) blister agents that cause severe irritation to the skin and other body parts, (4) nerve agents that block nerve impulse transmission, and (5) riot control agents that affect the eyes and other body parts. This chapter does not examine riot control agents, which are normally intended to temporarily incapacitate rather than cause more serious injuries or kill people.

Table 2.1 identifies some of the CWA from each of the other four types as agents that are commonly associated with North Korea.[9] The defense community provides a two-character code for each of these, which is also given. The usual form of the CWA relates to how it would be used in warfare, delivered as a gas or as a liquid. Of course, all liquids eventually evaporate, and sarin in particular would evaporate about as rapidly as water, such that it would cause much of its effects as a gas. But VX is like oil and would produce very little gas, thereby remaining primarily a liquid contact threat for a protracted period. Chemicals such as VX can also absorb

---

[6] Andrew Scobell and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles*, Carlisle, Penn.: Strategic Studies Institute, U.S. Army War College, April 2007, p.103.

[7] International Crisis Group, 2009, pp. 5–6.

[8] Federation of American Scientists, 1998.

[9] Not included in Table 2.1 are various other chemical agents such as lewisite (L) and tabun (GA), which North Korea likely possesses but which have received less attention. See Anthony H. Cordesman and Aaron Lin, *The Changing Military Balance in the Koreas and Northeast Asia*, Washington, D.C.: Center for Strategic and International Studies, March 25, 2015, pp. 216–217.

Table 2.1. Likely North Korean Chemical Weapons

Chemical	Type	Usual Form	Lethal Doses (LD) and Casualty-Causing Doses (ED)[a]			
			Skin LD_{50}	Skin ED_{50}	Inhaled LCT_{50}	Inhaled ECT_{50}
Chlorine (CL)	Choking	Gas	—	—	13,500 mg-min/m^3	1,300 mg-min/m^3
Phosgene (CG)	Choking	Gas	—	—	1,500 mg-min/m^3	250 mg-min/m^3
Cyanide (AC)	Blood	Gas	—	—	2,860 mg-min/m^3	1,100 mg-min/m^3
Mustard (HD)	Blister	Liquid	1,400 mg	600 mg	1,000 mg-min/m^3	25 mg-min/m^3
Sarin (GB)	Nerve	Liquid/gas	1,700 mg	1,000 mg	35 mg-min/m^3	25 mg-min/m^3
Soman (GD)	Nerve	Liquid	350 mg	200 mg	35 mg-min/m^3	25 mg-min/m^3
VX	Nerve	Liquid	5 mg	2 mg	15 mg-min/m^3	10 mg-min/m^3

SOURCES: U.S. Army, *Potential Military Chemical/Biological Agents and Compounds*, UFM 3-11.9, January 2005; for chlorine plus ECT_{50} for Phosgene, Cyanide, and mustard, see Sean M. Oxford, Lucas A. LaViolet, Kristen A. Bishop, Julia K. Burr, Carl A. Curling, Lusine Danakian, Deena S. Disraelly, Brian A. Haugh, Margaret C. Hebner, Audrey C. Kelley, Royce R. Kneece, Preston J. Lee, Christina M. Patterson, Daniel K. Rosenfield, Hans C. Sitarz, Robert S. Sneddon, Terri J. Walsh, Mike O. Wheeler, and Robert A. Zirkle, *Technical Reference Manual to Allied Medical Publication 7.5 (AMedP-7.5) NATO Planning Guide for the Estimation of CBRN Casualties*, Alexandria, Va.: Institute for Defense Analyses, October 2016.

[a] Lethal and effective (injury-causing) doses are given for a roughly 70 kg (154 pound) man.

into many surfaces such as concrete, asphalt, and soil.[10] The chemical can then "off-gas" slowly, creating a potentially protracted low-level threat that may gradually cause casualties to those who operate in affected areas.

According to a North Korean escapee, North Korea does possess VX, as the North demonstrated in its February 2017 assassination of Kim Jong-un's older half-brother, Kim Jong-nam.[11] According to that escapee, North Korea also acquired the procedures for producing binary VX from Russia. Binary weapons create a CW such as VX from two generally less toxic chemicals that combine to make the CW just before it is delivered. They are thus safer to work with and can maintain potency longer.

The final four columns of Table 2.1 characterize the toxicity of these agents in either liquid or gas form in terms of

- the median lethal dose (LD) of the chemical liquid on the skin at which roughly 50 percent of unprotected personnel would be expected to die
- the median effective dose (ED) of the chemical liquid on the skin at which roughly 50 percent of unprotected personnel would be expected to suffer severe injury
- the median inhaled lethal concentration (LCT) of the chemical gas at which roughly 50 percent of unprotected personnel would be expected to die
- the median effective concentration (ECT) of the chemical gas at which roughly 50 percent of unprotected personnel would be expected to suffer severe injury.

[10] Environmental Protection Agency, *Persistence of Chemical Warfare Agent VX on Building Material Surfaces*," EPA/600/S-19/074, Washington, D.C., 2019.

[11] Colin Dwyer, "Banned Nerve Agent Killed Kim Jong Nam Within 20 Minutes, Malaysia Says," NPR, February 26, 2017.

The concentrations include a time factor. For example, a median lethal dose of sarin could involve exposure to 35 mg/m^3 for one minute or 7 mg/m^3 for five minutes. Thus, CW gases that go indoors and remain there can be lethal at much lower concentrations because of the expected continued exposures over time.

The actual toxicity of CW varies around the values shown in Table 2.1 and are affected by temperature and humidity, as well as the weight and other characteristics of the victim. With a chemical such as VX that penetrates through the skin, the effect varies by the area of the body affected. Thus, British human testing designed to achieve a 70-percent reduction in erythrocyte cholinesterase activity (a serious but less than lethal level) determined that this effect was achieved by 5.1 μg/kg (0.35 mg for a 70 kg man) applied to the cheek but 132 μg/kg (9.2 mg for a 70 kg man) applied to the palm of the hand.[12]

The authors have found no evidence that North Korea possesses the Novichok family of nerve agents that Russian agents used in Britain in 2018 in attempting to assassinate a former Russian spy. But we have also not found any evidence that eliminates this possibility. The Novichok nerve agents appear to be very persistent and more lethal than VX.[13]

The very small amount of these CWA required for lethal and casualty effects is notable. For example, LD_{50} of VX being 5 mg suggests that a kilogram of VX would be sufficient to kill or seriously injure 200,000 or so people. But that level of effects would require equal distribution of just the right amount of VX to each of those people. In practice, the delivery of VX or other CWA by artillery, special forces, aircraft, or missiles would see most of this lethality lost.

Quantity of North Korean Chemical Weapons

"In May 1996 ROK Foreign Minister Yu Chong-ha reported to the National Assembly that it was estimated that North Korea possessed approximately 5,000 tons of biological and chemical weapons. Given the extensive production facilities, this later estimate may constitute the low end of the actual stockpile."[14] It is therefore interesting that more than two decades later, the ROK *2018 Defense White Paper* says: "North Korea began producing chemical weapons in the 1980s and currently holds a stockpile of an estimated 2,500–5,000T of chemical weapons."[15] The ROK Defense Ministry has been including in its White Papers the same estimate of the North Korean

---

[12] Timothy C. Marrs, Robert L. Maynard, and Frederick Sidell, eds; *Chemical Warfare Agents. Toxicology and Treatment*, 2nd ed., Chichester, UK: John Wiley and Sons, 2007, p. 233. This difference explains why the women who attacked Kim Jong-nam in the airport in Malaysia in 2017 were able to apply VX to their hands, rub it on his cheeks, and then go wash their hands to remove the VX. They survived, but he died.

[13] "Some variants of Novichok are thought to be five to eight times more toxic than the VX nerve agent." "Navalny 'Poisoned': What Are Novichok Agents and What Do They Do?" BBC, September 2, 2020.

[14] Federation of American Scientists, 1998.

[15] Republic of Korea, Ministry of National Defense, *2018 Defense White Paper*, 2018, p. 34.

CW stockpile since 2000,[16] and many other sources, including the U.S. Army, have given a similar estimate over time.[17]

The consistency of these estimates over time is suspicious, especially because it is reported that North Korea "is capable of producing 4,500 tons of chemical weapons a year in peace-time and 12,000 tons in war."[18] Did North Korea build a large CW production capacity and then decide not to use that production capacity or perhaps convert it to civilian production of chemicals? We do not know, but if these production capacities are anywhere close to being accurate, the North Korean CW inventory may be greater than 5,000 tons. But the transfer is also possible: One senior North Korean escapee said that the North Korean military industry personnel opposed production of new CW, fearing leaks and possible spills.[19] At the very least, North Korea may have upgraded its CW over time. As of 1995, "North Korea is estimated to have up to 5,000 tons of chemical weapons, most of which is sarin (GB) gas . . . and only a limited stock of other types of chemical weapons, such as those that have suffocating and blood-affecting properties."[20]

In contrast, a senior North Korean military escapee said that he was told in roughly 2012 that North Korea had 2,000 tons of CW. He also said that CW weaponized in artillery shells and rockets is essentially all stored in the forward area and not arrayed as a defense in depth: Kim Jong-un was so terrorized by CW that he refused to allow weaponized CW to be stored within artillery range of Pyongyang.[21]

It is also quite possible that North Korea has imported other CW. According to one prominent North Korean escapee, North Korea checked with many parts of the former Soviet Union for Soviet CW that those countries would be willing to sell in the aftermath of the Cold War. They were successful in acquiring several thousand tons of former Soviet CW, 90 percent of which were nerve agents and 90 percent was also weaponized in 240 mm multiple rocket launcher (MRL) rockets (and these were mostly filled with VX) and a few Scud warheads.[22]

Chemical Weapon Delivery

North Korea has diverse means of CW delivery. "The KPA possesses artillery, multiple rocket launchers, mortars, aerial bombs, and missiles capable of distributing chemical weapons."[23]

---

[16] Speaking of chemical weapons, the 2000 ROK Defense White Paper says: "Their quantity is estimated to be somewhere between 2,500 and 5,000 tons." Republic of Korea, Ministry of National Defense, *2000 Defense White Paper*, 2000, p. 58.

[17] U.S. Department of the Army, 2020, pp. 1-11 and G-3.

[18] "South Says North Korea Has 1,000 Tons of Chemical Weapons," Yonhap News Agency, Seoul, March 21, 1995.

[19] Interview with a North Korean escapee, May 2017.

[20] "South Estimates DPRK Has 5,000 Tons of Chemical Weapons, Mostly Sarin," *Seoul Shinmun*, April 15, 1995, p. 1.

[21] Interview with a North Korean escapee, May 2017.

[22] Interviews with a North Korean escapee, November 2016 and May 2017.

[23] U.S. Department of the Army, 2020, p. G-3.

North Korea could also use drones for CW delivery.[24] Based in part on the killing of Kim Jong-nam, the elder half-brother of Kim Jong-un, we believe that North Korea can also deliver CW for assassinations.[25] If the statement about North Korea acquiring rockets filled with VX is true, North Korean multiple rocket launchers could become a source of very serious and persistent CW contamination.

We have found no information that describes the amount of CW that could be delivered by each of these means. But it is important to make such estimates so that we have an idea of the quantity of CW that potentially must be dealt with. It is expected that North Korean artillery (including multiple rocket launchers) would likely be the key means for CW delivery, but ballistic missiles are also a reported major means of CW delivery.[26] If North Korea has about 3,000 tons of CW (which is toward the lower end of the 2,500 to 5,000 range cited above), we postulate that the distribution of North Korean CW delivery would be *roughly* as shown in Table 2.2. The large quantity of CW dedicated to artillery would also be supported by the report that North Korea imported several thousand tons of nerve agent artillery rockets. We assume that several hundred North Korean theater ballistic missiles carrying roughly 300 kgs of CW each would also be used for CW delivery.[27] We further assume that a similar amount of CW would be reserved for drone and perhaps aircraft delivery. We postulate that about 10 percent or so of the CW could be held in bulk storage and be available to fill more delivery systems as needed. Note that these numbers are very approximate; rough guesses to provide a context for counters to CW later in this chapter.

Table 2.2. Possible Delivery Means for North Korean Chemical Weapons

Delivery Means	Postulated Quantity	Postulated Rounds[a]
Artillery shells, rockets	2,400 tons	800,000 shells and rockets
Ballistic missiles	150 tons	500 warheads
Aircraft, drones, special operations forces (SOF)	150 tons	?
Bulk agent	300 tons	Refills for any of the above

[a]The numbers here postulate that the average North Korean artillery shell and rocket warhead is about 3 kg of chemical weapons and that the average ballistic missile carries 300 kg of chemical weapons.

[24] U.S. Department of the Army, 2020, p. 8-9.

[25] In 2012, a North Korean assassin attempted to use a "poison pen" for an assassination, though it is not clear whether it carried a chemical weapon or a biological toxin. See Paula Hancocks and K.J. Kwon, "'Poison' Pen Mightier Than Sword for Would-Be North Korean Assassin," CNN, November 26, 2012.

[26] U.S. Department of the Army, 2020 pp. 1-11, 1-14.

[27] The 3 kgs of a CW per artillery shell is an average derived from "Chemical Weapons: New Information Analysed," *Jane's Defence Weekly*, February 27, 1988, p. 370. The 300 kgs of sarin per Scud warhead is derived from Lord Lyell**,** "Chemical and Biological Weapons: The Poor Man's Bomb," Brussels: Committees of the North Atlantic Assembly, October 4, 1996.

Finally, because the ROK has a vast array of chemical industries, it is also possible that North Korea could attack ROK storage or production of toxic industrial chemicals and create a release or spill that would cause serious health effects in the ROK. Done covertly, such an attack might not have the escalatory effect that a North Korean CW attack would have.

What Impact Might Chemical Weapon Use Have?

CW can have five kinds of effects: (1) killing or injuring people; (2) causing psychological reactions such as panic and psychosomatic reactions; (3) causing the loss of personnel who would be providing medical care and other support to the casualties; (4) denying operations and activities from areas that might be contaminated; (5) forcing personnel and especially military personnel into protective clothing, which will degrade their activities.

Table 2.3 provides estimates of the relative ability of chemical, biological, and nuclear weapons to kill people. Because chemical and biological weapons are carried by wind, the nature of atmospheric conditions matters, but that is far less true for airburst nuclear weapons, and thus there is a single-column estimate for them. The area affected in Table 2.3 is the amount of a city in which lethal effects would dominate. The indicated nuclear and biological weapons would affect larger areas and thus cause more fatalities than a ton of sarin, though sarin would be quite deadly on a clear, calm night. Of course, delivering 1,000 kgs of the nerve agent sarin sounds like a very large amount. But a single 240 mm multiple rocket launcher battery could deliver that much sarin, and the North has dozens of such batteries that could deliver rockets into Seoul.[28]

Table 2.3. Possible Effects of Chemical, Biological, and Nuclear Weapons

Nuclear, Biological, or Chemical Weapons	Area Affected, Potential Fatalities[a]		
	Clear, Sunny Day	Overcast Day	Clear, Calm Night
Nuclear air burst (12.5 kt, blast effects)		7.8 km^2, 125,000	
Biological (10 kg of anthrax)	4.6 km^2, 75,000	14 km^2, 220,000	30 km^2, 480,000
Chemical (1,000 kg of sarin)	0.74 km^2, 11,000	0.8 km^2, 13,000	7.8 km^2, 125,000

SOURCE: U.S. Congress, Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks*, Washington, D.C., August 1993, pp. 53–54.

[a] The original table in the cited source assumed a moderate wind on an overcast day or night, and an average population density of 3,000 to 10,000 people living in each square kilometer of a city. These fatalities estimates are adjusted to reflect the average Seoul population density being much greater: 16,000 people per km^2. For chemical and biological weapons, the fatalities would be for untreated people.

[28] Bennett, 2018, p. 92.

CW can have severe psychological impacts. With nerve agents, part of the problem is that psychological trauma can in some ways resemble CW effects. For example, in the 1995 sarin attack on the Tokyo subway, 54 people were critically injured, 980 suffered mild exposure symptoms, and more than 5,500 visited hospitals in the area with presumed chemical symptoms. In short, those apparent "worried-well" persons outnumbered the actual casualties by a factor of about 4.5.[29] The threat of chemical exposure can also lead to mass evacuation of the potential area of exposure.

When large numbers of people are affected by CW, many who are otherwise healthy are forced to divert their attention to the care and support of those affected. Thus, a large number of people were required to assist and treat the 5,500 people who went to the hospital as the result of the Tokyo subway attack.

The affected areas described in Table 2.3 would be the areas that would largely be denied immediately after an attack. The sarin threat would then dissipate, whereas a comparable VX attack could deny utilization of such areas to unprotected people for weeks.

Finally, forcing personnel into protective clothing against CW would reduce their ability to perform most functions. Many of the examinations of these degradations were done with older protective equipment in the 1980s,[30] and so it is difficult to estimate how seriously the current generation of protective clothing would affect operations. But the degradations can be expected to be fairly significant (some individual tasks even had more than 100-percent degradation in the time required to carry out a task, with more performance losses expected in coordinated combat).[31] Moreover, even to perform functions such as eating, soldiers would need to be moved out of contaminated areas, thereby reducing military presence in those areas.

Potential North Korean Use of Chemical Weapons

This section suggests various ways that North Korea could use CW. The North has already used CW for assassinations, as discussed above, and has reportedly tested CW on North Korean prisoners to determine the lethality of the various CWA.[32] But otherwise we have found no record of North Korean CW use and no documentation of North Korean tactics for CW use. Nevertheless, the U.S. Army argues that "it is likely the KPA will not hesitate to use chemical weapons in both offensive and defensive operations."[33] This is probably true because North

---

[29] Amy E. Smithson, "Rethinking the Lessons of Tokyo," in Leslie-Anne Levy and Amy Smithson, eds., *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Washington, D.C.: Stimson, October 9, 2000.

[30] See, for example, Henry L. Taylor and Jesse Orlansky, "The Effects of Wearing Protective Chemical Warfare Combat Clothing on Human Performance," Alexandria, Va.: Institute for Defense Analyses, August 1991.

[31] Taylor and Orlansky, 1991, p. B-3. The old protective equipment caused far more heat buildup, though it also caused degradations in, for example, hearing, seeing, and overall situational awareness.

[32] Scobell and Sanford, 2007.

[33] U.S. Department of the Army, 2020, p. G-1.

Korea considers CW to be conventional weapons, not WMD,[34] and thus as being less likely to cause a U.S. nuclear response.

Given the previous discussion of North Korean CW assassination efforts, this section examines limited CW attack possibilities that North Korea might consider beyond assassinations, as well as CW attacks as part of major North Korean warfare.

How North Korea Might Use Chemical Weapons for Limited Attacks in Peacetime

Historically, North Korea has carried out a significant number of limited attacks on the ROK, though none except for a few assassinations involving CW. The ROK *2020 Defense White Paper* identifies 1,118 North Korean provocations, not counting infiltrations, since the 1950s.[35] North Korea carried out limited attacks on the ROK especially in the 1960s to try to destabilize the ROK government and stimulate opposition to that government, including three attempts to assassinate the ROK president (in 1968, 1974, and 1983). When those efforts proved unsuccessful, North Korea transitioned to selected attacks apparently intended to demonstrate North Korean empowerment to its internal audience.

The North has probably avoided limited attacks in recent years for three reasons. First, as ROK conventional capabilities grew, the North has been decreasingly able to claim success in its limited attacks. Suffering a defeat would be bad for the North's internal politics and stability. Second, North Korea learned in 2010 that attributable attacks on the ROK (such as the shelling of Yeonpyeong Island) drive the ROK closer to the United States, which is the opposite of the political outcome that North Korea wants. Third, the North worries about the potential for escalation that could endanger North Korean regime survival. These developments apparently led to the North reducing and then largely stopping its limited attacks after 2010. Instead, it has focused on missile test provocations, which are prohibited by UN Security Council Resolutions. Historically, the ROK-U.S. could have treated any sizable, attributable North Korean use of CW as a major act of war, requiring a response akin to that required by the 1941 attack on Pearl Harbor, which would place the regime in jeopardy. As will be discussed more in Chapter 6, we therefore postulate that North Korea is unlikely to use CW for limited attacks.

North Korean Chemical Weapons Proliferation

North Korea has been a proliferator of CW and reportedly continues to be. "Since the 1990s there have been repeated reports that the DPRK has provided chemical weapons, agents or technology to Egypt, Iran, Libya and Syria. Most of these reports center around the sales of

[34] Former-U.S. Forces Korea commander General Leon LaPorte said, "They don't view using chemical weapons as weapons of mass destruction. They see it as part of their normal doctrine." "Nuclear Nightmare—Understanding North Korea," Discovery Channel, August 6, 2003. This view was also expressed by a North Korean escapee who was a former senior elite, interviewed in May 2017.

[35] Republic of Korea, Ministry of National Defense, *2020 Defense White Paper*, 2020, p. 393.

defensive equipment, manufacturing technology, assistance in developing chemical warheads for Scud class ballistic missiles and development of chemical warfare production infrastructure."[36] "The North Koreans have proliferated CW programs to Syria and have also brought Syrians to North Korea for training and weapons transfers. . . . Pyongyang is currently helping Syria produce the precursors and is also providing chemical weapons parts to Syria."[37] In 2013, the South Korean media reported: "A diplomatic source last Friday claimed the North has transferred technologies for synthesizing chemical agents and making chemical warheads to Syria since the mid-1990s by dispatching chemical weapons experts there."[38] North Korean has also provided Syria with ballistic missiles and ballistic missile production technology.[39] North Korea's "other key client for both chemical weapons and nuclear collaboration [is] Iran."[40]

How North Korea Might Use Chemical Weapons for Major Attacks and War

For several decades, U.S. commanders in Korea have felt confident that a North Korean invasion of the ROK could be defeated and thus deterred. For example, in 2002, then–Combined Forces Command (CFC) Commander General Schwartz testified: "Although an attack on the ROK would cause many casualties and great destruction, CFC would rapidly defeat North Korean forces."[41] In 2021, the retiring U.S. commander in Korea, General Robert Abrams, testified to Congress that the ROK-U.S. CFC was "fully capable of responding to a crisis and defeating any adversary that threatens the ROK."[42]

This U.S. confidence in victory has been based on ROK-U.S. conventional force superiority over North Korea. But peninsula conditions have been changing. The ROK Army has declined from 560,000 active-duty personnel in 2000 to about 400,000 in 2021 and may fall to roughly 300,000 by 2027.[43] In 2005, the ROK Ministry of National Defense, anticipating this manpower decline, put together Defense Reform Plan 2020 to provide a technology versus manpower trade-off to balance these reductions from 2006 through 2020. But the ROK government underspent

---

[36] Joseph S. Bermudez, Jr., **"**North Korea's Chemical Warfare Capabilities," 38 North, October 10, 2013.

[37] Bruce E. Bechtol, Jr., *North Korean Military Proliferation in the Middle East and Africa*, Lexington: University Press of Kentucky, 2018, pp. 107–110, 113–114.

[38] "N. Korea 'Exporting Chemical Weapons Parts to Syria'" *Chosun Ilbo*, June 17, 2013.

[39] Bechtol, 2018.

[40] "Interview: Syria, Iran Main Buyers of North Korean Chemical Weapons," Radio Free Asia, October 3, 2013.

[41] General Thomas A. Schwartz, "Statement of the Commander in Chief United Nations Command/Combined Forces Command & Commander, United States Forces Korea Before the 107th Congress, Senate Armed Services Committee," Washington, D.C., March 5, 2002, p. 10.

[42] Robert B. Abrams, "Statement of General Robert B. Abrams," Washington, D.C.: House Armed Services Committee, March 10, 2021, p. 13.

[43] Bennett, Bruce W., "South Korea: Capable Now, Questions for the Future," in Gary J. Schmitt, ed., *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners*, Carlisle, Penn.: Strategic Studies Institute and U.S. Army War College Press, 2nd ed., October 2020, pp. 269–270.

the planned budget by 100 trillion won (roughly $80 billion) as of 2020, cutting the planned technology improvements by roughly one-third.[44]

This leaves the ROK Army forces in the forward defensive lines increasingly fragile. If North Korea invades the ROK, "The first front would consist of a massive conventional assault across the DMZ [demilitarized zone], using substantial firepower and chemical attacks on selected forward-position targets to isolate Seoul before moving farther south. Additionally, ballistic missile strikes—including missiles with chemical warheads—could hit South Korean and U.S. air bases, ports, and C2 [command and control], communications, computers, intelligence, surveillance, and reconnaissance assets throughout South Korea and in Japan."[45] "In 2005, Gen. Leon LaPorte, former commander of U.S. Forces-Korea, warned that every third round fired from North Korea's vast artillery fields would be a chemical weapon."[46] Nonpersistent CW such as sarin fired against the ROK Army forward forces could cause more ROK casualties than high explosives and scare some soldiers into abandoning their posts, potentially leaving holes in the defenses. Persistent CW fired at avenues of maneuver could block ROK Army efforts to use neighboring ground forces to stop a developing breakthrough. In addition, "The KPA has developed a policy of operational 'first use' of chemical weapons against strategic targets (e.g., airfields, command and control centers, ports, missile batteries) in the ROK."[47] Thus, while the ROK-U.S. have planned to use air forces to prevent North Korean breakthroughs on the ground, North Korean use of CW against ROK combat airfields could impair combat aircraft availability to perform this function.

The ROK-U.S. are also dependent on a major flow of U.S. military forces into the ROK in a time of war. CW attacks on the airfields that support this force flow could reduce the flow, especially as transport aircraft become contaminated with CW. Fearing CW effects, governments outside of Korea may resist the landing of contaminated aircraft on their airfields, thereby also reducing the flow of U.S. forces to Korea. "Operational exclusion is to selectively deny an extraregional force access to or use of forward operating bases or sites within the region. North Korea could attempt operational exclusion by launching nuclear or chemical missiles at existing military bases in Japan, Guam, Alaska, or Hawaii."[48]

North Korea may hope that its emphasis on surprise, rapid ground force advances and the use of mixed forces such as CW could buy it the time to conquer the peninsula. If North Korea adds only CW to its use of high explosives, it is not clear that the North can defeat ROK-U.S. forces and conquer the ROK. The North Korean regime could be destroyed if a North Korean invasion of the ROK fails, a very high risk to the North. Given the priority of North Korean regime survival as an objective, we believe that North Korea is unlikely to take such a risk short of a major internal threat

---

[44] Bennett, 2020, pp. 273–274.

[45] U.S. Department of the Army, 2020, p. 1-14.

[46] Alan W. Dowd, "Capstones: The Korea Conundrum," Indianapolis: Sagamore Institute, October 18, 2017.

[47] Bermudez, 2000, p. 194.

[48] U.S. Department of the Army, 2020, p. 1-22.

to the regime. But the addition of biological and nuclear weapons could shift the outcome to be more favorable for North Korea, though with different risks, as will be discussed in Chapter 6.

Potential Republic of Korea and United States Counters to North Korean Chemical Weapons

The ROK-U.S. can seek to minimize CW effects by destroying the delivery means, preventing their delivery, protecting against the CW, and neutralizing the delivered CW. The ability to perform these functions would contribute to denying North Korea the benefits of CW use and, it is hoped, thereby deter the North Korean use of CW. Deterrence can also be achieved by threatening North Korea with serious retaliation and being able to effectively execute those threats.

This section addresses these options. It describes key means for minimizing CW effects and the likely effectiveness of these means, while recognizing the substantial uncertainties that would be associated with North Korea CW use. It discusses the likelihood that the ROK-U.S. capabilities and declaratory policy in these areas would deter North Korean CW use. These assessments reflect the information available outside of North Korea, without direct contact with the key North Korean decisionmakers. Since we do not even know which North Korean leaders might be involved in deciding to use CW in the future, we conclude that the ROK-U.S. must maintain a strong deterrent against North Korea to hedge against any potential North Korean CW use.

Left of Launch

Most thinking about defeating WMD threats focuses on missile defense. But General John Hyten, formerly the commander of U.S. Strategic Command (STRATCOM), urged a different approach: "So when you look at missile defense and missile defeat, it's important to look at the entire kill chain, and instead of starting from the back end, where Patriot works in a point defense system, it's important to think about how you defeat and defend left of launch first."[49] "Left of launch" means before launch, when the CW warheads, their delivery means, and the leaders who would order their launch are on the ground and targetable. There are two key components of such operations. First, the ROK-U.S. must identify the location of the targets, including some that may be mobile. Second, the ROK-U.S. must be able to strike those targets effectively and in a time-urgent manner to try to prevent their movement and launch.

Locating Targets

Much of the process of locating the targets needs to be done in peacetime. Many North Korean military assets are hidden in underground facilities to prevent knowledge of where they

[49] John Hyten, "Missile Defense and Defeat: A Conversation with the Vice Chairman," in Tom Karako, ed., Washington, D.C.: Center for Strategic and International Studies, February 24, 2021.

are located and of the character and quantity of those weapons. The ROK-U.S. rely heavily on satellites and other overhead reconnaissance to locate the North Korean weapons. But locating targets across all of North Korea with even these capabilities is very hard unless the overhead assets can be focused on likely hiding areas.

A North Korean limited attack, especially if executed as a surprise, may prevent the ROK-U.S. from locating the specific forces used in the attack. Moreover, preemption may not be politically or militarily possible: North Korea could just launch different weapon(s). But against a major North Korean attack, the ROK-U.S. should be able to gain unambiguous warning and prepare to cause major damage to the North Korean attackers after they do their initial launches, if not before if there is the political will for preemption.

The specific targets to be pursued are:

CW and delivery means storage. To maintain control of North Korean CW, the North Korean military apparently tries to store CW away from the delivery systems in a limited number of locations because of Kim Jong-un's fears of CW, as described above. That might mean a dozen or fewer storage facilities (one per base) for ballistic missiles, 50 or so artillery regiments/brigades along the DMZ,[50] and perhaps another dozen locations for bulk storage and other delivery means—perhaps 75 total, a manageable number to find and confirm if the right cueing is available. If, as a North Korean escapee argued, CW is controlled and guarded by North Korean Strategic Force personnel,[51] many former North Korean soldiers may be able to provide information on where those personnel operate. Because the CW warheads/rockets/shells would be heavy, the storage is presumably located close to existing roads.

Dealing with dispersal of CW and delivery means. If North Korean CW storage can be located in peacetime, those locations could be monitored for dispersal in preparation for war, with trucks and transporter erector launchers (TELs) leaving those locations being followed. CW storage locations would probably not be fully evacuated by the start of a conflict, making those targets valuable for some time. When a missile is fired from a TEL, ROK-U.S. aircraft in that area should be able to locate and strike the TEL before it can be moved. Many trucks carrying CW shells and rockets should also be locatable.

North Korean leadership. The North Korean leadership has a history of disappearing when committing major provocations that it apparently feels could cause a ROK-U.S. retaliation.[52] Because Kim Jong-un has used body doubles, it may not be possible to identify with certainty his location in either a limited or a major conflict. Given the probable desire to eliminate both Kim Jong-un and other members of his leadership, the ROK-U.S. need to identify likely regime dispersal facilities, many of which have apparently been identified.[53]

---

[50] Interview with a North Korean escapee, May 2017. We assume that only about half of the artillery brigades /regiments would have chemical weapons.

[51] Interview with a North Korean escapee, May 2017.

[52] See, for example, "Kim Jong Il Vanishes from Public Eye," *Donga Ilbo*, August 7, 2006.

[53] One article identifies 33 "villas" used by Kim Jong-un. See Moon Seong-hwi, "The Location of Kim Jong-un's Villas in North Korea," *Liberty Korea Post*, July 16, 2018.

Destroying Targets Associated with North Korean Chemical Weapons

The ROK-U.S. have a large number of precision munitions that could be used to attack and destroy North Korean underground storage locations and missiles preparing to launch. If ROK-U.S. aircraft and missiles are ready when North Korea begins pulling its CW out of its underground facilities or soon thereafter, the ROK-U.S. should be able to destroy the storage locations before they are fully evacuated. This should be particularly easy with North Korean artillery shells and rockets because it will take days to remove these shells and rockets from their storage locations.[54] The ROK-U.S. may not be able to destroy these targets before some CW have been delivered; thus, active defenses are very important early in any major conflict. But once North Korea uses CW, the ROK-U.S. should be able to destroy much of the remaining North Korean CW, thereby reducing the demand on active defenses thereafter.

More difficult to destroy would be the North Korea leadership dispersal facilities, at least some of which are reportedly hardened and deeply buried.[55] According to the U.S. National Academies, "Many of the more important strategic hard and deeply buried targets are beyond the reach of conventional explosive penetrating weapons and can be held at risk of destruction only with nuclear weapons."[56] The United States is producing a nuclear bomb of modest yield that penetrates into the ground to cause enhanced ground shock coupling, achieving effects comparable to ground bursts that have 15 to 25 times as much nuclear yield.[57] These weapons should be able to destroy leadership facilities while causing far less fallout than has been historically expected from counter-leadership nuclear attacks.

Active Defenses

Active defenses seek to destroy the weapons or people delivering CW (and other weapons) that are en route to their targets. The ROK-U.S. have deployed a variety of missile defenses in the ROK that should be able to destroy many of the incoming North Korean ballistic missiles carrying CW. Because of their limited range, the biggest challenge with missile defenses is having enough batteries to cover all key targets. Missile defenses such as the Patriot system could also destroy incoming North Korean aircraft and drones and perhaps even cruise missiles.

---

[54] Motoko Rich, "In North Korea, 'Surgical Strike' Could Spin into 'Worst Kind of Fighting,'" *New York Times*, July 5, 2017.

[55] See, for example, Moon Sung-hwi, "North Korea Moves Its Wartime Command Center to Nampo Taesan," *Liberty Korea Post*, July 7, 2018.

[56] National Research Council of the National Academies, *Effects of Nuclear Earth-Penetrator and Other Weapons*, Washington, D.C.: National Academies Press, 2005, p. 1.

[57] National Research Council of the National Academies, 2005, p. 2. The new B61-12 tactical nuclear bomb reportedly has a yield of up to 50 kilotons, and yet if it penetrates roughly 3 meters into the ground before detonating, "the maximum destructive potential of the B61-12 against underground targets is equivalent to the capability of a surface-burst weapon with a yield of 750 kt to 1,250 kt." Hans M. Kristensen and Matthew McKinzie, "Video Shows Earth-Penetrating Capability of B61-12 Nuclear Bomb," Washington, D.C.: Federation of American Scientists, January 14, 2016.

Active defense against artillery is more difficult because of the large volume of artillery that would be fired. The ROK-U.S. have been working on several alternative defenses against artillery shells and rockets. One option is a variant of the Israeli Iron Dome system, which uses interceptor missiles,[58] and another is a laser system.[59] It will be several years before the ROK-U.S. will field any significant quantity of these defenses. If, as reported, North Korean artillery fire could amount to 300,000 rounds in the first hour of a major conflict,[60] none of the proposed systems would be able to intercept more than a small number of this total. Still, that limited number might be sufficient to protect a few, small targets as long as North Korea does not know what is being protected (so the North cannot fire enough extra rounds at those locations to saturate the defenses). These defenses also may become sufficient to deal with limited attacks.

In addition, active defense can be aided by directed energy (DE) weapons, including high-energy lasers and high-power microwave devices, which use a beam of concentrated electromagnetic energy or atomic/subatomic particles to disable missiles and artillery shells. Although this technology is still considered nascent, the U.S. has begun fielding DE weapons systems, and if successfully improved and employed, they can complement the current active defenses in the next few years.[61]

Passive Defenses

Passive defenses are designed to protect people and resources from the effects of delivered CW. Passive defenses focus on individual and collective protection, but also involve preemptive contamination avoidance.

Individual protection involves masks, suits, gloves, and boots that keep CW away from a person's body. Individual protection can also include expedient medical treatments such as atropine, which is designed to counter CW effects in persons who are exposed to nerve agents. These protections can keep personnel alive and able to operate, though at a seriously degraded level of military performance, because the protections reduce the ability of personnel to see, hear, and engage adversaries and otherwise perform military functions.[62] But these degradations are usually considered preferable to the casualties and deaths that would otherwise occur as the result of CW exposure. The other key downsides of individual protection are the psychological effects of wearing this restrictive clothing and the risks associated with periodically removing

---

[58] Stephen M. Lepore and Alastair Talbot, "'If We Can't Defend Guam It's Really Hard to Project Power into the Pacific': US Builds Iron Dome on America's Closest Military Base to China," *Daily Mail*, November 9, 2021.

[59] Alessandra Giovanzanti, Mark Cazalet, Dae Young Kim, and George Papangelopoulos, "South Korea's ADD Develops Laser-Power Enhancing Technology," *Janes*, May 25, 2021.

[60] Rich, 2017.

[61] Joint Publication 3-13.1, *Electronic Warfare*, Washington, D.C.: Joint Chiefs of Staff, February 8, 2012; Army Rapid Capabilities and Critical Technologies Office, "Army Directed Energy Strategy," August 20, 2021.

[62] The U.S. government did a series of experiments examining military performance by personnel wearing an older generation of protective clothing. See Taylor and Orlansky, 1991.

individual protection for to eat, sleep, and perform other bodily functions, which leave personnel vulnerable for a period of time. Passive defenses also include CW detection devices that determine what areas are contaminated and where it is safe to temporarily remove individual protection equipment. Once removed, masks can often be decontaminated, but suits may need to be replaced if they have become contaminated. A key challenge is having enough individual protection for such replacements over weeks of conflict.

Collective protection involves creating buildings and other facilities with overpressure inside to keep CW out and filters that prevent chemical contamination from coming in. Unfortunately, the ROK and U.S. governments have decided not to invest in such protections for most military and government facilities in Korea, and it is difficult to create much more than small-scale expedient collective protection against CW. When entering areas with collective protection, personnel need to be examined for any contamination on them, and any contamination needs to either be decontaminated or the contaminated surface needs to be removed from the individual before he or she enters the area having collective protection.

For air and other forces based at fixed facilities, a key aspect of passive defense against WMD and conventional attacks involves the ability to disperse assets to make it more difficult for North Korea to destroy ROK-U.S. military forces. For example, during the Cold War, the United States and the Soviet Union had dispersal airfields for many of their primary airfields. This approach would be particularly important in the ROK because of the limited number of combat airfields.[63] While there are often smaller airfields that fighter aircraft could use, it is not clear that logistical supplies, security, and maintenance have been distributed to these facilities and whether personnel have been trained in peacetime to operate from these dispersal airfields; trying to do such dispersal in wartime without peacetime preparation could allow military assets concentrated on the few fixed bases to be targeted and destroyed before dispersal could be completed.

Consequence Management

There are various consequence management functions that need to be performed against North Korean use of CW. Contamination avoidance is one key function. Decontamination is a second function. A third is medical treatment of the chemical casualties.

Avoiding chemically contaminated areas or protecting personnel who must go into these areas requires the detection and marking of these areas. Detecting CW at an airfield after a chemical attack can be tricky because asphalt, concrete, and other surfaces can absorb CW, making detection difficult. But detection must nevertheless be done because the gradual "off-gassing" of the chemicals from concrete and asphalt could harm unprotected personnel

[63] Because the ROK was not expecting a serious North Korean threat against its airfields, the ROK Air Force has been abandoning almost a dozen highway landing strips it used to operate as dispersal airfields. The ROK should consider building dispersal runways by widening some of the roads it is building. During the Cold War, Sweden's "BAS 90" was one of the most impressive plans for creating such dispersal airfields. See Garrett Reim, "How Sweden's Austere Basing System Influenced the Gripen," *Flight Global*, July 15, 2020.

over time, especially during periods of rain when the CW can be pushed to the surface. One way to do this is to place chemical detection paper or tape in some form of a grid around the airfield before any CW attacks and then check where the paper/tape is contaminated after a CW attack.

To the extent possible, chemical contamination needs to be decontaminated. This is most critical with people who may have been exposed to CW before the CW cause casualties to those exposed. Solutions that can perform this function and also deal with contamination on surfaces such as unpainted metal and glass have been developed. Decontamination can also be performed on personal protection equipment such as masks and to some extent protective suits, thereby allowing this equipment to be reused.

As Table 2.1 suggests, many people exposed to CW may suffer injury but not death. Those injured will require medical care. And many of those who think they may have been injured will also demand some kind of care. Thus, in the aftermath of the sarin attack on the Tokyo subway stations in 1995, some 1,000 medical injuries were treated, as noted earlier, but roughly 4,500 more people were apparently "worried-well" and consumed some degree of hospital capacity.[64] The burden of handling CW casualties in this case was serious even though only 13 people were killed by this attack.[65]

Retaliation and Cost Imposing

As noted in Chapter 1, deterrence is usually achieved by some combination of actions to deny adversary benefits from an attack and actions to impose costs in retaliation for the attack. The U.S. *2018 Nuclear Posture Review* describes the U.S. cost-imposing approach to North Korean nuclear weapon use as not letting the North Korean regime survive.[66] That threat seems to have a deterrent effect on North Korea: The North Korean leaders appear to not value much beyond their own survival and continued control of North Korea.

Thus, even against North Korean CW use, the threat of some form of retaliation against the North Korean regime and military leaders appears to be an appropriate cost-imposing strategy. Because they have renounced CW, the ROK-U.S. cannot use CW (a symmetric means of retaliation), and ROK-U.S. defense policy appears to make no specific military threat to deter CW use. (What happens to North Korea if it uses CW that would not happen if it uses only conventional weapons?) The North Korean regime should probably be told that limited CW use is illogical: It risks regime survival. A U.S. retaliation against even limited CW use could target the North Korean regime and might include U.S. nuclear weapon use.[67] Moreover, any

---

[64] Smithson, 2000.

[65] "Tokyo Sarin Attack: Japan Executes Last Aum Shinrikyo Members on Death Row," BBC, July 26, 2018.

[66] U.S. Department of Defense, *2018 Nuclear Posture Review Report*, February 2018, p. 33.

[67] The 2010 U.S. Nuclear Posture Review said: "After the United States gave up its own chemical and biological weapons (CBW) pursuant to international treaties (while some states continue to possess or pursue them), it reserved the right to employ nuclear weapons to deter CBW attack on the United States and its allies and partners." U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010, pp. vii–viii.

ROK-U.S. retaliation could cause serious escalation to major warfare and the destruction of the regime. And if a conflict does escalate from limited warfare, it would also deny North Korea the advantages of surprise, a major strategy component of North Korean war planning.[68]

In a major war, North Korea could use a substantial quantity of CW. In retaliating against that CW use, the ROK-U.S. could still threaten regime survival, which could include nuclear weapon use. In addition, deterrence would probably be increased by focusing the retaliation against CW use on the destruction of the North Korean Strategic Force leadership, many of whom are unlikely to be as seriously protected as the regime. The ROK-U.S. could establish and publish a chain of responsibility for North Koreans involved in CW use, starting with the commander of the firing battery, then going to the battalion and the brigade commanders and on to the Strategic Force commander and his staff. In addition, the North Korean general staff and regime leadership would also be appropriate targets. The North Korean regime and its subordinates need to be told that they could be targeted in retaliation for even a limited CW attack. Threats to strike these leaders might convince some commanders not to order CW use, even if they are directed to do so. In part, this could be accompanied by ROK-U.S. psychological operations in peacetime to explain that when the ROK-U.S. win a conflict started by North Korea, any commanders who supported WMD use would be tried for war crimes.

Combining Defenses and Retaliation to Achieve Deterrence

None of the individual responses described above will be sufficient to prevent or neutralize the effect of North Korean CW attacks. But each element of the defenses reduces the ability of North Korean CW to overwhelm the other elements of defense. And General Hyten's observation quoted above makes it clear that early actions "left of launch" are key to limiting the effects of North Korean CW attacks. Eight years ago, that led the ROK to adopt a "proactive deterrence strategy, which will include preemptive strikes. Before the National Assembly on March 6, Jung Seung-jo, chairman of the joint chiefs of staff, made clear that preemptive strikes on the North's nuclear facilities are a matter of exercising the right of self-defense and Seoul does not require Washington's consent to make them."[69] The ROK-U.S. need to establish the thresholds of North Korean actions at which they would execute "left of launch" attacks, if they have not already done so.

Otherwise, the ROK-U.S. do not appear to be adequately prepared to counter the damage that would be done by North Korean CW use in a major war started by the North. The ROK-U.S. need to reevaluate the North Korean CW threat and prepare more serious capabilities to counter it. Nor do they currently have declaratory policy against such CW use that would impose unacceptable costs on the North Korean regime. The ROK-U.S. need to correct these shortfalls or face the prospects of massive North Korean CW use.

---

[68] U.S. Department of the Army, 2020, p. 1-13.

[69] Ser Myo-ja, "Park Tells Military to Strike Back If Attacked," *JoongAng Ilbo*, April 2, 2013.

Chapter 3. North Korean Biological Weapons Threat[1]

Biological warfare agents (BWA) are either organisms or poisonous substances produced by living organisms (i.e., toxins). The organisms of concern are generally bacteria and viruses. The main attraction of biological agents is their high potency—on the order of 10^2 to 10^8 times more potent than nerve agents, which are the most potent CWA. In many cases, this high potency is the result of the biological organism replicating once it is in the body.[2]

The chapter examines the potential North Korean BW threats, the risks they pose, and the actions the ROK-U.S. are taking to reduce these risks. Unfortunately, North Korea has made major efforts to deny the ROK-U.S. any detailed information about its BW, making this subject very uncertain. Nevertheless, BW has real potential utility for North Korea, and this supports the possibility that the North does indeed pose a BW threat.

Background on Biological Weapons[3]

Most BW would be expected to be dispersed as an aerosol, spread by air movement especially by the wind. BW agents are nonvolatile, so that once they have settled to the ground, they are significantly less hazardous, though movement through such an area can lead to the re-aerosolization of the BW. Most BW agents have little percutaneous effect and generally must be inhaled or ingested to be dangerous, though some penetration into the body can come from BW getting on people's hands and wiped into the eyes. Once in the environment, most BWA quickly dies or is inactivated (although there are a few important exceptions). While many CWA kill in minutes, biological toxins can take hours to be effective, and biological diseases do not manifest themselves for days or even weeks. The fragility of BWA means that the most likely delivery method is using sprayers either on the ground or attached to drones. Delivery by explosive munitions can destroy much of the agent, though the Soviets planned such delivery.[4]

Many biological agents do not necessarily kill the majority of their victims, who may just be disabled for lengthy periods, depending upon the type of BW agent used. This could be seen as a plus by the attacker since a low level of fatalities might undercut the rationale for a severe retaliatory response such as using nuclear weapons. Biological agents can be either contagious or noncontagious. Contagious agents could have more impact since the disease can spread to

---

[1] This chapter was prepared by Gregory S. Jones and Du Hyeogn Cha.

[2] U.S. Army Medical Research Institute of Infectious Diseases, *USAMRIID's Medical Management of Biological Casualties Handbook*, 9th ed., Frederick, Md.: September 2020.

[3] This section draws upon Lester C. Caudle III, "The Biological Weapon Threat," in Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz, eds., *Medical Aspects of Chemical and Biological Warfare*, Washington, DC: Office of the Army Surgeon General, 1997.

[4] Robert Windrem, "Soviets Planned Smallpox Attack," MSNBC, August 21, 2001.

places far away from where the attack took place. However, there would be a danger of it spreading back to the attacker's troops or even the attacker's country. Noncontagious agents would not have this danger and would keep the impact of the attack focused on the enemy in the area where the BW is released.

North Korean Biological Weapons Threat

Given the difficulty of obtaining intelligence on North Korea's military programs, it is not surprising that there is little hard information on North Korea's BW program. This lack of hard information has led to a wide range of assessments about the dangers of North Korean BW. On the one hand, analysts such as Elisa D. Harris of the Henry L. Stimson Center and John Parachini of the RAND Corporation have argued that there is no unclassified evidence that North Korea has produced and stockpiled BW.[5] Though North Korea has the technology to produce BW, Harris and Parachini argue that many other countries do as well. Parachini has cast doubt on defector reports of North Korean BW testing, saying that "many of these reports are based on indirect or secondhand knowledge, repeat what has appeared in the open press or are evidently inaccurate."[6] Harris goes so far as to call North Korea's BW weapons program "purported."

Current and past ROK-U.S. government sources present a different perspective. Andrew C. Weber, a former assistant secretary of defense for Nuclear Chemical and Biological Defense Programs, has said: "North Korea is far more likely to use biological weapons than nuclear ones."[7] Similarly, the U.S. Department of State has said: "The United States assesses that the Democratic People's Republic of Korea (North Korea) has an offensive BW program. . . . North Korea is assessed to have had BW capabilities since at least the 1960s."[8] In addition, the U.S. Army Surgeon General's report on chemical and biological weapon threats quotes a 1993 Russian Foreign Intelligence Report that says:

> North Korea is performing applied military-biological research in a whole number of universities, medical institutes and specialized research institutes. Work is being performed in these research centers with inducers of malignant anthrax, cholera, bubonic plague and smallpox. Biological weapons are being tested on the island territories belonging to the DPRK (Democratic People's Republic of Korea).[9]

---

[5] Elisa D. Harris, "North Korea and Biological Weapons: Assessing the Evidence," 38 North and Stimson Center, November 2020; John Parachini, "Why We Should Be Skeptical About Recent Reports on North Korea's Biological Weapons Programs," 38 North, January 30, 2019.

[6] John Parachini, "North Korea's CBW Program, How to Contend with Imperfectly Understood Capabilities," *Prism* 7, No. 3, May 2018, pp. 94–95.

[7] Emily Baumgaertner and William J. Broad, "North Korea's Less-Known Military Threat: Biological Weapons," *New York Times*, January 15, 2019.

[8] U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments," Washington, D.C., April 2021, p. 48.

[9] Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz, *Medical Aspects of Chemical and Biological Warfare*, Falls Church, Va.: Office of the Surgeon General (Army), July 1, 1997, pp. 461–462.

In addition, the July 15, 1998, Donald Rumsfeld Commission report declared: "North Korea also possesses biological weapon production and dispensing technology."[10] And the *2020 ROK Defense White Paper* argues that North Korea has a biological weapon program,[11] as does the 2022 *Annual Threat Assessment* by the U.S. Director of National Intelligence.[12]

The fact that North Korea may not have stockpiled BW is not of great significance. Given the short "shelf life" of many agents, stockpiling them would make little sense. This fact, combined with the high potency of biological agents, makes the production of biological agents "on demand" a reasonable option. The Soviet Union planned to produce the bulk of its anthrax weapons by this method,[13] though the Soviets still maintained rather substantial BW stocks for use in a war until production could be ramped up.[14] Nevertheless, an expert on North Korean WMD programs cites several other U.S. government sources to argue that "it would be prudent to assume that the DPRK possesses a stockpile of biological weapons."[15]

South Korean governmental sources have stated on various occasions that North Korea has 14 possible BWA.[16] These agents are anthrax, botulinum toxin, cholera, Korean hemorrhagic fever (KHF), plague, smallpox, typhoid fever, yellow fever, dysentery, brucellosis, staphylococcal enterotoxin B (SEB), tularemia, typhus, and T-2 mycotoxin. North Korea has no need to have dissipated its biological weapons development efforts by developing all 14 agents. Indeed, some of these agents, such as cholera and dysentery, are not going to be very effective in a modern country such as South Korea. Space does not allow us to discuss all 14 agents in detail. Instead, Table 3.1 describes ten of these agents, and in the text we will focus on two, anthrax and KHF. Anthrax is the agent most likely to have been developed as a biological weapon by North Korea, given evidence uncovered in the last several decades. KHF has particular utility in the Korean context because it is endemic to Korea (it occurs naturally), and it is known that North Korea has cultured significant quantities of the virus in order to produce a vaccine.

---

[10] George Melloan, "Bush Reveals His Foreign Policy in the Kim Meeting," *Wall Street Journal*, March 13, 2001.

[11] Republic of Korea, Ministry of National Defense, *2020 Defense White Paper*, 2020, p. 32.

[12] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community,* February 2022.

[13] Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from Inside by the Man Who Ran It*, New York: Random House, New York, 1999a, pp. 88–89.

[14] Alibek, 1999a, p. 112. In a briefing Dr. Alibek gave at the U.S. Air University in 1999, he said that the Soviet Sverdlovsk facility had an annual production capacity of 1,000 tons of anthrax and kept stockpiled 100+ tons. The Soviet Kirov facility had a capacity to produce 200 tons of plague annually and kept 20 tons stockpiled. And the Soviet Zagorsk facility had a production capacity of 100 tons of smallpox annually and kept a stockpile of 20 tons. Kenneth Alibek, *Biological Weapons*, Cambridge, Mass.: Hadron Inc., November 1, 1999b.

[15] Bermudez, 2000.

[16] Hyun-Kyung Kim, Elizabeth Philipp and Hattie Chung, *North Korea's Biological Weapons Program: The Known and Unknown,* Cambridge, Mass.: Belfer Center for Science and International Affairs, October 2017, pp. 5–6. Tularemia is included in Republic of Korea, Ministry of National Defense, *2012 Defense White Paper*, 2012, p. 36.

Table 3.1. Characteristics of Some Potential North Korean Biological Weapons

Biological Weapon	Cases in 2021	Incubation Period	Duration of Illness	Untreated Lethality	Contagious	Aerosol Persistence
Anthrax	0	1–6 days	3–5 days	High	No	High
Botulinum toxin	0	12 h–5 d	1–3 d if lethal, months otherwise	High	No	Moderate
Brucellosis	8	5–60 d	Weeks to months	< 5%	No	Moderate
KHF	260	4–42 days	Weeks to months	5–15%	Rare	Low
Pneumonic Plague	0	1–7 days	1–6 days	High	Moderate	Low
SEB	0	3–12 hours	1–2 weeks[a]	< 1%	No	Low
Smallpox	0	7–17 days	4 weeks	High to moderate	High	Moderate
Q Fever	48	7–41 days	2–14 days	Very low	Rare	High
Ricin	0	18–24 hours	Days	High	No	Low
Tularemia	0	1–21 days	2+ weeks	Moderate	No	Low

SOURCE: U.S. Army Medical Research Institute of Infectious Diseases, *USAMRIID's Medical Management of Biological Casualties Handbook*, 9th ed., September 2020.
[a] There is a debate on how severely SEB affects people. This was the view presented by Bill Patrick, former technical director of the U.S. BW program, in a seminar in 1998.

Anthrax

Anthrax has always been considered a BWA. One property of anthrax that is very advantageous from the attacker's point of view is that it forms hardy endospores that are very resistant to environmental degradation.[17] Whereas most bacteria and viruses will survive outside of a host for only a day to a week, anthrax endospores can survive for decades. This property of endospores means that anthrax can be dispersed much more effectively than most other biological agents and the anthrax threat can persist for a long time. For example, Gruinard Island off the coast of Scotland was used by the British to test possible anthrax weapons in 1942. In the 1980s the island was still contaminated, but a special formaldehyde solution was used to clean the island for human habitation in 1987.[18]

Inhalational anthrax is caused by inhaling anthrax endospores. It is the form of the disease that is of the greatest BW concern and has a very high untreated mortality of almost 100 percent.[19] Anthrax is noncontagious so that the effects would be limited to where the attack took place. Inhalational anthrax has an incubation period of one to six days. Death occurs three to six days after the start of symptoms.

[17] The endospores play no role in the reproduction of the disease organism, but rather allow the bacteria to survive for long periods during adverse conditions. In their natural life cycle, anthrax endospores are usually found in soil.

[18] Kate Aaron, "Operation Dark Harvest—The Story of Scotland's 'Anthrax Island,'" History of Yesterday, August 17, 2021.

[19] Centers for Disease Control and Prevention, "Anthrax," November 20, 2020.

There is a human vaccine for anthrax, but the vaccination schedule requires five shots spread over 18 months, followed by yearly boosters.[20] The large number of required shots limits the number of people who can be vaccinated. The disease can be successfully treated with antibiotics during the incubation period. If vaccination starts at the same time as the antibiotic treatment, then a 42-day course of antibiotics is required.[21] If the vaccine is not available, then a 60-day course of antibiotics is required.

However, without the recognition that exposure to anthrax has taken place, treatment may well be delayed until victims are ill. In this case, even with aggressive treatment including multiple antibiotics, only 55 percent will survive.[22] In the aftermath of the 2001 anthrax attacks, half of the survivors had not returned to work one year later.[23]

Anthrax is one of the few BWA that can have cutaneous effects. If anthrax's persistent endospores enter the skin through a cut or abrasion, cutaneous anthrax can occur. This results in a "malignant pustule" forming at the point of entry. In about 20 percent of the untreated cases, the disease can become systemic and lead to death.[24] Otherwise, the patient will recover. If treated with antibiotics in a timely manner, the mortality is less than 1 percent.

On a weight basis, the inhaled lethal dose of anthrax is about 100,000 times smaller than the lethal dose for the nerve agent sarin. This fact means that effective anthrax attacks would involve the use of far less agent than chemical attacks.

Kim Jong-un's visit to a North Korean biopesticide plant on June 6, 2015, raised serious concerns that anthrax is a North Korean BWA.[25] The biopesticide Kim was examining is Bacillus thuringiensis (Bt). The endospores of this organism can be sprayed over large areas. Bt is lethal to a number of insect pests but is harmless to other animals including humans. The North Korean media published a large number of photos of Kim Jong-un's visit, which show a great deal of the equipment in this facility.

However, Bt is in the same genus as anthrax. The equipment that can produce the Bt endospores can just as easily produce anthrax endospores. The same procedures that "weaponize" the Bt endospores against insects can be used to weaponize anthrax endospores against humans.

---

[20] Centers for Disease Control and Prevention, "Anthrax Vaccination: What Everyone Should Know," undated.

[21] William A. Bower, Jarad Schiffer, Robert L. Atmar, Wendy A. Keitel, Arthur M. Friedlander, Lindy Liu, Yon Yu, David S. Stephens, Conrad P. Quinn, and Katherine Hendricks, "Use of Anthrax Vaccine in the United States: Recommendations of the Advisory Committee on Immunization Practices, 2019," *Morbidity and Mortality Weekly Report*, Vol. 68, No. 4, December 19, 2019, Table 4.

[22] Centers for Disease Control and Prevention, 2020.

[23] Dori B. Reissman, Ellen A. S. Whitney, Thomas H. Taylor, Jr., James A. Hayslett, Peter M. Dull, Ileana Arias, David A. Ashford, Eddy A. Bresnitz, Christina Tan, Nancy Rosenstein, and Bradley A. Perkins, "One-Year Health Assessment of Adult Survivors of Bacillus anthracis Infection," *JAMA*, Vol. 291, No. 16, 2004, pp. 1994–1998.

[24] Centers for Disease Control and Prevention, 2020.

[25] Melissa Hanham, "Kim Jong Un Tours Pesticide Facility Capable of Producing Biological Weapons: A 38 North Special Report," 38 North, July 9, 2015.

Both Iraq and the Soviet Union used the production of Bt as a cover for the production of anthrax.[26]

While Kim Jong-un strolling through this facility without any protective gear demonstrated that the plant was not producing anthrax,[27] this misses the point. Though the parts of the plant shown may not have produced any anthrax in 2015, the plant could start producing anthrax any time Kim Jong-un ordered it to do so.

Further, since North Korea managed to obtain the equipment needed for the Bt production facility, it could have just as easily obtained additional equipment for a separate dedicated anthrax production facility. The Bt facility is concerning because North Korea has no need to produce Bt, since it could easily obtain this biopesticide from China. In addition, the timing of Kim Jong-un's visit, coming only ten days after it had been announced that the U.S. had accidentally sent live anthrax to South Korea,[28] seems to have been intended to send a message regarding North Korea's biological warfare capabilities.

Prior analysis by RAND has shown that the amount of anthrax that North Korea would need to conduct significant attacks is not large.[29] RAND modeled a major outdoor attack on a large urban area involving the release of 75 kg of anthrax slurry (containing around 1–2 kg of anthrax endospores). Taking into account the reduction in exposure to people indoors and that antibiotic treatment would begin once the attack was recognized, about 37,000 people would be killed, another 60,000 would be permanently disabled due to long-term sequelae of the disease, 20,000 would be temporarily disabled, and 1.9 million would require medical treatment for weeks (mainly antibiotic prophylaxis).[30]

RAND also modeled a second attack that involved the release of a small amount of anthrax inside a 50-story office building with 10,000 occupants. Since it would take several days for the attack to be recognized, an additional 4,250 people would enter the building and be affected. Despite the reduction in exposure due to the building's ventilation system filters and antibiotic treatment once the attack was recognized, 2,750 would be killed, another 4,500 permanently disabled, 1,500 would be temporarily disabled, and 5,500 would require medical treatment.[31] Due to the delay in recognizing that an attack had occurred, finding specific evidence that North Korea was behind the attack might be difficult unless the attacker was somehow "caught in the act."

---

[26] Hanham, 2015; and Alibek, 1999a, p. 146.

[27] John Parachini, "Why We Should Be Skeptical About Recent Reports on North Korea's Biological Weapons Programs," 38 North, January 30, 2019.

[28] This announcement occurred on May 27, 2015. See Sara Reardon, "US Military Accidentally Ships Live Anthrax to Labs," *Nature*, May 28, 2015.

[29] Stephen J. Carroll, Tom LaTourrette, Brian G. Chow, Gregory S. Jones, and Craig Martin, *Distribution of Losses from Large Terrorist Attacks Under the Terrorism Risk Insurance Act*, Santa Monica, Calif.: RAND Corporation, MG-427-CTRMP, 2005.

[30] Carroll et al., 2005, p. 21.

[31] Carroll et al., 2005, p. 21.

Long-term contamination of a building would also be a major problem. In the aftermath of the 2001 anthrax mail attacks in the United States, about $250 million was spent decontaminating the Senate office building and postal facilities in New Jersey and Washington, D.C.[32] The American Media Inc. small office building in Florida was abandoned. Note that the total amount of anthrax used in these attacks was on the order of 10 grams.[33]

Korean Hemorrhagic Fever

Of the other 12 biological agents that North Korea might possess, one that might have particular utility in the Korean setting is KHF,[34] a serious form of the disease hemorrhagic fever with renal syndrome (HFRS). It is caused by the Hantaan virus of the genus *Hantavirus* of the family *Bunyaviridae*. Hantaviruses' main reservoir is rodents, in which the viruses cause inapparent, chronic infections. Each hantavirus is maintained in one specific rodent, which in the case of the Hantaan virus is the striped field mouse, found in Eastern Asia. It is believed that when humans and the mice come into close contact, aerosols or fomites contaminated with the urine, saliva, or feces of the mice result in human infections. The disease is not contagious person-to-person.

Cases of HFRS have a long history in East Asia. The disease was encountered by Japanese and Soviet forces during World War II and UN forces during the Korean War. However, neither the Japanese nor Soviet nor U.S. doctors were able to determine the cause of the disease. It was not until 1976 that a South Korean research team lead by Dr. Ho Wang Lee demonstrated that the disease was caused by a virus carried by the striped field mouse.[35] The Hantaan virus was the first Hantavirus to be isolated. In South Korea, approximately 300 to 600 cases occur each year.[36] Since the striped field mouse avoids humans, the disease occurs mainly in rural areas in soldiers and farmers concentrated near the DMZ. In China 12,000 to 20,000 cases are reported each year.[37]

The incubation period of KHF is generally two to three weeks but may vary from four to 42 days.[38] The clinical course of the disease can be mild, moderate, or severe. Treatment of the severe disease requires weeks of extensive hospitalization, including in an intensive care unit.

---

[32] Leonard A. Cole, *The Anthrax Letters*, New York: Skyhorse Publishing, 2009.

[33] Cole, 2009, p. 254.

[34] Much of this section is derived from the fairly comprehensive Centers for Disease Control and Prevention, "Hemorrhagic Fever with Renal Syndrome," January 18, 2017.

[35] Ho Wang Lee and Guido van der Groen, "Hemorrhagic Fever with Renal Syndrome," in J. L. Melnick, ed., *Progress in Medical Virology*, Vol. 36, 1989, pp. 77–79.

[36] Ji Yun Noh, Jaehun Jung, and Jin-Won Song, "Hemorrhagic Fever with Renal Syndrome," *Infection & Chemotherapy*, Vol. 51, No. 4, December 2019, p. 408.

[37] Ji Yun Noh, Jaehun Jung, and Jin-Won Song, 2019, p. 408.

[38] This description of the disease is from Ho Wang Lee and Guido van der Groen, 1989, pp. 77–79.

Since HFRS is a viral disease, antibiotics have no effect on it. No antiviral drugs have been developed to specifically treat HFRS. Treatment is supportive and consists of managing fluids and blood chemistry with intravenous fluids and hemodialysis. The fatality rate of KHF differs according to the patient and period. In the 1960s it was as high as 25 percent for South Korean civilians but now is around 1 percent.[39] However, if hospital resources are not available, the fatality rate could be significantly higher. Recovery from severe cases can take two to three months.

An inactivated virus vaccine has been developed in South Korea by Dr. Ho Wang Lee.[40] It has been marketed as Hantavax in South Korea since 1990.[41] The vaccination regime is three shots at 0 months, 1 month and 13 months. The immunity lasts for at least several years. A similar vaccine is in use in China with approximately 2 million doses being administered each year.[42] Interestingly, Dr. Lee was told by a North Korean colleague that the North Koreans developed a similar vaccine, which by 1989 had already been given to about 30,000 people.[43] There is no vaccine against the hantavirus approved by the Food and Drug Administration (FDA).

The current vaccines in use in South Korea and China provide only modest protection. One source said, "The vaccines elicit suboptimal immune responses, confer inadequate protection and may cause safety concerns."[44] Clearly there is a need for an improved vaccine, but such a development is likely to occur only in China, given the low incidence of the disease elsewhere.[45] This is probably the case for any antiviral treatments as well.

Since aerosols of the virus spread the disease, an aerosol release would be the typical means for carrying out an attack. Experiments with a related hantavirus showed that in a wet environment at room temperature, the virus remained infectious for five days.[46] In addition, there can be rodent-to-rodent spread without any direct contact but rather via contaminated bedding. The bedding remained contagious for up to 15 days. The exact mechanism whereby

---

[39] Ji Yun Noh, Jaehun Jung, and Jin-Won Song, 2019, p. 409.

[40] Ho Wang Lee, C. N. Ahn, J. W. Song, L. J. Baek, T. J. Seo, and S. C. Park, "Field Trial of an Inactivated Vaccine Against Hemorrhagic Fever with Renal Syndrome in Humans," *Archives of Virology*, Supplement 1, 1990, pp. 35–47.

[41] Joon Young Song, Heung Jeong Woo, Hee Jin Cheong, Ji Yun Noh, Luck Ju Baek, and Woo Joo Kim, "Long-Term Immunogenicity and Safety of Inactivated Hantaan Virus Vaccine (Hantavax™) in Healthy Adults," *Vaccine*, Vol. 34, 2016.

[42] Rongrong Liu, Hongwei Ma, Jiayi Shu, Qiang Zhang, Mingwei Han, Ziyu Liu, Xia Jin, Fanglin Zhang, and Xingan Wu, "Vaccines and Therapeutics Against Hantaviruses," *Frontiers in Microbiology*, Vol. 10, January 2020.

[43] Lee et al., 1990, p. 46.

[44] Liu et al., 2020, p. 15.

[45] Connie S. Schmaljohn, "Vaccines for Hantaviruses: Progress and Issues," *Expert Review of Vaccines*, Vol. 11, No. 5, 2012, p. 512.

[46] Eva R. Kallio, Jonas Klingstrom, Elisabeth Gustafsson, Tytti Manni, Antti Vaheri, Heikki Henttonen, Olli Vapalahti, and Ake Lundkvist, "Prolonged Survival of Puumala Hantavirus Outside the Host: Evidence for Indirect Transmission via the Environment," *Journal of General Virology*, Vol. 87, 2006, p. 2131.

the rodents were infected by the contaminated bedding is unknown, but these infections raise the possibility that the virus could be spread to humans by fomites. Therefore, this virus may be a cutaneous threat as well as an inhalational one. The risk of exposure after an attack will persist for at least five days and perhaps up to two weeks.

It is difficult for the United States and South Korea to determine just how effective an attack with KHF would be. There is no "animal model" of this disease, meaning there is no animal that contracts KHF and suffers the same type of illness as humans. Usually, to determine how potent a given BWA preparation such as anthrax endospores are, animals are exposed to the disease. This cannot be done for KHF.

Only with experimentation on humans can the effectiveness of a prospective KHF attack be determined. While this is not an option for South Korea and the United States, it may be for North Korea. A number of defectors have reported that North Korea has conducted tests of biological agents on political prisoners.[47] If North Korea has performed human testing of KHF, it may have gained significant insight into the utility of KHF as a biological weapon. In addition, if China were to develop an improved vaccine and antiviral treatments for KHF and provide them to North Korea, KHF might be a very effective North Korean biological weapon.

Since the KHF vaccine is an inactivated virus preparation, significant quantities of the virus must be produced in a cell culture to create the vaccine. Since North Korea produces a KHF vaccine, it must have the capability to produce the virus. Vaccine production and other protective measures against KHF could be used by North Korea as a cover for the production of KHF weapons.

Possible North Korean Uses of Biological Weapons

How might North Korea use BW, how might it be delivered, and what impact might it have?

Peacetime

In peacetime, it is normally assumed that North Korea has not used biological weapons. Nevertheless, several decades ago a senior ROK officer said that he and colleagues believed that North Korea had done some very limited experimentation with anthrax in the ROK, seeking to determine the ROK ability to detect anthrax and attribute its outbreak.[48] North Korea has apparently not used BW for assassinations in the way that Bulgaria reportedly used ricin for some assassinations in 1978, likely with Soviet assistance.[49] It is normally assumed that North Korea has been careful to avoid such uses because of the possibility of serious

[47] Bennett, 2013a, pp. 2–3.

[48] Discussion with a senior ROK officer in roughly 1998.

[49] Public Broadcasting System, "Secrets of the Dead. Umbrella Assassin: Clues and Evidence," June 3, 2014.

ROK-U.S. escalation in response. In addition, Kim Jong-un has struggled to plant an image of North Korea in the international community as a "normal state"; he may fear that the use of BW could completely thwart such existing efforts.

Nevertheless, if North Korea experiences increasing instability, Kim may be tempted to carry out some local, limited BW attacks, trying to avoid attribution. Such attacks would best be done with diseases that are endemic to the ROK such as typhoid fever (66 cases in 2021) or KHF (252 cases in 2021), as listed by the Korean Disease Control and Prevention Agency.[50] In the ROK but also possibly in Japan and the United States, North Korean agents could

- release very limited amounts of anthrax near U.S. military facilities to sow discord between U.S. and ROK, since it could be portrayed as an "accidental" U.S. release during its "biowarfare experiments"[51]
- release anthrax in a building and cause major economic disruption since workers may then stay away from any related major building.
- infect ROK ground forces near the DMZ with small amounts of KHF or typhoid fever, which may be hard to differentiate from a natural outbreak
- contaminate food with botulinum, which may be hard to differentiate from a natural outbreak
- assassinate an individual with ricin.

These attacks could cause serious panic, with people fearing that BW attacks could recur and seriously disrupt the South Korean economy and society. But North Korea would take a serious risk that its attackers could be caught. Moreover, any BW attack would raise suspicion of North Korean involvement. Repeated attacks would tend to confirm this involvement and potentially leading to serious ROK-U.S. retaliation.

Wartime

In wartime, North Korea may well decide to use BW. But if it does, it must do so understanding that the incubation period of the various kinds of BWA will delay the incapacitating effects of any attack. That incubation delay could induce North Korea to begin some BW attacks before its main attack on the ROK in the hope of achieving at least some incapacitation of ROK personnel early in the North's main attack. But to achieve surprise, the North could carry out only selected BW attacks before its main attack. After the main attack begins, the North would have great incentive to use BW to attack key targets while not worried about giving the ROK-U.S. warning.

---

[50] Korean Disease Control and Prevention Agency, *Public Health Weekly Report: National Notifiable Infectious Diseases,* December 25, 2021.

[51] USFK reportedly carried out 16 BW defense tests with theoretically dead anthrax and one with dead plague from 2009 to 2015. Shin Hyon-hee, "'USFK Conducted 16 Covert Anthrax Tests Since 2009,'" *Korea Herald*, December 17, 2015. Unfortunately, one of the anthrax samples was actually live, opening the United States to future accusations of mistakes with anthrax samples. "Live Anthrax Shipped Accidentally to S Korea and US Labs," BBC, May 28, 2015. The result has been serious subsequent ROK demonstrations, fearing of further U.S. contamination. Jo He-rim, "Fear of Biological Agent Strikes Busan as US Troops Continue Biosurveillance Project," *Korea Herald*, April 16, 2019.

We anticipate that North Korea could employ several kinds of BW attacks:

- Disrupt key military facilities (airfields, ports, and command and control) especially in the ROK but also in Japan, with widespread aerosol releases of anthrax or tularemia.[52] The aerosol could be made into a cocktail using toxins such as SEB[53] and botulinum to achieve a more rapid impact and agents such as Q-fever, KHF, or even brucellosis to achieve a longer-term effect;[54] anthrax would be used on facilities North Korea will not want to use (because of its persistence), while tularemia would be used on facilities it wanted to use
- Interfere with military reinforcement and resupply by contaminating key ROK, Japanese, and U.S. airfields and ports with anthrax (because of its persistence) or exposing critical personnel in those areas to smallpox or plague, with Pusan being a particular target; this could be done by aerosol release or sending in infected persons (North Korean SOF wittingly infected or third parties unwittingly infected, for example by infecting people flying into Pusan on a commercial aircraft)
- Deny the use of logistics and related facilities using aerosol releases of anthrax, especially in the ROK
- Disrupt the advance of ROK-U.S. forces north of the DMZ by contaminating the water supplies in that area with diseases such as cholera and typhoid
- Execute an end of the NK regime retaliation by widely spreading anthrax or contagious agents such as smallpox and pneumonic plague in cities in the ROK, U.S., Japan, or even China by aerosol release or by sending in infected persons as noted above.

Any of these uses could cause as much if not more damage to the ROK-U.S. war effort through psychological effects, including chaos and panic, as through casualties. Panic could come in the form of other countries closing their borders to the ROK to avoid BW spread, and even the United States pausing its flow of forces into Korea to avoid BW spread to its personnel and aircraft. This could keep many U.S. forces from joining the defense of the ROK, disrupt the flow of needed supplies (including food) into the ROK, and prevent U.S. and allied noncombatant evacuation from Korea—all major effects on theater military operations. The use of contagious BW would have particularly serious psychological effects, as in the case of the 1994 plague outbreak in Surat, India, when some 600,000 people fled the city in one night in response to 5,000 reported

[52] If China makes any effort to intervene in the North, its forces could also be targeted while assembling in China.

[53] While the botulinum toxin is deadly, it is a complex protein that quickly degrades in the environment. The U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) argues that SEB is more stable and is lethal only at high doses; some troops might be able to fight despite their symptoms. This is the official U.S. perspective as described in U.S. Army Medical Research Institute of Infectious Diseases, 2020. However, at a seminar in 1998, Bill Patrick, at one point the technical director of the U.S. offensive BW program, argued that most personnel infected with SEB would be incapable of military operations for a week or two. This observation was based on the fairly extensive human subject testing of SEB done as part of the U.S. offensive BW program.

[54] A BW cocktail is a combination of several BW agents that have differing incubation and incapacitating periods. The U.S. offensive BW program developed such a cocktail, which involved SEB, VEE, and Q fever, in the early 1960s for use against Cuba. That cocktail was expected to incapacitate opposing military personnel for up to three weeks or so. See Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War*, New York: Simon & Schuster, 2001, pp. 56–57

plague cases, of which only 167 cases were confirmed.[55] The use of anthrax in particular would lead to many people using antibiotics for prophylaxis to prevent themselves for becoming infected in case they were exposed, and therefore to people hoarding antibiotics in the ROK and making it difficult for others to get antibiotics if they become infected. And that would cause further chaos.

North Korea will worry about causing negative international public opinion due to its use of BW and also worry about the possibility of a massive retaliation by the ROK-U.S. Therefore, the extent and intensity of North Korea's wartime BW use will depend on North Korea's confidence in the performance and effectiveness of its nuclear weapons and causing needed effects against the ROK-U.S. In any case of BW use, North Korea will strongly insist that it was not involved and threaten to respond with nuclear weapons against any retaliation by the ROK-U.S.

Delivery of biological agents by explosive munitions such as artillery or missile warheads would be difficult. BWA tend to be fragile, and the explosive release of the agent would destroy much of the BW.[56] Still, North Korea is reported to have been experimenting with various key parts of BW delivery by ballistic missile.[57] In particular, anthrax spores are resilient and thus more able to survive delivery by missiles or aircraft (probably AN-2s). More BW delivery would be expected by North Korean special forces using aerosol sprayers in the ROK rear areas, something that could also be done by North Korean sleeper agents living in the ROK. North Korea has some 200,000 SOF,[58] some fraction of which could be given BW delivery as their mission. Given the potency of biological agents, North Korean SOF using hand-held sprayers could carry out a major biological attack anywhere in South Korea and even in Japan or the United States (or China). In addition, large BW sprayers could be vehicle-mounted and used. Drones or perhaps even AN-2 aircraft could be used to release BW in specific rear areas of the ROK, especially if the North judges the ROK air defense network to be weaker than expected. In order to protect the BW from the sun's ultra-violet radiation, the BW release would probably occur at night, during stable weather conditions.

Because aerosolized BW would be carried by the wind, the use of BW is not advised near the DMZ, as the wind could shift and persistent BW such as anthrax could also affect North Korean

---

[55] V. Ramalingaswami, "Psychosocial Effects of the 1994 Plague Outbreak in Surat, India," *Military Medicine*, Vol. 166, Supplement 2, December 2001, pp. 29–30.

[56] Nevertheless, the Soviets planned to deliver BW using ICBMs. See Alibek, 1999a, pp. 5–9. And the North Koreans appear to be following the Soviet example. Reports indicate that "North Korea had begun tests to load anthrax onto intercontinental ballistic missiles." John Bacon, "Anthrax Antibodies in Defector Raise Fears North Korea Is Developing Chemical Weapons," *USA Today*, December 27, 2017. Alibek explained: "From the late 1960s, single-warhead missiles for delivering biological weapons were developed and prepared for possible applications. . . . In 1988, the decision was made to use multiple warhead missiles for biological weapons." Jonathan B. Tucker, ed., "Biological Weapons in the Former Soviet Union: An Interview with Dr. Kenneth Alibek," *Nonproliferation Review*, Spring–Summer 1999, p. 3.

[57] Jack Moore, "North Korea Wants to Hit the U.S. with an Anthrax-Tipped Missile: Report," *Newsweek*, December 20, 2017.

[58] Republic of Korea, Ministry of National Defense, *2020 Defense White Paper*, 2020, p. 32.

personnel. The use of CW, with smaller and thus more controlled areas of contamination, might thus be preferred by the North in attacking ROK ground forces at or near the front.

North Korea could carry out BW attacks "several days or weeks in advance of a conventional military attack, to degrade critical U.S./ROK personnel (e.g., pilots, senior officers), overload U.S./ROK medical systems, and spread panic among the civilian population."[59] It would nevertheless want to use care and limit very early attacks in order not to give the ROK-U.S. strategic warning of a North Korean attack. An anthrax attack on rear-area personnel would take a number of days to have an effect because of the incubation period, but if combat were ongoing, such an attack could have a significant impact. Biological detectors might give an alarm of such an attack within a day. Appropriate prophylaxis or early antibiotic treatment could prevent serious disease, but it may be difficult to provide appropriate antibiotics to all of the troops in combat for the two months potentially needed, especially since those exhibiting symptoms should be treated with intravenous antibiotics.[60] Attacks with persistent agents such as anthrax or perhaps even KHF on the port of Busan or on important airbases could seriously disrupt operations and create substantial panic and chaos. They could also cause alliance friction if the United States were to provide antibiotics to its personnel on a base that has suffered a BW attack but not to the ROK contractors on the base or the ROK civilians living around the base.

As was also described above, a large-scale anthrax attack on a major urban area could kill at least tens of thousands.[61] Indeed, since Seoul is more densely populated than the city used in a prior RAND analysis (Chicago), the total dead might approach 100,000. The number of deaths may actually be even higher, as it may be difficult to provide antibiotic prophylaxis to millions of people. North Korea's development of nuclear weapons has decreased the chance that such an attack might occur, but this is only because a nuclear attack could kill even more people.

Because BW is normally delivered by the wind, North Korea may worry that a wind shift or a military advance could lead to North Koreans being infected with BW. Considering the poor health conditions and medical infrastructure in the North, the impact of BW on North Koreans could be much greater. Because North Korea would generally lack sufficient vaccines, treatments, or quarantine equipment, North Koreans faced with BW use might rebel against the regime. ROK-U.S. experts have therefore anticipated that if North Korea is serious about BW use, the North would vaccinate at least the special forces that would carry BW along with those developing BW. It is therefore not surprising that a North Korean defector in 2017 had anthrax antibodies, suggesting that he had been vaccinated against anthrax.[62] And "a secret federal intelligence assessment, completed in 1998 and based on substantial evidence including recently vaccinated North Korean soldiers, concluded that Iraq, North Korea and Russia are likely to be

[59] Bermudez, 2000, p. 197.

[60] U.S. Army Medical Research Institute of Infectious Diseases, 2020, pp. 32–33.

[61] Carroll et al., 2005.

[62] Bacon, 2017.

concealing smallpox virus for military use."[63] Alternatively, the North may reserve BW use for areas south of the Seoul metropolitan area,

Potential Republic of Korea and United States Counters to North Korean Biological Weapons

The ROK-U.S. can seek to minimize BW effects in many of the same ways as they would minimize CW effects. But there are ways in which countering BW would differ from countering CW.

Left of Launch

Little is known about possible biological agent production facilities in North Korea except for the Bt facility visited by Kim Jong-un. As was discussed above, North Korea may not even possess stockpiles of BWA but rather produce the needed agent on-demand. Even if North Korea does have stockpiles of BWA, the amount of material may be less than 100 kg, and the required storage facilities would be small and easily concealed. Without better knowledge, conducting preemptive strikes against these facilities would be difficult.

Delivery of BWA would probably be by ground-based sprayers, aerial platforms such as drones or AN-2 aircraft, or SOF. It is unlikely that the biological agents are mated with their delivery systems in peacetime (for example, because many BWA require refrigeration until the time of actual use). Even if some potential BW weapon delivery systems are preemptively destroyed, the BWA could be delivered to the surviving delivery assets for use.

Active Defenses

The ROK-U.S. have deployed a variety of missile defenses that could be used to intercept the drones or aircraft that could spray BWA. However, intercepting low-flying, low-radar cross-section targets may not be easy.

Once a major war is underway, it may be difficult for North Korean SOF to infiltrate South Korea. At the start of such a war, many SOF units may be sent into South Korea to attack a number of targets with conventional weapons. SOF carrying BW could be mixed in with these other SOF units.

In peacetime, stopping SOF carrying BW will be less demanding, since the defenses against the SOF would need to be only partially effective. Given the possible serious consequences of ROK-U.S. forces killing or capturing North Korean SOF carrying BW, North Korea would probably want a high degree of certainty that an attack would succeed before undertaking such an operation.

---

[63] S. Van McCrary, "Smallpox and Bioterrorism: A Growing Threat," University of Houston, Health, Law, and Policy Institute, August 3, 1999.

Passive Defenses and Consequence Management

Detection

As was discussed above, a BW attack may not cause illness for many days. Therefore, disease surveillance by itself will not detect an attack until many people are already infected, sick, or dead. By then it may be too late to take many prophylactic measures. Being able to detect an attack soon after it has occurred would offer many advantages. The United States has been developing detection systems for the last two decades, including Biowatch, which has been deployed in the United States. However, it could only detect a handful of biological agents, has had an unacceptably high false alarm rate, and has been expensive to operate.

The United States has been testing improved BW detection technologies in South Korea since 2013 as part of Project Joint U.S. Forces in Korea Portal and Integrated Threat Recognition (JUPITR). This effort is designed to protect specific installations rather than provide wide-area surveillance. The project ran into trouble in 2015, when live samples of anthrax were accidentally sent to South Korea instead of inactivated samples. This has led to persistent opposition to the project from South Korean civilians who do not believe it was an accident and that U.S. BW testing is occurring in South Korea.[64] The Chinese media has helped to stoke these fears.[65]

The U.S. Army is testing a new integrated chemical and biological detection system known as Capabilities to Enhance Threat Awareness, Understanding, and Response (CENTAUR). It is expected to be tested each summer at Dugway Proving Ground through 2026.[66] Clearly, whatever technology is finally selected, it will not be deployed operationally until at least 2027.

Individual and Collective Protection

Since most biological agents need to be inhaled to be effective, soldiers would need to don just the mask, not the full mission-oriented protective posture (MOPP) gear, in order to be protected. However, the early detection of an attack, which is required to don the mask in a timely fashion, may not be available, as BW is usually "detect-to-treat," not "detect-to-protect."[67] If reliable real-time detection of biological attack were available, then soldiers would need to wear the masks only during the few hours that the attack was in progress (as the cloud of agent passed over them). Unfortunately, it appears that it will be many years before such a detection capability will be available.

Collective protection involves creating structures with overpressure inside to keep BW out and filters that prevent BW from coming in. However, the ROK and U.S. governments have decided

---

[64] Jo He-rim, 2019.

[65] "From Jupitr to Centaur, Fears over U.S. Military's Biochemical Experiment Grow in South Korea," *Xinhuanet,* July 16, 2020.

[66] Al Vogel, "New Chem/Bio Detector Faces Test for Next Six Years," *U.S. Army*, May 20, 2020.

[67] Michael J. Sailor, "Detect to Protect," *ACS Sensors*, Vol. 5, No. 5, 2020, pp. 1247–1248.

not to invest in such protections for most military and government facilities in Korea. Even if such protected structures were to exist, the long interval (perhaps days) between when a biological attack occurs and when it is detected poses a significant problem. The structure provides protection only if contamination from people entering it can be prevented, but until it is known that an attack has taken place, no decontamination of the entries will take place. As a result, collective protection will have more utility against CW than BW.

Medical Prophylaxis and Treatment

Vaccines are an effective prophylaxis against BW—a means of providing preexposure protection. A number of vaccines are mandatory "for DoD [Department of Defense] personnel (military, civilian & contractors) traveling for any period of time in theater."[68] Of the 14 possible North Korean BWA, vaccinations are required for three: anthrax, smallpox, and typhoid. Vaccines do not exist for many of the other agents, and South Korea's KHF vaccine is not FDA approved. But then, South Korean military forces are not vaccinated against anthrax and smallpox. Some members of the South Korean military who are at high risk of contracting the disease naturally are vaccinated against KHF. Clearly there needs to be some better coordination between U.S. and South Korean military forces as to which vaccines are administered. While it would be preferred that South Korean military forces be vaccinated for anthrax, for example, U.S. military forces should still be vaccinated even if the South Korean forces are not, in order to attempt to deter limited anthrax attacks on U.S. forces and also reduce the potential theater demand for antibiotics if North Korea were to use anthrax. Vaccines for some other BW that may be used under Investigational New Drug (IND) protocols are being developed.

A variety of treatments can be used against BW infections. Antibiotics are useful against all bacterial agents, though some BW is better treated with specific antibiotics. In the last few decades, effective antiviral drugs have been developed against some diseases, but they tend to be disease-specific. The antiviral tecovirimat was FDA approved in 2018 for treatment of smallpox, and two other antivirals may be used against smallpox under IND protocols.[69] Several of the other viral BW can also be treated with ribavirin or other IND protocols.[70] The smallpox vaccine (ACAM2000) is recommended as a treatment within four days of exposure either to prevent the disease or to limit its severity.[71] Toxins cannot be treated with either antibiotics or antivirals and instead require an antitoxin, which is also disease specific. Further, the antitoxin must be administered before the person is serious ill. Given the relatively fast action of the toxins and the limited supplies of antitoxins, successful treatment is rather unlikely.

---

[68] United States Forces Korea, "Force Health Protection (FHP) Requirements for the Korean Theater," Regulation 40-9, February 8, 2018, p. 9.

[69] U.S. Army Medical Research Institute of Infectious Diseases, 2020, p. 80.

[70] U.S. Army Medical Research Institute of Infectious Diseases, 2020, pp. 98–104.

[71] U.S. Army Medical Research Institute of Infectious Diseases, 2020, p. 81.

Table 3.2. Managing Possible North Korean Biological Warfare Agents

Biological Weapon Agent	Contagious Person to Person	Can Be Treated With Antibiotics	Effective Vaccine	USFK Vaccination Required
Anthrax	No	Yes	Yes	Yes
Botulinum toxin	No	No	No	No
Cholera	No	Yes	Yes[a]	No
KHF	No	No	Yes[b]	No
Plague	Yes	Yes	No	No
Smallpox	Yes	No	Yes	Yes
Typhoid fever	No	Yes	Yes	Yes
Yellow fever	No	No	Yes	No
Dysentery	No	No	No	No
Brucellosis	No	Yes	No	No
Staphylococcal Enterotoxin B	No	No	No	No
Tularemia	No	Yes	Yes	No
Typhus	No	Yes	No	No
T-2 mycotoxin	No	No	No	No

SOURCES: Compiled by the authors from Centers for Disease Control and Prevention webpages on each disease and United States Forces Korea, "Force Health Protection (FHP) Requirements for the Korean Peninsula," Regulation 40-9, October 20, 2021.
[a] Protection is short-lived.
[b] This vaccine is not FDA approved

Table 3.2 lists the generally referenced 14 possible North Korean BW agents and whether they are contagious, can be treated by antibiotics, whether there is a vaccine that can prevent the disease, and whether United States Forces Korea (USFK) requires vaccination. It is interesting to note that only two of the 14 are contagious. Seven of the agents can be treated by antibiotics, but for both anthrax and plague the treatment must be started early to be effective. There are vaccines for seven of the agents, but for cholera the protection does not last much beyond three to six months, and the vaccine for KHF is not FDA approved. USFK already vaccinates for three of the four remaining agents. The vaccine for yellow fever is quite effective, and if the threat was seen to be serious, U.S. and South Korean forces could be vaccinated against it as well. Limited quantities of the tularemia vaccine are available under IND protocols. The vaccine's effectiveness does start to decline at high exposure doses but is otherwise effective.

The bottom line is that there are many holes in medical responses if North Korea selects the right BW; thus, it has incentives for pursuing development of multiple BW agents.

But Kim Jong-un needs to recognize that the world has changed. The development of biological synthesis now allows some companies or even individual scientists to be able to produce BW to retaliate against North Korean BW use. They could also acquire drones and sprayers for the delivery of those agents. It may take days to weeks to prepare a response, but in peacetime such a delay in the response would not be problematic. These organizations

would understand the importance of targeting such attacks against the North Korean elites in Pyongyang and especially the government center, which is roughly 1.5 km north-northeast of the Pyongyang train station.

Retaliation and Cost Imposing

Both the ROK and the United States have abandoned the development and stockpiling of BW for military attacks. Thus, they would not have the ability to respond in kind against a North Korean BW attack and would require an asymmetric response. If the North Koreans were to conduct large-scale use of BW during wartime that resulted in a large number of casualties and deaths, then it would not be hard to imagine that nuclear retaliation would be in order—regardless of any prewar U.S. declarations on the use of nuclear weapons. Indeed, the United States could consider a nuclear response to even more limited BW attacks—for example, attacks against U.S. military bases in the ROK or Japan, which could cause thousands of casualties. Providing clear attribution of a BW attack, which North Korea would almost certainly deny, would be key to justifying a nuclear weapon or any other response. The United States could strengthen deterrence of North Korean BW attacks by more clearly threatening the possibility of a nuclear weapon response.[72]

The ROK-U.S. could also threaten conventional weapon responses to North Korean BW use. Because of the large damage that such BW use could cause, such response should seek to cause proportionate, serious damage in North Korea. For example, the attacks could destroy North Korean C2 capabilities (including regime leadership), power-generation capabilities, or transportation links to China that support North Korean trade.

Combining Defenses and Retaliation to Achieve Deterrence

Unlike North Korean use of CW, there do not appear to be many good options to preempt North Korean use of BW "left of launch." Protective measures such as active defenses, individual protection, and medical prophylaxis and treatment have the ability to limit but not eliminate the impacts of a BW attack. A key element will be the ability to detect a biological attack in near real time, which would significantly increase the effectiveness of the protective measures against BW attacks. Unfortunately, such detection capabilities are at least five years away, since only the CENTAUR system offers any hope of providing them.[73]

---

[72] Reportedly, the 2022 U.S. Nuclear Posture Review will not preclude U.S. use of nuclear weapons in response to adversary chemical or biological weapon use, but neither will it provide a serious threat. Michael R. Gordon, "Biden Sticks with Longstanding U.S. Policy on Use of Nuclear Weapons Amid Pressure from Allies," *Wall Street Journal*, March 25, 2022. The threat of a U.S. nuclear response to BW use was clearer in the 2010 U.S. Nuclear Posture Review. U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010, pp. 15–16.

[73] See Vogel, 2020.

For the near term, the ROK-U.S. will need to rely on retaliation to deter North Korean use of BW. This retaliation can range from limited, precise conventional attacks to a full-scale nuclear response, depending on the scale of the North Koran biological attack. The ROK-U.S. need to develop a declaratory policy against such BW use if the threat of retaliation is going to effectively deter North Korea from using such weapons.

Chapter 4. The North Korean Electromagnetic Pulse Threat[1]

This chapter addresses the electromagnetic pulse (EMP) threats potentially available to North Korea. It provides a basic description of EMP and the damage it can cause, which could be very significant.[2] It explains that North Korea likely has sufficient nuclear weapons to commit some of them to EMP attacks. The chapter then describes how North Korea might use nuclear EMP attacks and the impact that such attacks could have. It also describes the possibilities for North Korea having nonnuclear EMP capabilities. It concludes by discussing potential ROK-U.S. options for countering North Korean EMP threats.

An Electromagnetic Pulse Overview

It was expected from the beginning of the nuclear age that nuclear explosions would generate transient electrical fields. However, even for nuclear explosions near the ground, the effects were greater than anticipated. Far stronger and widespread electrical fields can be generated by nuclear explosions detonated above most of the earth's atmosphere, at altitudes of between about 30 km and 500 km. These electrical fields are generated by the interaction of radiation from the nuclear explosion with molecules of air in the upper atmosphere and by the heated plasma of the weapon debris itself. These electrical fields are known as the electromagnetic pulse (EMP). Since it is caused by explosions at high altitude, it is sometimes known as a high-altitude electromagnetic pulse (HEMP). The effects can extend out to the line-of-sight of the explosion, meaning that the EMP can cover very large areas, though with decreasing intensity toward the edges of the field. The electrical fields can be quite powerful and can potentially damage electrical equipment and electronic devices on the ground. For a technical description of EMP, see the Appendix.

It is also possible to generate an EMP by nonnuclear means. The effects of such weapons would be far more localized, but they could potentially generate field strengths even greater than that produced by a nuclear weapon. North Korea has demonstrated its interest in disabling electronics (the key effect of EMP) by repeatedly carrying out Global Positioning System (GPS) jamming attacks on various South Korean targets.[3] Thus, from this example we believe the North would also be interested in electronic disruptions using EMP. A nuclear EMP attack on South Korea would be indiscriminate and could potentially cause damage in North Korea or even

---

[1] This chapter was prepared by Gregory S. Jones and Park Jiyoung.

[2] A particularly useful discussion of EMP can be found in George H. Baker, William A. Radasky, and James L. Gilbert, "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment," National Coordinating Center for Communications (NCC), February 5, 2019.

[3] Aerospace Center for Strategic and International Studies, "Space Threat 2018: North Korea Assessment," April 12, 2018.

China. However, the use of nonnuclear EMP weapons would allow North Korea to conduct far more targeted EMP attacks on South Korea.

On July 9, 1962, the United States conducted the Starfish Prime nuclear test. It involved a 1.4 mt nuclear weapon detonated 400 km above the earth, near Johnston atoll in the middle of the Pacific Ocean. Though Hawaii is about 1,450 km away, the EMP from this test knocked out streetlights and triggered numerous burglar alarms, causing largely transient damage,[4] although it also "damaged or destroyed as many as one third of the satellites in lower earth orbit."[5] Also in 1962, the Soviets tested three 300 kt nuclear devices at altitudes ranging from 59 km to 290 km over what is now Kazakhstan. These tests damaged diesel generators, shut down a long transmission line, and started a fire in an electrical power plant.

During the Cold War, concerns about EMP effects on military systems motivated the United States to harden many such systems against EMP effects. There was not too much concern about EMP effects on civilian systems since in a large-scale nuclear war, it was thought that the direct effects of a nuclear attack would be far more serious. Since the end of the Cold War, there has been more concern about how EMP could affect civilian systems since even a small nuclear power could cause substantial EMP damage by exploding a nuclear weapon over the United States.

North Korean Nuclear Forces

North Korea tested its first nuclear device in 2006. Due to the low yield of this test (1.4 kt) and of the subsequent test in 2009 (5.0 kt), there were some doubts as to whether North Korea had actually mastered nuclear explosive technology.[6] However, three successive tests (one in 2013 and two in 2016) with yields in the 10 to 20 kt range has put an end to such doubts. Similarly, there were some initial doubts as to whether North Korea could produce a weapon that was small and light enough to be carried by a ballistic missile. In comparison, China was able to develop ballistic missile deliverable nuclear warheads by its fourth nuclear test. Given that North Korea has already conducted six nuclear tests, it probably has ballistic missile deliverable nuclear warheads.

Before 2010 it was thought that the size of North Korean's nuclear arsenal would necessarily be limited since the small plutonium production reactor at Yongbyon could produce only enough plutonium for roughly one nuclear weapon per year. However, North Korea's revelation in 2010 that it possessed a centrifuge enrichment plant changed this calculus. Recent estimates of North Korean's nuclear arsenal are much larger. A RAND/Asan study estimated that in 2020

---

[4] Edward Savage, James Gilbert, and William Radasky, "The Early-Time (E1) High Altitude Electromagnetic Pulse (HEMP) and It Impact on the U.S. Power Grid," Goleta, Calif.: Metatech Corporation, Meta-R-320, January 2010, pp. 3-4 to 3-6.

[5] Comprehensive Nuclear-Test-Ban Treaty Organization, "9 July 1962: 'Starfish Prime,' Outer Space," undated.

[6] Dimitri P. Voytan, Thorne Lay, Esteban J. Chaves, and John T. Ohman, "Yield Estimates for the Six North Korean Nuclear Tests from Teleseismic P Wave Modeling and Intercorrelation of P and Pn Recordings," *Journal of Geophysical Research: Solid Earth*," May 23, 2019, p. 4934, Table 7, Column 5.

North Korea had around 70 to 110 nuclear weapons and might have 151 to 242 by 2027.[7] Siegfried Hecker, a professor at Stanford University and former director of Los Alamos Nuclear Laboratory, has produced a lower 2020 estimate of 20 to 60 weapons with a most likely estimate of 45.[8]

Whether North Korea has 45 or 90 nuclear weapons makes little difference when evaluating the likelihood of a North Korean EMP attack. When North Korea had only five or ten nuclear weapons, it might have seemed unlikely that North Korea would devote several of them to conduct EMP attacks. But with the much larger arsenal estimated today and especially for 2027, it is not difficult to imagine that North Korea might devote a small number of nuclear weapons for EMP attacks. Indeed, North Korea might especially design several weapons to have enhanced EMP effects. While some may doubt that North Korea has the scientific expertise to do so, it is entirely possible that North Korea has received the needed scientific advice from Russian scientists.[9]

Potential North Korean Nuclear Electromagnetic Pulse Attacks

In discussing its nuclear weapons, North Korea has noted that they can be used to produce EMP.[10] Nuclear EMP is usually generated from high-altitude (25 km or more) nuclear explosions in the atmosphere. The EMP effects propagate out to the line-of-sight associated with the curvature of the earth. How might North Korea conduct a nuclear EMP attack?

Nuclear Electromagnetic Pulse Attacks on the Republic of Korea

While South Korea could readily be attacked by a North Korean nuclear-armed, medium-range ballistic missile, it would be difficult to devise a nuclear EMP attack that affected South Korea but not North Korea. Indeed, the effects could extend well into China.

Even if a nuclear weapon were to be detonated just 30 km above Busan, the EMP effects would cover almost all of North Korea, though with a lesser intensity.[11] Further, this low-burst altitude would be significantly less than optimal for causing EMP effects in the ROK. If a nuclear weapon were exploded near the optimal altitude for E1 effects of 75 km over Busan, the EMP effects would reach the major Chinese city of Shenyang.[12]

---

[7] Bennett et al., 2021, p. 37.

[8] 38 North, "Estimating North Korea's Nuclear Stockpiles: An Interview with Siegfried Hecker," April 30, 2021.

[9] Interview with a North Korean escapee, December 2017.

[10] Mun Dong Hui, "North Korean Propaganda Promotes EMP Attacks Using Nuclear Weapons," *Daily NK*, November 23, 2018.

[11] The EMP effects extend out to the line-of-sight from the blast. It is easy to calculate that for a burst height of 30 kilometers, this is about 620 kilometers. Pyongyang is about 525 kilometers from Busan.

[12] For a blast at an altitude of 75 kilometers, the line-of-sight is about 970 kilometers. Shenyang is about 885 kilometers from Busan.

Just how serious a problem this would be depends on how rapidly the E1 EMP intensity falls off near the edge of the EMP field. Published diagrams show widely differing EMP intensities near the edge of the field. One diagram indicates that near the edge of the EMP field, the intensity falls to near zero,[13] while another shows the intensity to be 50 percent of the maximum at the field's edge.[14] A further complication is that neither diagram states the yield of the nuclear weapon producing the E1 EMP field nor the absolute magnitude of this field. North Korea may well not be in a position to know which alternative would apply to its possible EMP attacks.

North Korea could explode the weapon farther south, but this would lessen the EMP intensity in South Korea. North Korea could harden some of its systems against EMP and, since it would know when the attack was going to take place, even turn off some systems.[15] Still, there would be EMP damage in North Korea, though North Korea apparently depends on far fewer electronic devices (which could be a benefit if they have work-arounds or a problem if the destruction of their few essential electronic devices leaves them without redundant options). Perhaps North Korea would find this an acceptable trade-off for gaining an edge over South Korea. On the other hand, North Korea might not want to run the risk of causing major damage in China and would forgo attacking South Korea with nuclear weapon–generated EMP.

Nuclear Electromagnetic Pulse Attacks on the United States

Any North Korean EMP attack on the United States would not have the problem of causing damage in North Korea or China. The problem for North Korea is how to deliver it. North Korea has successfully launched two satellites that at various times pass over the United States. The first satellite launched in December 2012, Kwangmyongsong-3 Unit 2, weighed only 100 kg and was thought to be tumbling out of control. The second satellite launched in 2016, Kwangmyongsong-4, weighed 200 kg and is believed to have maintained stable control.[16] Both of those satellites were probably too light to carry a nuclear weapon that the North could build. In addition, their orbits are about 500 km above the earth, which would significantly diminish the EMP field (especially E1 and E3B). However, North Korea's newer ballistic missiles could launch satellites heavy enough to carry a nuclear weapon, and those satellites would maintain a stable orbit for at least a limited time if the orbit were to be as low as 200 km, though even this altitude would be higher than optimal for an EMP attack. The previous two North Korean satellites were launched southward from North Korea. A similar future launch would result in a satellite passing over the United States from the south, thereby evading some U.S. missile detection systems.

---

[13] Savage, Gilbert, and Radasky, 2010, p. 2-4.

[14] John S. Foster, Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry (Hank) M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report," 2004, p. 6.

[15] Electronic systems that are turned off tend not to be vulnerable to EMP damage.

[16] Andrea Shalal and David Bunnstrom, "North Korea Satellite in Stable Orbit but Seen Transmitting: U.S. Sources," Reuters, February 9, 2016.

Three times in 2017, North Korea tested intercontinental ballistic missiles (ICBMs). Twice in July 2017, North Korea tested the Hwasong 14. The tests used a very lofted trajectory, which made it somewhat difficult to determine the missile's maximum range. It was calculated that with a light payload the missile could reach the United States. It is not clear that this missile has sufficient range to reach the United States carrying a nuclear warhead.[17]

In November 2017, North Korean tested the Hwasong-15, followed likely by another Hwasong-15 in March 2022. Both missiles also flew a highly lofted trajectory. Calculations for even the first missile indicate that this missile can probably carry a nuclear warhead to most of the United States,[18] and it could potentially be detonated to cause EMP during the missile's descent. In addition, it has been suggested that North Korea could affect at least part of the United States using an EMP attack where the nuclear warhead is mounted on a short-range ballistic missile or even a balloon, which would be launched by a freighter or submarine located off the U.S. coast.[19]

However, the impact of an EMP attack is highly uncertain. The result of this uncertainty is that evaluations of the EMP threat range from catastrophic to not very serious. The most pessimistic view is that of the U.S. EMP Commission and various articles by its chairman, William R. Graham. More recently these views have been taken up by Peter Pry, the EMP Task Force's executive director. Graham and Pry believe that EMP poses an existential threat to the United States. Pry quotes Henry Cooper, former director of the U.S. Strategic Defense Initiative, who claims that EMP damage could cause life-threatening conditions.[20] Such conditions could result from possible EMP damage to extra-high-voltage transformers that might cause large-scale shutdowns of the electrical grid.

However, it is unclear whether any transformers would be destroyed. The Electric Power Research Institute (EPRI) undertook a three-year study of the threat posed by EMP produced by nuclear weapons.[21] They found that though regional blackouts involving multiple states would be possible, it did not expect widespread transformer damage to occur. William Radasky, a member

---

[17] Theodore A. Postol, Markus Schiller and Robert Schmucker, "North Korea's 'Not Quite' ICBM Can't Hit the Lower 48 States," *Bulletin of the Atomic Scientists*, August 11, 2017.

[18] Michael Elleman, "The New Hwasong 15 ICBM: A Significant Improvement That May Be Ready as Early as 2018," 38 North, November 30, 2017.

[19] William R. Graham, "North Korea Nuclear EMP Attack: An Existential Threat," 38 North, June 2, 2017.

[20] Peter Pry, "North Korea EMP Attack: An Existential Threat Today," *Cipher Brief*, August 22, 2019. Graham (2017) claims that his view of EMP severity is "the consensus view of EMP experts who have advanced degrees in physics and electrical engineering along with several decades of experience in the field—with access to classified data throughout that time—and who have conducted EMP tests on a wide variety of electronic systems, beginning in 1963." Graham also talks about extremely high EMP effects from "super-EMP" warheads, as discussed in the subsequent paragraphs herein.

[21] Electric Power Research Institute, *High Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies,* Palo Alto, Calif.: April 2019.

of the EMP Task Force, and Pry have denounced the EPRI study as "junk science." Their doing so illustrates the wide degree of disagreement over the EMP threat.[22]

Another area of disagreement is the strength of the E1 field that might be generated. The Los Alamos National Laboratory computed some benchmark cases for the EPRI study, which generated a peak E1 field of around 25 kV/m. EPRI doubled this to a maximum of 50 kV/m for some of its cases. Graham and Pry in various writings have raised the possibility that North Korea could have obtained from Russia "super-EMP" weapons that could generate up to 200 kV/m.[23] Such weapons could have yields as low as a few kilotons, and Pry has even suggested that North Korea's first test in 2006 was such a weapon, though this seems unlikely.[24] Moreover, Graham and Pry fail to point out that such a low-yield weapon would not produce a significant E3 field regardless of how strong an E1 field was produced.

This latter point illustrates another problem with the current analyses of the EMP threat. The three components of the EMP threat (E1, E3A, and E3B) tend to be looked at separately, and the analysis often assumes the highest level of the particular threat component. But there is no combination of weapon yield, burst location, and burst height that maximizes all three components. For example, E1 tends to be maximum at locations somewhat south of the point beneath the explosion (for detonations in the Northern Hemisphere), E3B tends to be maximum directly below the burst point, and E3A at its maximum tends to be well north of the point beneath the burst point (for explosions in the Northern Hemisphere). In order for the maximum field for E3A to occur over the United States, the burst must be over Mexico or locations even farther south.

An integrated threat analysis would look at all three EMP components from a single explosion and would try to adjust the weapon yield, burst location, and height to maximize the impact of the EMP attack. One can see why such an effort might be classified, but to get organizations (such as electric utilities) to spend money on various hardening efforts, there needs to be an authoritative government statement on the seriousness of the threat and what the appropriate hardening levels should be.

North Korea's Nonnuclear Electromagnetic Pulse Capabilities

It is also possible to build nonnuclear EMP weapons that are also known as radio-frequency weapons. Russia is thought to be a world leader in such weapons.[25] Despite much speculation on the internet, there is no official open explanation of how such weapons operate or what they look

[22] William A. Radasky and Peter Vincent Pry, "Blackout Warfare: High-altitude Electromagnetic Pulse (HEMP) Attack on the U.S. Electric Power Grid," EMP Task Force on National and Homeland Security, August 6, 2021, p. 1.

[23] Graham, 2017.

[24] Peter Vincent Pry, "North Korea: EMP Threat, North Korea's Capabilities for Electromagnetic Pulse (EMP) Attack," EMP Task Force on National and Homeland Security, June 6, 2021, pp. 3–4.

[25] Peter Pry, "Russia: EMP Threat," EMP Task Force on National and Homeland Security, January 2021.

like. It is unknown if North Korea has developed nonnuclear EMP capabilities, though it could have acquired the technology from Russia. However, given that a nuclear EMP attack on South Korea could cause significant damage in North Korea, North Korea may find nonnuclear EMP weapons preferable for causing EMP effects because their effects have much shorter range and can be focused on specific targets. Further, North Korea has demonstrated its interest in disabling electronics by repeatedly carrying out GPS jamming attacks on various South Korean targets, and it is not unreasonable to assume that it does have some nonnuclear EMP capabilities.[26] Nonnuclear EMP weapons can be customized to produce a variety of frequencies to attack a diverse set of targets.

Nonnuclear EMP weapons may be being developed and deployed by both the United States and Russia. The weapons could be packaged inside of a standard MK84 bomb casing and delivered by aircraft. Or the weapons could be placed inside of a cruise missile, which would be the delivery system. Delivery by multiple rocket launchers would be another option. Drone delivery is also a possibility, though it may not have sufficient payload to produce an effective weapon. Since the EMP field is small, the weapon needs to be delivered accurately. This requirement may rule out some of the older North Korean ballistic missile systems.

Nonnuclear EMP weapons have several advantages when compared with the EMP that would be produced by a high-altitude nuclear burst. As stated above, a high-altitude nuclear burst could cause serious EMP damage in North Korea. But while covering far less area than a nuclear-generated field, the nonnuclear field can actually achieve higher destructive voltages—100 kV/m as opposed to 50 kV/m.[27] Finally, for North Korea to detonate a nuclear weapon even at high altitude runs the risk of being highly escalatory and provoking a U.S. nuclear response. The use of even a large number of nonnuclear EMP weapons would probably not run this risk. For these reasons, North Korean use of nonnuclear EMP weapons could be preferred to its use of a high-altitude nuclear burst. Table 4.1 compares the characteristics and threats of nuclear and nonnuclear EMP weapons.

Potential Republic of Korea and United States Counters to North Korean Electromagnetic Pulse Attacks

EMP protection can be achieved by counterforce attacks to destroy the weapons that would cause EMP before their launch, active defenses that destroy the weapons en route to their detonation location, and by passive defense measures taken to prevent EMP damage after a nuclear or conventional EMP explosion. This section focuses on passive defense against EMP because much has already been said about counterforce and active defense options. The key passive defense concern is protecting major electrical transformers because their loss can cripple

[26] Aerospace Center for Strategic and International Studies, 2018.

[27] Unpublished estimate by the Korea Institute of Defense Analyses.

Table 4.1. Characteristics, Conditions of Use, and Damage Patterns of Nuclear and Nonnuclear Electromagnetic Pulse Weapons

Criteria	Nuclear EMP		Nonnuclear EMP	
Maximum electric field strength	~50kV/m		~100kV/m	
Height of burst	30 to 500 km		Near ground surface	
Extent of damage	A radius of hundreds or thousands of kilometers		A radius of hundreds of meters	
Use phase	Early > middle > end of a war		Crisis or early in a war	
Major target	Overall infrastructure • Power system • Communication system		Military target • Early-warning radar station • Communication antenna	
Damage	Nonmilitary field	Power outage Communication breakdown Traffic congestion Gas station fire Water supply interruption Internet outage Interruption of financial service Interruption of administrative service	Non-military field	Temporary power outage Temporary breakdown of communications Traffic congestion Temporary interruption of water supply Temporary internet outage Temporary interruption of financial service Temporary interruption of administrative service
	Military field	Disruption to operations command Limited operation of strategic assets	Military field	Disruption to the command, control, communications, computer, and intelligence (C4I) system Limited early-warning system

the electrical grid, and EMP damage to them can take a significant amount of time, perhaps months to years, to resolve. But there are passive defense measures against EMP that can be taken with all electronic devices.[28]

How serious is the threat of a major transformer failure due to EMP, and how many transformers might fail? Is the number small enough that the expansion of transformer manufacturing plants in the United States might help to solve this problem? Though discussions often inaccurately refer to "melted transformers," in fact it is the copper windings in the transformer that could melt, leading to a short circuit. The transformers could be returned to the manufacturing plants and repaired. This would not be a speedy process, but it would be faster than the up to a year needed to manufacture a new one.[29]

Graham and Pry have proposed a wide variety of measures to deal with what they believe is the existential threat to the United States posed by North Korean nuclear weapon–generated

[28] A particularly good description of options for these measures can be found in Baker, Radasky, and Gilbert, 2019, p. iii.

[29] Personal communication from an extra-high-voltage transformer repair expert.

EMP.[30] The most obvious action is to harden key elements of the U.S. electrical grid. Graham and Pry have provided no estimate of how much time would be required to achieve adequate hardening or what it would cost, though they claim that this could be achieved by a "slight increase in user electric rates."[31]

The basic hardening method is the use of a conductive (usually metallic) enclosure around the system (a "Faraday cage").[32] This can surround an individual device, a room, or an entire building. A problem is that what is inside the enclosure must have connections with the outside to provide electric power, communications, or even air for the occupants. Steps must be taken to reduce the EMP field admitted by these openings by various means such as protective circuits, surge protectors, waveguide protection, or fiber optic wires. Even so, some EMP will leak into the enclosure, and tests must be performed to ensure that the protected devices can withstand this residual EMP field.

For other electronic systems and especially for C2 facilities, there are several options to provide protection. For example, sophisticated surge protectors can be provided to protect computers or other electronics from EMP surges on electrical lines. Turning electronics off and disconnecting them from electrical lines is also possible if warning of an EMP attack can be obtained and generated in time. And analog electronic systems are less vulnerable to EMP and could be provided as backups to the more vulnerable digital systems, though they would still require a power source.[33]

Additional measures proposed by Graham and Pry include strengthening U.S. ballistic missile defenses by deploying space-based missile defenses, Aegis ships around the United States to intercept missiles approaching from the south, or missiles launched from ships off the U.S. coasts. They also propose a crash program to provide long-term emergency power to all U.S. nuclear reactors to prevent meltdowns and the use of national technical means (U.S. satellites) to ascertain whether any North Korean satellites are carrying nuclear weapons. Ultimately, they want the United States to declare that EMP or cyberattacks that threaten to cause major electrical blackouts justify preemptive and retaliatory responses using all means including nuclear weapons. They want the United States to develop its own "super-EMP" nuclear weapons to be part of this nuclear response. These weapons would presumably be able to black out North Korean electronic communications and perhaps destroy the electronics in many missiles, their launchers, and related key devices.

---

[30] William R. Graham and Peter Vincent Pry, *Statement for the Record, Dr. William R. Graham, Dr. Peter Vincent Pry, Chief of Staff, Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack to U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, Hearing, "Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland,"* Washington, D.C., October 12, 2017, pp. 11–14.

[31] Graham and Pry, 2017, p. 14.

[32] Radasky and Savage, 2010, pp. 4-1–4-4.

[33] Solar panels are a potentially interesting power source unlikely to be seriously affected by EMP. However, the electrical connections from these panels to any equipment requiring power would also have to be protected.

The U.S. government does not appear to share Graham and Pry's apocalyptic view of the North Korean nuclear EMP threat and has not undertaken to implement their suggestions. Resolving more of the uncertainty involving the seriousness of the threat would seem to be a prerequisite to taking major EMP-related counteractions. This would include testing more modern electronics for their vulnerability to EMP and releasing enough classified information to indicate how much counter-EMP action is needed. However, it should be recognized that short of conducting additional high-altitude nuclear tests (which is not likely to happen), there will always be significant uncertainties regarding the seriousness of the EMP threat.

Protective measures against nonnuclear EMP weapons are the same as those for nuclear EMP. However, the scope of nonnuclear EMP attacks will be much more limited, and protective measures can probably be restricted to key facilities, and especially those in the ROK.

Chapter 5. The Threat of North Korean Cyber Capabilities[1]

The word "cyber" refers to computers, the processes they control, and the data they store. North Korea has been and is building cyber capabilities to attack the cyber domain of other parties. The North refers to its cyber capabilities as the regime's cyber (싸이버) toolkit.[2] This toolkit is among the most useful, asymmetric, and potentially strategically highly effective North Korean capabilities, a weapon Kim Jong-un has reportedly described as the regime's "all-purpose sword."[3] Indeed, no tool in North Korea's arsenal has the reach and diversity of potential impact as its offensive cyber capabilities, which can target adversaries overseas at relatively low cost and in fairly short order. Nevertheless, the open literature has only limited and primarily anecdotal descriptions of North Korean cyber capabilities, not all of which have been openly attributed to North Korea, and this limits our ability to deal with this threat comprehensively. The anecdotal descriptions reflect the effects of cyberattacks that North Korea has been executing in peacetime primarily to earn money for the regime, with little or no information about its penetrations of ROK-U.S. information systems that could be exploited in wartime. As such, some analysts have argued that, "If you're worried about North Korea's nukes, you probably should be even more concerned about Pyongyang's cyber weapons."[4] Yet other experts assess the North's cyber tools to be more a criminal and intelligence threat than an operational military tool, arguing that "despite progress in developing its cyber-attack capabilities, [North Korea] does not possess the advanced skills needed to cause physical damage" and noting further that "no cyber attack has ever caused casualties, and only three or four resulted in physical damage."[5] Between these two views, which is more likely to be accurate, the one that sees the regime's cyber tools as on par with its nuclear arsenal or the other that dismisses it as largely a tool for bank heists and intimidating private businesses but not taking down key U.S. military infrastructure? Just how great is the threat posed by the DPRK's offensive cyber capabilities for information warfare (정보전)?

While the North Korean regime's leadership has characterized its own cyber capabilities in expansive terms, this chapter seeks to describe these as objectively as possible within the

[1] This chapter was prepared by Scott W. Harold and Go Myong-Hyun.

[2] This definition provides the scope of cyber capabilities used herein. Thus, we consider North Korean computerized attacks that steal data and other assets, damage data, and otherwise disrupt computerized operations. We do not include electronic warfare, the use of weapons such as EMP, physical attacks on computer-related equipment, or information warfare.

[3] Kong Ji-Young and Lim Jong In, "The All-Purpose Sword: North Korea's Cyber Operations and Strategy," in T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky, eds., *2019 11th International Conference on Cyber Conflict*, Talinn, Estonia: NATO CCD COE Publications, 2020.

[4] Rhea Siers, "North Korea: The Cyber Wild Card," *Journal of Law and Cyber Warfare*, Vol. 4, No. 1, Winter 2014.

[5] James A. Lewis, "The Likelihood of North Korean Cyber Attacks," Washington, D.C.: Center for Strategic and International Studies, September 7, 2017.

limits of open information and to characterize the scale of their potential impact when used within peacetime restraints and if used to create mass effects in wartime. In order to evaluate Pyongyang's cyber toolkit, we draw on official reports issued by the governments of the United States, the Republic of Korea, and Japan. We also leverage academic assessments, think-tank analyses, and open-source media reporting. We conclude that while the potential for North Korean cyber to constitute a strategic threat exists, in peacetime the more likely case is that the regime will use its capabilities for less widespread, less escalatory, and more discrete goals that are intended to remain below the level of armed conflict and to sustain the regime. Indeed, to date this has been how the regime has used computer network operations: for intelligence collection, intimidation, revenue generation, and to damage its adversaries' economies.[6] In contrast, North Korea has not demonstrated truly strategic deterrent or operational effects that we might see in wartime or approaching war. These effects would require that the North gain accesses and execute types of cyberattacks that it has not demonstrated an ability to achieve, or at least a willingness to execute. This could be because gaining such accesses is extremely difficult; alternatively, it could be that the North has obtained them, but that out of a recognition of the escalatory nature of such attacks, it is harboring them in case it needs to use them during an actual warfight. It may also be harboring such attacks to achieve surprise when executing them, as surprise is a key element of North Korean major war planning.[7] Additionally, given the complexity of the cyber domain, it is at least possible that the North, while executing a lower-level intrusion or attack, could unintentionally cause the partial or complete collapse of a portion of an adversary's critical infrastructure, such as its electrical grid, air traffic control system, or nuclear power plants. While not possible to rule out, these would represent outcomes substantially more consequential than the DPRK has shown an ability to achieve as of late 2021.[8]

We begin by briefly describing the evolution of North Korea's overall cyber capabilities. We trace the origins of North Korea's interest in such systems; lay out what is known about the regime's C2, goals, and strategy for employing its cyber capabilities; and take note of key instances of past usage. We then turn to a short evaluation of the future evolution and prospective uses of the DPRK's cyber tools before closing with a discussion of the implications for U.S. and South Korean policy.

---

[6] Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses,* Washington, D.C.: Center for Strategic and International Studies, 2016; Mathew Ha and David Maxwell, *Kim Jong Un's "All-Purpose Sword": North Korean Cyber-Enabled Economic Warfare*, Washington, D.C.: Foundation for the Defense of Democracies, 2018.

[7] U.S. Department of the Army, 2020, p. 1-13.

[8] One possible caveat to this argument is that the North may have achieved such accesses, and outside observers would not have a way to know. Pyongyang would have an incentive to harbor such exploits until they must be used, either to establish escalation dominance, to complicate an adversary's military operations, or to advance some other strategy goal. The regime would not necessarily be able to demonstrate such capabilities and at the same time preserve such accesses; the North is likely to execute such attacks only in the event of an actual conflict, not prior to such an eventuality.

Overview of the North Korean Cyber Threat

Any discussion of North Korea's cyber threat should begin with a discussion about the policy goals that the Kim regime has and then seek to identify how offensive cyber missions that the regime has conducted or could conduct would connect its aims to its ends. The United States Defense Intelligence Agency's 2021 report *North Korea Military Power: A Growing Regional and Global Threat* describes cyber as serving the North's goals of deterrence and coercion, supporting its military operations, psychological warfare, intelligence-gathering, and revenue generation through four main types of cyber operations: "computer network attack and intimidation," "cyber-enabled propaganda," "intelligence collection," and "currency generation."[9] Cyber-enabled propaganda is more part of the North Korean information warfare program and lies outside the scope of this chapter.

North Korea trains its hackers from an early age. Youngsters who show great promise in math and science are selected from elementary schools across the country[10] and trained in coding and problem-solving skills at specialized high schools such as Keumseong 1 and 2 High-Middle schools, and finish their education at top technology universities such as Kim Chaek University of Technology, Kim Il Sung University, and Mirim University, though other universities in North Korea (such as the Hamhung Computer College) also train hackers.[11] In the early days of the North Korean cyber training program at Mirim University, "25 Russian professors were invited from the Frunze Military Academy in the former Soviet Union to give lectures."[12] While many North Koreans must complete their mandatory military service before going to college, the hackers in these programs are usually exempted from military service until they complete their college studies, and then they are committed to a cyber operations service period of roughly ten years (similar to military service), which begins immediately.

In terms of organization, North Korea's cyber capabilities are distributed among various government organizations. The Reconnaissance General Bureau (RGB) reportedly has the largest cyber force,[13] followed by the North Korean police and security services, and then the KPA, but other organizations also have cyber forces.[14] Each year, the graduates of the various cyber training programs are spread across these organizations.

---

[9] Defense Intelligence Agency, *North Korea Military Power: A Growing Regional and Global Threat*, Washington, D.C., 2021, pp. 33–34.

[10] As in most positions in North Korea, an individual's family and own *songbun* (political reliability) are important factors in selection for this kind of training. See Robert Collins, *Marked for Life: Songbun*, The Committee for Human Rights in North Korea, June 6, 2012.

[11] "North Korea Recruits Hackers at School," *Al-Jazeera*, June 20, 2011; "A Look at Mirim College, Hotbed of Cyber Warfare," *DailyNK*, May 6, 2011.

[12] "N. Korea Trains Up Hacker Squad," *Chosun Ilbo*, March 8, 2011.

[13] The RGB sits under the General Staff Department within the Ministry of the People's Armed Forces and reports directly to Supreme Commander Kim Jong-un.

[14] Interview with a former senior elite North Korean escapee, January 14, 2022.

Most of the internet in North Korea is an internal network—most North Koreans have no access to the worldwide web. But for more than a decade China has reportedly provided North Korea with thousands of connections to the worldwide web, mainly for use in hacking. Then in roughly 2017, Russia added a second set of North Korean connections to the global internet.[15] These connections provide an interesting chokepoint to use against cyber activities emanating from North Korea, but do not restrict North Korean hackers sent overseas, as discussed below.

In peacetime, many North Korean hackers operate overseas, especially in China.[16] North Korean cyber groups maintain talent brokers in China and elsewhere. These brokers contract with local firms to provide "programmer" assistance, often sending groups of 20 or 30 North Korean programmer/hackers to work for the firm. The hackers are told to do their very best programming in supporting the local firm during the day and to then transition to hacking at night using the computer facilities of the local firm. Most of these hackers work about seven years in various firms in the host country and then return to North Korea to complete their counterpart of "military service."[17] North Korea has also established companies of its hackers in other countries; these companies produce online games, allowing the hackers access to the computers of those who download and log in to those games.[18] In addition, North Korea reportedly maintains at least one large facility for hacker operations in China.[19]

If the North were to initiate a conflict with South Korea (perhaps because its nuclear forces gave the leadership a sense of invulnerability and a capacity to deter U.S. intervention) or feel that conflict had been forced upon it and become unavoidable, it might employ cyberattacks to achieve operational military effects. In such a case, the North might "barrage the ROK with sophisticated cyberattacks," together with a variety of kinetic attacks, aiming to cripple the South's ability to wage a coordinated, joint defense.[20]

The Character and Quantity of North Korean Cyber

While in the late 2000s and early 2010s skepticism of North Korea's ability to wage offensive cyberattacks was common, by the mid-2010s and onward, analysts increasingly recognized that Pyongyang had developed its computer network operations capabilities to the

---

[15] Martyn Williams, "Russia Provides New Internet Connection to North Korea," 38 North, October 1, 2017.

[16] Lee Min-seok, "N. Korean Hackers 'Work out of Chinese Hotels,'" *Chosun Ilbo*, April 25, 2022.

[17] Interview with a former senior elite North Korean escapee, August 2016. In subsequent interviews with this escapee, the individual said that many North Korean hackers departed China as the December 22, 2019, UN deadline approached for all North Korean workers to return to North Korea. Many of the hackers later reportedly returned to China, however, when Beijing opted not to enforce the expulsion of many North Koreans.

[18] Interview with a former senior elite North Korean escapee, August 2016.

[19] Interview with a former senior political elite North Korean escapee, April 2018.

[20] Benjamin R. Young, "Understanding North Korea's 'Final Victory' and Why It Matters," *NK News*, September 6, 2021.

point where they could do significant damage.[21] The Republic of Korea's 2020 Ministry of National Defense white paper, for example, assessed that the North was actively training cyber warfare specialists and had developed a cadre of approximately 6,800 hackers, listing cyber as one of the North's "asymmetrical capabilities."[22] The *2021 Worldwide Threat Assessment* by the U.S. Director of National Intelligence noted that North Korea's cyber program "poses a growing espionage, theft, and attack threat."[23] And Japan's defense white paper *Defense of Japan 2021* lists China, Russia, and North Korea (in that order) as cyber threat actors, adding that "North Korea is alleged to have been developing capabilities to steal money and secret military information through cyberattacks, as well as developing attack capabilities against key foreign critical infrastructure that would be executed using cyberattacks."[24]

Government reports by the United States, the Republic of Korea, and Japan similarly characterize North Korea as among the most threatening national cyber actors. This is, however, an assessment of the effectiveness of North Korean hacking in peacetime and not its potential in wartime. In wartime, North Korea would seek to use cyber weapons in an operational sense to advance its goals during a conflict as opposed to its strategic value during peacetime for intimidation, intelligence collection, and revenue generation.

What Cyber Capabilities Would North Korea Likely Use?

For a small and poor country, North Korea's use of cyber has been impressive for its clever adaptation of existing exploits and its ability to achieve outsized impacts. But in terms of the technical sophistication of its cyber toolkit, North Korea's cyber capabilities look somewhat less impressive. As Robert Potter has argued:

> when North Korea conducts cyberattacks it often does so from already known and well-understood technical networks. To be sure, the networks required to support large-scale cyberattacks are frequently difficult to build and maintain, and used to mask approaches and mitigate against the risk of direct attribution. . . For all their publicity, North Korean cyber operations do not use a

---

[21] Mark Clayton, "In Cyberarms Race, North Korea Emerging as a Power, Not a Pushover," *Christian Science Monitor*, October 19, 2013; David Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 17, 2017; Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary, *North Korean Cyber Capabilities: In Brief*, Washington, D.C.: Congressional Research Service, 2017.

[22] Republic of Korea, Ministry of National Defense, *2020 Defense White Paper*, Seoul, 2021, p. 29. For many years, estimates of the North's contingent of hackers grew steadily from 600 in 2004 to between 1,000 and 3,000 in 2011 before the figure of 6,800 became the most widely cited following its use in the ROK Ministry of National Defense white paper series. Some analysts have speculated that the North may even have as many as 20,000 hackers. See "N. Korea's Elite Military Hackers Trained to Attack High Tech Powers," *East-Asia-Intel*, October 12, 2004; "N. Korea's Cyber Warfare Unit in Spotlight After Their Attack on S. Korean Bank," Yonhap News Agency, May 3, 2011; "Defector Claims North Grooms Hackers," *Joongang Daily*, June 1, 2011; "N. Korea Trains Up Hacker Squad," *Chosun Ilbo (English)*, March 8, 2011.

[23] Office of the Director of National Intelligence, *Threat Assessment of the U.S. Intelligence Community*, Washington, D.C., 2021, p. 15.

[24] Japan Ministry of National Defense, *Defense of Japan 2021*, Tokyo, 2021, p. 182.

> large number of ultra-sophisticated exploitations. Rather, their code base slowly evolves. They rapidly incorporate new knowledge but generally have not shown a flair for unique development. Much of North Korea's current cyber exploitation kit is composed of modified versions of previous tools that have been slowly refined and set into identifiable patterns of attack and behavior.[25]

Still, as North Korea's unsophisticated cyberattacks (such as distributed denial of service—DDoS) regularly demonstrate, sophisticated cyber operations are not required to break into major companies such as Sony Pictures and can potentially cause extensive damage. And despite the fact that much is known about the North's cyber toolkit, many ROK-U.S. computer systems and individual computer users are still unprepared to counter a variety of North Korean cyberattacks.

If it is indeed correct that known North Korean cyber capabilities are likely restricted to the realm of already relatively established techniques, then looking at past North Korean uses of cyber, other nations' uses, and well-known vulnerabilities may provide a helpful guide to what the North could achieve in the future.[26] In terms of its own past uses, North Korea has demonstrated use of the following techniques:

- Phishing and spear phishing: "Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems." The attack succeeds if the target opens the attachment or selects the link containing malware.[27] Spear phishing is a phishing attack that targets specific individuals, posing as a trusted source.
- DDoS traffic generation attacks: This is an attack technique that exhausts the network bandwidth of the service targeted usually through the use of botnets.[28]
- Zero-day exploits: This technique employs "zero-day vulnerability," a software vulnerability that the attackers discovered before the vendors did.[29]
- Ransomware attacks: "Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker."[30]
- "Disk wipe" attacks: Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources.[31]

---

[25] Robert Potter, "Toward a Better Understanding of North Korea's Cyber Operations," 38 North, August 5, 2019. accessed December 6, 2021.

[26] Note, however, that at least some cyber experts, most notably Priscilla Moriuchi of Harvard University's John F. Kennedy School of Governance Belfer Center for Science and International Security, believe the North's techniques are more advanced and novel than purely derivative, and should therefore not be underestimated. Moriuchi is quoted in Ed Caesar, "The Incredible Rise of North Korea's Hacking Army," *New Yorker*, April 19, 2021.

[27] MITRE ATT&CK, "Phishing," undated d.

[28] MITRE ATT&CK, "Network Denial of Service," undated c.

[29] Kaspersky, "What Is a Zero-Day Attack? Definition and Explanation," undated.

[30] Proofpoint US, "What Is Ransomware? Definition, Prevention & More," undated.

[31] MITRE ATT&CK, "Disk Wipe," undated a.

- Watering hole attacks: In this technique, malicious codes infect the browser when an individual visits a compromised website. Because the website that is targeted for attack is visited by a specific community, the attacker can compromise a specific target group.[32]
- Data exfiltration through Domain Name System (DNS) tunneling: DNS tunneling exploits the DNS server, which translates human-friendly website addresses (uniform resource locators, or URLs) to numeric internet protocol addresses. External requests to DNS servers are granted unfettered network data access across the firewall because DNS requests are always allowed and often not monitored. Hackers exploit this feature to exfiltrate data from within the network.[33]
- Credential harvesting: This applies to a wide spectrum of techniques for password pilfering, ranging from brute-force password cracking to social engineering techniques that convince the user to voluntarily provide passwords and credentials to the attacker. Once credentials and passwords are gained, attackers penetrate the network and exfiltrate data with a low chance of detection.[34]

Some of North Korea's more widely discussed victims have been individuals; foreign businesses, banks and other financial actors, and media outlets; foreign critical infrastructure, including South Korea's nuclear power agency;[35] and adversary defense institutions.

North Korea may have a more advanced toolkit for use against military and other highly protected cyber targets. In peacetime, the North could use this toolkit to collect information and to insert "trapdoors" in adversary operating systems that it could access in a conflict. North Korean hackers would presumably be actively involved in seeking such penetrations into sensitive adversary computing systems, though it would limit such activities to avoid calling attention to their successes, leaving the trapdoors in place for use in a conflict.

Other nations' uses of cyber may be examples that the North could use to inform its own conception of how to effectively employ cyber. Such uses could include the use of disinformation for political warfare inspired by Russian, Chinese, or Iranian operations. More directly relevant to a military operation could be an effort by North Korean cyber actors to target U.S. C2, logistics, or other systems that would be necessary to support military operations in defense of South Korea in a conflict, inspired by Chinese or other writings about key point and system destruction warfare.[36] Separately, the alleged U.S. and Israeli deployment of the Stuxnet virus to damage Iran's nuclear enrichment centrifuges, the 2017 NotPetya supply chain attack by Russia against Ukraine, the 2021 ransomware attacks on the Colonial Pipeline refined petroleum distribution

---

[32] MITRE ATT&CK, "Drive-by Compromise," undated b.

[33] Palo Alto Networks, "What Is DNS Tunneling?" undated b.

[34] Palo Alto Networks, "Email Credential Harvesting at Scale Without Malware," undated a.

[35] "Lawmaker Claims N. Korean Hackers Breached Nuclear Power Agency in S. Korea," *Pulse News*, June 18, 2018.

[36] Edmund J. Burke, Kristen Gunness, Cortez A. Cooper, III, and Mark Cozad, *People's Liberation Army Operational Concepts*, Santa Monica, Calif.: RAND Corporation, RR-A394-1, 2020; Jeffrey Engstrom, *Systems Confrontation and Systems Destruction Warfare*, Santa Monica, Calif.: RAND Corporation, RR-1708-OSD, 2018.

system in the United States, and the 2022 Russian malware scheme accompanying its invasion of the Ukraine could all serve as examples for North Korea to emulate.[37] Indeed, North Korean hackers also "work with all kinds of cyber criminals around the world, including Russian cyber criminals,"[38] giving the North's hackers access to the strategies and tactics of hackers beyond the North. These attacks suggest the potential for adversaries with state resources, patience, and sophistication to develop bespoke attacks that target hardware, sophisticated infections that could spy on or cripple large numbers of systems, or cause mass-effect takedowns of critical infrastructure.

Potential North Korean Uses of Cyber for Strategic Effects in Peacetime

Among the myriad ways North Korea employs its cyber toolkit, several possible targets stand out as worth noting for their strategic impact.

First, the North could hack its way into adversary intelligence, planning, or C2 systems in ways that would degrade or complicate U.S. and ROK military planning. These attacks could enable the North's other forces to achieve greater battlefield successes, a sort of indirect contribution of cyber to accomplishing strategic effect. In 2016, according to a South Korean lawmaker, Pyongyang allegedly broke into the computer networks of the ROK's Ministry of National Defense and made off with the combined ROK-U.S. joint war plan.[39] Such plans could enable the Korean People's Army to better target U.S. and South Korean joint forces and counteract the warfighting approach the allies might seek to execute in a conflict, potentially prolonging the war and possibly affecting its outcome in significant ways.

Second, the regime has already demonstrated that it can use its cyber tools to amass enough financial resources that it can afford, even under international sanctions, to continue advancing its nuclear weapons and other WMD programs, as well as its ballistic and cruise missile delivery systems, and even to sustain the selective modernization of key aspects of its conventional forces.[40] Indeed, Chainalysis estimates North Korea stole US$1.75 billion worth of cryptocurrency between 2017 and 2020.[41] For its part, the UN has estimated in 2019 that Pyongyang's bank heists and cryptocurrency exchange raids had netted the regime at least US$2 billion. And in a single

---

[37] Kate Conger and David E. Sanger, "U.S. Says It Secretly Removed Malware Worldwide, Pre-Empting Russian Cyberattacks," *New York Times*, April 6, 2022.

[38] Byun Duk-kun, "N. Korea Works with All Kinds of Cyber Criminals, Including Russians: Sullivan," Yonhap News Agency, March 23, 2022.

[39] Choe Sang-hun, "North Korean Hackers Stole U.S.–South Korean Military Plans, Lawmaker Says," *New York Times*, October 10, 2017.

[40] Michelle Nichols, "North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: UN Report," Reuters, August 5, 2019; Caesar, 2021.

[41] Chainalysis Team, "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options," Chainalysis blog, February 9, 2021.

operation in 2022, North Korea reportedly stole $620 million in bitcoin.[42] Regardless of the specifics, such figures represent a staggering haul, considering that the country's gross domestic product was estimated to have shrunk 4.5 percent in 2020 to just $27.4 billion under the pressures of COVID-19 and the regime's decision to shutter its borders to trade.[43]

Third, the regime has clearly sought not only to strengthen itself by hacking for intelligence gains and revenues, but also to damage others' overall economic well-being, including South Korea's.[44] Indeed, the Seoul-based Korea Institute for Industrial Economics and Trade, a government-linked think tank, estimated in 2014 that the 2013 "Dark Seoul" attack by North Korea that targeted three South Korean television stations and a bank may have cost ROK banks and media outlets as much as $820 million, and projected that by 2020 the South might be exposed to hacks that cost it up to $25 billion annually, with most of those attacks coming from North Korea.[45]

Finally, the regime could, notionally at least, use its hacking tools to break things, lock up critical systems, and kill people. This would be the most damaging approach to employment, but is, again, one the regime has not shown either a capacity or possibly a willingness to use yet, which is to say that the regime may be deterred from such activities in peacetime.

However, if it felt that it needed to use cyber to regain escalation dominance in a spiraling crisis, or if it felt that its adversaries were closing in and it had nothing left to lose and so wanted to use all of its remaining tools to harm the ROK and the United States, then it is conceivable that the regime might attempt to employ cyber in a military operational sense. The next section examines how that might look.

How Might North Korea Use Cyber for Coercive and Warfighting Purposes?

North Korea's computer network operations appear to come both from abroad, with operatives distributed across China, Southeast Asia, and elsewhere, and from inside North Korea, where the regime can exercise a more granular degree of control. Because North Korea possesses just two external servers (being hosted by China and Russia), it may face incentives to use its cyber weapons early in a large-scale conflict lest Beijing, Moscow, Washington, and/or Seoul shut down or cripple the North's access to the internet.[46] Of course the regime may have operatives overseas who could execute large-scale, destructive cyberattacks if those servers were knocked out, but in a major armed conflict with the United States or South Korea, the North's C2 systems may themselves be

---

[42] Ifang Bremer, "Dutch Intelligence Says North Korea Using Netherlands-Based Servers for Hacking," *NKNews*, April 29, 2022.

[43] Jeong-ho Lee, "North Korea's Economy Contracted Most in Two Decades in 2020," Bloomberg, July 29, 2021; Randall S. Jones, "North Korean Economy Shrinks in 2020," Korean Economic Institute, October 1, 2021.

[44] Ha and Maxwell, 2016.

[45] K. J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," CNN, April 22, 2015.

[46] Williams, 2017.

degraded, with the possible consequence that the regime's overseas agents may be cut off and might hesitate to act without explicit approval. Some experts suspect that North Korean hackers posted overseas may behave autonomously when supervision from Pyongyang becomes lax.[47]

Should the regime seek to employ its cyber tools as weapons of war in support of military operations, North Korean leaders would face a set of choices about their strategy and targets. Would they be looking to intimidate or coerce their adversaries? Or would they be looking to slow and complicate adversary military operations? And wouldn't they employ every last weapon in their arsenal so as to harm their enemies once the regime perceives its survival is being seriously threatened (which may be the regime's perspective from the beginning of a conflict)?

If Pyongyang believed that conflict was imminent or had started, but was not yet clearly going to be all-out, it could seek to brandish its cyber tools, together with other capabilities, in an attempt to "escalate to deescalate"—that is, to deter ROK-U.S. escalation by taking an escalatory step in the hopes of compelling Seoul and Washington to back down and deescalate. Taking such a path could lead North Korean leaders to favor targets that are of medium to high strategic value, but not so catastrophic in impact that they would lead to calls by Washington and Seoul for the regime to be destroyed. Examples could include, but not be limited to, the South Korean or Japanese banking sectors and electrical power grids, though even with these, North Korea would risk not knowing what the ROK-U.S. escalation redlines are.

By contrast, if a crisis had already spiraled into a major conflict but had not escalated to the point that the regime was convinced its end was near, it might seek to deploy cyber weapons to create panic in South Korea; hamper the abilities of the ROK, the United States, and others to press north or evacuate their own personnel from the peninsula; coordinate their political-military strategies; or deliver additional forces into the theater. This might lead to an approach that sought to damage the South Korean air traffic control systems near Incheon; complicate port operations out of Osan, Kunsan, and/or Busan (which the United States would use in any noncombatant evacuation operation and for force flow onto the peninsula); disrupt traffic signals to cause accidents and gridlock in major cities; target the ability of U.S. forces to flow into Korea from the Continental United States (CONUS) or U.S. bases in Japan; attack U.S. private-sector logistical support networks; or strike at critical infrastructure in Guam and Hawaii. And given the growing ROK-U.S. use of unmanned systems, the North may well target the control of these systems to neutralize them or, worse, to turn them back against the ROK-U.S.[48] A particularly attractive target for the North might be Japan, inasmuch as any desire by Japan to respond to North Korean aggression could be resisted by South Korea, where many actors would be loath to accept Japanese forces either on the peninsula or attacking the North.

---

[47] Min Hur, "North Korea's RGB Controlling at Least Six Hacking Units . . . Vaccine Producers Also Targeted" [北정찰총국, 최소 6개 해킹그룹 관리. . .백신 제약사도 '타깃'], *Munhwa Ilbo*, August 21, 2021.

[48] While the North probably cannot do this, it might be able to hijack a software update on some of these systems to insert a Trojan horse control system that, when triggered, would give North Korean hackers the ability to crash unmanned systems or take control of them.

Finally, if the North were convinced that the ROK and/or the United States had decided to take down the regime and were on an inevitable path to doing so (which could be determined even before the start of a conflict), and if it still possessed a capacity to access computer networks connected to the global internet (which would seem by no means guaranteed by that point in a crisis), the North might seek to gamble for resurrection or play the Samson card of bringing everyone down with it by attempting to strike at critical infrastructure that would carry enormous consequences for other targets. This could mean trying to hit South Korean dams and electric power grids; water treatment plants; hospitals; subway, train, and bus lines as well as air and seaport infrastructure; radio, television, cellular and internet service; and other private-sector actors, including firms or individuals via internet malware such as the WannaCry worm. Of course, many of these targets have been penetrated by North Korea before and may be better prepared against repeat cyberattack. If so, the North could aim to go lower but broader on the escalation ladder, targeting individuals through rapidly proliferating hacks intended to harm South Korean society. Such attacks could come in the form of ransomware, but could also take the form of targeted or broad-brush disinformation intended to sow social mistrust in the ROK leadership or the ROK-U.S. alliance or to induce an upwelling of anger at Japan (and subsequently U.S. and the ROK leadership).

What Impact Might North Korean Cyberattacks Have?

Assessing the prospective damage or impact from a hypothetical North Korean cyberattack requires bounding the problem and acknowledging the limitations of attempting to model complex, networked system attacks at an as-yet undefined point sometime in the future. While we were not able to develop such a model here, we do identify several considerations that could shape the impact North Korean cyberattacks could achieve:

- What effect is North Korea aiming at?
- Which actors is North Korea targeting?
- How quickly do the victims recognize and seek to counter the attack?
- How effective are the victims and their computer support personnel at remediating the effects of the attack?

In terms of lives lost, people injured, and economic losses, a North Korean cyberattack could potentially cause between zero and thousands of deaths. To date, it is unclear if anyone has actually died directly from a cyberattack, though some attacks in other regions appear to have caused deaths indirectly by delaying treatment, causing stress, of fueling a misallocation of resources.[49] Yet as far back as 2012, then–U.S. Secretary of Defense Leon Panetta warned of the threat of a "cyber-Pearl Harbor," an attack that could "derail passenger trains, or even more

[49] Melissa Eddy and Nicole Perlroth, "Cyberattack Suspected in German Woman's Death," *New York Times*, September 18, 2020.

dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shut down the power grid across large parts of the country."[50] The actual Pearl Harbor attack, if taken as a literal, as opposed to merely figurative, reference point claimed approximately 2,400 lives and gravely damaged U.S. military capabilities in the Pacific. More recently, Federal Bureau of Investigation Director Christopher Wray, in an interview with the *Wall Street Journal* in June 2021, compared the surge of ransomware attacks in recent years with the terror attacks of September 11, 2001.[51] Those attacks were estimated to have killed just shy of 3,000 people, injured roughly 25,000, and done billions of dollars in damage (or trillions if the attacks are considered as having led directly to the United States wars in Afghanistan and Iraq). Thus, it seems reasonable to speculate that a cyberattack that is truly large scale could conceivably kill and/or injure thousands and do hundreds of millions to billions of dollars in damages. Indeed, North Korean hacks on banks and other institutions are already estimated to have caused hundreds of millions in losses, so estimates of billions of dollars for a strategic scale cyberattack seem plausible.

Potential Republic of Korea and United States Responses to North Korean Employment of Cyber

South Korean and U.S. options for addressing the cyber threat posed by North Korea can be divided into four basic bins: negotiations, deterrence by denial, deterrence by punishment, or attempting to leverage third parties. In reality, no single category of responses is likely to prove sufficient, and indeed even if both parties adopt all four collectively, the North is still unlikely to be deterred from at least some types of cyber intrusions and/or attacks.

Negotiations

First, although negotiations are highly unlikely to succeed and any agreements would be difficult if not impossible to enforce, the United States and South Korea could seek to negotiate norms with North Korea that seek to ban the use of cyber weapons, at least against certain types of targets such as critical infrastructure where the primary victims would be civilians. The cyber domain is at best an extremely difficult and at worst nearly impossible domain in which to negotiate credible, binding, monitorable, and enforceable agreements. The uncertainty surrounding attribution of cyberattacks can even play into North Korea's hands: The United States and South Korea could disagree on the threshold of attribution and on attribution of specific attacks, which could lead to disagreements between the allies. Nonetheless, despite these difficulties, the United States has held both formal and Track 1.5/Track 2 dialogues on the subject of cyber norms

[50] Elizabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, October 11, 2012.

[51] Julian E. Barnes, "F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat," *New York Times*, June 4, 2021.

with adversary nations such as China and Russia,[52] both of which are regarded as far more capable cyber adversaries than North Korea (though they also have more equities that the United States can hold at risk and a greater desire for at least a modicum of positive interactions with Washington).[53] Furthermore, as indicated in their May 2021 Joint Statement, both the United States and South Korea have indicated a willingness to engage in "diplomacy and dialogue" with North Korea, suggesting that talks on cyber, while certainly not promising, are at least not off the table if the North were to respond favorably to initiatives by Washington and/or Seoul.[54]

Defensive Responses

A second set of approaches the allies could undertake would focus on defensive steps aimed at deterring North Korean cyberattacks by denying their effects. This would essentially amount to a combination of steps aimed at raising the difficulty of the North gaining access to allied military or civilian computer systems; making improvements in users' cyber hygiene through multifactor authentication and improved passwords; enhanced intrusion and anomaly detection; and/or advanced post-intrusion remediation. Such options are challenging in that they require large numbers of South Korean and U.S. actors to take action and potentially involve significant financial costs for what may appear to some to be ambiguous or low-level returns. Somewhat less challenging than coordinating across the totality of both ROK and U.S. societies would be steps aimed at enabling U.S. and ROK armed forces to fight on while enduring North Korean cyberattacks and securing critical infrastructure within the United States and the ROK. In addition, the ROK-U.S. could create their own hacking teams to find weaknesses in the cyber environments of key businesses and then fix those weaknesses.[55]

Recent RAND work has highlighted that true measures of readiness need to reflect the ability of the total force to continue operating despite persistent adversary cyberattack, including those portions of the commercial sector to which the U.S. military outsources aspects of logistics, maintenance, and transportation.[56] At a broader level than just purely military readiness,

---

[52] Track 1 dialogues are between government officials of two or more countries. Track 2 dialogues are between nongovernment personnel. Track 1.5 negotiations involve a mixture of government and nonofficial participants.

[53] Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2016; White House Office of the Press Secretary, "Fact Sheet: President Xi Jinping's Visit to the United States," September 25, 2015; U.S. Department of Justice, Office of Public Affairs, "First U.S.–China Law Enforcement and Cybersecurity Dialogue: Summary of Outcomes," October 6, 2017; Brian Bennett, "Biden Administration Says Talks with Russia on Cyber Attacks Are Progressing. Privately, Staffers Are Skeptical," *Time*, July 8, 2021.

[54] The White House, "U.S. –ROK Leaders' Joint Statement," May 21, 2021.

[55] The ROK Defense Acquisition Program Administration is starting exactly such an effort to examine 85 companies. Song Sang-ho, "Gov't to Check Cybersecurity Vulnerabilities of Local Defense Firms," Yonhap News Agency, March 4, 2022.

[56] Don Snyder, Elizabeth Bodine-Baron, Mahyar A. Amouzegar, Kristen F. Lynch, Mary Lee and John G. Drew, *Robust and Resilient Logistics Operations in an Information Degraded Environment*, Santa Monica, Calif.: RAND Corporation, RR-2015-AF, 2017.

U.S., South Korean, and third-country actors could seek to prioritize the defense of privacy, information, and information systems, recognizing that "data are power" and that in order to secure data, like-minded nations need to establish clear, legally embodied standards to govern and protect them, perhaps building around the European Data Protection Regulations or Japan's concept of Data Free Flow with Trust.[57]

Peacetime defensive options could also include actions to reveal North Korean cyber operations and discourage third parties from falling victim to the North Koreans. For example, the ROK-U.S. could post information in gaming chatrooms about the identity of North Korean–developed gaming websites, identifying them as posing serious risks to users' data. The ROK-U.S. could also collect information on North Korean programmers/hackers operating in China and other countries, identifying the companies hosting such hackers and applying secondary sanctions to those companies to discourage this continuing practice. And the ROK-U.S. could identify and sanction the North Korean cyber brokers operating in other countries, making their continued efforts more difficult. The ROK-U.S. could look for cases in which North Korea hackers steal funds from their host companies and expose that behavior. More seriously, ROK-U.S. hackers could identify the software being developed for third-party companies by North Korean hackers and insert bugs and logic bombs in that software to discourage third-party use of North Korean "programmers." As U.S. and allied capabilities for cyber forensics and technical attribution continue to improve, Washington and Seoul could consider consistently naming North Korea when they assess it is the source of cyberattacks anywhere in the world.

Offensive Responses

By contrast, a third set of options would focus more on offensive steps that the United States and/or South Korea would take to deter North Korean network attacks by holding at risk things North Korea values. In peacetime, the ROK-U.S. could need a joint committee to establish criteria for attribution and to attribute specific North Korean cyberattacks to justify such actions. Offensive actions could focus on taking down North Korean computer networks directly via cyber or kinetic means after an attack is detected,[58] or seeking to dissuade the North from conducting such attacks by linking the cyber issue to other issue sets, such as punitive sanctions or aid cut-offs. Higher up the escalatory ladder, the United States and/or South Korea could seek to physically destroy North Korean military units, C2, or hardware in retaliation for cyberattacks by the DPRK, essentially seeking to deter cyber with noncyber tools and potentially with escalation and responses not directly related or proportional to the

[57] Matthew J. Slaughter and David H. McCormick, "Data Is Power: Washington Needs to Craft New Rules for the Digital Age," *Foreign Affairs,* Vol. 100, No. 3, May/June 2021.

[58] A pseudonymous hacker has reportedly taken such action in response to North Korean hackers attacking him. See Nils Weisensee, "New Cyberattack Hits North Korea After Hacker Claims Responsibility for Outages," *NKNews*, February 3, 2022.

original attacks. The United States could also seek to co-opt North Korean hackers, inducing them to defect or at least adjust their allegiance such that in wartime, many target their fellow hackers rather than the ROK-U.S.[59]

In framing peacetime offensive responses, it is important to remember that Kim Jong-un may be more sensitive to asymmetric responses that send outside information into North Korea than to almost any other measure the allies could take. Thus, as noted in Chapter 1, Kim has called ROK culture and K-pop in particular a vicious cancer corrupting North Korean youth, which could cause the regime to collapse like a damp wall[60]—what could be more fearful to Kim? Examples could include finding better ways to deliver South Korean soap operas, dramas, and K-pop into North Korea; providing outside news to recipients in the North; transmitting ROK offers to assist North Koreans that Kim has rejected or likely would reject; depicting North Korean documentable graft and corruption; and depicting Kim Jong-un's lifestyle. The ROK-U.S. could even invite North Korean visits to the ROK or the United States, for example, by inviting graduate students from North Korea to come study business, the arts, and social science.[61]

But in wartime, in circumstances in which the North anticipates a conflict escalating to very high levels of violence or in which such escalation already appears to be unfolding, threats to impose sanctions or attempt to cut off the North's access to the internet are unlikely to play any deterrent role, as Pyongyang would already be anticipating far worse consequences. Moreover, the North may believe that its attacks give it plausible deniability, or it may believe that its nuclear or other strategic systems such as its chemical or biological weapons, long-range artillery or other military assets will deter allied retaliation or permit it to achieve escalation dominance.

Thus, the ROK-U.S. need to develop means for rapidly isolating North Korean hackers from the global internet in a war. The peacetime efforts described above to reduce the number of North Korean hackers working in China and Russia would be very helpful in this process. There should also be an effort in combination with efforts to disrupt communications between North Korea and its hackers in China and Russia in a conflict. In addition, the ROK-U.S. should put serious pressure on China and Russia to terminate North Korean remote internet connections in wartime, with a backup plan to find the cables supporting those connections and to cut or break them.

---

[59] This could be a challenging, as in the case of recruiting any foreign agent. But some North Korean escapees claim to have contacts with North Korean hackers who are operating in China and may be able to help recruit those disliking the regime. The potential susceptibility of North Korean hackers is demonstrated by those hackers who have defected from North Korea. Interview with a former senior elite North Korean escapee, August 2016.

[60] Choe Sang-Hun, 2021.

[61] In several discussions with North Korean escapees, one author has been told that the senior elite in North Korea would very much like to have their children come to study in the United States. And according to an interview with the ROK unification minister in December 2019, Kim Jong-un has told his faculty at Kim Il-sung University that they need to be publishing in outside academic journals to enhance the academic stature of North Korea. Kim could be told that there may be no better way to accomplish that objective than to have North Korean graduate students at major U.S. universities, at least some of whom would presumably publish in major U.S. journals. They could then return to the North with established relationships with those journals.

Third-Country Involvement

Additionally, or alternatively, the United States and South Korea could work with allies, partners, and third countries around the world in an effort to identify, track, and prosecute North Korean criminal cyber actors, cutting off their access and terminating the threat they pose to the allies' security. As noted above, it may be the case that in any contingency that North Korea expects will escalate to high levels of violence, Pyongyang may have an incentive to use its best cyber tools early in anticipation of losing over time its ability to access the internet via its servers in China and Russia.

Conclusion

Overall, North Korea's employment of cyber means to achieve strategic effects has significant impact in peacetime. Nevertheless, "the most dire predictions" of cyber doomsday scenarios from a decade ago "did not come to pass," probably because those making these predictions misunderstood the way the domain functions as a space for contestation and conflict.[62] It is hoped that with continued counter-cyber diligence, the ROK-U.S. and other global actors can moderate North Korean cyber effects in peacetime. If not, it is always possible that the North's hackers could surprise outside observers by hacking into systems that, if disrupted, would cause costly, hard-to-remediate, wide-area effects.

North Korean cyberattacks will become even more important after the outbreak of a large-scale armed conflict, though after the start of major war the use of WMD could dwarf the relative importance of cyberattacks. While the North's use of offensive cyber may not be as relatively consequential as nuclear usage or even large-scale conventional long-range artillery, it could still cause hundreds of millions to billions of dollars in damages and potentially kill thousands of people in South Korea, the United States, Japan, or elsewhere, both directly and indirectly.

U.S. and South Korean options to counter cyber tools need to focus on deterrence by denial and policing and intelligence cooperation (or pressure) on third countries to identify and cut off North Korean internet access in peacetime and especially at the outset of a crisis. Thus far, deterrence by punishment or negotiation seems poorly suited to the challenge of reducing the North Korean cyber threat. Realistically, the challenge posed by the DPRK's cyber tools will persist for years to come and grow in scale so long as Pyongyang does not pursue the kinds of outright confrontation that could lead Washington and Seoul to seek to cripple the North's accesses to the global internet by sanctioning Chinese, Russian, and other entities giving access to North Korean hackers. If the regime is able to develop increasingly sophisticated attacks such as its recent move into ransomware suggest, the strategic threat to the North's cyber toolkit poses is likely to grow.

---

[62] Sue Gordon and Eric Rosenbach, "America's Cyber Reckoning," *Foreign Affairs*, January/February 2022.

Chapter 6. Characterizing and Countering North Korean Combined Weapons of Mass Destruction and Cyber Employment[1]

Chapters 2 through 5 have treated each of the OWMD threats and the cyber threat independently and focused on what North Korea could do as opposed to what it is more likely to do. In this chapter, we look more at how we expect North Korea would use cyber threats and OWMD in conjunction with nuclear weapons (thus, all WMD) to achieve its objectives. These uses differ during peacetime, crises in North Korea, and a major conflict. In peacetime, we expect North Korea to employ its cyber capabilities fairly aggressively, but to avoid employing OWMD out of fear of ROK-U.S. retaliation that would jeopardize the survival of the regime. In a crisis, North Korea may be more aggressive with both OWMD and cyber employment because the crisis situation jeopardizes regime survival to some extent. And in a major conflict, the North Korean regime would undoubtedly use its WMD and cyber capabilities; and it would not be constrained by moral brakes or other considerations in using such weapons, knowing that if it lost such a conflict, the regime would not survive. The regime would therefore use its WMD and cyber capabilities very aggressively, seeking to achieve synergistic effects beyond the effects described in the previous chapters.

This chapter describes how North Korea's use of its WMD (including nuclear weapons) and cyber capabilities would likely be a function of what the North perceives it can gain from such uses and what costs it may suffer from that use. This trade-off is fundamental to deterrence. We therefore begin by describing the conditions that could limit North Korean WMD and cyber usage, including ROK-U.S. deterrence. We then turn to describing how the North has historically used these capabilities and how it might use them in the future in peacetime, crisis, and war. Finally, we conclude by recommending how the United States should respond to these North Korean WMD and cyber threats. Note that throughout this chapter, we use only open sources and therefore are more able to address the potential threats and options for responding to them. In practice, "'deterrence is in the eyes of the beholder,'"[2] which means it is Kim Jong-un who decides when he will be deterred from any given action. It is not clear that even he can predict all of the circumstances in which he would or would not be deterred.

While the earlier chapters do not say much about North Korean nuclear weapon use, in this chapter we do consider nuclear weapon use to adequately reflect the WMD synergies that the North could seek. Even in peacetime, the growing North Korean nuclear threat may well embolden North Korea's use of its OWMD and cyber capabilities, an effect usually referred to as

[1] This chapter was prepared by Bruce Bennett and Choi Kang.

[2] Lawrence Freedman, *Britain and Nuclear Weapons*, London: Macmillan for RIIA, 1980, p. 27.

the "nuclear shadow."[3] In addition, the increasing number of North Korean nuclear weapons and appropriate delivery means increases the likelihood of North Korea's employing nuclear weapons. Nevertheless, this chapter does not examine the full details of North Korean nuclear weapon use, which is discussed in more detail in the predecessor to this report.[4]

Projecting North Korean Weapons of Mass Destruction and Cyber Employment

While North Korea appears to have the OWMD and cyber capabilities described in Chapters 2 through 5, its use of those capabilities may be limited by what it can actually (not just theoretically) do and what it wishes to do with the capabilities. We address these issues here.

What Can North Korea Do with Its Other Weapons of Mass Destruction and Cyber Capabilities?

There is relatively little concrete information on North Korean OWMD and cyber capabilities. While the North may be able to carry out very limited attacks with its OWMD capabilities, it may lack sufficient OWMD to do major attacks or nationwide attacks against the ROK or other neighbors despite current open assessments. It could also make a mistake such as the Aum Shinrikyo did in the early 1990s, acquiring and working with a vaccine strain of anthrax rather than the lethal strain.[5] And the North might not have the types or capacity of the means to deliver its OWMD. With its cyber capabilities, the North may be able to carry out basic hacking but lack the capability to carry out far more sophisticated attacks against well-defended computer systems. And even the North may not know for sure what it can do with the capabilities it has developed. For example, it may think it has many missiles for delivering chemical, biological, and nuclear weapons, but there could be fundamental flaws in the North's missile designs that would lead to many missile failures when a larger number of launches are tried simultaneously as opposed to when a few launches are done as a test after the missiles have been checked and prepared for the tests.

Ultimately, what North Korea can do is an issue of confidence. For example, North Korea is testing ballistic missiles in peacetime because it wants to use those tests to establish the importance of North Korean empowerment both internally and externally, and it is fairly confident that most of those tests will succeed. Alternatively, North Korea has not invaded the ROK because it is not at

---

[3] For example, as part of his invasion of Ukraine, Russian leader Vladimir Putin has threatened that any NATO intervention could lead to Russian nuclear weapon use. And that threat has severely limited NATO action. If Putin eventually uses CW, he may well threaten again that any NATO response would lead to Russian nuclear weapon use, something none of the NATO countries want. For more on the nuclear shadow, see, for example, Estes, 2020.

[4] Bennett et al., 2021.

[5] Philipp C. Bleek, "Revisiting Aum Shinrikyo: New Insights into the Most Extensive Non-State Biological Weapons Program to Date," Nuclear Threat Initiative, December 10, 2011.

all sure its weapons will make enough difference to allow it to defeat ROK-U.S. forces. In such an invasion, if North Korean BW cannot sufficiently suppress air operations from airfields in the ROK and its CW cannot cause enough damage to the ROK-U.S. ground forces, the North's invasion could very well fail and lead to the destruction of the regime. And that outcome would be unacceptable because regime survival is the regime's primary objective. As another example, North Korea has demonstrated that it has a fairly high degree of confidence in its cyber capabilities, which it has used extensively for intelligence gathering and financial purposes, but it could be very uncertain about its ability to cause major cyber damage to the ROK-U.S. militaries or societies.

North Korea can enhance its confidence in using its OWMD and cyber capabilities in several ways. One way is to increase the quantity and quality of those capabilities, so that even if some attacks fail or are not as effective as expected, the overall regime objectives for using these weapons can still be achieved. Another approach is to perform more extensive operational testing of these capabilities. Traditionally, the North Korean military-industrial complex has tested weapons for developmental purposes but did not require operational testing.[6] But North Korea's recent testing of its ballistic missiles appears to have added operational testing.[7]

Achieving Synergistic Effects

North Korean WMD and cyber threats can have various synergistic effects that will affect peacetime and conflict more seriously. These vary from physical effects to psychological and financial effects. Some examples of actions and effects are as follows:

- North Korean cyber and EMP attacks could disrupt C4I systems, making it more difficult to respond to and recover from WMD attacks
- North Korean cyber and EMP attacks could deny warning of WMD attacks and disrupt defenses against these attacks, making the WMD attacks more effective
- North Korean cyberattacks could steal money from other countries and use that money to enhance North Korean WMD capabilities
- North Korean nuclear weapon attacks could expose people to radiation and physical trauma, leaving them more vulnerable to chemical and biological weapons effects
- North Korean use of some BW can have the effect of suppressing the immune system, making people more vulnerable to chemical or nuclear weapon attacks
- North Korean WMD attacks could make it difficult or impossible to gain access to where WMD damage has been done, exacerbating the rescue and recovery effort
- North Korean WMD attacks would cause psychological effects that would only be compounded by subsequent WMD attacks.

We expect that North Korea will seek to maximize these and other synergistic effects.

---

[6] Developmental testing examines whether or not a weapon system being developed will actually function as expected. Operational testing examines whether weapon production provides weapons that actually work and can be used effectively by their military forces. The North Korean focus on developmental testing was described in 2017 by a North Korean escapee who had been a senior leader in the North Korean military industrial complex.

[7] See, for example, Chaewon Chung, "North Korea Fires Two Presumed Ballistic Missiles Toward the East Sea: JCS," *NKNews*, January 27, 2022.

Would North Korea Be Willing to Employ Its Other Weapons of Mass Destruction and Cyber Capabilities?

Most countries look at the employment of their military capabilities from a benefits and costs perspective. When countries perceive that there are clear benefits to gain that are greater than the potential costs associated with obtaining those benefits, they are often inclined to employ their military forces. Still, major war on the Korean peninsula has been avoided in recent decades, suggesting that North Korea lacks confidence in achieving more benefits than costs in such wars. For example, North Korea's apparent belief that an invasion of the ROK would be defeated (not providing the benefit of the North controlling the ROK) and would lead to the destruction of the North Korean regime (an absolutely unacceptable cost) has probably contributed to deterrence on the Korean peninsula. But many North Korean provocations have not been deterred (including 13 days with a total of 20 or so missile launches from January through April 2022). In April 2021, President Biden had promised "stern deterrence" of North Korea,[8] but the United States apparently failed to make threats adequate to deter these North Korean provocations.

And deterrence is not static, so North Korea has sought more powerful military capabilities that might give it an ability to conquer or at least influence the ROK. Nevertheless, deterrence still holds because the North apparently perceives that it still lacks the military capabilities needed. The ROK-U.S. can enhance deterrence of a North Korean invasion by some combination of fielding capabilities to (1) reduce the likelihood that North Korea could gain a victory while (2) enhancing the ability to punish North Korea if it does invade the ROK (and regime destruction is the most serious punishment that the ROK-U.S. could impose on the North Korea regime). The ROK Ministry of National Defense's "three axis system" (now called the "WMD response system") follows this framework by applying denial through the "kill chain" (counterforce operations) and Korean air and missile defense while applying punishment through "Korean Massive Punishment and Retaliation."[9]

Deterrence is complicated by the uncertainties in the benefits and costs, by circumstances surrounding the action, by the willingness of the parties to take risks, and because any given action might actually become a chain of actions. Leaders who contemplate waging war, for example, are seldom assured of victory but may face circumstances in which the status quo appears even more risky than war (for example, if Kim senses that the North Korean regime is on the verge of collapse). Alternatively, the United States is often reluctant to militarily respond to North Korean limited attacks, fearing that the North might then escalate and cause serious societal damage; North Korea often recognizes this U.S. reluctance. In the end, many

---

[8] *Washington Post* Staff, "Read President Biden's First Address to a Joint Session of Congress," *Washington Post*, April 28, 2021.

[9] ROK Ministry of National Defense, *2020 Defense White Paper*, December 31, 2020, p. 76.

experts argue that deterrence is "in the eye of the beholder" and that the risk-taking propensity of an actor such as North Korea may reduce ROK-U.S. deterrence.

Note that the willingness to use military force applies two ways. That is, the ROK-U.S. must be prepared to use military force to impose sufficient costs on North Korea or North Korea will not be deterred. In trying to deter North Korean use of WMD, the United States has committed a nuclear umbrella to its ROK ally, effectively promising to use nuclear weapons if needed in response to North Korean nuclear weapon employment and potentially OWMD employment. This deterrent threat has been expressed as follows:

> Our deterrence strategy for North Korea makes clear that any North Korean nuclear attack against the United States or its allies and partners is unacceptable and will result in the end of that regime. There is no scenario in which the Kim regime could employ nuclear weapons and survive.[10]

Since the regime will almost certainly hide in deep underground facilities in any major war, and since those facilities can only be destroyed with nuclear weapons,[11] this is effectively a commitment of a U.S. nuclear response to North Korean nuclear weapon use.

Kim Jong-un understands this threat and is building ICBMs that will carry nuclear weapons to target the United States. He apparently hopes that by threatening a few U.S. cities with nuclear weapons, he can get the United States to abort its "nuclear umbrella" commitment to the ROK. To sustain the U.S. deterrent against North Korean nuclear weapon use, the United States must demonstrate a willingness to execute a nuclear retaliation against North Korea in response to any North Korean nuclear weapon use. Without such a U.S. commitment, North Korea may perceive that the United States lacks the will to use nuclear weapons against North Korea in such a case, and therefore Kim Jong-un may conclude that there would be no major cost to his nuclear weapon use, leading to a classical failure to deter North Korea.[12]

North Korean Peacetime Uses of Other Weapons of Mass Destruction and Cyber Capabilities

North Korea seeks to deter ROK-U.S. military intervention that might (1) depose the North Korean regime, (2) destroy key North Korean military capabilities, or (3) retaliate against and/or punish North Korean provocations. An expert familiar with North Korean thinking explained:

---

[10] Department of Defense, *Nuclear Posture Review Report*, February 2018, p. 33.

[11] National Research Council of the National Academies, 2005, p. 1.

[12] While deterrence is a major constraint on North Korean willingness to employ its OWMD and cyber capabilities, there can be other reasons why North Korea would constrain this employment. For example, Kim Jong-un might conclude that he must follow his father's proscription of war, in part because a North Korean conquest of the ROK would open North Korea to an immense flow of outside information that could seriously jeopardize the Kim regime. Alternatively, Kim might decide that the use of a contagious biological weapon such as smallpox is too dangerous because it could spread back into North Korea and have far more lethal effects in the North because of the poor health system there.

"The DPRK views its unconventional arsenal primarily as a means of deterrence, believing that as long as it is able to 'inflict pain' on the United States, the ROK, and Japan, the United States will be deterred from attacking the DPRK."[13] And the North's WMD offers very effective means for inflicting pain on the United States and its allies. The regime has been very clear that it views nuclear weapons as a "'powerful treasured *sword* to protect the sovereignty of the country and the dignity of the nation and provides a sure *guarantee* for focusing efforts on preserving peace and security, building economy and improving the standard of the people's living.'"[14] Of course, by "protect the sovereignty of the country," the regime means regime survival and continued control. In short, the North views its nuclear weapons as playing a major strategic deterrence role in peacetime.

The North does not speak similarly of CW and BW. Nevertheless, the North's OWMD and even conventional military capabilities play a role in deterring ROK-U.S. attacks on North Korea. The ROK-U.S. have feared that even limited military responses to North Korean provocations or attacks (such as the sinking of the ROK warship *Cheonan* or the North Korean shelling of Yeonpyeong Island) could lead to an unacceptable North Korean military response that causes ROK-U.S. casualties and could spiral into a major war with massive casualties. This view reflects the ROK-U.S. reluctance to risk even a few casualties.[15]

Kim Jong-un has also been a risk-taker with some of his military forces in peacetime, though most of the risks he takes are at the low end of escalation. Moreover, they are often risks he has taken before without facing significant costs, and thus he seems confident that he can get away with taking these risks again. For example, Kim has committed dozens of ballistic-missile test provocations despite multiple UN Security Council Resolutions prohibiting these tests. But in doing so, he has significantly limited the tests of ICBMs, clearly understanding that those tests could lead to a U.S. response, whereas according to both the Trump and Biden administrations, short-range missile tests posed no immediate threats to the United States or its allies.[16] In fact, Kim is fairly expert at testing the thresholds of escalation and of conditioning outside responses, apparently attempting to demonstrate his empowerment, especially for internal audiences, and allow his military to test developing weapons without suffering consequences.

Thus, Kim has had his hacker forces actively involved in cyberattacks for years and has apparently gotten away with many of them. In response to the 2014 hack of Sony Pictures, President Barack Obama promised an "appropriate and proportional" response.[17] But in

---

[13] Bermudez, 2000, pp. 193–194.

[14] Alexandre Y. Mansourov, *Kim Jong Un's Nuclear Doctrine and Strategy: What Everyone Needs to Know,* Berkeley, Calif.: Nautilus, December 16, 2014. Emphasis in original.

[15] See, for example, Andrei Lankov, "How to Stop the Next Korean War," *Foreign Policy*, December 16, 2010.

[16] David E. Sanger and William J. Broad, "North Korea Missile Tests, 'Very Standard' to Trump, Show Signs of Advancing Arsenal," *New York Times*, September 2, 2019; "North Korea Tests Longest-Range Missile Since 2017," NPR, January 29, 2022.

[17] Devin Dwyer and Mary Bruce, "Sony Hacking: President Obama Says Company Made 'Mistake' in Canceling 'The Interview,'" *ABC News*, December 19, 2014.

practice, it does not appear that the United States carried out his threat, likely undermining some future deterrence efforts. Still, North Korea has mainly pursued a fairly low level of cyberattacks, recognizing that disabling power grids or causing the failure of a nuclear reactor could well be treated by the ROK-U.S. as an act of war to which they would respond strongly.

Table 6.1 summarizes North Korea's recent peacetime use of OWMD and cyber capabilities (green shading), and our assessment of the relative likelihood of future uses in conditions short of a major war (yellow, orange, and red shading). North Korea has reportedly tested CW and BW effects on people and attempted several assassinations with CW.[18] Moreover, the assassination of Kim Jong-nam was committed in Malaysia, probably reducing the chances of a ROK-U.S. retaliation. North Korea has not tested its nuclear EMP capabilities, but we do not know if North Korea has tested any conventional EMP capabilities. There appears to be no peacetime history of combined use of multiple types of OWMD simultaneously, probably because such actions would be too escalatory. Nevertheless, the ongoing North Korean use of its cyber capabilities has allowed North Korea to collect intelligence and steal billions of dollars of hard currency denied by UN/U.S. sanctions (part of which will fund WMD and missile development),[19] while causing some damage and disruptions in an increasingly cyber-oriented world and bringing a different kind of warfare

Table 6.1. North Korean Peacetime and Crisis Employment of Other Weapons of Mass Destruction and Cyber Weapons

Weapons	Weapon Tests	North Korean Targeting of			
		Individual	Small Group/Area/Firm	Large Group/Area/Firm	Nationwide
Chemical	On prisoners	Kim Jong-nam, 2017 Park Sang-hak, 2011	Possible—toxic industrial chemicals?	Too high a risk of serious retaliation, escalation?	Inappropriate: insufficient chemicals, delivery means
Biological	On islands, on prisoners	Possible; Soviets and Bulgarians have without U.S. retaliation	Possible—use endemic disease?	Possible but risky; would likely try to deny attribution	Possible with contagious disease; very risky
EMP	Conventional EMP possible	Possible with isolated individual, conventional EMP	Possible: conventional EMP, not nuclear EMP	Possible with nuclear EMP but very risky	Possible with nuclear EMP but extremely risky
Cyber	→	Ongoing stealing of cryptocurrency, hacking computers	Ongoing stealing of cryptocurrency	Sony 2014, Bangladesh Bank 2016	WannaCry 2017

SOURCES: Authors' assessment based on analysis of sources cited in this chapter, as well as Bruce W. Bennett, *The Challenge of North Korean Biological Weapons*, Santa Monica, Calif.: RAND Corporation, CT-401, 2013a.
NOTE: Green = the North has done this. Yellow = a possible use. Orange = a possible but dangerous use. Purple = not possible or too dangerous.

[18] Julian Ryall, "North Korean Defector Details 'Human Experiments,'" DW, December 30, 2014; Caudle, 1997; Richard C. Paddock and Choe Sang-Hun, "Kim Jong-nam Was Killed by VX Nerve Agent, Malaysians Say," *New York Times*, February 23, 2017.

[19] Nichols, 2019.

even to periods of "peace."[20] Still, North Korea has sought plausible deniability in its cyberattacks and limited its extreme cyberattacks (in some cases, perhaps to reserve major attacks to be a surprise in a war, as discussed below), presumably seeking to avoid ROK-U.S. retaliation.

We expect that North Korea will largely follow these historical precedents because it knows it has avoided serious consequences in doing so. In this regard, its employment of CW in assassinations appears to reflect a desire to demonstrate empowerment, as well as a perception that very limited CW employment appears very powerful but less likely than even very limited BW employment to cause a serious ROK-U.S. retaliation. While North Korea reportedly believes that CW is not WMD,[21] the North's general avoidance of CW employment in peacetime compared with more common conventional weapon attacks suggests that the North recognizes CW employment as posing a much greater risk of a serious ROK-U.S. response. North Korea could carry out a terrorist CW attack such as the Aum Shinrikyo did on the Tokyo subway system in 1995, but it seems unlikely that North Korea would perceive a significant benefit from doing so, and it could risk serious retaliation. As noted in Table 6.1, North Korea might execute a covert conventional weapons attack against a ROK toxic industrial chemical production facility to cause CW-like casualties, analogous to the way that a toxic gas leak at Bhopal, India, in 1984 killed thousands of people and injured hundreds of thousands.[22] It might be difficult to determine whether such a spillage was an accident or purposeful and thus whether to execute a ROK-U.S. response.

Any North Korean provocation poses the risk of causing unintended escalation. Thus, in 2010 when North Korea shelled the ROK's Yeonpyeong Island, the ROK prepared to escalate by striking North Korean missile bases, and it was feared that North Korea would escalate in response. At the time, one article said: "Diplomats and analysts in Washington and elsewhere around the world warned that while neither the North nor the South wanted all-out war, the risk of incidents such as today's was that it could tip the peninsula into an accidental war."[23] Situations such as this could lead to limited OWMD attacks as a next or subsequent escalation step. Avoiding any North Korean provocations is thus critical to avoiding escalation to OWMD use—an escalation that the North Korean "nuclear shadow" potentially makes more likely. It is possible that future ROK-U.S. leaders will be as risk averse as past leaders relative to escalation with North Korea, though they may also conclude that a failure to respond adequately to North Korean provocations also makes war more likely. Kim will likely perceive a bias toward caution by ROK-U.S. leaders; if instead these leaders decide that adequate responses are required, they need to pose clear threats to North Korea and make it also clear that they have the will to execute those threats.

---

[20] See Chapter 5.

[21] "Nuclear Nightmare," 2003.

[22] "What Was Bhopal Gas Tragedy?" *Business Standard*, undated.

[23] Branigan and MacAskill, 2010.

North Korean Uses of Other Weapons of Mass Destruction and Cyber Capabilities in Crisis or Limited Conflict

In a future situation in which the North Korean regime perceives that it is facing a crisis or limited conflict, North Korea may decide to be more aggressive with its military capabilities, though still being careful with its OWMD and cyber capabilities. For example, if the regime perceives that internal instability is growing, it might decide to attack a ROK warship or fire artillery at a ROK island, as it did in 2010. Still, we have heard from several senior ROK military personnel that artillery firing into Seoul is a redline that would be treated by the ROK as the start of a major war. This could be an exaggeration, but the risk to the North Korean regime of firing on Seoul or using OWMD is clearly greater than the risks it faced in its 2010 conventional attacks; this means that North Korea would require some significant increase in the benefits it seeks to justify taking such risks. That said, if the regime can be confident that an attack will be plausibly deniable, the risk to the regime would be significantly less. Thus, according to Table 6.1, North Korea could consider using special forces or North Korean agents in the South to cause a covert release of toxic industrial chemicals or spread a limited amount of an endemic disease such as KHF. But such plausibly deniable uses would limit the benefit of those attacks for building the appearance of regime strength. Alternatively, North Korea could seek to use a ballistic missile carrying a conventional warhead to damage ROK toxic chemical facilities or a nuclear power plant, potentially releasing lethal chemicals or a radioactive cloud but hoping to avoid a U.S. nuclear response. Such a serious act of war could lead to a ROK-U.S. preemptive counterforce attack on North Korea even if the United States chose not to execute a nuclear weapon response.

Unfortunately, at some future time North Korea may conclude that it can return to more frequent limited attacks on the ROK. Two factors could potentially lead to such a decision. First, the growing North Korean nuclear weapon inventory may convince the North Korean regime that it could avoid retaliation against its limited attacks (perhaps even OWMD) by threatening to escalate to nuclear weapon use against any ROK-U.S. retaliation—another effect of the so-called nuclear shadow. Second, if the North Korean regime perceives that it is increasingly challenged by internal instability, it may conclude that it needs success in limited attacks to motivate greater support for the regime besieged by claimed ROK-U.S. aggression and thereby manage its internal instability. Still, the North Korean regime could fear that threatening nuclear weapon use might not deter a major ROK-U.S. retaliation against a large or perhaps even a small attributable North Korean OWMD attack, and that would be even more true if North Korea used multiple types of OWMD. In considering limited attacks on the ROK, the trade-off between the risks of escalation and the potentially greater damage caused by OWMD would be key to the North determining whether to use OWMD.

North Korean Uses of Other Weapons of Mass Destruction and Cyber Capabilities in Major War

We postulate above that Kim Jong-un would prefer to avoid a major war with the ROK-U.S. But if Kim felt that internal instability was seriously jeopardizing the regime, he might consider a major war as a way of unifying his elites and diverting attention from the regime's failings. Much of the examination of a major war in Korea focuses on a purely conventional war, in which, as noted in Chapter 2, U.S. commanders in Korea have consistently argued that victory would be easily within their grasp.[24]

It should therefore be no surprise that for decades, North Korea has sought WMD and cyber capabilities to augment conventional military capabilities in an invasion of the ROK. Kim Jong-un has developed a fairly significant nuclear arsenal. Soon after his father's death, he reportedly ordered his military to prepare a new war plan for rapidly taking control of Seoul and all of South Korea, a plan that he approved in 2012. This plan included the use of nuclear weapons and all elements of North Korean national power, including OWMD and conventional forces, to establish control over the ROK and achieve North Korea–controlled unification.[25] Conceptually, this plan would be executed in three phases: (1) North Korean mobilization and alerting for war accompanied by selective precursor attacks, (2) the North Korean main attack and follow-up, and (3) North Korean attacks designed to stop the conflict before regime destruction, should the war go badly for North Korea. North Korea could also have to plan to deal with Chinese intervention.

North Korean Preparations for Major War

As noted in previous chapters, North Korea feels that surprise is critical to a successful outcome of an invasion of the ROK. It apparently hopes that surprise will delay and disrupt ROK-U.S. defensive preparations before an invasion while allowing many of the North Korean preparations. The North would especially like to delay the deployment of U.S. forces to the peninsula. The North may try to delay ROK-U.S. preparations by making it appear that the North's preparations are only to put pressure on the ROK-U.S., claiming that any ROK-U.S. preparations would precipitate a war that could be otherwise avoided. Alternatively North Korea could adopt a subterfuge such as claiming that it has detected covert ROK-U.S. preparations to invade the North and that the North is simply activating its defenses to deter the ROK-U.S. aggression (as it has claimed before).

As part of its preparations, the North may consider precursor attacks to undermine the strength of ROK-U.S. forces. As long as these attacks are not immediately detectable or are plausibly deniable, the ROK-U.S. may not retaliate. If they do retaliate, North Korea may lose any advantage

[24] See, for example, Abrams, 2021, p. 13; and Schwartz, 2002, p. 10.

[25] Jeong Yong-soo and Ser Myo-ja, "Kim Jong-un Ordered a Plan for a 7-Day Asymmetric War: Officials," *Joongang Daily*, January 7, 2015.

from these precursor attacks. This is especially true because any North Korean attack would constitute an act of war. And North Korean WMD precursor attacks could justify a ROK-U.S. counterforce attack on North Korea, which would seriously defeat key elements of the overall North Korean offensive. ROK-U.S. ballistic missiles can be delivered against North Korean targets so rapidly in the counterforce role that the North would probably decide to delay its CW, nuclear, and EMP attacks until the beginning of its full offensive because these could be detected and attributed and risk a ROK-U.S. counterforce response. Use of these weapons could be interpreted as a precursor attack rather than an isolated limited attack, especially in the context of other North Korean preparations for war. The ROK-U.S. could begin preparation to preempt the North's main attack even during ambiguous warning of war,[26] including alerting and targeting missiles, preparing combat aircraft, putting U.S. bombers on airborne alert over neighboring sea areas, and surging U.S. air and naval forces to the peninsula.

But North Korea could be expected to carry out cyber precursor attacks and possibly also BW precursor attacks. The North would have to be careful with its cyberattacks not to take an action that is so serious that the ROK-U.S. would interpret that as unambiguous evidence that a war is starting. North Korea may also be able to use BW in precursor attacks if it can avoid detection of the BW and if the incubation period of the BW delays the disease effects until after the start of the North Korean main assault. Nevertheless, North Korea would be taking a risk even with these precursor attacks: An astute ROK-U.S. C2 system may detect even these attacks as precursors and escalate to a counterforce attack.

CW attacks and more extensive BW attacks and cyberattacks designed to cause high damage might be used selectively in the last ten to 20 minutes before the main North Korean attack, as these would establish a condition of war and trigger a counterforce attack[27]—but ten to 20 minutes might be too little for the ROK-U.S. to put most weapons on target in North Korea before the North would launch its main attack. These North Korean attacks would be designed to shatter ROK-U.S. C2, create chaos and panic in both the ROK-U.S. military and society, break the cohesion of the ROK ground forces so that the main North Korean ground attack could rapidly achieve multiple exploitable breakthroughs, and delay the arrival of U.S. forces in Korea. In addition, North Korean strategic special forces could target the various missile defense batteries in the ROK using mortars, large-caliber sniper rifles, and drones from standoff positions. These attacks would then facilitate the delivery of the North's WMD.

---

[26] The word "preemption" here is not adequately precise. A classical preemption would have the ROK-U.S. launch a counterforce strike because North Korea is clearly preparing for war. But preemption in the case discussed in the text would actually be in response to North Korea starting the war with precursor attacks, causing the ROK-U.S. to attack before the North Korean main attack but in response to the North Korean precursor attacks.

[27] As noted in Chapter 4, an EMP attack over the ROK could also affect electronic systems in North Korea. If the North wanted to achieve broad EMP effects over the ROK, it would need to turn off and shield its own electronics for the period of EMP effects and then launch its major attack. But the timing would be sensitive, and a timing failure could lead to the North's own EMP degrading the North Korean main attack—a serious risk.

North Korean Execution of a Major War

North Korea is unlikely to withhold any of its WMD from its main attack against the ROK-U.S.[28] Any WMD that it withholds would be subjected to an early ROK-U.S. counterforce attack, potentially destroying much of it. Thus, the ROK-U.S. counterforce capability has three effects: (1) It makes many North Korean precursor attacks too risky, (2) it forces North Korea into a "use it or lose it" position with regard to its WMD forces, and (3) it makes the historical North Korean strategy of building several missiles per TEL a risky approach, but nevertheless something North Korea might do because of limited financial resources. Still, North Korea may have historically planned for a secure reserve force of missiles and nuclear weapons. Today, it could well lose this force early in a war unless it denies information about it to the ROK-U.S.

The North Korean main attack would involve six components. First, North Korean artillery, including CW use, would seek to expand the chaos caused by the precursor attacks in the forward ROK-U.S. ground forces, allowing the North Korean infantry to create rapid breakthroughs. It could use a mixture of a nonpersistent CW (sarin would be best) to disrupt the forward forces but allow North Korean forces to proceed into those areas within an hour or so. It could use a persistent CW (VX would be best) to protect the flanks of the North Korean penetration.[29] If each of the 7,000 or so forward-deployed North Korean artillery pieces fired just an average of 50 shells or rockets in the first hour, that would amount so some 350,000 total shells and rockets. If, as argued in Chapter 2, one-third of North Korean artillery shells and rockets were to carry CW and the average shell/rocket carried 3 kg of CW, that would amount to some 400 tons of CW delivered in the forward ROK area in the first hour—enough to cause massive damage, cohesion failures in many ground force units, and many initial breakthroughs. simultaneously, North Korean tactical special forces that were positioned in tunnels under the DMZ would break out of those tunnels, attack any cohesive defenders, and lead the North Korean infantry through defensive gaps.

Second, after North Korean infantry opened breakthroughs of modest (5 to 10 km) depth, the North Korean heavier forces would seek to exploit these breakthroughs, rapidly moving through any gaps that develop and racing to capture and destroy ROK-U.S. military forces and facilities in

---

[28] Under Kim Jong-il in the 1990s, North Korea had apparently concluded that it could mount a conventional attack on the ROK that also used CW, expecting that such an attack might succeed and would not lead to a U.S. nuclear response. The ability to avoid a U.S. nuclear response was confirmed by the insufficient international responses to the chemical weapons use by Iraq in the 1980s and in Syria in the 2010s. The growing ROK-U.S. counterforce capability makes this North Korean strategy a losing proposition. See Bermudez, 2000, p. 194; Ted Regencia, "Chemical Attacks on Iran: When the US Looked the Other Way," *Al-Jazeera*, April 19, 2018; "The United States estimates that the Assad regime has used chemical weapons against the Syrian people at least 50 times since the conflict began." While this State Department declaration talks of future accountability for the Assad regime, uncertain future accountability is unlikely to appear as much of a cost to Assad. Ned Price, "Syria: Eighth Anniversary of the Ghouta Chemical Weapons Attack," Washington, D.C.: U.S. State Department, August 21, 2021.

[29] As discussed in Chapter 2, CW would be best if used against ground forces in the forward areas because it would affect smaller, more controlled areas than BW, would promptly affect the military personnel, and would also be effective against any gaps in the protective clothing or the soldiers. In contrast, most BW would take days to incubate and affect the troops and would need to be inhaled (thus, a good mask would provide effective protection for ROK soldiers); a wind shift could also blow a substantial amount of BW back over the North Korean forces.

the rear. In addition, to widen the breakthrough and dissolve still-coherent forward ground forces, North Korean artillery fire, including nonpersistent CW (possibly on flechettes), could move down the defensive lines from the breakthroughs to cause casualties and panic. North Korean infantry and some special forces could move immediately behind the forward defensive lines to roll up any of those defenses not broken by artillery fire and panic. Some North Korean artillery fires (including CW) would shift to ROK-U.S. ground force reserves and to ROK-U.S. artillery units in an effort to suppress them. Some North Korean special forces would be assigned to attack the ROK forward artillery shelters to disable the fire of those units possibly using fuel-air explosives (thermobaric weapons). Other North Korea special forces would seek to locate ROK-U.S. self-propelled artillery units to facilitate North Korean fires against them.

Third, the ROK has focused much of its military force modernization on the development of advanced fighter aircraft capable of interdicting North Korean ground-force breakthroughs. The ROK-U.S. fighter forces in the ROK are located on a small number of military airfields, making those airfields valuable targets of the North Korean ballistic missiles carrying nuclear weapons. These airfields could also be targeted by ballistic missiles carrying CW, strategic special forces and agents employing BW, and North Korean drones carrying BW and fuel-air explosives. The use of redundant attacks would seek to ensure serious damage or destruction of the air forces and personnel on these airfields.

Fourth, similar North Korean forces would be used against ROK-U.S. C2 facilities in order to try to further degrade the C2 that had been targeted by precursor attacks.

Fifth, the North would want to degrade the flow of U.S. forces to Korea. It could do so by damaging and/or contaminating the planned reception airfields and ports in the ROK with nuclear weapons delivered by ballistic missiles, persistent CW (such as VX) delivered by missiles and drones, and persistent BW (such as anthrax) delivered by SOF and drones. As noted in Chapter 3, North Korean use of BW could cause psychological effects more serious than even the physical casualties, with other countries closing their borders to the ROK, the United States being unwilling to flow forces or personnel into the ROK, and chaos within the ROK resulting from fear of BW. The North could also execute attacks against Japan using nuclear weapons, EMP, and BW delivered by missiles and cyber warfare. And the North could threaten nuclear and BW attacks on the United States if U.S. deployments continue and seek to coerce the United States into abandoning the ROK.

Sixth, North Korea would reportedly also target U.S. populations in the ROK (especially Camp Humphreys[30]) with similar means (nuclear weapons, CW, and BW) also seeking to coerce U.S. disengagement from its alliance with the ROK. The North apparently believes that killing thousands of American military personnel and civilians in Korea would cause the United States to abandon

[30] North Korea has designated Camp Humphreys as "our military's foremost strike target." Park Won Gon, "Strategic Implications of the USFK Relocation to Pyeongtaek," Seoul, South Korea: Korea Institute for Defense Analyses, No. 164, October 20, 2017, p. 4.

the ROK and withdraw U.S. forces, decoupling the ROK-U.S. alliance and allowing the North a rapid victory against the ROK[31] without the North facing a serious U.S. nuclear retaliation.[32] Such North Korean hopes could be a significant miscalculation: the U.S. people could still demand the end of the North Korean regime. North Korea would probably attempt to deter U.S. nuclear weapon use by threatening to retaliate against U.S. cities with ICBMs carrying nuclear weapons.[33] This potential would provide the United States with strong incentives for preemptive counterforce and counter-leadership attacks.

North Korea apparently hopes to cause so much damage and chaos with its precursor attacks and the invasion main attacks that the North would gain a substantial margin of military superiority over the ROK and perhaps even gain the ability to dictate ROK surrender.

Regime Survival After a North Korean Invasion of the Republic of Korea Is Stopped

North Korea knows that any invasion of the ROK would be highly risky and could fail. The regime would therefore likely keep a reserve of WMD forces intended to degrade ROK-U.S. capabilities and coerce war termination once the North recognizes that its invasion is failing. The most important elements of this strategic reserve could be ICBMs carrying nuclear weapons and contagious BW, theater missiles with the same payloads, and North Korean special forces infected with contagious BW. North Korea would use the ICBMs to coerce the United States into war termination, potentially issuing a series of threats and then carrying out attacks on the United States if it fails to yield to the threats. The North would use its theater missiles to coerce ROK termination and also to put pressure on Japan not to support the United States. The North could use its own personnel infected with contagious BW to expose many people in the ROK, Japan, or the United States, trying to create chaos and a strong desire in the targeted countries to terminate the conflict before destroying the regime. North Korea could also use its strategic reserve nuclear weapons in an attempt to deter U.S. employment of nuclear weapons against the North.

North Korea's strategic reserve of WMD would have a major problem: Survival until its employment is required. North Korea could not hold just three to five nuclear weapons to serve as

---

[31] According to a senior North Korean military escapee: "Some Americans believe that even if North Korea possessed the ability to strike the United States, it would never dare to because of the devastating consequences. But I do not agree with this idea. . . . Kim Jong-il believes that if North Korea creates more than 20,000 American casualties in the region, the U.S. will roll back and the North Korea will win the war." U.S. Senate, "North Korean Missile Proliferation," Hearing Before the Subcommittee on International Security, Proliferation, and Federal Services of the Committee on Governmental Affairs, Washington, D.C., October 21, 1997, p. 5.

[32] While some in the United States might be inclined to support U.S. withdrawal in those circumstances, setting such a precedent would probably destabilize global peace and lead to widespread nuclear weapon proliferation, something the United States would be extraordinarily foolish to do.

[33] North Korea has already fielded ICBMs that might be able to reach the United States. See Joseph S. Bermudez, Jr. and Victor Cha, "Undeclared North Korea: The Yusang-ni Missile Operating Base," *Beyond Parallel*, May 9, 2019. The North has also completed a second ICBM base to increase its ICBM threat. See Joseph S. Bermudez, Jr., Victor Cha, and Jennifer Jun, "Undeclared North Korea: The Hoejung-ni Missile Operating Base," *Beyond Parallel*, February 7, 2022.

a nuclear reserve force because many of those weapons could be destroyed as a result of the initial and subsequent ROK-U.S. counterforce attacks. In practice, North Korea might want to hold as much as a third of its nuclear weapon and BW forces as a strategic reserve in order to sustain its reserve through major combat, but even then, little or none of the force might survive for a conflict-ending operation. North Korean CW could lack sufficient power to be a meaningful part of this strategic reserve, and any nuclear weapons withheld could be best employed directly against targets rather than used to cause EMP. North Korean cyber forces might retain some capability as a strategic reserve, though they would need to be able to cause major damage to the ROK-U.S. to play a meaningful role.

Seeking to Counter Chinese Intervention

Chinese leader Xi Jinping has been very clear "that China would 'absolutely not permit war or chaos on the [Korean] peninsula.'"[34] To support Chinese security, China reportedly has plans to intervene in North Korea in the case of war on the peninsula or a North Korea collapse.[35] If China does intervene in North Korea without a North Korean invitation, it is possible that North Korea could also employ its WMD and cyber capabilities to counter such an intervention. Despite this possibility, China has generally avoided putting pressure on North Korea to restrict its nuclear weapon development, apparently believing that North Korean denuclearization can occur only when outside threats against North Korea are reduced.

Proposed Republic of Korea and United States Responses

Based upon available open information, we believe that there are many actions that the ROK-U.S. can take to deter North Korean employment of OWMD and cyber capabilities and to counter that employment if deterrence fails. With regard to the individual types of OWMD and cyber capabilities, Chapters 2 through 5 offer many recommendations especially focused on defending against North Korean OWMD and cyber employment, and those recommendations will not be repeated here except where there is synergy between actions taken against the different kinds of OWMD. Instead, this section focuses on imposing costs in peacetime in response to North Korean OWMD and cyber activities and provocations, and appropriate warfighting (denial) in wartime against OWMD and cyber employment. Because cyberattacks are in many ways separate from OWMD attacks, most of the material on countering North Korean cyberattacks is found in Chapter 5.

---

[34] Michael Auslin, "In Search of the Xi Doctrine," War on the Rocks, May 30, 2016.

[35] Bonnie Glaser, Scott Snyder, and John S. Park, *Keeping an Eye on an Unruly Neighbor: Chinese Views of Economic Reform and Stability in North Korea*, Washington, D.C.: Center for Strategic and International Studies and U.S. Institute of Peace, January 3, 2008, p. 19. China has even threatened to bomb North Korea's nuclear facilities if North Korea is too aggressive. See Tyler Durden, "China Threatens to Bomb North Korea's Nuclear Facilities If It Crosses Beijing's 'Bottom Line,'" Zero Hedge, April 11, 2017.

Peacetime Responses

In peacetime, North Korean provocations pose a risk of escalation to war, including WMD use. And North Korean provocations such as missile and nuclear weapon tests facilitate the growth in North Korean WMD threats—something the ROK-U.S. want to prevent. The ROK-U.S. face three challenges in responding to North Korean provocations. The first, especially true with North Korean cyberattacks but potentially also with CW and BW employment, is detecting the North Korean attack and attributing that attack to North Korea. The second challenge is finding the means for deterring and responding (should deterrence fail) to all North Korean provocations. The ROK-U.S. must deter direct North Korean employment of its OWMD and cyber capabilities, as well as broader North Korean provocations that could create an escalation spiral to OWMD use and perhaps even general war. The third challenge is preempting North Korean provocations by providing the North more positive means for demonstrating its empowerment.

Recognizing the uncertainties in North Korean strategy and what is required to deter the North, our project compiled a series of actions that could be taken in peacetime. These are offered as options. Many have been discussed with U.S. and ROK government personnel and with North Korean escapees, but the choice among these options would still require a clear ROK-U.S. strategy tailored to the specific conditions in peacetime.

First, some North Korean provocations are relatively easy to detect and attribute. But others are more difficult, especially when North Korea seeks plausible deniability. For example, attribution is a key challenge with cyberattacks and likely would be with OWMD attacks because North Korea would be seeking to avoid a ROK-U.S. response. The ROK-U.S. have worked on improving detection and attribution of OWMD and cyberattacks, but they need to increase these efforts.

Second, preventing North Korean employment of its OWMD and cyber capabilities requires that the ROK-U.S. establish a credible deterrence framework for preventing most North Korean provocations and anything related to OWMD in particular.[36] North Korea must be convinced that the use of OWMD is too dangerous and that even other military provocations should be avoided because of the risk that they could trigger an uncontrolled escalation into OWMD use. This is particularly important because confrontation on the peninsula tends to be escalatory, and North Korea may perceive that it can escalate to OWMD use in challenging the ROK-U.S. because of the North's "nuclear shadow." A framework for deterring North Korean provocations could have ten components, described below.

Establish a Set of Minimum Redlines That Are Clearer and Actionable Against North Korean Provocations

As noted above, the ROK-U.S. have failed to deter many North Korean provocations in 2022 alone. Against whatever of these provocations that the ROK-U.S. find unacceptable, and other

[36] Deterring North Korean cyber provocations is a more difficult task and is addressed in Chapter 5.

escalated North Korean actions such as limited attacks with CW, the ROK-U.S. must define and communicate clear redlines with more specific ROK-U.S. responses threatened that must be credible.[37] Less serious North Korean behavior (e.g., a submarine incursion into ROK waters) might or might not cause a ROK-U.S. offensive response. To deter North Korea, the ROK-U.S. must communicate to the North which of the most serious provocations are unacceptable and the potential consequences that would be imposed for those provocations. And these consequences cannot be idle threats—the ROK-U.S. must have the will to execute them, or future deterrence would be undercut. North Korea has learned that the ROK-U.S. threaten the North with strong rhetoric but are weak on imposing the threatened costs. As a result, this rhetoric has little influence in deterring North Korea. The ROK-U.S. should also be clear that North Korean provocations below the minimum redlines could also lead to real ROK-U.S. responses. Otherwise, the North might feel safe to challenge the ROK-U.S. with provocations below the minimum redlines.

Remove the North Korean Justification for Escalation by Asserting and Demonstrating That South Korea and the United States Are Not Hostile Toward North Korea

This will require the ROK-U.S. to find alternative ways to impose costs on North Korea that are not as escalatory or overly hostile. For example, appropriate ROK-U.S. information operations, the often-neglected component of ROK-U.S. strategy, might appear far less hostile than military attacks or economic sanctions. Thus, the ROK-U.S. could publicly comment on North Korean hostility in indoctrinating its people against the ROK-U.S. and argue that the truly hostile country in Northeast Asia is North Korea. After all, the ROK-U.S. do not indoctrinate their people against North Korea. The ROK-U.S. could also explain that Kim Jong-un is responsible (not the United States) for the suffering of the North Korean people that results from the sanctions imposed by the United Nations. These sanctions could cease if Kim terminated his flagrant violations of conditions set by the United Nations, conditions agreed to by China and Russia. The ROK-U.S. should further explain that North Korea is continually in violation of UN Security Council Resolutions and refuses to recognize the authority of the United Nations.[38]

---

[37] Some in the United States prefer vague threats, often referred to as strategic ambiguity, that they hope will deter Kim Jong-un. But against many provocations, including ICBM and reported hypersonic missile tests, such vague threats have not deterred Kim: He has observed that the ROK-U.S. have not taken action that is unacceptable to him and probably expects that pattern to continue. Only by threatening more serious and substantial consequences that the ROK-U.S. are willing to impose can they expect to deter Kim.

[38] While Kim Jong-un will perceive these information operations as hostile, many in his leadership may not because they are not directly harmed. In contrast to economic sanctions, which tend to have limited impact on Kim Jong-un, this approach focuses the deterrent punishment on Kim, the decisionmaker, and not so much on other North Koreans.

Impose Costs on Kim Jong-un with Outside Information

Kim Jong-un is afraid of outside information, and especially the example of ethnic Koreans living well in the ROK. Indeed, Kim has been ruthless in trying to prevent that information from reaching his people. The ROK-U.S. should use ROK soap operas, dramas, and K-pop, more actively broadcasting and otherwise transmitting such information into North Korea. And to discourage North Korea from doing another ballistic missile test, the ROK-U.S. could threaten to respond by scattering hundreds of thousands of USB drives with this material all over Pyongyang. These USB drives and external broadcasts into the North could also include outside-world facts and facts about the corruption in the North Korean government interspersed between the programs that we already know are very popular in North Korea.

Punish North Korean Provocations Economically

For example, the ROK-U.S. could threaten to tighten the economic sanctions efforts by interdicting or at least identifying North Korean ships involved in illicit ship-to-ship transfers[39] and by more explicitly identifying the Chinese and other country violations of existing sanctions.[40] The United States should also mount a major information operation to counter the North Korean claims that the existing sanctions are all due to the United States. The United States should explain that many of the sanctions have been imposed by the United Nations and were supported by China and Russia.

Establish a Baseline of Day-to-Day Peacetime Defenses of South Korea, Recognizing the Likely Growing Potential for North Korean Limited Attacks in Peacetime

Some ROK-U.S. air and missile defenses (including fighter aircraft) should be actively operating daily in a random pattern, and others should be available to operate based on an hour or so of warning. The ROK-U.S. should do an assessment of protecting military forces and civilian populations, identifying air and missile defense gaps, and acquiring, if needed, more air and missile defenses to fill those gaps. The ROK-U.S. should also identify potential targets of North Korean drones or SOF (such as Patriot missile batteries or the production or storage of toxic industrial materials) and enhance means for identifying attackers and the ability to defeat such attackers (for example, identifying forged passports to intercept SOF infiltrating into the ROK and ensuring sufficient guards to protect potential SOF targets).

---

[39] Ideally, the ROK-U.S. should tell China that they want the Chinese Navy to take this action. They should tell China that if it refuses, the ROK-U.S. are prepared to send ROK-U.S. Navy ships into the northern West Sea to take this action, something they know that China would prefer to avoid.

[40] With the 2022 Winter Olympics, China made significant efforts to repress freedom of the press in order to maintain a positive image of China. See, for example, Human Rights Watch, "China: Censorship Mars Beijing Olympics," February 18, 2022. China might be responsive to correcting problems that tarnish its image.

Provide Enhanced Peacetime Defenses of South Korea for Periods of Crisis and Ambiguous Warning of War

These would involve greater readiness of air and missiles defenses; more guards (including reserve military personnel) for potential targets (such as nuclear plants); and provisions for dispersal, hardening, and deception around potential targets such as ROK airfields. In normal peacetime, exercises involving "red teams" should be used to test these defenses and improve protection efforts.

Respond in a Strong If Not Escalated Manner Against Any North Korean Conventional Attack on South Korea

This involves employing the ROK concept of proactive deterrence.[41] For example, the ROK-U.S. could threaten to attack known North Korean CW storage facilities associated with the North Korean artillery if North Korea fires conventional artillery across the DMZ, preventing North Korean use of that CW. Alternatively, a North Korean conventional missile attack near a ROK city could be met by an attack on the North Korean central military headquarters and/or North Korean CW production and storage facilities.

Prepare for an Early Conventional Counterforce Response Against North Korean Limited Chemical or Biological Weapon or Electromagnetic Pulse Employment

Because limited CW, BW, and/or EMP employment would be acts of war and expected as precursors to a North Korean invasion of the ROK, such attacks would justify a ROK-U.S. counterforce response against the North. The ROK-U.S. could tell North Korea that it would be nearly impossible to differentiate a North Korean limited OWMD attack from an OWMD invasion precursor, and that OWMD terrorism is therefore too risky for the North. If the North Korean attack is very limited and a counterforce attack is considered too escalatory, the ROK-U.S. could threaten to destroy parts or all of the two North Korean oil refineries with conventional weapons in response to an isolated North Korean nuclear EMP attack that affects the ROK (identifying such options could strengthen deterrence of North Korean OWMD employment).[42]

Recognize That North Korea Could Respond with Escalation

North Korea has traditionally used the threat of escalation to deter ROK-U.S. punishment for its provocations, thereby undermining the deterrence of the North Korean provocations. The ROK-U.S. must therefore threaten a sequence of escalating actions against North Korea if the North escalates. The ROK-U.S. must have a multistep strategy much as good chess players do,

---

[41] Song Sang-ho, "Cheonan Sinking Reshapes Military Strategies," *Korea Herald*, March 20, 2011.

[42] North Korea has an oil refinery in Dandong and one on the Tumen River border with Russia. Even if the Dandong refinery were destroyed, preventing the refining of Chinese oil supplies, "'North Korea would not survive on its own for three months and everything in North Korea would be paralysed." Tony Munroe and Jane Chung, "For North Korea, Cutting Off Oil Supplies Would Be Devastating," Reuters, April 13, 2017.

and they must let North Korea know that they are prepared for those multiple steps and that the North will find the costs of its escalation will not be justified by the benefits that it seeks. In particular, the ROK-U.S. must have an effective approach to warfighting, as described below, in order to deter North Korea from considering escalation to war.

Demonstrate the Will to Execute These Actions and Accept the Risks of Escalation

The primary way to demonstrate this will is to impose costs on North Korea for its next and subsequent provocations. North Korea perceives itself as becoming increasingly powerful given its possession of nuclear weapons, against which the historically passive ROK-U.S. behavior becomes increasingly dangerous. North Korea needs to be told that while it perceives its nuclear shadow gives it more freedom to provoke and attack, that nuclear shadow requires more serious ROK-U.S. responses to disrupt the North Korean escalation strategy.

Deterring North Korean employment of its cyber capabilities is more difficult, in part because these activities are diverse and ongoing and partially sheltered by the support of China and other countries. Chapter 5 discusses options for deterring cyberattacks

A "Carrot and Stick" Strategy

Because the Kim regime will continue to require opportunities to display its empowerment, the ROK-U.S. must induce North Korea to make those demonstrations in more positive ways. This is where the ROK-U.S. need a "carrot and stick" strategy, offering carrots that would allow North Korea to positively demonstrate its empowerment. For example, the United States could offer North Korea a relationship "warm-up" deal: The United States could give the regime 3 million doses of the Pfizer and Moderna vaccines (enough for the senior elites), provide 10 kgs of rice for every North Korean, offer to place 25 North Korean graduate students in some of the best universities in the United States to establish them as international scholars (a goal Kim Jong-un set in late 2019), and agree to coordinate with the United Nations to allow selected North Korean textile exports, all major accomplishments if the North Korean regime accepts them. In exchange, North Korea would be asked to allow U.S. inspection of the presumed Kangson uranium enrichment facility and inspection of the KN-23 missile, small prices for North Korea to pay (not requiring dismantlement, yet). The United States could make this offer very publicly and unilaterally, bypassing the requirement to negotiate with North Korea, but putting pressure on North Korea to accept the offer because it is generous and should be particularly attractive to the North Korean elites. Even if Kim refuses such an offer, one "stick" is that many North Korean elites could be upset with Kim because they would find the offer personally attractive.

As a second step with carrots and sticks, the United States should provide North Korea with balance sheets showing the U.S. perceptions of what North Korea wants in negotiations and what the United States wants, and the U.S. perceptions of the percentage of the end state reflected by each individual item on the U.S. "wants" balance sheet and on the North Korean "wants" balance sheet. The United States should invite North Korea to propose adjustments to the balance sheets.

Then the United States should make offers to North Korea that might involve a 5-percent deal from each balance sheet. Doing so would again allow the United States to bypass the need to get North Korea to come to the negotiating table, forcing the North to negotiate on the U.S. proposals or potentially face embarrassment both internally and externally for refusing specific, important offers. The regime could, of course, claim any such agreements as major victories, but unless the ROK-U.S. want to fight a war with North Korea to reduce its nuclear weapons, such negotiations offer the potential for peacefully reducing at least the growth in the North Korean nuclear weapon threat.

Wartime Responses

Much of the historical discussion of a potential war on the Korean peninsula assumes that such a war would be largely a traditional, conventional force conflict with perhaps some minor overlays of WMD. As described herein, that appears to be a very unrealistic perspective that needs to be abandoned and replaced by a view of Korean conflict in which WMD and cyberattacks are actively employed. This replacement was the perspective of U.S. and Soviet forces on the North Atlantic Treaty Organization (NATO) Central Front during the 1980s, but most current ROK-U.S. military personnel have not been trained on what to expect from, and how to operate in, such a conflict. The ROK-U.S. need a "strategic deterrence and warfighting group" of government officials and experts to develop potential North Korean WMD and cyber employment scenarios, to assist in formulating a strategy for responding to WMD/cyberattacks, to coordinate counter-WMD and cyber actions across government agencies, to organize regular education and training relative to WMD and cyber threats, and to help with testing the strategy in training and war plans. This group should identify specific roles for each of the relevant organizations and specific ways for them to cooperate in any contingency. ROK-U.S. strategy needs to reflect these conditions and to make U.S. nuclear weapon use a more integral part of war planning and training in order to demonstrate ROK-U.S. readiness.[43]

Countering a North Korean WMD invasion would require a mixture of excellent detection, counterforce, defense, and reconstitution capabilities. As in peacetime, the ROK-U.S. need to maintain finely tuned warning systems to detect North Korean preparation for war, and especially North Korean precursor attacks. The ROK-U.S. need to establish minimum precursor attack redlines to designate when a state of war exists that potentially justifies early ROK-U.S. conventional counterforce responses. Such responses could selectively or comprehensively neutralize North Korean WMD capabilities and delivery means. The ROK defense minister recently described the developing ROK capabilities and strategy: "The military currently has a large number of missiles with significantly improved range, accuracy, and power, and it can accurately and swiftly strike any targets in North Korea. . . . If signs of a missile launch are

[43] This action would really worry China and hopefully induce more Chinese pressure on North Korea to moderate its efforts to build WMD.

especially clear, it has the ability and posture to precisely strike at the origin of the launch as well as command and support facilities."[44] While North Korea interpreted this statement as the threat of a preemptive ROK counterforce attack,[45] such a counterforce attack would not be a true preemption that starts a war if it is responding to a North Korean precursor attacks; it would instead be simply responding to the war that North Korea had already started.

A clear definition of such ROK-U.S. minimum redlines may cause North Korea to defer or even forgo some precursor attacks in order to maintain strategic/operational surprise. And the risks to the North of early ROK-U.S. counterforce responses could potentially deter Kim Jong-un from deciding to invade. Even if the ROK-U.S. fail to execute a counterforce response before the main North Korean attack, they need to have sufficient capability, with a second strike, to eliminate most North Korean WMD and delivery means soon after the start of a war. The ROK-U.S. need to be able to deny North Korea continuing use of its WMD throughout a war and especially once the regime fears defeat. Doing so requires continuing ROK efforts to deploy theater ballistic missiles (land- and sea-based) and a U.S. deployment of theater ballistic missiles in the ROK, potentially including hypersonic missiles. Fighter aircraft, cruise missiles, and drones would take longer to reach North Korean targets and thus should be prepared to perform armed reconnaissance and cleanup of North Korean facilities that somehow survive ballistic-missile strikes.

The ROK-U.S. also need to posture their forces and prepare their civilians for surviving WMD warfare and being able to continue to operate. That means providing adequate warning systems and prompt counterforce capabilities, air and missile defenses, defenses against North Korean special forces, passive defenses such as dispersal and hardening, provisions for evacuation of targets North Korea will likely strike and establishing effective military capabilities at alternative locations, protective clothing and buildings with collective protection, denial and deception to limit North Korean knowledge of potential target locations, and medical and repair capabilities to manage the consequences of North Korean attacks. Reconstitution after a North Korean major attack could be supported by backup C2 means, dispersed military units, better trained and armed reserve forces, and hidden or dispersed stockpiles of weapons and supplies (potentially some stored in other countries). Substantial capabilities for decontamination, medical treatment, and quarantine should be created in the ROK-U.S. military reserve forces and other governmental agencies, in addition to extra airfields and equipment to facilitate rapid U.S. force flow into Korea in the aftermath of North Korean WMD use. In all of these areas, military capabilities need to be acquired where they are currently insufficient; personnel need to be trained to achieve high performance and resilience;

---

[44] "Defense Minister Warns North Korea, 'If There Are Signs of NK Missile, We Will Prepare for a Precision Strike'," One Korea Network, April 4, 2022.

[45] "He must be crazy or silly to speak of 'preemptive attack' on a nuclear weapons state." Jeongmin Kim, "North Korea Says Seoul 'Crazy' to Talk of Preemptive Strike on 'Nuclear Power,'" *NKNews*, April 3, 2022. After a North Korean precursor attack, especially one using OWMD, the ROK, recognizing that a state of war already exists, would actually be crazy not to attempt to preempt and neutralize much of the North's main attack.

and C2 need to be improved, including interagency coordination. All of these actions should enhance deterrence of North Korean WMD employment, making it clear that the ROK-U.S. are prepared to survive North Korean WMD attacks and respond appropriately.

Conclusions

North Korea has deployed substantial WMD and cyber capabilities and is enhancing those capabilities on a continuing basis. The ROK-U.S. need to take these threats seriously and develop an integrated deterrence and warfighting strategy for countering them.

The ancient Roman author Vegetius said, "If you want peace, prepare for war."[46] If you are prepared for war, opponents are unlikely to attack you. North Korea recognized that it would almost certainly lose a war limited to conventional weapons and has thus followed this concept, developing WMD and cyber capabilities to challenge the traditional ROK-U.S. concept of war on the Korean peninsula.[47] And having developed these capabilities, the North can also use them offensively.

The ROK-U.S. must therefore adjust their war paradigms to focus on the actual threat that North Korea poses. It is critical to prepare for the right war, and that will require new efforts by the ROK-U.S. because they have been too focused on conventional war in Korea as it may have occurred in the past. Making this change will require significant U.S. adjustments in strategy, military education, and military capability development. Such efforts are needed now to deter North Korean threats, provocations, and potential war initiation.

[46] N. S. Gill, "Who Said 'If You Want Peace, Prepare for War'?" Thought Company, July 5, 2019.

[47] Years ago, when asked about whether North Korea would use CW in a war, the most senior North Korean escapee to date said that North Korea was not a rich country, and thus it would not invest money in capabilities it did not plan to use. US debriefing of Hwang Jang-yop, 1997.

Appendix. Technical Description of Nuclear Electromagnetic Pulse

The EMP caused by a nuclear weapon exploded in space starts within a nanosecond of the nuclear explosion and lasts for several minutes.[1] There is an electrical field of varying strength during this time. The EMP is broken into three components, E1, E2, and E3.[2] E1 peaks about ten nanoseconds after the explosion and lasts to about one microsecond after. Because the short-lived E1 generates very large electrical voltages that could damage a wide variety of electrical devices, it is the component of the greatest concern. E2 occurs from about one microsecond to about ten milliseconds after the explosion. The strength of the electrical field at this time is much lower than earlier, and its general characteristics are similar to a lightning strike. Since many electrical systems are hardened against lightning, the E2 component of EMP is not of much concern. E3 lasts from about one second after the explosion to about five minutes after. The strength of this electrical field is much lower than even E2, but the long duration means that substantial currents can develop in electrical transmission lines and transformers, which could collapse the electrical grid. If there is sufficient damage to transformers, then power restoration could take months, leading to substantial disruption and potentially loss of life. The E1 and E3 components of EMP are thus the ones of concern.

The magnitude of the various components of EMP can be affected by the nuclear weapon yield, its burst altitude, the weapon design, the strength of the earth's magnetic field at the burst site, whether it is day or night, the solar sunspot cycle, and the earth's composition underneath the electrical devices being affected. The strength of the E1 component increases only slowly with increases in weapon yield. This is especially the case for thermonuclear weapons, since the E1 component is produced by the relatively low-yield fission trigger of the weapon. The gamma radiation from the fission trigger ionizes the atmosphere so that the radiation from the main thermonuclear part of the weapon has a greatly diminished effect.

One implication of this fact is that even low-yield nuclear weapons can generate worrying E1 strengths. The E1 electrical field is generated by the prompt gamma rays released as the nuclear fission is occurring. For many nuclear weapon designs, the fissioning nuclear material is buried well inside the weapon and the weapon's high explosives; the tamper and weapon casing absorb many of the gamma rays, reducing the E1 field. Presumably, weapons designed specifically to

[1] A basic description of nuclear weapons is provided in U.S. Department of Defense, *Nuclear Matters Handbook*, Washington, D.C., 2020, Chapter 13. A nuclear explosion in space would also affect satellites in low earth orbit and thus be very escalatory.

[2] For a general discussion of EMP, see Michael K. Rivera, Scott N. Backhaus, Jesse Richard Woodroffe, Michael Gerard Henderson, Randall J. Bos, Eric Michael Nelson, and Andjelka Kelic, *EMP/GMD Phase 0 Report: A Review of EMP Hazard Environments and Impacts*, LA-UR-16-28380, Los Alamos, N.M.: Los Alamos National Laboratory, October 24, 2016, pp. 16–39.

enhance E1 would use lesser amounts of high explosive, use thinner, more gamma ray transparent tampers, and use thinner cases. There is an optimal altitude for a weapon explosion to produce the highest E1 strength. The optimal altitude increases as the weapon's yield increases, but it is generally about 60 to 100 km. Regardless of these factors, the E1 strength is generally in the range of tens of kilovolts (kV) per meter and for ordinary nuclear weapons is thought not to exceed about 50 kV per meter.

E3 is broken into two components, E3A and E3B. E3A occurs about one to ten seconds after the explosion. E3B occurs about ten seconds to around five minutes after the explosion. E3A is strongest for explosions occurring at night during the solar sunspot minimum and weakest for explosions occurring during the day during the solar sunspot maximum. E3A is maximized for explosion altitudes of about 500 km, whereas E3B is maximized for explosion altitudes of about 130 km.

The strength of the E3A field depends linearly on the yield of the weapon and is important only for weapons with yields above 100 kt.[3] The strength of the E3B field tends to plateau for yields above ten kt. However, at this low yield the area affected is rather small. It is only for yields above about 100 kt that the E3B field is important. Therefore, while large-yield weapons can produce significant E3, weapons with a yield of under about 100 kt do not.[4] Also, for burst altitudes below about 100 kt, the E3A and E3B fields are not significant. The strength of the E3 field is strongly dependent on the earth's conductivity (impedance) underneath the electrical device being affected. Most analyses have assumed a nominal impedance, but recent work looking at actual impedance leads to wide variation (factor of 3 or 4) in the calculated E3 field.[5]

For a given explosion location, the places on the earth where the E3A effects are the strongest do not coincide with the locations where the E3B effects are the strongest. The E3A effects are displaced far to the north (in the Northern Hemisphere) of the burst point, whereas the E3B effects tend to occur near the burst point. Since the E1 effects also occur near the burst point, an EMP attack would aim to explode a weapon over the point where the attacker would want the effects to be felt. Therefore, only E1 and E3B are the primary effects of concern in an EMP attack. For weapons with a yield less than 100 kt or burst heights below 100 km, only E1 will be of concern. If a weapon is burst high enough to produce significant E3B fields, the E1 production will be suboptimal. Note also that the E1 and E3B effects are not maximized at the same locations near the burst point.[6]

---

[3] James Gilbert, John Kappenman, William Radasky, and Edward Savage, "The Late-Time (E3) High Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid," Goleta, Calif.: Metatech Corporation, Meta-R-321, January 2010, p. 2-8.

[4] Rivera et al., p. 39.

[5] Jeffrey J. Love, Greg M. Lucas, Benjamin S. Murphy, Paul A. Bedrosian, E. Joshua Rigler, and Anna Kelbert, "Down to Earth with Nuclear Electromagnetic Pulse: Realistic Surface Impedance Affects Mapping of the E3 Geoelectric Hazard," *Earth and Space Science*, Vol. 8, No. 8, 2021, p. e2021EA001792.

[6] For an illustration of the E1 extent and its intensity, see Savage, Gilbert, and Radasky, 2010, p. 2-4. For an illustration of the E3B extent and intensity, see Gilbert et al., 2010, p. 2-12. Note that in each diagram the weapon is exploded at the near-optimum altitude for the given effect so that for E1, the burst altitude is 75 km, and for E3B, 130 km.

The impact of an EMP attack is highly uncertain. There have been no high-altitude nuclear tests since 1962, and the measurements of the EMP from these tests were far from comprehensive. All EMP threat fields used today to determine the vulnerability of various electrical components are based on computer models. Furthermore, the best ones are all classified. All that is available on an unclassified basis are very simple generic EMP threat fields.

What is worse, electronics have changed drastically since 1962, when many devices depended on vacuum tubes. Today's microchips may be much more vulnerable, and the fact is that far more devices from cars to refrigerators now use microchips, and society is much more dependent on electronics such as computers and cell phones.

A key issue is whether major damage would occur to extra-high-voltage transformers resulting in a long-term shutdown of the electrical grid. Long-distance transmission of electricity requires the use of very high voltages. Once the electricity is generated, a transformer is used to greatly increase the voltage, which is then transmitted for long distances. When the electricity is near its destination, another transformer lowers the voltage, allowing the electricity to be distributed to consumers. The main high voltages used for long-distance transmission in the United States are 765 kV, 500 kV and 345 kV.[7] For transmission in South Korea, the voltages are 765 kV and 345 kV.[8]

The manufacture of new, large transformers can take more than a year, and they are custom designed. They require special steel, which is produced by relatively few manufacturers. There are about 2,000 such transformers in the United States, but less than 100 units are manufactured a year worldwide.[9] The transformers weigh between 100 and 400 tons. Moving the finished product to the required location is difficult. Specialized railcars are needed, of which there are only about 30 in the United States.

The E3 portion of the EMP can set up a quasi-DC current in transmission lines. This current would then pass into the transformers. Various effects could cause grid collapse. By itself, the grid could be restored in a day or two. However, if the current is strong enough, it could cause sufficient heating in the transformer to lead to catastrophic failure.[10] The current created in the transmission lines would be quite variable, as it would depend on the line length, orientation of the line to the nuclear detonation, and the impedance of the earth beneath the transmission line. Still, the destruction of even a small fraction of the transformers would pose serious problems for restoring the grid.

---

[7] Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability, "Large Power Transformers and the U.S. Electric Grid," Washington, D.C.: U.S. Department of Energy, April 2014 update.

[8] Kepco, "National Power Grid," undated.

[9] Lee Layton, "Electromagnetic Pulse and Its Impact on the Electric Power Industry," PDHonline Course E402, Fairfax, Va.: PDHonline, 2016, p.28.

[10] Rivera et al., 2016, p. 67.

Abbreviations

Bt	Bacillus thuringiensis
BW	biological weapon
BWA	biological warfare agent
C2	command and control
C4I	command, control, communications, computer, and intelligence
CFC	Combined Forces Command
COVID-19	coronavirus disease 2019
CW	chemical weapon
CWA	chemical warfare agent
CWC	Chemical Weapons Convention
DDOS	distributed denial of service
DE	directed energy
DMZ	demilitarized zone
DNS	Domain Name System
DPRK	Democratic People's Republic of Korea (North Korea)
E1, E2, E3 (E3a, E3b)	alternative EMP effects
ECT	effective concentration
ED	effective dose
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
FDA	Food and Drug Administration
GB	sarin
HEMP	high-altitude electromagnetic pulse
HFRS	hemorrhagic fever with renal syndrome
ICBM	intercontinental ballistic missile
IND	Investigational New Drug

KHF	Korean hemorrhagic fever
KPA	Korean People's Army
LCT	lethal concentration
LD	lethal dose
MOPP	Mission Oriented Protective Posture
NATO	North Atlantic Treaty Organization
OWMD	other weapons of mass destruction
RGB	Reconnaissance General Bureau
ROK	Republic of Korea
ROK-U.S.	Republic of Korea/United States
SEB	staphylococcal enterotoxin B
SOF	special operations force
STRATCOM	U.S. Strategic Command
TEL	transporter erector launcher
UN	United Nations
USAMRIID	U.S. Army Medical Research Institute of Infectious Diseases
USFK	United States Forces Korea
WMD	weapons of mass destruction

Bibliography

38 North, "Estimating North Korea's Nuclear Stockpiles: An Interview with Siegfried Hecker," April 30, 2021. As of April 7, 2022: https://www.38north.org/2021/04/estimating-north-koreas-nuclear-stockpiles-an-interview-with-siegfried-hecker/

Aaron, Kate, "Operation Dark Harvest—The Story of Scotland's 'Anthrax Island,'" History of Yesterday, August 17, 2021. As of April 7, 2022: https://historyofyesterday.com/operation-dark-harvest-the-story-of-scotlands-anthrax-island-ee334d26df25

Abrams, Robert B., "Statement of General Robert B. Abrams," Washington, D.C.: House Armed Services Committee, March 10, 2021. As of April 7, 2022: https://docs.house.gov/meetings/AS/AS00/20210310/111316/HHRG-117-AS00-Bio-AbramsR-20210310.pdf

Aerospace Center for Strategic and International Studies, "Space Threat 2018: North Korea Assessment," April 12, 2018. As of April 7, 2022: https://aerospace.csis.org/space-threat-2018-north-korea/

Alibek, Ken, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from Inside by the Man Who Ran It*, New York: Random House, 1999a.

Alibek, Kenneth, *Biological Weapons*, Cambridge, Mass.: Hadron, Inc., November 1, 1999b.

Army Rapid Capabilities and Critical Technologies Office, "Army Directed Energy Strategy," webpage, August 20, 2021. As of April 7, 2022: https://www.army.mil/standto/archive/2021/08/20/

Auslin, Michael, "In Search of the Xi Doctrine," War on the Rocks, May 30, 2016. As of May 30, 2022: https://warontherocks.com/2016/05/in-search-of-the-xi-doctrine/

Bacon, John, "Anthrax Antibodies in Defector Raises Fears North Korea Is Developing Chemical Weapons," *USA Today*, December 27, 2017. As of April 7, 2022: https://www.usatoday.com/story/news/world/2017/12/27/anthrax-defector-raises-new-fears-north-korea-developing-biological-weapons/983810001/

Baker, George H. William A. Radasky, and James L. Gilbert, "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment," National Coordinating Center for Communications (NCC), February 5, 2019. As of May 30, 2022:

https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf

Barnes, Julian E., "F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat," *New York Times*, June 4, 2021.

Baumgaertner, Emily, and William J. Broad, "North Korea's Less-Known Military Threat: Biological Weapons," *New York Times*, January 15, 2019. As of April 7, 2022: https://www.nytimes.com/2019/01/15/science/north-korea-biological-weapons.html

Beauchamp-Mustafaga, Nathan, Derek Grossman, Kristen Gunness, Michael S. Chase, Marigold Black, and Natalia D. Simmons-Thomas, *Deciphering Chinese Deterrence Signaling in the New Era: An Analytic Framework and Seven Case Studies*, Santa Monica, Calif.: RAND Corporation, RR-A1074-1, 2021. As of May 17, 2022: https://www.rand.org/pubs/research_reports/RRA1074-1.html

Bechtol, Bruce E., Jr., *North Korean Military Proliferation in the Middle East and Africa*, Lexington: University Press of Kentucky, 2018.

Bennett, Brian, "Biden Administration Says Talks with Russia on Cyber Attacks Are Progressing. Privately, Staffers Are Skeptical," *Time*, July 8, 2021. As of May 30, 2022: https://time.com/6078997/biden-cyber-attacks-putin

Bennett, Bruce W., *The Challenge of North Korean Biological Weapons*, Santa Monica, Calif.: RAND Corporation, CT-401, 2013a. As of May 17, 2022: https://www.rand.org/pubs/testimonies/CT401.html

———, *Preparing for the Possibility of a North Korean Collapse*, Santa Monica, Calif.: RAND Corporation, RR-331-SRF, 2013b. As of May 30, 2022: https://www.rand.org/pubs/research_reports/RR331.html

———, "South Korea: Capable Now, Questions for the Future," in Gary James Schmitt, ed., *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key U.S. Allies and Security Partners*, Carlisle, Penn.: U.S. Army War College Press, 2015, pp. 255–291.

———, *Alternative Paths to Korean Unification*, Santa Monica, Calif.: RAND Corporation, RR-2808-KOF, 2018. As of May 17, 2022: https://www.rand.org/pubs/research_reports/RR2808.html

Bennett, Bruce W., Kang Choi, Myong-Hyun Go, Bruce E. Bechtol, Jr., Jiyoung Park, Bruce Klingner, and Du-Hyeogn Cha, *Countering the Risks of North Korean Nuclear Weapons*, Santa Monica, Calif.: RAND Corporation, PE-A1015-1, 2021. As of May 17, 2022: https://www.rand.org/pubs/perspectives/PEA1015-1.html

Bennett, Bruce W., and Darren Wheeler, *Chemical Challenge Level Analysis for Special Operations*, Santa Monica, Calif.: RAND Corporation, TR-791, 2010.

Bermudez, Joseph S., Jr., "The Democratic People's Republic of Korea and Unconventional Weapons," in Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, eds., *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*, Ithaca, N.Y.: Cornell University Press, 2000, pp. 182–201.

———, "North Korea's Chemical Warfare Capabilities," 38 North, October 10, 2013. As of April 7, 2022: http://38north.org/2013/10/jbermudez101013/

Bermudez, Joseph S., Jr., and Victor Cha, "Undeclared North Korea: The Yusang-ni Missile Operating Base," *Beyond Parallel*, May 9, 2019. As of April 7, 2022: https://beyondparallel.csis.org/undeclared-north-korea-the-yusang-ni-missile-operating-base

Bermudez, Joseph S., Jr., Victor Cha, and Jennifer Jun, "Undeclared North Korea: The Hoejung-ni Missile Operating Base," *Beyond Parallel*, February 7, 2022. As of April 7, 2022: https://beyondparallel.csis.org/undeclared-north-korea-hoejung-ni-missile-operating-base/

Berstein, Richard, "Intelligence Has Its Limitations," *New York Times*, January 13, 2010. As of April 7, 2022: https://www.nytimes.com/2010/01/14/us/14iht-letter.html

Bleek, Philipp C., "Revisiting Aum Shinrikyo: New Insights into the Most Extensive Non-State Biological Weapons Program to Date," Nuclear Threat Initiative, December 10, 2011. As of April 7, 2022: https://www.nti.org/analysis/articles/revisiting-aum-shinrikyo-new-insights-most-extensive-non-state-biological-weapons-program-date-1/

Bower, William A., Jarad Schiffer, Robert L. Atmar, Wendy A. Keitel, Arthur M. Friedlander, Lindy Liu, Yon Yu, David S. Stephens, Conrad P. Quinn, and Katherine Hendricks, "Use of Anthrax Vaccine in the United States: Recommendations of the Advisory Committee on Immunization Practices, 2019," *Morbidity and Mortality Weekly Report*, Vol. 68, No. 4, December 19, 2019. As of June 9, 2022: https://www.cdc.gov/mmwr/volumes/68/rr/rr6804a1.htm

Branigan, Tania, and Ewen MacAskill, "North Korea: A Deadly Attack, a Counter-Strike—Now Koreans Hold Their Breath," *The Diplomat*, November 23, 2010. As of April 7, 2022: https://www.theguardian.com/world/2010/nov/23/north-south-korea-crisis-conflict

Bremer, Ifang, "Dutch Intelligence Says North Korea Using Netherlands-Based Servers for Hacking," *NKNews*, April 29, 2022. As of July 7, 2022: https://www.nknews.org/2022/04/dutch-intelligence-says-north-korea-using-netherlands-based-servers-for-hacking/

Bumiller, Elizabeth, and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012. As of April 7, 2022: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper, III, and Mark Cozad, *People's Liberation Army Operational Concepts*, Santa Monica, Calif.: RAND Corporation, RR-A394-1, 2020. As of May 17, 2022: https://www.rand.org/pubs/research_reports/RRA394-1.html

Byun Duk-kun, "N. Korea Works with All Kinds of Cyber Criminals, Including Russians: Sullivan," Yonhap News Agency, March 23, 2022. As of April 7, 2022: https://en.yna.co.kr/view/AEN20220323000200325

Caesar, Ed, "The Incredible Rise of North Korea's Hacking Army," *New Yorker*, April 19, 2021. As of April 7, 2022: https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army

Carroll, Stephen J., Tom LaTourrette, Brian G. Chow, Gregory S. Jones, and Craig Martin, *Distribution of Losses from Large Terrorist Attacks Under the Terrorism Risk Insurance Act*, Santa Monica, Calif.: RAND Corporation, MG-427-CTRMP, 2005. As of May 17, 2022: https://www.rand.org/pubs/monographs/MG427.html

Caudle, Lester C., III, "The Biological Warfare Threat," in Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz, eds., *Medical Aspects of Chemical and Biological Warfare*, Washington, D.C.: Office of the U.S. Army Surgeon General, 1997, pp. 451–466. As of April 7, 2022: https://www.ojp.gov/ncjrs/virtual-library/abstracts/medical-aspects-chemical-and-biological-warfare

Centers for Disease Control and Prevention, "Anthrax Vaccination: What Everyone Should Know," webpage, undated. As of April 7, 2022: https://www.cdc.gov/vaccines/vpd/anthrax/public/index.html#:~:text=To%20build%20up%20protection%20against,each%20year%20to%20stay%20protected

———, "Hemorrhagic Fever with Renal Syndrome," webpage, January 18, 2017. As of April 7, 2022: https://www.cdc.gov/hantavirus/hfrs/index.html

———, "Anthrax," webpage, November 20, 2020. As of April 7, 2022: https://www.cdc.gov/anthrax/basics/types/index.html

Cha Du Hyeogn, "Kim Jong Un's Policy Plans in the Revision of the KWP Rules: Continued Goal of Communizing South Korea, Enhancing Political Power, and Internal Solidarity," Asan Institute, August 10, 2021. As of June 11, 2022: https://en.asaninst.org/contents/kim-jong-uns-policy-plans-in-the-revision-of-the-kwp-rules-continued-goal-of-communizing-south-korea-enhancing-political-power-and-internal-solidarity/

Chainalysis Team, "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options," Chainalysis blog, February 9, 2021. As of December 15, 2021: https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack/

Chanlett-Avery, Emma, Liana W. Rosen, John W. Rollins, and Catherine Theohary, *North Korean Cyber Capabilities: In Brief*, Washington, D.C.: Congressional Research Service, 2017. As of April 7, 2022: https://sgp.fas.org/crs/row/R44912.pdf

Charap, Samuel, "Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to 'Deterrence,'" *Security Insights*, No. 062, September 2020. As of April 7, 2022: https://www.marshallcenter.org/en/publications/security-insights/strategic-sderzhivanie-understanding-contemporary-russian-approaches-deterrence-0

"Chemical Weapons: New Information Analysed," *Jane's Defence Weekly*, February 27, 1988, p. 370.

Choe Sang-Hun, "North Korean Hackers Stole U.S.–South Korean Military Plans, Lawmaker Says," *New York Times*, October 10, 2017. As of April 7, 2022: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html

———, "North Korea, Seeking 'Equal Footing,' Rejects Preconditions for U.S. Talks," *New York Times*, March 3, 2018. As of April 7, 2022: https://www.nytimes.com/2018/03/03/world/asia/north-korea-nuclear-talks.html

———, "Kim Jong-Un Calls K-Pop a 'Vicious Cancer' in the New Culture War," *New York Times*, June 10, 2021. As of April 7, 2022: https://www.nytimes.com/2021/06/11/world/asia/kim-jong-un-k-pop.html

Choi Kang, Shin Beomchul, and Kang Jae-Kwang, "The Shifting Environment in Northeast Asia and Our Responses," Asan Institute, September 2019. As of June 11, 2022: https://en.asaninst.org/contents/the-shifting-environment-in-northeast-asia-and-our-responses/

Chow, Brian G., Gregory S. Jones, Irving Lachow, John Stillion, Dean A. Wilkening, and Howell Yee, *Air Force Operations in a Chemical and Biological Environment*, Santa Monica, Calif.: RAND Corporation, DB-189/1-AF, 1998. As of May 30, 2022: https://www.rand.org/pubs/documented_briefings/DB189z1.html

Chung, Chaewon, "North Korea Fires Two Presumed Ballistic Missiles Toward the East Sea: JCS," *NKNews*, January 27, 2022. As of April 7, 2022: https://www.nknews.org/2022/01/north-korea-fires-unidentified-projectile-towards-the-east-sea-jcs-2/?t=1658947120866

Clayton, Mark, "In Cyberarms Race, North Korea Emerging as a Power, Not a Pushover," *Christian Science Monitor*, October 19, 2013.

Cole, Leonard A., *The Anthrax Letters*, New York: Skyhorse Publishing, 2009.

Collins, Robert, *Marked for Life: Songbun, North Korea's Social Classification System*, Washington, D.C.: The Committee for Human Rights in North Korea, 2012. As of April 7, 2022: http://www.hrnk.org/uploads/pdfs/HRNK_Songbun_Web.pdf

Comprehensive Nuclear-Test-Ban Treaty Organization, "9 July 1962: 'Starfish Prime,' Outer Space," webpage, undated. As of April 7, 2022: https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space

Conger, Kate, and David E. Sanger, "U.S. Says It Secretly Removed Malware Worldwide, Pre-Empting Russian Cyberattacks," *New York Times*, April 6, 2022. As of April 7, 2022: https://www.nytimes.com/2022/04/06/us/politics/us-russia-malware-cyberattacks.html

Cordesman, Anthony H., and Aaron Lin, *The Changing Military Balance in the Koreas and Northeast Asia*, Washington, D.C.: Center for Strategic and International Studies, June 2015, 2015. As of April 7, 2022: https://www.csis.org/analysis/changing-military-balance-koreas-and-northeast-asia

"Defector Claims North Grooms Hackers," *Joongang Daily*, June 1, 2011. As of December 13, 2021: https://koreajoongangdaily.joins.com/2011/06/01/politics/Defector-claims-North-grooms-hackers/2937036.html

Defense Intelligence Agency, *North Korea Military Power: A Growing Regional and Global Threat*, Washington, D.C., 2021. As of April 7, 2022: https://www.dia.mil/Portals/110/Documents/News/North_Korea_Military_Power.pdf

"Defense Minister Warns North Korea, 'If There Are Signs of NK Missile, We Will Prepare for a Precision Strike,'" One Korea Network, April 4, 2022. As of April 7, 2022: https://onekoreanetwork.com/2022/04/04/defense-minister-warns-north-korea-if-there-are-signs-of-nk-missile-we-will-prepare-for-a-precision-strike/

Dowd, Alan, "Capstones: The Korea Conundrum," Indianapolis: Sagamore Institute, October 18, 2017. As of April 7, 2022: https://sagamoreinstitute.org/capstones-the-korea-conundrum/

Durden, Tyler, "China Threatens to Bomb North Korea's Nuclear Facilities If It Crosses Beijing's 'Bottom Line,'" Zero Hedge, April 11, 2017. As of April 7, 2022: https://www.zerohedge.com/news/2017-04-11/china-threatens-bomb-north-koreas-nuclear-facilities-if-it-crosses-beijings-bottom-l

Dwyer, Colin, "Banned Nerve Agent Killed Kim Jong Nam Within 20 Minutes, Malaysia Says," NPR, February 26, 2017. As of April 7, 2022: https://www.npr.org/sections/thetwo-way/2017/02/26/517340990/banned-nerve-agent-killed-kim-jong-nam-within-20-minutes-malaysia-says

Dwyer, Devin, and Mary Bruce, "Sony Hacking: President Obama Says Company Made 'Mistake' in Canceling 'The Interview,'" *ABC News*, December 19, 2014. As of April 7, 2022: https://abcnews.go.com/Politics/obama-sony-made-mistake-canceling-film-release/story?id=27720800

Eddy, Melissa, and Nicole Perlroth, "Cyberattack Suspected in German Woman's Death," *New York Times*, September 18, 2020. As of April 7, 2022: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Electric Power Research Institute, *High Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies*, Palo Alto, Calif.: April 29, 2019. As of April 7, 2022: https://www.epri.com/research/products/3002014979

Elleman, Michael, "The New Hwasong-15 ICBM: A Significant Improvement That May Be Ready as Early as 2018," 38 North, November 30, 2017. As of April 7, 2022: https://www.38north.org/2017/11/melleman113017/

Engstrom, Jeffrey, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, Santa Monica, Calif.: RAND Corporation, RR-1708-OSD, 2018. As of May 17, 2022: https://www.rand.org/pubs/research_reports/RR1708.html

Environmental Protection Agency, *Persistence of Chemical Warfare Agent VX on Building Material Surfaces*, EPA/600/S-19/074, Washington, D.C., 2019. As of April 7, 2022: https://www.hsdl.org/?view&did=826721

Estes, Madison A., *Prevailing Under the Nuclear Shadow*, Arlington, Va.: Center for Naval Analyses, September 2020. As of April 7, 2022: https://www.cna.org/CNA_files/PDF/DRM-2020-U-027973-Final%20(003).pdf

Federation of American Scientists, "North Korea: Chemical Weapons Program," Washington, D.C.: 1998. As of April 7, 2022: http://www.fas.org/nuke/guide/dprk/cw/

Foster, John S., Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry (Hank) M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report," 2004. As of April 7, 2022: http://www.empcommission.org/docs/empc_exec_rpt.pdf

Freedman, Lawrence, *Britain and Nuclear Weapons*, London: Macmillan for RIIA, 1980.

"From Jupitr to Centaur, Fears over U.S. Military's Biochemical Experiment Grow in South Korea," *Xinhuanet*, July 16, 2020. As of April 7, 2022: http://www.xinhuanet.com/english/2020-07/16/c_139217819.htm

Gilbert, James, John Kappenman, William Radasky, and Edward Savage, "The Late-Time (E3) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid," Goleta, Calif.: Metatech, Meta-R-321, January 2010. As of April 7, 2022: http://www.futurescience.com/emp/ferc_Meta-R-321.pdf

Gill, N.S., "Who Said 'If You Want Peace, Prepare for War'?" Thought Company, July 5, 2019. As of April 7, 2022: https://www.thoughtco.com/if-you-want-peace-prepare-for-war-121446

Giovanzanti, Alessandra, Mark Cazalet, Dae Young Kim, and George Papangelopoulos, "South Korea's ADD Develops Laser-Power Enhancing Technology," *Janes*, May 25, 2021. As of April 7, 2022: https://www.janes.com/defence-news/news-detail/south-koreas-add-develops-laser-power-enhancing-technology

Glaser, Bonnie, Scott Snyder, and John S. Park, *Keeping an Eye on an Unruly Neighbor: Chinese Views of Economic Reform and Stability in North Korea*, Washington, D.C.: Center for Strategic and International Studies and U.S. Institute of Peace, January 3, 2008. As of April 7, 2022: https://www.csis.org/analysis/keeping-eye-unruly-neighbor

Go Myong-Hyun, "Moon's North Korea Policy: Reengaging North Korea to Regain Strategic Initiative," Asan Institute, June 28, 2017. As of June 6, 2022: https://en.asaninst.org/contents/moons-north-korea-policy-reengaging-north-korea-to-regain-strategic-balance/

Gordon, Michael R., "Biden Sticks with Longstanding U.S. Policy on Use of Nuclear Weapons Amid Pressure from Allies," *Wall Street Journal*, March 25, 2022. As of April 7, 2022: https://www.wsj.com/articles/biden-sticks-with-longstanding-u-s-policy-on-use-of-nuclear-weapons-amid-pressure-from-allies-11648176849

Gordon, Sue, and Eric Rosenbach, "America's Cyber Reckoning," *Foreign Affairs*, January/February 2022. As of July 8, 2022: https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning

Graham, William R., "North Korea Nuclear EMP Attack: An Existential Threat," 38 North, June 2, 2017. As of April 7, 2022: https://www.38north.org/2017/06/wgraham060217/

Graham, William R., and Peter Vincent Pry, *Statement for the Record, Dr. William R. Graham, Dr. Peter Vincent Pry to U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, Hearing, "Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland,"* Washington, D.C., 2017. As of April 7, 2022: https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Wstate-PryP-20171012.pdf

Ha, Mathew, and David Maxwell, *Kim Jong Un's "All-Purpose Sword": North Korean Cyber-Enabled Economic Warfare*, Washington, D.C.: Foundation for the Defense of Democracies, 2018. As of November 8, 2021: https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf

Hancocks, Paula, and K. J. Kwon, "'Poison' Pen Mightier Than Sword for Would-Be North Korean Assassin," CNN, November 26, 2012. As of April 7, 2022: https://www.cnn.com/2012/11/25/world/asia/north-korea-assassination-weapons/index.html

Hanham, Melissa, "Kim Jong Un Tours Pesticide Facility Capable of Producing Biological Weapons: A 38 North Special Report," 38 North, July 9, 2015. As of April 7, 2022: https://www.38north.org/2015/07/mhanham070915/

Harold, Scott W., Martin C. Libicki, and Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-1335-RC, 2016. As of May 17, 2022: https://www.rand.org/pubs/research_reports/RR1335.html

Harris, Elisa D., "North Korea and Biological Weapons: Assessing the Evidence," Washington, D.C.: Stimson Center, November 2020. As of April 7, 2022: https://www.stimson.org/wp-content/uploads/2020/11/38-North-SR-2011-Elisa-Harris_North-Korea-Biological-Weapons-Assessment.pdf

Human Rights Watch, "China: Censorship Mars Beijing Olympics," February 18, 2022. As of April 7, 2022: https://www.hrw.org/news/2022/02/18/china-censorship-mars-beijing-olympics

Hyten, John, "Missile Defense and Defeat: A Conversation with the Vice Chairman," in Tom Karako, ed., Washington, D.C.: Center for Strategic and International Studies, February 24, 2021. As of April 7, 2022: https://www.csis.org/analysis/missile-defense-and-defeat-conversation-vice-chairman

Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability, "Large Power Transformers and the U.S. Electric Grid," Washington, D.C.: U.S. Department of Energy, April 2014. As of April 7, 2022: https://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf

International Crisis Group, "North Korea's Chemical and Biological Weapons Programs," Asia Report No. 167, Brussels, June 18, 2009. As of April 7, 2022: https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/north-korea-s-chemical-and-biological-weapons-programs

"Interview: Syria, Iran Main Buyers of North Korean Chemical Weapons," Radio Free Asia, October 3, 2013. As of April 7, 2022: https://www.rfa.org/english/news/korea/interview-10032013130040.html/

Ishimaru, Jiro, "Inside N. Korea: Maximum Punishment Under the 'Korean Wave Suppression Act' Is Death . . . Still, K-Pop Is Popular," *Rimjin-Gang*, May 19, 2021. As of April 7, 2022: https://www.asiapress.org/rimjin-gang/2021/05/recommendations/kpop-2/

Jang, Seulkee, "코로나 정보 전문 탈취 정찰총국 325국, 김정은 직접 챙긴다" [Kim Jong Un Taking Personal Care of Office 325, a Dedicated COVID-19 Intelligence Gathering Unit], *Daily NK*, February 4, 2021. As of December 13, 2021: https://www.dailynk.com/코로나-정보-전문-탈취하는-정찰총국-산하-325국-김정은/

Japan Ministry of National Defense, *Defense of Japan 2021*, Tokyo, 2021. As of November 12, 2021: https://www.mod.go.jp/en/publ/w_paper/wp2021/DOJ2021_EN_Full.pdf

Jeong Yong-soo, "Kim Jong-il's Final Orders: Build More Weapons," *JoongAng Ilbo*, January 29, 2013. As of April 7, 2022: https://koreajoongangdaily.joins.com/2013/01/29/politics/Kim-Jongils-final-orders-Build-more-weapons/2966344.html

Jeong Yong-soo and Ser Myo-ja, "Kim Jong-un Ordered a Plan for a 7-day Asymmetric War: Officials," *Joongang Daily*, January 7, 2015. As of April 7, 2022: http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=2999392

Jo He-rim, "Fear of Biological Agent Strikes Busan as US Troops Continue Biosurveillance Project," *Korea Herald*, April 16, 2019. As of April 7, 2022: http://www.koreaherald.com/view.php?ud=20190415000701

Joint Chiefs of Staff, *Electronic Warfare*, Washington D.C., January 25, 2007. As of April 7, 2022: https://apps.dtic.mil/sti/citations/ADA464647

Joint Publication 3-13.1, *Electronic Warfare*, Washington, D.C.: Joint Chiefs of Staff, February 8, 2012.

Jones, Randall S., "North Korean Economy Shrinks in 2020," Korea Economic Institute, October 1, 2021. As of December 9, 2021: https://keia.org/the-peninsula/north-korean-economy-shrinks-in-2020/

Jun, Jenny, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses*, Washington, D.C.: Center for Strategic and International Studies, December 2015. As of April 7, 2022: https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations

Kallio, Eva R, Jonas Klingstrom, Elisabeth Gustafsson, Tytti Manni, Antti Vaheri, Heikki Henttonen, Olli Vapalahti, and Ake Lundkvist, "Prolonged Survival of Puumala Hantavirus Outside the Host: Evidence for Indirect Transmission via the Environment," *Journal of General Virology*, Vol. 87, No. 8, August 2006, pp. 2127–2134. As of April 7, 2022: https://www.ncbi.nlm.nih.gov/pubmed/16847107

Kaspersky, "What Is a Zero-Day Attack? Definition and Explanation," webpage, undated. As of January 27, 2022: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

"KBS Reports Plan to Topple Kim Il Sung," *Washington Times*, March 25, 1994, p. 16.

Kepco, "National Power Grid," webpage, undated. As of April 7, 2022: https://home.kepco.co.kr/kepco/EN/B/htmlView/ENBAHP003.do?menuCd=EN020103

Kim, Hyun-Kyung, Elizabeth Philipp, and Hattie Chung, *North Korea's Biological Weapons Program: The Known and Unknown*, Cambridge, Mass.: Belfer Center for Science and International Affairs, October 2017. As of April 7, 2022: https://www.belfercenter.org/publication/north-koreas-biological-weapons-program-known-and-unknown

Kim Il Gi, and Kim Ho Heung, *"*김정은 시대의 북한 정보기구" [North Korea's Intelligence Agencies in the Kim Jong Un Era], INSS Research Report 2020-6, Washington, D.C.: Institute for National Security Strategy, June 2020.

Kim, Jeongmin, "North Korea Says Seoul 'Crazy' to Talk of Preemptive Strike on 'Nuclear Power,'" *NKNews*, April 3, 2022. As of April 7, 2022: https://www.nknews.org/2022/04/north-korea-says-seoul-crazy-to-talk-of-preemptive-strike-on-nuclear-power/

"Kim Jong Il Vanishes from Public Eye," *Donga Ilbo*, August 7, 2006.

Kong Ji-Young, Lim Jong In, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky, eds., *2019 11th International Conference on Cyber Conflict (CyCon)*, Talinn, Estonia: NATO CCD COE Publications, 2020. As of November 8, 2021: https://ieeexplore.ieee.org/document/8756954

Korean Disease Control and Prevention Agency, *Public Health Weekly Report: National Notifiable Infectious Diseases*, December 25, 20211. As of April 7, 2022: https://www.kdca.go.kr/upload_comm/syview/doc.html?fn=164091746630800.pdf&rs=/upload_comm/docu/0032/

Kristensen, Hans, M., and Matthew McKinzie, "Video Shows Earth-Penetrating Capability of B61-12 Nuclear Bomb," Washington, D.C.: Federation of American Scientists, 2016. As of April 7, 2022: https://fas.org/blogs/security/2016/01/b61-12_earth-penetration/

Kwon, K.J., "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," CNN, April 22, 2015. As of April 7, 2022: https://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html

Lankov, Andrei, "How to Stop the Next Korean War," *Foreign Policy*, December 16, 2010. As of April 7, 2022: www.foreignpolicy.com/articles/2010/12/16/how_to_stop_the_next_korean_war

Lankov, Andrei, and Peter Ward, "No, You're the Puppet: Why North Korea Isn't a Chinese Satellite," *NKNews*, May 14, 2020. As of April 7, 2022: https://www.nknews.org/2020/05/no-youre-the-puppet-why-north-korea-isnt-a-chinese-satellite/

"Lawmaker Claims N. Korean Hackers Breached Nuclear Power Agency in S. Korea," *Pulse News*, June 18, 2018. As of December 15, 2021: https://pulsenews.co.kr/view.php?sc=30800024&year=2021&no=591225

Layton, Lee, "Electromagnetic Pulse and Its Impact on the Electric Power Industry," PDHonline Course E402, Fairfax, Va.: PDHonline, 2016. As of April 7, 2022: https://pdhonline.com/courses/e402/e402content.pdf

Lee Chae Un, "N. Korean Middle School Student Sentenced to 14 Years of Forced Labor for Watching S. Korean Film," *Daily NK*, 2021. As of April 7, 2022: https://www.dailynk.com/english/north-korean-middle-school-student-sentenced-14-years-forced-labor-watching-south-korean-film/

Lee, Ho Wang, C. N. Ahn, J. W. Song, L. J. Baek, T. J. Seo, and S. C. Park, "Field Trial of an Inactivated Vaccine Against Hemorrhagic Fever with Renal Syndrome in Humans," *Archives of Virology*, Supplement 1, 1990.

Lee, Ho Wang, and Guido van der Groen, "Hemorrhagic Fever with Renal Syndrome," in J. L. Melnick, ed., *Progress in Medical Virology*, Vol. 36, 1989, pp. 63–102.

Lee Je-hun, "N. Korea No Longer Pursues Unification Through Revolution in S. Korea," *Hankyoreh,* June 1, 2021. As of May 30, 2022: https://english.hani.co.kr/arti/english_edition/e_northkorea/997545.html

Lee, Jeong-ho, "North Korea's Economy Contracted Most in Two Decades in 2020," Bloomberg, July 29, 2021. As of April 7, 2022: https://www.bloomberg.com/news/articles/2021-07-30/north-korea-s-economy-contracted-most-in-two-decades-in-2020

Lee Min-seok, "N. Korean Hackers 'Work out of Chinese Hotels,'" *Chosun Ilbo*, April 25, 2022. As of April 7, 2022: http://english.chosun.com/site/data/html_dir/2022/04/25/2022042501085.html

Lee Sang-heon, "‹北사이버전 전담부대 `110호연구소'는›" [North Korean Cyber Warfare Unit 'Research Center 110], Yonhap News Agency, July 10, 2009. As of December 9, 2021: https://www.yna.co.kr/view/AKR20090710197700043

Lee, Sang Sin, Tae-un Min, Kwang-il Yoon, Bon-sang Koo, and Peter Gries, "KINU Unification Survey 2020: Press Briefing," Seoul: Korea Institute of National Unification, June 26, 2020.

Lepore, Stephen M., and Alastair Talbot, "'If We Can't Defend Guam It's Really Hard to Project Power into the Pacific': US Builds Iron Dome on America's Closest Military Base to China," *Daily Mail*, November 9, 2021. As of April 7, 2022: https://www.dailymail.co.uk/news/article-10183037/U-S-tests-Iron-Dome-Guam-defense-against-Chinese-cruise-missiles.html

Lewis, James A., "The Likelihood of North Korean Cyber Attacks," Washington, D.C.: Center for Strategic and International Studies, September 7, 2017. As of April 7, 2022: https://www.csis.org/analysis/likelihood-north-korean-cyber-attacks

Liu, Rongrong, Hongwei Ma, Jiayi Shu, Qiang Zhang, Mingwei Han, Ziyu Liu, Xia Jin, Fanglin Zhang, and Xingan Wu, "Vaccines and Therapeutics Against Hantaviruses," *Frontiers in Microbiology*, Vol. 10, January 30, 2020. As of April 7, 2022: https://www.frontiersin.org/article/10.3389/fmicb.2019.02989

"Live Anthrax Shipped Accidentally to S Korea and US Labs," BBC, May 28, 2015. As of April 7, 2022: https://www.bbc.com/news/world-us-canada-32910020

"A Look at Mirim College, Hotbed of Cyber Warfare," *Daily NK*, May 6, 2011. As of December 6, 2021: https://www.dailynk.com/english/a-look-at-mirim-college-hotbed-of/

Lord Lyell, *Chemical and Biological Weapons: The Poor Man's Bomb*, Brussels: Committees of the North Atlantic Assembly, October 4, 1996. As of April 7, 2022: https://irp.fas.org/threat/an253stc.htm

Love, Jeffrey J., Greg M. Lucas, Benjamin S. Murphy, Paul A. Bedrosian, E. Joshua Rigler, and Anna Kelbert, "Down to Earth with Nuclear Electromagnetic Pulse: Realistic Surface Impedance Affects Mapping of the E3 Geoelectric Hazard," *Earth and Space Science*, Vol. 8, No. 8, 2021, p. e2021EA001792. As of April 7, 2022: https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/2021EA001792

Lurie, Ranan R., "In a Confrontation, 'North Korea Will Definitely Be Annihilated,'" *Los Angeles Times (Washington)*, March 24, 1994, p. 11.

Mansourov, Alexandre Y., *Kim Jong Un's Nuclear Doctrine and Strategy: What Everyone Needs to Know*, Berkeley, Calif.: Nautilus Institute, December 16, 2014. As of April 7, 2022: http://nautilus.org/napsnet/napsnet-special-reports/kim-jong-uns-nuclear-doctrine-and-strategy-what-everyone-needs-to-know/

"[3·20 사이버테러' 북한 소행] 대남공작·사이버전 총괄 핵심기구. . . 정예 해커만 3000여명 보유 추정" ['March 20th Cyber Terrorist Attack' by North Korea] Top Command Agency Responsible for Counter-South Operations and Cyber Warfare. . . Believed to Have at Least 3,000 Elite Hackers], *Seoul Shinmun*, April 11, 2013. As of December 15, 2021: https://www.seoul.co.kr/news/newsView.php?id=20130411008007

Maresca, Thomas, "N. Korea Warns of Nuclear Response to South If Attacked: 'Total Destruction and Ruin,'" United Press International, April 5, 2022. As of May 30, 2022: https://www.upi.com/Top_News/World-News/2022/04/05/Kim-Yo-Jong-nuclear-response-destruction-preemptive-strike/9391649142526/

Marrs, Timothy C., Robert L. Maynard, and Frederick Sidell, *Chemical Warfare Agents: Toxicology and Treatment,* 2nd ed. Chichester, UK: John Wiley and Sons, 2007.

Melloan, George, "Bush Reveals His Foreign Policy in the Kim Meeting," *Wall Street Journal*, March 13, 2001. As of April 7, 2022: https://www.wsj.com/articles/SB984443811922091876

Miller, Judith, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War*, New York: Simon & Schuster, 2001.

Min Hur, "North Korea's RGB Controlling at Least Six Hacking Units . . . Vaccine Producers Also Targeted" [北정찰총국, 최소 6개 해킹그룹 관리. . .백신 제약사도 '타깃'], *Munhwa Ilbo*, August 21, 2021. As of May 30, 2022: http://www.munhwa.com/news/view.html?no=2021081201030742000001

MITRE ATT&CK, "Disk Wipe," webpage, undated a. As of January 27, 2022: https://attack.mitre.org/techniques/T1561/.

———, "Drive-by Compromise," webpage, undated b. As of January 27, 2022: https://attack.mitre.org/techniques/T1189/

———, "Network Denial of Service," webpage, undated c. As of January 27, 2022: https://attack.mitre.org/techniques/T1498/

———, "Phishing," webpage, undated d. As of January 27, 2022: https://attack.mitre.org/techniques/T1566/001/

Moon Seong-hwi, "North Korea Moves Its Wartime Command Center to Nampo Taesan," *Liberty Korea Post*, July 7, 2018. As of April 7, 2022: http://www.lkp.news/news/article.html?no=4808

———, "The Location of Kim Jong-un's Villas in North Korea," *Liberty Korea Post*, July 16, 2018. As of April 7, 2022: https://www.lkp.news/news/article.html?no=4872

Moore, Jack, "North Korea Wants to Hit the U.S. with an Anthrax-Tipped Missile: Report," *Newsweek*, December 20, 2017. As of April 7, 2022: https://www.newsweek.com/north-korea-wants-hit-us-anthrax-tipped-missile-753355

Motoko, Rich, "In North Korea, 'Surgical Strike' Could Spin into 'Worst Kind of Fighting,'" *New York Times*, July 5, 2017. As of April 7, 2022: https://www.nytimes.com/2017/07/05/world/asia/north-korea-south-us-nuclear-war.html

Mun Dong Hui, "North Korean Propaganda Promotes EMP Attacks Using Nuclear Weapons," *Daily NK*, November 23, 2018. As of April 7, 2022: https://www.dailynk.com/english/north-korean-propaganda-promotes-emp-attacks-using-nuclear-weapons/

Munroe, Tony, and Jane Chung, "For North Korea, Cutting Off Oil Supplies Would Be Devastating," Reuters, April 13, 2017. As of April 7, 2022: https://www.reuters.com/article/us-northkorea-nuclear-china-oil/for-north-korea-cutting-off-oil-supplies-would-be-devastating-idUSKBN17F17L

National Research Council of the National Academies, *Effects of Nuclear Earth-Penetrator and Other Weapons, the National Academies Press*, Washington, D.C.: National Academies Press, 2005.

"Navalny 'Poisoned': What Are Novichok Agents and What Do They Do?" BBC, September 2, 2020. As of April 7, 2022: https://www.bbc.com/news/world-europe-43377698

Nichols, Michelle, "North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: UN Report," Reuters, August 5, 2019. As of April 7, 2022: https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

"N. Korea 'Exporting Chemical Weapons Parts to Syria,'" *Chosun Ilbo*, June 17, 2013. As of April 7, 2022: http://english.chosun.com/site/data/html_dir/2013/06/17/2013061700887.html

"N. Korea's Cyber Warfare Unit in Spotlight After Their Attack on S. Korean Bank," Yonhap News Agency, May 3, 2011. As of May 30, 2022: https://en.yna.co.kr/view/AEN20110503010600315

"N. Korea's Elite Military Hackers Trained to Attack High Tech Powers," *East-Asia-Intel*, October 12, 2004.

"N. Korea Trains Up Hacker Squad," *Chosun Ilbo*, March 8, 2011. As of April 7, 2022: http://english.chosun.com/site/data/html_dir/2011/03/08/2011030800611.html

Noh, Ji Yun, Jaehun Jung, and Jin-Won Song, "Hemorrhagic Fever with Renal Syndrome," *Infection & Chemotherapy*, Vol. 51, No. 4, December 2019, pp. 405–413. As of April 7, 2022: https://doi.org/10.3947/ic.2019.51.4.405

"North Korea Recruits Hackers at School," *Al-Jazeera*, June 20, 2011. As of December 15, 2021: https://www.aljazeera.com/features/2011/6/20/north-korea-recruits-hackers-at-school

North Korea Strategic Information Center, "Full Text of Kim Jong-il's Will," translated by Diana Myers, *You Korea News*, 2012. As of April 7, 2022: http://www.ukoreanews.com/news/articleView.html?idxno=657

"North Korea Tests Longest-Range Missile Since 2017," NPR, January 29, 2022. As of April 7, 2022: https://www.npr.org/2022/01/29/1076751251/north-korea-missile-launch

"Nuclear Nightmare—Understanding North Korea," Discovery Channel, August 6, 2003.

Office of Senator James M. Inhofe, "ICYMI: Inhofe Requests Honest Assessment from Military Leaders on State of Readiness," press release, September 16, 2016. As of June 21, 2022: https://www.inhofe.senate.gov/newsroom/press-releases/icymi-inhofe-requests-honest-assessment-from-military-leaders-on-state-of-readiness

Office of the Director of National Intelligence, *Threat Assessment of the U.S. Intelligence Community*, Washington, D.C., 2021.

———, *Annual Threat Assessment of the U.S. Intelligence Community*, Washington, D.C., February 2022. As of April 7, 2022: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community

Oxford, Sean M., Lucas A. LaViolet, Kristen A. Bishop, Julia K. Burr, Carl A. Curling, Lusine Danakian, Deena S. Disraelly, Brian A. Haugh, Margaret C. Hebner, Audrey C. Kelley, Royce R. Kneece, Preston J. Lee, Christina M. Patterson, Daniel K. Rosenfield, Hans C. Sitarz, Robert S. Sneddon, Terri J. Walsh, Mike O. Wheeler, and Robert A. Zirkle, *Technical Reference Manual to Allied Medical Publication 7.5 (AMedP-7.5) NATO Planning Guide for the Estimation of CBRN Casualties*, Alexandria, Va.: Institute for Defense Analyses, October 2016. As of May 31, 2022: https://apps.dtic.mil/sti/pdfs/AD1039464.pdf

Paddock, Richard C., and Choe Sang-Hun, "Kim Jong-nam Was Killed by VX Nerve Agent, Malaysians Say," *New York Times*, February 23, 2017. As of April 7, 2022: https://www.nytimes.com/2017/02/23/world/asia/kim-jong-nam-vx-nerve-agent-.html

Palo Alto Networks, "Email Credential Harvesting at Scale Without Malware," webpage, undated a. As of January 27, 2022: https://unit42.paloaltonetworks.com/credential-harvesting/

———, "What Is DNS Tunneling?" webpage, undated b. As of January 27, 2022: https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Parachini, John, "North Korea's CBW Program: How to Contend with Imperfectly Understood Capabilities," *Prism*, Vol. 7, No. 3, 2018, pp. 94–95. As of April 7, 2022: https://cco.ndu.edu/News/Article/1516496/north-koreas-cbw-program-how-to-contend-with-imperfectly-understood-capabilities/

———, "Why We Should Be Skeptical About Recent Reports on North Korea's Biological Weapons Programs," 38 North, January 30, 2019. As of April 7, 2022: https://www.38north.org/2019/01/jparachini013019/

Park Won Gon, "Strategic Implications of the USFK Relocation to Pyeongtaek," Seoul, South Korea: Korea Institute for Defense Analyses, No. 164, October 20, 2017. As of March 28, 2022: As of April 7, 2022: https://kida.re.kr/frt/board/frtPcrmBoard.do?sidx=366&depth=3

Pike, Steven, "What Are the Most Common Types of Chemical Warfare Agent (CWA)?" Luton, UK: Argon, 2019. As of April 7, 2022: https://www.argonelectronics.com/blog/what-are-the-most-common-types-of-chemical-warfare-agent-cwa

Postol, Theodore A., Markus Schiller, and Robert Schmucker, "North Korea's 'Not Quite' ICBM Can't Hit the Lower 48 States," *Bulletin of the Atomic Scientists*, August 29, 2017. As of April 7, 2022: https://thebulletin.org/2017/08/north-koreas-not-quite-icbm-cant-hit-the-lower-48-states/

Potter, Robert, "Toward a Better Understanding of North Korea's Cyber Operations," 38 North, August 5, 2019. As of December 6, 2021: https://www.38north.org/2019/08/rpotter080519/

Price, Ned, "Syria: Eighth Anniversary of the Ghouta Chemical Weapons Attack," Washington, D.C.: U.S. Department of State, August 21, 2021. As of April 7, 2022: https://www.state.gov/syria-eighth-anniversary-of-the-ghouta-chemical-weapons-attack

Proofpoint, "What Is Ransomware?" webpage, undated. As of January 27, 2022: https://www.proofpoint.com/us/threat-reference/ransomware

Pry, Peter Vincent, "North Korea EMP Attack: An Existential Threat Today," *Cipher Brief*, August 22, 2019. As of April 7, 2022: https://www.thecipherbrief.com/column_article/north-korea-emp-attack-an-existential-threat-today

———, "Russia: EMP Threat," EMP Task Force on National and Homeland Security, January 2021. As of April 7, 2022: https://apps.dtic.mil/sti/pdfs/AD1124730.pdf

———, "North Korea: EMP Threat, North Korea's Capabilities for Electromagnetic Pulse (EMP) Attack," EMP Task Force on National and Homeland Security, June 6, 2021. As of April 7, 2022: https://emptaskforce.us/wp-content/uploads/2021/06/REPORTempthreatNK21A.pdf

Public Broadcasting System, "Secrets of the Dead. Umbrella Assassin: Clues and Evidence," June 3, 2014. As of April 7, 2022: https://www.pbs.org/wnet/secrets/umbrella-assassin-clues-evidence/1552/

Radasky, William, and Edward Savage, *High-Frequency Protection Concepts for the Electric Power Grid*, Goleta, Calif.: Metatech Corporation, January 2010.

Radasky, William A., and Peter Vincent Pry, "Blackout Warfare: High-Altitude Electromagnetic Pulse (HEMP) Attack on the U.S. Electric Power Grid," EMP Task Force on National and Homeland Security, August 6, 2021. As of April 7, 2022: https://emptaskforce.us/wp-content/uploads/2021/08/BLACKOUTWARFAREhemp REPORTfinal21X.pdf

Ramalingaswami, V., "Psychosocial Effects of the 1994 Plague Outbreak in Surat, India," *Military Medicine*, Vol. 166, Supplement 2, December 2001, pp. 29–30.

Ray, Siladitya, "Kim Jong-Un's Powerful Sister Threatens Nuclear Elimination of South Korea's Military After Pre-Emptive Strike Warning," *Forbes*, April 5, 2022. As of April 7, 2022: https://www.forbes.com/sites/siladityaray/2022/04/05/kim-jong-uns-powerful-sister-threatens-nuclear-elimination-of-south-korea-after-pre-emptive-strike-warning/?sh=86b0eb64694c

Reardon, Sara, "US Military Accidentally Ships Live Anthrax to Labs," *Nature*, May 28, 2015. As of April 7, 2022: https://doi.org/10.1038/nature.2015.17653

Regencia, Ted, "Chemical Attacks on Iran: When the US Looked the Other Way," *Al Jazeera*, April 19, 2018. As of April 7, 2022: https://www.aljazeera.com/news/2018/4/19/chemical-attacks-on-iran-when-the-us-looked-the-other-way

Reim, Garrett, "How Sweden's Austere Basing System Influenced the Gripen," *Flight Global,* July 15, 20200. As of April 7, 2022: https://www.flightglobal.com/fixed-wing/how-swedens-austere-basing-system-influenced-the-gripen/139316.article

Reissman, Dori B., Ellen A. S. Whitney, Thomas H. Taylor, Jr., James A. Hayslett, Peter M. Dull, Ileana Arias, David A. Ashford, Eddy A. Bresnitz, Christina Tan, Nancy Rosenstein, and Bradley A. Perkins, "One-Year Health Assessment of Adult Survivors of Bacillus Anthracis Infection," *JAMA*, Vol. 291, No. 16, 2004, pp. 1994–1998. As of February 24, 2022: https://doi.org/10.1001/jama.291.16.1994

Republic of Korea, Ministry of National Defense, *2000 Defense White Paper*, 2000.

———, *2012 Defense White Paper*, 2012.

———, *2018 Defense White Paper*, 2018. As of July 20, 2021: https://mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_20190807015339084O.pdf

———, *2020 Defense White Paper*, 2020. As of November 12, 2021: https://mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_202106300300426680.pdf

Rivera, Michael Kelly, Scott N. Backhaus, Jesse Richard Woodroffe, Michael Gerard Henderson, Randall J. Bos, Eric Michael Nelson, and Andjelka Kelic, *EMP/GMD Phase 0 Report: A Review of EMP Hazard Environments and Impacts*, Los Alamos, N.M.: Los Alamos National Laboratory, LA-UR-16-28380, 2016. As of April 7, 2022: https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-16-28380

Ryall, Julian, "North Korean Defector Details 'Human Experiments,'" DW, December 30, 2014. As of April 7, 2022: https://www.dw.com/en/north-korean-defector-details-human-experiments/a-18161851

Sailor, Michael J., "Detect to Protect." *ACS Sensors*, Vol. 5, No. 5, 2020, pp. 1247–1248. As of April 7, 2022: doi:10.1021/acssensors.0c00920

Sanger, David E., and William J. Broad, "North Korea Missile Tests, 'Very Standard' to Trump, Show Signs of Advancing Arsenal," *New York Times*, September 2, 2019. As of April 7, 2022: https://www.nytimes.com/2019/09/02/world/asia/north-korea-kim-trump-missiles.html

Sanger, David, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 17, 2017.

Savage, Edward, James Gilbert, and William Radasky, "The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid," Goleta, Calif.: Metatech Corporation, January 2010. As of April 7, 2022: http://large.stanford.edu/courses/2019/ph241/rogers1/docs/meta-r-320.pdf

Schmaljohn, Connie S., "Vaccines for Hantaviruses: Progress and Issues," *Expert Review of Vaccines*, Vol. 11, No. 5, May 2012, pp. 511–513. As of April 7, 2022: https://www.ncbi.nlm.nih.gov/pubmed/22827236

Schwartz, Thomas A., "Statement of the Commander In Chief United Nations Command/Combined Forces Command & Commander, United States Forces Korea, Before the 107th Congress, Senate Armed Services Committee," Washington, D.C., 2002.

Scobell, Andrew, and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles*, Carlisle, Penn.: Strategic Studies Institute, 2007. As of April 7, 2022: https://www.hsdl.org/?view&did=473134

Ser Myo-ja, "Park Tells Military to Strike Back If Attacked," *JoongAng Ilbo*, April 2, 2013. As of April 7, 2022: http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2969490

Shalal, Andrea, and David Bunnstrom, "North Korea Satellite in Stable Orbit but Seen Transmitting: U.S. Sources," Reuters, February 9, 2016. As of April 7, 2022: https://www.reuters.com/article/us-northkorea-satellite-orbit/north-korea-satellite-in-stable-orbit-but-not-seen-transmitting-u-s-sources-idUSKCN0VI1XN

Shin Hyon-hee, "USFK Conducted 16 Covert Anthrax Tests Since 2009," *Korea Herald*, December 17, 2015. As of April 7, 2022: http://www.koreaherald.com/view.php?ud=20151217001153

Sidell, Frederick R., Ernest T. Takafuji, and David R. Franz, *Medical Aspects of Chemical and Biological Warfare*, Falls Church, Va.: Office of the Surgeon General (Army) July 1, 1997. As of April 7, 2022: https://apps.dtic.mil/sti/citations/ADA398241

Siers, Rhea, "North Korea: The Cyber Wild Card," *Journal of Law and Cyber Warfare*, Vol. 4, No. 1, Winter 2014, pp. 1–12.

Slaughter, Matthew J., and David H. McCormick, "Data Is Power: Washington Needs to Craft New Rules for the Digital Age," *Foreign Affairs*, Vol. 100, No. 3, May/June 2021. As of December 15, 2021: https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

Smithson, Amy E., "Rethinking the Lessons of Tokyo," in Leslie-Anne Levy and Amy E. Smithson, eds., *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Washington, D.C.: Stimson, October 9, 2000. As of April 7, 2022: https://www.stimson.org/2000/ataxia-chemical-and-biological-terrorism-threat-and-us-response/

Snyder, Don, Elizabeth Bodine-Baron, Mahyar A. Amouzegar, Kristin F. Lynch, Mary Lee, and John G. Drew, *Robust and Resilient Logistics Operations in a Degraded Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2015-AF, 2017. As of May 17, 2022:
https://www.rand.org/pubs/research_reports/RR2015.html

Song, Joon Young, Heung Jeong Woo, Hee Jin Cheong, Ji Yun Noh, Luck Ju Baek, and Woo Joo Kim, "Long-Term Immunogenicity and Safety of Inactivated Hantaan Virus Vaccine (Hantavax™) in Healthy Adults," *Vaccine,* Vol. 34, No. 10, 2016, pp. 1289–1295. As of April 7, 2022:
https://www.sciencedirect.com/science/article/pii/S0264410X1600075X

Song Sang-ho, "Cheonan Sinking Reshapes Military Strategies," *Korea Herald*, March 20, 2011. As of April 7, 2022:
http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110320000368

———, "Gov't to Check Cybersecurity Vulnerabilities of Local Defense Firms," Yonhap News Agency, March 4, 2022. As of April 7, 2022:
https://en.yna.co.kr/view/AEN20220304003000325

"South Estimates DPRK Has 5,000 Tons of Chemical Weapons, Mostly Sarin," *Seoul Shinmun*, April 15, 1995, p. 1.

"South Says North Korea Has 1,000 Tons of Chemical Weapons," Yonhap News Agency, March 21, 1995.

Stout, Brady, "Email Credential Harvesting at Scale Without Malware," Palo Alto Networks, September 30, 2021. As of January 27, 2022:
https://unit42.paloaltonetworks.com/credential-harvesting/

Taylor, Henry L., and Jesse Orlansky, *The Effects of Wearing Protective Chemical Warfare Combat Clothing on Human Performance*, Alexandria, Va.: Institute for Defense Analyses, August 1991. As of April 7, 2022:
https://apps.dtic.mil/sti/citations/ADA250716

"Tokyo Sarin Attack: Japan Executes Last Aum Shinrikyo Members on Death Row," BBC, July 26, 2018. As of April 7, 2022:
https://www.bbc.com/news/world-asia-44962581

Tucker, Jonathan, ed., "Biological Weapons in the Former Soviet Union: An Interview with Dr. Kenneth Alibek," *Nonproliferation Review*, Spring–Summer 1999. As of April 7, 2022:
https://www.nonproliferation.org/wp-content/uploads/npr/alibek63.pdf

United States Forces Korea, "Force Health Protection (FHP) Requirements for the Korean Peninsula," Regulation 40-9, October 20, 2021. As of April 7, 2022:
https://8tharmy.korea.army.mil/g1/assets/regulations/usfk/USFK-Reg-40-9-FHP-Requirements-kn.pdf

U.S. Army, *Potential Military Chemical/Biological Agents and Compounds*, UFM 3-11.9, January 2005. As of May 31, 2022: https://irp.fas.org/doddir/army/fm3-11-9.pdf

U.S. Army Medical Research Institute of Infectious Diseases, *USAMRIID's Medical Management of Biological Casualties Handbook*, 9th ed., Frederick, Md., September 2020. As of April 7, 2022: https://www.usamriid.army.mil/education/bluebookpdf/USAMRIID's%20Blue%20Book%209th%20edition%20-%20PDF%20format.pdf

U.S. Congress, Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks*, Washington, D.C., August 1993. As of May 31, 2022: https://www.princeton.edu/~ota/disk1/1993/9341/9341.PDF

U.S. Department of the Army, *North Korean Tactics*, ATP 7-100.2, Washington, D.C., July 24, 2020. As of April 7, 2022: https://irp.fas.org/doddir/army/atp7-100-2.pdf

U.S. Department of Defense, *Nuclear Posture Review Report*, Washington, D.C., April 2010. As of April 7, 2022: https://dod.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf

———, *2018 Nuclear Posture Review*, Washington, D.C., February 2018. As of April 7, 2022: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-Nuclear-Posture-Review-Final-Report.pdf

———, *Nuclear Matters Handbook,* Washington, D.C., 2020, Chapter 13. As of April 7, 2022: https://www.acq.osd.mil/ncbdp/nm//NMHB2020rev/Chapters/chapter13.html

U.S. Department of Justice, Office of Public Affairs, "First U.S.–China Law Enforcement and Cybersecurity Dialogue: Summary of Outcomes," Washington, D.C., October 6, 2017. As of December 10, 2021: https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue

U.S. Department of State, "Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments," Washington, D.C., April 2021. As of April 7, 2022: https://www.state.gov/2021-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments/

U.S. Senate, "North Korean Missile Proliferation: Hearing Before the Subcommittee on International Security, Proliferation, and Federal Services of the Committee on Governmental Affairs," Washington, D.C., 1997. As of April 7, 2022: www.gpo.gov/fdsys/pkg/CHRG-105shrg44649/pdf/CHRG-105shrg44649.pdf

Van McCrary, S., "Smallpox and Bioterrorism: A Growing Threat," University of Houston, Health, Law, and Policy Institute, August 3, 1999. As of April 7, 2022: https://www.law.uh.edu/healthlaw/perspectives/Bioethics/990803Smallpox.html

Vogel, Al, "New Chem/Bio Detector Faces Test for Next Six Years," *U.S. Army*, May 20, 2020. As of April 7, 2022: https://www.army.mil/article/235749/new_chembio_detector_faces_test_for_six_years

Voytan, Dimitri P., Thorne Lay, Esteban J. Chaves, and John T. Ohman, "Yield Estimates for the Six North Korean Nuclear Tests from Teleseismic P Wave Modeling and Intercorrelation of P and Pn Recordings," *Journal of Geophysical Research: Solid Earth*, Vol. 124, No. 5, 2019, pp. 4916–4939. As of April 7, 2022: https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/2019JB017418

Walker, Paul F., "Presentation to the 22nd CWC Conference of States Parties," paper presented at the 22nd CWC Conference of States Parties, Organization for the Prohibition of Chemical Weapons, 2017.

Washington Post Staff, "Read President Biden's First Address to a Joint Session of Congress," *Washington Post*, April 28, 2021. As of April 7, 2022: https://www.washingtonpost.com/politics/2021/04/28/transcript-biden-joint-session-congress/

Weisensee, Nils, "New Cyberattack Hits North Korea After Hacker Claims Responsibility for Outages," *NKNews*, February 3, 2022. As of April 7, 2022: https://www.nknews.org/2022/02/new-cyberattack-hits-north-korea-after-hacker-claims-responsibility-for-outages/

"What Was Bhopal Gas Tragedy?" *Business Standard*, undated. As of April 7, 2022: https://www.business-standard.com/about/what-is-bhopal-gas-tragedy

The White House, "U.S.–ROK Leaders' Joint Statement," Washington, D.C.: May 21, 2021.

White House Office of the Press Secretary, "Fact Sheet: President Xi Jinping's Visit to the United States," Washington, D.C.: September 25, 2015.

Williams, Martyn, "Russia Provides New Internet Connection to North Korea," 38 North, October 1, 2017. As of January 27, 2022: https://www.38north.org/2017/10/mwilliams100117/

Windrem, Robert, "Soviets Planned Smallpox Attack," MSNBC, August 21, 2001.

Young, Benjamin R., "Understanding North Korea's 'Final Victory' and Why It Matters," *NK News*, September 6, 2021. As of December 13, 2021: https://www.nknews.org/2021/09/understanding-north-koreas-final-victory-and-why-it-matters/

Zwirko, Colin, “Kim Jong Un’s Body ‘Withered’ as He ‘Suffered’ for the People, State TV Says,” *NK News*, 2022. As of April 7, 2022: https://www.nknews.org/2022/02/kim-jong-un-completely-withered-as-he-suffered-for-the-people-state-tv-says/

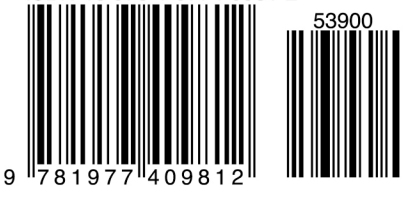
NATIONAL SECURITY RESEARCH DIVISION

To secure the survival of its regime, dominate the Republic of Korea (ROK), and impose unification of the Korean Peninsula, North Korea has amassed a variety of weapons of mass destruction (WMD)—nuclear, chemical, and biological—to include nuclear and likely conventional capabilities that produce highly destructive or even lethal electromagnetic pulse. It also has diverse offensive cyber capabilities that it uses for covert and illegal purposes. The authors of this report focus on how the North could use, and does use, these weapons and capabilities to affect peacetime relations on the peninsula and to prepare for a major war with the ROK, as well as the possible effects of their employment on the military, on civilians, and on critical infrastructure.

The authors present a theory of deterrence and suggest how the ROK-U.S. alliance could rein in North Korean efforts to augment or enhance its WMD and cyber capabilities and deter the North from attacking the ROK and beyond. Throughout, the authors acknowledge the uncertainties involved and argue that any effective action on the part of the ROK-U.S. alliance will require recognizing and managing those uncertainties.

$39.00

ISBN-10 1-9774-09814
ISBN-13 978-1-9774-0981-2



www.rand.org

RR-A2026-1