



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Thesis for the Degree of Doctor of Philosophy

The Dilemma of Software Uniformity and Cybersecurity in South Korea

by

John Gustave Swanda

Department of International & Area Studies

The Graduate School

Pukyong National University

August 26, 2016

The Dilemma of Software Uniformity and Cybersecurity in South Korea

Advisor: Prof. Dongsoo Kim

by

John Gustave Swanda

A thesis submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
in Department of International & Area Studies, The Graduate School,
Pukyong National University

August 26, 2016

The Dilemma of Software Uniformity and Cybersecurity in South Korea

A Doctoral dissertation

by

John Gustave Swanda

Approved by

김저우

(Chairman)

이홍종

(Member)

고종환

(Member)

Sean O'Malley

(Member)

김동수

(Member)

August 26, 2016

존 거스텝 스완다

부경대학교 국제지역학과 대학원

국문초록

이번 논문에서는 소프트웨어 획일성의 맥락에서 한국의 사이버 보안에 대해 살펴보기로 한다. 이를 통해 연구저자는 한국의 사이버 역동성이라는 틀 안에서 동기와 역량, 행동, 기술적 특징들에 대해 확인한다. 이번 논문은 계속적인 공개키 정책과 전략이 윈도우와 인터넷 익스플로러의 보안 취약성의 형태로 국가활동세력과 비국가활동세력의 위협에 공헌하였다고 본다. 또한, 국내 바이러스 퇴치프로그램 제작회사인 안철수연구소(Ahnlab)와 이소프트(Esoft) [프로그램이 각각 V3와 알약(Alyac)임]에서는 한국의 바이러스퇴치 시장에서 과점의 형태로 시장을 공유하고 있고, 유사한 취약한 부분을 해결하는데 공헌하고 있다. 운영체제 (윈도우), 브라우저 (인터넷 익스플로러), 바이러스퇴치용소프트웨어 (V3와 알약)의 획일성이 한국의 사이버보안에 부정적인 영향을 미칠 뿐만 아니라 해커들에게도 동기를 부여해 줄 수 있는, 즉 해커의 성공이 한국컴퓨터사용자들의 위험한 온라인 행동의 결과로서 결국 도움을 얻게 되는 환경을 만들어 낸다는 것이 바로 연구저자의 주장이다. 이것은 잠재적으로 한국 시스템의 완전성에 상당한 차이를 만들어낼 수 있다. 이번 연구는 한국의 주요한 사이버보안결정에 대해 문서로 기록하고, 주요한 변수 (관련된 행위자, 국제적 구조와 지역보안 패러다임과의 관계, 권력 대 국가보안역동성)를 해부하고, 국가활동세력과 비국가활동세력과 관련된 상호관련된 증거자료를 찾는다. 대규모 사이버습격과 관련한 공격 빈도, 범위, 기원, 방법에 대한 조사를 실시하여 한국 내 온라인 행동이나 규범과 관련된 이러한 공격에 대비한 정책의 효과성에 대해 파악하였다.

이번 연구는 여러 가지 이유로 독특한 특성을 지니고 있다. 첫째, 이번 연구에서는 한국 사이버보안전략에 있어서 소프트웨어 획일성의 특정한 유해한 효과를 추론하기 위해 관련성은 있지만 아직 종종 간과되는 비국가활동세력을 통해 수집한 자료를 사용한다. 개별최종사용자 행동이나 개별해커동기에 관한 광범위한 조사를 실시하여 어떻게 한국의 개별 컴퓨터 사용자들이 국가공개키정책을 실시한 결과 행동을 수정하게 되는지, 이러한 정책을 통해 생성된 사이버보안의 취약함이 해커들에 의해 이용당할 수 있는지에 대해 파악하였다. 그리고, 가장 중요하게, 이번 논문은 제시된 증거자료에 대해 상호교차성의 기본틀 안에서 검사를 실시하였다는 점에서 사이버보안에 관한 오리지널 접근법을 제시하였고, 한국의 사이버 위협 중 일부가 정책, 행동, 기술의 상호교차임을 시사했다.

연구저자는 한국의 과거와 현재의 사이버 전략이 시스템을 위험한 상태에 빠뜨릴 수 있는 방식으로 비국가활동세력들에게 영향을 미칠 수 있다는 결론을 내렸다. 입법 절차가 너무 느리고 정치적으로 편향되어 있어서 사이버환경의 변화에 반응할 수 없다. 그 결과, 좀 더 선제적이고 북한에 대해 선방하는 행정명령과 군사전략을 통해 많은 정책들이 유도되고 있다. 하지만,

그러한 정책들은 한국의 국가중심 사이버보안전략으로 감지할 수 없는 대규모의 해킹 위협을 잠재적으로 유인하면서, 사용중인 기술의 다양성을 협소화시키고 한국인들의 고위험 온라인 행동에 공헌하는 의도하지 않은 영향을 끼친다. 이러한 중앙 통제형 솔루션은 비국가활동세력으로부터의 위협과 기회라는 범위 전체에 완벽하게 또는 적절하게 적응할 수 없기 때문에, 한국사이버방어의 취약성에도 기여하지 못한다.

핵심어: 한국, 사이버보안, 해커, 소프트웨어획일성, 사이버공격, 상호교차성, 정책, 공개키



The Dilemma of Software Uniformity and Cybersecurity in South Korea

John Gustave Swanda

**Department of International & Area Studies, The Graduate School,
Pukyong National University**

Abstract

This dissertation examines South Korea's cyber security dilemma in the context of software uniformity. In doing so, the author ascertains the motives, capabilities, behavior and technical characteristics of actors within the South Korean cyber dynamic. It makes the supposition that continuous public-key policies and strategies have contributed to threats from both state and non-state actors, in the form of security vulnerabilities in *Windows* and *Internet Explorer*. In addition, domestic antivirus manufacturers *Ahnlab* and *Esoft*, whose programs are *V3* and *Alyac* respectively, share in an oligopoly of the South Korean antivirus market, and also contribute to similar vulnerabilities. It is the author's contention that the uniformity of operating systems (*Windows*), browsers (*Internet Explorer*), and antivirus software (*V3* and *Alyac*) have created an environment that not only negatively impacts cybersecurity in South Korea, but also may motivate hackers, the success of whom is aided by South Korean computer users' risky online behavior. This can potentially create significant gaps in the integrity of South Korean systems. This research documents major cyber security decisions in South Korea and dissects its main variables (the actors involved, relation to the international structure and regional security paradigm, and power vs. national security dynamic) and finds correlating evidence involving state and non-state actors. The frequency, scope, origins and method of attack of large-scale cyber incursions are investigated to determine the effectiveness of policy against these attacks as they concern online behavior and norms in South Korea.

This study is unique for several reasons. First, it uses data collected from relevant yet often ignored non-state actors to infer certain deleterious effects of software uniformity in South Korean cyber security strategy. Extensive surveys on individual end-user behavior and individual hacker motives and capabilities were conducted to determine both how individual computer users in South Korea possibly amend their behavior as a result of national public-key policies, and whether weaknesses in cyber security created by these policies could be exploited by hackers. Most importantly, this dissertation offers an original approach to cyber security in that the evidence presented is examined within a framework of intersectionality, and suggests that some of South Korea's cyber threats are the intersection of policy, behavior, and technology.

The author concludes that past and current cyber strategies in South Korea have effected non-state actors in ways that may put systems at risk. The legislative process is too slow and politically polarized to respond to changes in the cyber environment. As a result, many policies are derived through executive orders and military strategies, which are more proactive and defend well against North Korea. However, they have had the unintended consequences of narrowing the diversity of technology in use and contributing to high-risk online behavior of South Koreans, while potentially attracting a larger range of hacking threats which may go undetected by the nation's state-centered cybersecurity strategy. These centrally controlled solutions cannot completely or adequately adapt to the entire range of threats and opportunities from non-state actors, and therefore also contribute to vulnerabilities in South Korean cyber defense.

Key Words: South Korea, cybersecurity, hackers, software uniformity, cyber attack, intersectionality, policy, public-key

TABLE OF CONTENTS

List of Figures	xiv
List of Tables	xv
Acknowledgements	xvi
CHAPTER ONE: Introduction:	1
1.1 Purpose of Research:	5
1.1.1 Research Questions	6
1.1.2 Research Objectives	7
1.1.3 Chronology and Scope of Study	8
1.2 Background:	8
1.2.1 South Korean Policy Formation	8
1.2.2 Regulating Encryption	10
1.2.3 National Public Key System	17
1.3 Literature Review	20
1.4 Taxonomy:	36
1.4.1 Technical Terminology	38
1.4.2 Conceptual Terminology	39
1.4.3 Normative Terminology	41
1.5 Organization of This Dissertation	42
CHAPTER TWO: The Theory of Intersectionality:	
An Intersection of Theory	44
2.1 The Theory of Intersectionality	50
2.2 Neorealism	59
2.3 Social Constructivism	65
2.4 Cyber Westphalian Theory	77
2.5 The Intersection of Theory: An Integrated Approach	90
CHAPTER THREE: Methodology: A Mixed Approach	99
3.1 Quantitative Methodology:	101
3.1.1 Validity of Online Surveys	101
3.1.2 KISA Survey Methodology	106
3.1.3 South Korean End-user Survey:	108
3.1.3.1 Demographics of Participants	111
3.1.3.2 Operating System	111
3.1.3.3 Browser Software	112
3.1.3.4 Security Software	112

3.1.3.5	Frequency and Location of Internet access	112
3.1.3.6	Response to <i>ActiveX</i> Warnings	112
3.1.3.7	Behavior towards Unknown Websites Links	113
3.1.3.8	Behavior towards E-mail Links	114
3.1.3.9	Occurrence, Location and Mode of Incursions	114
3.1.3.10	Connectivity between Home System and Work/School Network	115
3.1.4	Hacker Survey:	115
3.1.4.1	Question about Orientation	116
3.1.4.2	Questions on Target Acquisition and Motives	117
3.2	Qualitative Study:	117
3.2.1	Dr. Keechang Kim	118
3.2.2	Jim Jackson	118
3.2.3	Dr. Bright Gameli	119
CHAPTER FOUR: A Statistical Analysis		120
4.1	Overview:	120
4.1.1	User Survey:	121
4.1.1.1	The Security of Software:	121
4.1.1.1.1	Operating Systems	122
4.1.1.1.2	Browser Software	125
4.1.1.1.3	Antivirus Software	126
4.1.1.2	Online Behavior	128
4.1.1.3	Occurrence, Location and Mode of Incursions	131
4.1.1.4	Accessibility of Organizational Networks	133
4.1.1.5	Most Vulnerable User Characteristic	134
4.1.2	Hacker Survey:	135
4.1.2.1	Hacker Orientation	136
4.1.2.2	Target Selection	137
4.2	Qualitative Analysis:	139
4.2.1	Dr. Kim Keechang	143
4.2.2	Jim Jackson	147
4.2.3	Dr. Bright Gameli	149
CHAPTER FIVE: Uniformity and Vulnerability		152
5.1	Major Cyber Attacks:	158
5.1.1	July 4-7, 2009	160
5.1.2	June 10 th , 2010	165
5.1.3	March 4 th , 2011	167

5.1.4 June 11 th , 2012	172
5.1.5 March 20 th , 2013	174
5.1.6 June 25 th , 2013	176
5.2 Cyber Dynamic	180
CHAPTER SIX: Conclusions	189
6.1 Empirical Findings	189
6.2 Theoretical Implications	191
6.3 Policy Implications	194
6.4 Recommendations for Future Research	196
6.5 Limitations of the Research	197
6.6 Closing Remarks	198
REFERENCES	200
APPENDICES	
<u>Appendix A:</u>	208
South Korean End-user Online Survey Questionnaire (Korean)	
<u>Appendix B:</u>	214
South Korean End-user Online Survey Questionnaire (English)	
<u>Appendix C:</u> Hacker Questionnaire	221

List of Figures:

2-1	Intersectional Approach Model for Software Uniformity	58
2-2	An Intersectional Analysis of North Korea	92
2-3	An Intersectional Analysis of the South Korean Govt.	93
2-4	An Intersectional Analysis of South Korean End-users	94
2-5	An Intersectional Analysis of Hackers	95
2-6	Multi-tier, Integrated Schematic for Intersectionality	97
3-2	ActiveX Download Warning Prompt	113
5-1	Effect of Software Diversity on Browser Integrity	154
5-2	Effect of Software Diversity of Antivirus Software Integrity	156
5-3	Cyber Defense Spending vs. Number and Frequency of Attacks	160



List of Tables:

3-1	The Statistical Parameters of South Korean Internet Survey	110
3-2	Statistical Parameters of Hacker Survey	116
4-1	Type of Operating systems (Home)	123
4-2	Type of Operating System (Work)	123
4-3	Version of Windows (Home)	124
4-4	Version of Windows (Work)	124
4-5	Type of Browser (Home)	125
4-6	Type of Browser (Work)	126
4-7	Antivirus Software (Home)	127
4-8	Antivirus Software (Work)	127
4-9	Frequency and Location of Internet Access, Analysis	130
4-10	Reaction to Warning Prompts	130
4-11	Linking to Unknown or Untrusted Third-Party Websites	131
4-12	Behavior towards Email Links	131
4-13	Compromised E-mail Accounts	132
4-14	People Who Have Been Hacked through SNS	132
4-15	Compromised CPU or Mobile Device (Home)	133
4-16	Compromised CPU or Mobile Device (Work)	133
4-17	Home Access to Work or School Network	134
4-18	Hacking Orientation	137
4-19	Hackers Response to Easy Targets	138
4-20	Hackers Response to Difficult Targets	138
4-21	Operating System Viewed as Most Easily Compromised	139
4-22	Browsers Viewed by Hackers as the Easiest to Comprise	139

ACKNOWLEDGEMENTS

First and foremost I would like to recognize the people to whom this dissertation is dedicated. Dr. John R. Swanda Jr., my father and mentor, who taught me the value of hard work and the pursuit of knowledge, and guided me through this process by the examples he set as a consummate academic. I must also acknowledge my late, younger brother, Dr. Brett Swanda, whose effort and strength of character overcame adversity, and whose love and encouragement will always be felt. In addition, my mother, Gwen Swanda, instilled in me the importance of writing clearly and with a purpose. My memories of them were ever present throughout this endeavor, and their legacies will stay with me forever. Also, I could not have finished this project without the unconditional support of my wife, Rosa Swanda (이은경).

This research would not have been possible without my family and friends. In particular, the input and expertise of Dr. Bright Gameli, Jim Jackson, Dr. Keechang Kim, and Dr. James Strohmaier not only brought salience to this dissertation's argument, but added to its credibility as well. It is also my sincerest hope that Sharon Sherman knows the depths of my appreciation for her much needed emotional support in the final stretch of this project.

It is also necessary to recognize the faculty and staff of the Department of International and Area Studies at Pukyong University, in particular my advisor, Dr. Dongsoo Kim for his eternal patience and guidance during this process. Lastly, I would like to thank the members of my committee, Dr. Hong-jong Lee, Dr. Jong-Hwan Ko, Dr. Sean O'Malley, and especially Dr. Kim Chul Woo, whose belief in my research also helped make this dissertation possible.

CHAPTER ONE:

INTRODUCTION

The world has become incredibly dependent on information technology. Virtually all aspects of daily life in almost every nation rely on the smooth transfer of digital information. Policy makers around the world, both civilian and military, have come to recognize the importance of cyber security to the social, economic and physiological well-being of society. Protecting the security of both digital and off-line infrastructure requires nations to recognize, anticipate and avoid all cyber threats as well as defend against and swiftly recover from them. Nowhere is this more evident than in South Korea. As one of the world's most wired nations¹, South Korea has benefitted greatly from its citizens' connectivity and vast cyber infrastructure in terms of its economy, communications and logistics. But such advantages have not come without a price. South Korean society's dependency on cyberspace has also increased the potential crippling effects of successful cyber attacks, and has left very little margin of error when defending such a vast and ensconced cyber infrastructure.²

South Korea's initial forays into cyber security focused on implementing unique encryption technology, as well as untested policies and strategies to protect its burgeoning IT infrastructure. Following the completion and

¹OECD Statistical Update: *Broadband by country*, June 2015;
<http://www.oecd.org/sti/broadband/broadband-statistics-update.htm>

² Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York: Ecco, 2010.

implementation of the nation's high-speed fiber optic network in the early 2000's, the Kim Dae-jung administration initiated a series of policies requiring South Korean-based websites to use a unique government-developed security protocol known as SEED. However as South Korea was the only nation to adopt this encryption framework, the SEED protocols made many South Korean websites incompatible with all foreign operating systems and browsers except *Windows* and *Internet Explorer*. Microsoft had developed a security software framework for its browser, *ActiveX*, which allowed South Korean websites to be accessed through its software. For policy makers, *ActiveX* not only bridged the gap between South Korea and the World Wide Web, but also had the added benefit of an additional layer of security. Eventually, compatibility with *ActiveX* would become a government requirement for all public and commercial websites in South Korea. Although other operating systems and browsers would develop SEED and *ActiveX* compatible software, Microsoft's early innovation allowed it to dominate the operating system and browser markets.³ Despite the gradual disappearance of SEED requirements and resultant technology, *Windows* and *Internet Explorer* continue to be used by an overwhelming majority of both commercial and personal pc-based internet users. This has created a relative lack of variation in the use of these types of programs among South Korean systems.⁴

³. Kim, Hyoung Shick, Jun Ho Huh, and Ross Anderson. *On the Security of Internet Banking in South Korea – A Lesson in How Not to Regulate Security*. Publication. Oxford University Computing Laboratory, 2011.

⁴ "Korea Paying Price for Microsoft Monoculture". *The Korea Times*. September 23, 2009.

Operating software and browsers are not the only characteristics of South Korean systems that exhibit uniformity. The types of antivirus software packages and updates used in South Korea also exhibit relatively little variation among pc-based users. At the inception of the South Korean internet proliferation, two domestic computer security companies emerged as the leaders of the antivirus software market. Through clever marketing strategies and political maneuvering, both Ahnlab and Esoft have remained dominant in this market. The combined market shares of these companies dwarf foreign competitors such as Norton, McAfee and Kasperski. The effect of this uniformity on South Korean cyber security is at the center of this research.

Over the past decade, South Korea has seen a rise cyber incursions. The number of total cyber attacks and both the frequency and scope of major successful attacks have increased.⁵ Its precarious relationship with its neighbor and enemy, North Korea, has certainly contributed to its cyber security dilemma. Since 2009, there have been several successful, large-scale cyber attacks targeting both commercial and government computers in South Korea. Many, if not all of these attacks have been attributed to Pyongyang's growing cyber command, as part the rogue nation's recent aggressive strategy towards the South.⁶ In response to this aggression, both the former Lee Myung-bak

⁵ "South Korea's Government Hit with 114,000 Cyberattacks in 5 Years"." *Tech Times*, September 22, 2015. Accessed January 15, 2016.

⁶ Jun, Jenny, Scott Lafoy, and Ethan Sohn. "The Organization of Cyber Operations in North Korea." *Korea Chair Platform - Center for Strategic and International Studies*, December 18,

administration and the current Park Geun Hye administration have taken steps to combat this growing threat in the form of public policy, military maneuvers and bureaucratic restructuring. The development of new cyber security policies, emergency response teams, both civilian and military international agreements, an integrated cyber command, and the creation of several cyber security agencies all represent the priority that the central authority in Seoul has placed on combatting the North Korean threat. In the melee of these events, both South Korean cyber security policy makers and the literature at large have overlooked the potential threat from the convergent nature of operating and security software in the nation's systems.

This dissertation documents and examines the narrow range of software used by a majority of South Korean end users, and proposes that this lack of variation could make these effected systems easier to compromise. Codes designed to infiltrate older, less secure operating systems and browsers are more easily generated, readily available and cheaper to purchase.⁷ This greatly increases the pool of those who are able to compromise these systems. The data gathered during the course of this research suggests that such software uniformity is a contributing factor to the threat of infiltration from cyber attacks on particular segment of South Korean systems accessing the internet. Furthermore, the

2014, 1-3.

⁷ Interview with Darkode co-creator Daniel Paycek: "Darkode". *Radiolab*. National Public Radio; September 21, 2015.

uniform characteristics of these systems may attract more attention from nefarious actors, such as national and international hackers, and possibly contribute to an increase from such threats. The goals of this research focus on establishing a potential correlation between certain individual non-state actors and the integrity of South Korean cybersecurity. Therefore quantitative methodology in this dissertation measures the possible effect that some characteristics of the internet in South Korea have on those non-state actors. To this end, the author of this dissertation employs empirical data to show the plausible causes and effects of independent variables on actors inside and outside South Korea. Qualitative data from security experts and others familiar with South Korean cyber security is employed to build a narrative explaining the relationship between cyber attacks and convergent characteristics of the cyber environment of South Korea.

1.1 *Purpose of Research*

The monolithic nature of both software and antivirus security services that have evolved in South Korea also lend themselves to potential vulnerabilities from both state and non-state actors. The encoding in malware designed to infiltrate multiple operating platforms and browsers is often more complex, needs to be updated often to adapt to the latest security protocols, and is used by a

smaller population of hackers.⁸ If the range of operating systems and browsers in use is smaller, then less complex encoding can infiltrate a larger percentage of systems in South Korea than those in nations with a more diverse pool of such software. Relative diversity in the antivirus security software of used by computers in a national network allows a broader range of malware to be detected, studied, and purged from the affected systems.⁹ The author contends that national computer networks which employ the wide-spread use of many different domestic and international antiviral software services have a greater capacity to defend against pernicious software. Competition among security software firms drives the discovery of threats and the development of defenses against them. This dissertation dissects the problem of software convergence in South Korea, and its potential effects on cybersecurity.

1.1.1 Research Questions

The assumptions made in the hypothesis of this research, can be verified by answering the following questions:

1. Is there a relative lack of variation in the types of operating, browsing and security software used for PC based online activity in South Korea?
2. What evidence suggests that such software uniformity constitutes a threat

⁸ Karyotis, Vasileios, and M. H. R. Khouzani. *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*. Morgan/Kauffman, 2016, pp. 170-72.

⁹ Siddiqui, Muazzam, Morgan C. Wang, and Joohan Lee. "A Survey of Data Mining Techniques for Malware Detection Using File Features." *Proceedings of the 46th Annual Southeast Regional Conference on XX - ACM-SE 46*, 2008. doi:10.1145/1593105.1593239. pp. 18-9.

to cyber security?

3. How do these factors affect the range of capabilities necessary to compromise systems in South Korea?
4. If a lack of variation in software does exist, what effect does it have on the motivations of state and non-state actors?

1.1.2 Research Objectives

To answer these key questions it is first important to measure the relative uniformity of software used in PC-based systems, and then to analyze how this aspects weakens the integrity of South Korea's cyber defenses. This objective must be addressed through a quantitative examination of individuals, and secondary databases. Data collected from a sample pool of South Koreans must measure the technological characteristics of South Korean end users. This information is then compared to international statistics to determine its relative uniformity. Data is similarly collected from individual hackers to determine their capabilities and motives relative to these technical characteristics. In order to assess the threat potential of software uniformity from state actors, a more qualitative methodology is also employed. Existing literature and interviews of relevant individuals both inside and outside of government cyber security agencies in South Korea should be examined at length to either refute or support the initial assumptions of this research.

1.1.3 Chronology and scope of study

Although the evolution of South Korean cyber security and SEED encryption policies of the early 2000's are discussed, the main analysis of this dissertation spans the time period from 2009 to 2014. However, early cyber strategies were used only to explain aspects of the current cyber dynamic. Also, SEED and other state mandated encryptions are discussed in the context of current non-state actors. Survey data was collected from January 2013 to December 2014. All other relevant qualitative and statistical data and analyses reflect the 2009-2014 timeframe.

1.2 Background

1.2.1 South Korean Policy Formation

As the progenitor of South Korean software uniformity was its early cyber security policies, it is important to know how those policies evolved. In order to do that however, it is first important to understand how cyber policy is formed in South Korea. This section explains the political structure of policy formation in South Korea and the actors involved.

As is the case in many countries, there are several types of policy requiring different degrees of cooperation between the executive and legislative branches. Some policies are exclusive to or require the consent of parliament (e.g. treaties, international trade agreements, any permanent amendments to the body

of laws and removal of officials) (Yang 1999, p. 489). Other public policies require parliamentary consensus to become permanent, but can be temporarily carried out through executive orders such as education reforms, certain energy policies, the creation of ministries and defining the jurisdictions of government institutions. Finally, there are policies that involve national security and therefore fall under the discretion of the president and the military chain of command such as declarations of war.¹⁰ For reasons of necessity, South Korean cyber policy most often lands in the national security category, and frequently sweeping changes are made in an ad hoc manner. Thus was the case with early cyber security policy.

The centralized nature of Korean government, the oscillation of political parties in power, as well as the relationship between the relatively few large conglomerates, and the politic often limit the abilities of the executive and legislative branches to come to a consensus. In order to draft and pass legislation that creates and enforces national policy and represents a more democratic model for cyber policy formation, such a consensus is necessary. While this is also true for cyber security policy, the timely expedition of cyber policy decisions is often not possible when considering the political goals of all the parties involved. The slow pace of the legislative process in South Korea does not adequately address security issues in the rapidly changing cyber dynamic. As a result, cyber security

¹⁰ *The Constitution of the Republic of Korea*. Cong. Seoul: Office of Public Information, Republic of Korea, 1956. Chapter 3, article 53.

policy has mainly become a function of the executive branch. Therefore, it is important to remember that although the constitutional mechanisms for the formation of public policy exist and are utilized, a disproportionate amount of civilian cyber security policy is made by the president. This is often done post hoc after a major cyber attack, due to logistical necessity.

1.2.2 Regulating Encryption

In the 1990's, South Korea had found itself behind most industrialized nations in terms of internet usage and connectivity. It would spend the next several years creating a cyber infrastructure rivaling any in the world. To protect this investment, the Kim Young Sam and Kim Dae Jung administrations initiated a number of cyber policies intended to set a standard of protection against cyber attacks. Despite the fact that the rapidly changing cyber environment rendered many of these policies obsolete, they have lived on long past both presidents' tenure, and have contributed to several unforeseen negative consequences on the current integrity of South Korean systems. The culmination of these consequences may contribute to the deluge of major cyber attacks that have been increasing in frequency and scope for the past decade.

Plans for the development of high-speed internet technology had been around since 1987. However, efforts to expand and upgrade South Korea's broadband infrastructure did not begin in earnest until the central government

stepped in with the establishment of the High Speed Network Development Commission in May of 1994. The Broadband Planning Division was established within the Ministry of Post and Telecommunication to conduct affairs associated with building comprehensive strategies for the development of a high speed communication network, designing a method of obtaining necessary resources per annual basis, and acquiring technologies pertaining to the development and operation of a high speed communication network.¹¹ However by 1995, as the internet revolution began in the west, South Korea had a mere fraction of internet users, and had not had the commercial success its western counterparts had in cyber space. The problem was rooted in both technical capabilities and economic factors. More specifically, South Korea lacked a privately-funded fiber optical infrastructure, service providers in the market, and knowledge on its use among the general population. However these things were already prevalent in the west. Legislation would be required to get this done. However, the political landscape was divisive. It had been only seven years since democratization, and only three years since president Kim Young Sam merged his Peaceful Democratic Party with his predecessor, Roh Tae Woo's conservative Democratic Justice Party. Kim won a minority victory in a three-way race. Despite the conglomeration of the two parties into the Liberal Democratic Party (LDP), Kim Dae Jung's opposition party still held 70 seats in parliament, potentially stymying the legislative process.

¹¹ Republic of Korea. Korean Internet Security Agency. MSIP(Ministry of Science, ICT and Future Planning), KCC(Korea Communications Commission), MSPA(Ministry of Security and Public Administration),. *2013 Korea Internet White Paper*. Seoul, Republic of Korea, 2013. p. 1

Realizing this, Kim Young Sam initiated a series of executive orders to fight widespread corruption that met with success and popularity. Matters of national security policy were similarly crafted, and eventually led to several executive initiatives to bring the South Korean cyber infrastructure up to speed.

Kim Young Sam and the LDP passed the Informatization Promotion Act in 1995, followed by the First Master Plan for Informatization Promotion in 1996. However, plans and construction were temporarily put on hold due to the Asian financial crisis. However, these policies were encouraged by traditional international allies. The World Bank and the IMF saw the logic of Korea becoming a more information-based economy. Such an economy would be less dependent on exports and manufacturing, and endorsed the CYBER KOREA 21 act in 1998 as an agent of recovery. In a 2004 report on South Korean IT the World Bank stated:

“In particular, CYBER KOREA 21 was one of the most important policies to cope with the changing environment as a result of the Asian financial crisis. Through these plans, Korea came one step closer to a knowledge-based society with the construction of an advanced information infrastructure, the introduction of various information systems in public services and in the private sector, as well as growth in the overall IT industry.” (Kim, 2008 p. 7)

From that point forward the central government, supported and often spearheaded by the president, would fund not only the creation of this information super highway, but be responsible for the education of the masses on its operation and functionality. This was often justified by the national security narrative (Oh and Larson, 2011 p. xxvii). For the next four years, the government would spend over \$1.2 billion USD connecting urban, suburban and rural areas, and educating Koreans in a program called “Ten Million People Internet Education Product.”¹² These funds also went to set up private corporations as service providers.

National security policy soon extended to the burgeoning South Korean cyber world. Having a strong, growing broadband network in place, it was decided that there must be security protocols instituted to protect this new investment against attacks. In 1999, the world and the United States in particular, were awash in fear of cyber doom’s day scenarios. The U.S. Senate held hearings on America’s vulnerability to cyber attack, coining the term “electronic Pearl Harbor”, as many believed the next major destructive terrorist attack would come in the form of a cyber attack. President Bill Clinton agreed, and made establishing a line of cyber defense a top priority. South Korea followed suit, and set about

¹² Atkinson, Robert D., Daniel K. Correa, and Julia A. Helmund. *Explaining International Broadband Leadership*. p. F2. Report. May 2008. Accessed March 13, 2012. http://www.itif.org/files/ExplainingBBLeadership.pdf?_ga=1.108746948.731530544.1462898497.1462898497. May 2008

devising an internet security protocol to stop hacks to their systems. It is at this point that then President Kim Dae Jung and his advisors made a decision that would encumber South Korean cybersecurity for the next 15 years.

Kim Dae Jung called upon the Korea Internet Security Agency (KISA), and other IT industry experts to come up with a security protocol unique to South Korea. The result was SEED, a 128-bit symmetric key block cipher that became the South Korean industry standard required by law. One major problem for the new encryption code was that no web browsers supported it directly. However SEED encrypted websites could be accessed through *Internet Explorer* by using an *ActiveX* control plug-in. Having this cutting-edge key cipher that was so different from more commonly used and internationally accepted protocols meant that attacks intended for other coding would be useless in Korea. Any malicious code would have to go through *ActiveX*'s security protocols, and finally be manually loaded by the user. The fact that only one browser worked with SEED seemed inconsequential at the time. Worse still, later versions of *Windows* would not be compatible with *ActiveX* forcing users to use outdated operating software and web browsers when performing common tasks such as online purchasing, registering for classes, online banking, social media and telecommunications. As Korea's connectivity and number of internet users grew, so too did its dependence on Microsoft *Windows*. No other operating platforms had made an approved private key plugin to read the SEED encryption until 2007, and

therefore all computers visiting Korean websites had to use *Windows* (or have a *Windows* conversion program). In 2008, Microsoft announced that it would not be updating *ActiveX* any more. Therefore, many Korean government and corporate sites were stuck using aging versions of *Windows*, or convoluted *ActiveX* plugins, and often required the same of its visitors. This not only slowed and complicated the process of online transactions, but also led to major security flaws.

The *ActiveX* plug-in that bridged the gap between *Windows* and Korea's SEED encryption was designed to allow the user the option to review every plug-in, upgrade or update encountered. To designers, it seemed a very secure way to protect against any malware as everything coming in must be scrutinized. However, it put the onus of scrutiny entirely on the user. He or she would have to decide whether to accept the download or not. A typical user would have to click "allow" several times when prompted by *ActiveX* to make even a single online purchase. Users routinely click "allow" regardless of whether they trusted or even knew what was being downloaded on to their computer, due the number of times they encountered the prompt and the necessity of uploading SEED plug-ins. Such automatic downloads often contain malware, and have been the method of many major cyber attacks in South Korea. The solution to this problem seems obvious; use virus protection software to recognize which downloads are safe which ones not. However, this also brings up another security problem unique to South Korea:

unsafe, conditioned behavior regarding downloads. This is discussed later in this paper.

In most industrialized countries, computer users have the choice of many widely-recognized international anti-virus software programs such as America-based McAfee and Norton, and Russia-based Kaspersky Lab, as well as other national and international brands. The relative diversity of these security programs provide heterogeneity in the firewall and protection software markets of each country. In South Korea on the other hand, 80% of all computers rely on one of two virus protection software programs – Ahnlab's *V3* or Esoft's *Alyac*. Their wide distribution in South Korea can be attributed more to the accessibility and price of both, rather than their reliability or performance against the latest malware. Ahnlab is the creation of its CEO, turned academic, turned left-wing presidential candidate Ahn Chul-soo. Known for his stance opposite the current and previous ruling New Frontier Party, Ahn vowed to make his software free to everyone. This allowed him to dominate the market while endearing him to the younger more tech-savvy voters. Ahnlab succeeded in creating an anti-virus program free to all South Korean users. Its *V3* program is often installed on new computers as the default security, and focuses primarily on viruses and problems prevalent in South Korea, and neglected many international malware that is rare to the country. In a similar manner, *Alyac* was also made free to consumers through agreements made with hardware and software manufacturers that often

rely on advertising. The wide distribution of these programs among the nation's computers also meant potentially greater access for hackers designing malicious code potentially targeting South Korean systems.

Poor policy decisions in the late 1990's and early 2000's bear some responsibility for the systemic vulnerabilities in current cyber security. Legislating and mandating technology and its resultant incompatibility issues, led to risky user behavior and monolithic software use in South Korea, and may all have contributed to the major cyber attacks that began in 2009. The data analysis portion of this research provides evidence to support this claim.

1.2.3 The National Public Key System

These encryption policies in South Korea are the foundation for what is known as a 'national public key infrastructure', or NPKI. Public key systems serve as the basis for verifying the identity of users and websites over the internet. A site that wants to be publicly accessed will request a digital certificate from server administrators. Once it receives the digital certificate, the site can now verify the digital identity of a user, and vice versa, through two encryptions, or keys, deciphered by the web browser. A 'public key' is generated for the site and a 'private key' is generated for the user. The unique or identifying quality of each key is referred to as a digital (or electronic) signature. If the web browser's decipher were the only entity verifying these keys, malicious users could steal the

private key and access the user's information. Such hackers could also steal the public key, make a false website and access the information of multiple users. To prevent this, servers rely on a certification authority or CA. These CAs are trusted third-parties that issue a digital certificate to the site and to the users. These certificates are confirmed by the web browser, so a CA must be trusted by all of the major web browsers to allow access to all, regardless of which browser the user uses. The digital certificates are often reissued automatically at random intervals to ensure that they have not been compromised. Periodic audits are also performed on the CA by auditing companies such as WebTrust and Verisign. However in South Korea, the public key infrastructure is not administered extra-governmentally. The country's national public key infrastructure relies on KISA as a central certificate authority, and falls under the jurisdiction of the Ministry of Science, ICT and Future Planning (MSIP). Acting as the 'root' CA, KISA dispenses control over the expedition of digital certificates for public and private keys to officially accredited and privately run CAs. Currently, there are five Korean companies that are accredited CAs.¹³

At its inception, the Electronic Signature Act directed all domestic websites running embedded technologies (such as credit card or other financial transaction processing, exchange rate and measurement conversion calculators,

¹³ KISA. "Public Key Authentication Service." Public Key Authentication Service. Accessed February 15, 2016. http://rootca.kisa.or.kr/kor/popup/foreigner_pop1_en.html.

geographical location devices, embedded database search engines, etc.) to require their users to provide proof of identity, in the form of the user's national ID number, in addition to his or her private key. It was this system that initially caused the incompatibilities with web browsers, as the great number of sites with these embedded technologies could not be accessed due to the inability of web browsers to properly generate SEED encrypted ID number verification. Fortunately for Microsoft, it had already developed *ActiveX* in 1996 to allow browsers using its earlier binary interface standards to access these embedded technologies. The *ActiveX* plug-in also allowed users in South Korea to download the SEED ID verification and all embedded technologies on Korean site. This is especially problematic from a security standpoint. Users must download the embedded programs through *ActiveX*, often multiple times during a single visit, each time potentially exposing their systems to malware implanted at the source or in systems with compromised *Internet Explorer* or *Windows*. Furthermore, these downloaded programs are deleted when the user's cache and/or temporary downloads are cleared, requiring the user to repeat the process each time he or she revisits the site. This increases the chances of the user downloading surreptitious malware. This mandated process is also a problem for frustrated users, whose interaction with these sites is constantly being interrupted by notifications of required downloads. He or she must then agree to the download while simultaneously acknowledging the risks of doing so. The idea behind this

process is that allowing a user to control downloads to his or her system will provide greater scrutiny of what is being downloaded, and thus help prevent the infiltration of malware. However, considering that the website cannot be accessed properly without downloading the program, a user's only choices are to either download the program or not use the site. It is the contention of the author that most users choose the former on a consistent basis. Furthermore, their repeated acceptance of these downloads desensitizes them to the dangers of such actions, and increases the number system incursions. In 2005, the Ministry of Public Administration and Security (MOPAS) had jurisdiction over the NPPI at that time, and amended the ID requirement to apply only to the websites of government institutions and websites that involve financial transactions or information.¹⁴ Despite this revision, there are still any educational institution, government, banking and e-commerce websites that fall under the original provision, and thus are required to employ *ActiveX* or similar plugins.

1.3 *Literature Review*

This research builds upon the existing scholarship in the field of cybersecurity, particularly how cybersecurity relates both directly and indirectly to South Korea and the problems stemming from a lack of software variation. The

¹⁴ Park, Hun Myoung. 2012. *45th Hawaii International Conference on System Sciences: (HICSS 2012) Maui, Hawaii, 4-7 January 2012*. Proceedings of The Web Accessibility Crisis of Korea's Electronic Government: Fatal Consequences of the Digital Singature Law. New York: IEEE, 2012. 2319-328. Accessed July 7, 2013.

author elucidates on leading scholarly works about the commercial effect from software uniformity, threats to cyber security, national cyber defense stratagem, technological solutions to cyber threats, and hackers. This dissertation investigates the threats to cybersecurity from software variation. Therefore it is important not only to define what constitutes a threat and assess its level of danger, but also the way in which these factors effect and are affected by the political, social and technological environment in South Korea must also be reviewed.

One of the difficulties in conducting a study such as this one is the lack of academic literature concerning software uniformity in South Korean cybersecurity. However Keechang Kim's recent paper in *The Asian Business Lawyer*, addresses issues on software uniformity in South Korean e-business that are surprisingly parallel to those of this dissertation. Specifically, he addresses the existence of software uniformity in South Korea and its evolution, a closer examination of the technical aspects of the national public key system, and the political entanglements associated with the issuance of digital certificates.¹⁵

Kim explains how the Electronic signature act of 1999 set up a national root certificate authority (KISA) as the sole issuer of the national encryption's 'root key', or 'public key', to subordinate Certificate Authorities (CA) licensed by the Ministry of Information and communication. He claims that this has

¹⁵ Kim, Keechang. "Recent Changes in the Regulatory Landscape for E-Commerce in South Korea."; *The Asian Business Lawyer*, Vol.16:87, Fall 2015. Accessed December 4, 2015.

contributed to the lack of infusion of international digital standards in South Korea:

“A ‘CA’ (Certificate Authority) is an entity which provides certification service (certifying the ownership of a digital certificate issued to a user or to a website). Root CA is an entity which certifies the identity of the CAs who offers such certification service. Art. 4(2) of ESA stipulates that “state organs, local governments or corporations” may apply to become a ‘licensed CA’. But it is not clear whether “corporations” mentioned here include foreign corporations. So far, no foreign corporation has applied to become a licensed CA under the Korean ESA. The implicit assumption, it seems, is that only Korean corporations are eligible to become a licensed CA under the ESA. This is because Art. 27-2 of ESA provides that the government may conclude a treaty with a foreign government so that foreign CAs may be granted the same status as the licensed CA under the Korean ESA. Foreign corporations wishing to be licensed CAs in Korea must therefore have their government conclude a treaty with the Korean government (rather than directly applying to become a licensed CA under Korean ESA). However, no such treaty for mutual recognition has yet been concluded. Since the introduction of the ESA in 1999 until now, Korea has had a ‘national’ trust chain which is isolated from the rest of the world: non-

Korean CAs are not 'trusted' in Korea. At the moment, there are 5 licensed CAs which are subordinate to the national root CA of Korea, KISA. All of the licensed CAs are Korean corporations.” (Kim, 2015 pp. 88-89)

However trust is a two-way street with electronic signatures, as software vendors must trust South Korea's electronic signature to guarantee to their users that accessing websites in South Korea (that are using its national public key) will be safe. He further criticizes the National Public Key Infrastructure (NPKI) for limiting the types of browsers available for use in South Korea:

“Other browser vendors such as Microsoft or Opera choose to trust KISA. But that is not because these browser vendors are subordinate to Korean government or required to trust KISA by the Korean law. These browser vendors independently — one hopes — came to a view that KISA's operation is trustworthy (on the basis of assertions and supporting materials provided by KISA).

The fact that a particular government, such as South Korean government, trusts a CA or legislates its national root CA shall be trusted, is entirely irrelevant and technically meaningless in the Internet. Even if a particular website or a CA is trusted by a government, there is no

technically sound means of reliably communicating such trust in the context of online connection. Trust in the Internet is currently maintained by a system of scrutiny undertaken by browser vendors and accredited security audit service providers.” (Kim, 2015 pp. 90-91)

These audit service providers are based internationally, but the Korean government does in some cases apply for accreditation of its NPKI. However, the fact that it must submit to foreign standards, highlights the incongruence between a nationalized system with the international cyber environment. Such incongruence can only serve to limit the options of South Koreans, thereby contributing to the problem of software uniformity.

Boo and Lee explore the political and theoretical nature of the South Korean approach to cyber security, and how the theoretical forces behind policy converge with national and regional security strategy.¹⁶ It is these forces behind cybersecurity policy makers’ preoccupation with North Korea that blind them to many of the vulnerabilities discovered in this research. The work of Hyeong-Wook Boo and Kang-Kyu Lee is directly relevant to this discussion as it defines the parameters of cyberspace by different theoretical approaches using South Korea as a case study. Subsequently, it delineates and identifies IR theoretical

¹⁶ Boo, Hyeong-wook, and Kang-kyu Lee. "Cyber War and Policy Suggestions for South Korean Planners." *International Journal of Korean Unification Studies* 21, no. 2 (2012): 97. Accessed March 11, 2013

concepts within the South Korean cyber security environment. But most importantly to this dissertation, Boo and Lee show the aspects of neorealism within South Korean cyber security that have shaped its state-centered approach, and recognize non-state individual actors as important to the integrity of cyber security. They also outline leading neoliberal thought on cyber warfare, and warn against neorealist deterrents in cyber conflict, specifically in South Korea. Lastly, they advocate a model of technology-based, pragmatic stratagem, and illustrate the necessity for regional cooperative efforts, similar to this dissertation. In addition, the authors detail the unique and asymmetric nature of the international and regional cyber paradigms (Boo and Lee, 2012 pp. 97-98). It is most germane to this research as it posits three important questions. First, “Is the cyber war approach appropriate in addressing cyberspace issues, when non-military concepts can be used to manage cyber security?” Also, “Which theoretical approach is appropriate in addressing cyberspace and cyber war issues at this point?” Lastly, “If South Korea adopts the cyber war approach, then has it carefully considered strategic issues, such as cyber deterrence?”

Boo and Lee begin by elucidating on Cho's (2012) definition on cyber space using two approaches: neoliberalism and neorealism. They cite Deibert (2010), among others, as an illustration of the prototypical neoliberal cyber security strategist. Deibert doesn't trust the neorealist motives of other states, complaining of their commercial stake in cyber conflict, goals of diminishing

privacy on the internet, and gains from the escalation of cyber hostilities between the U.S. and China (Deibert 2010). This seems quite ironic, as neoliberalism is based on openness, trust and international cooperation. Boo and Lee explain that to neoliberals, cyberspace is more akin to an open sea, while neorealists perceive it as a territory of sovereign states. A more apropos metaphor would be one that illustrates not only the openness or ease of global information flow, but the neoliberalist desire for international cooperation and belief in shared norms and agendas. At the opposite end of the spectrum, Boo and Lee rely on Richard Clarke and Robert Knake as the opposing voice of neorealism in cyber security. Boo and Lee then outline the steps of their approach to the "infinite problems" of cyber war. And in doing so, the authors make an extremely valid point germane to this dissertation, "Cyber security strategies must be grounded in technology and environmental differences." (Boo and Lee, 2012 p. 89) It is the contention of this research that exemplars in of such environmental differences in South Korea, can be found in the uniformity of end-user technology. Further examples include the difference between the cyber environment of international hackers and South Korea cyber security.

In a similar approach to this dissertation, Boo and Lee breakdown major cyber attacks into factors of actors, vectors (or methods of attack), objectives, targets and impact. It is with Boo and Lee's categorization of these factors that this dissertation's author finds a major weakness in their argument. Boo and Lee

choose the three largest cyber attacks at the time their work was published: the Estonian cyber attacks that occurred during the anti-Russian demonstrations of 2007, a similar attack (with similar causes) on Georgia in 2008, and the stuxnet Virus that infected the Iranian nuclear facility in 2009. If the ultimate goal of their work is to frame IR theory within the South Korean cyber dynamic, Boo and Lee should have analyzed factors involved with South Korean cyber attacks. At the time this work was published, there had already been three major cyber attacks in South Korea which could have been analyzed using their rubric. Perhaps the cyber attacks on South Korea were not severe enough to illustrate the worst-case scenario of Boo and Lee's hypothesis.¹⁷ Instead, the authors give a brief analysis of the Nonghyup Bank attack in 2011, but only as it pertains to the government's response and the unlikelihood of North Korea developing "stuxnet" (Boo and Lee, 2012 p. 92).¹⁸ This dissertation adds to Boo and Lee's argument and to the field of literature, in that it examines factors similar to the two authors, but specifically as those factors appeared in the South Korean cyber attacks.

¹⁷ The cyber wars in both Estonia and Georgia crippled large sections of their cyber infrastructures, completely shutting down the systems of both countries' financial industries for almost a week, and causing many public and private services to be suspended. Boo and Lee note, "...the impact of the (2011 South Korean) attack appears to be manageable in comparison to the case of internet banking system freeze." (Boo/Lee, 2012 p. 95)

¹⁸ At the risk of arguing semantics, this dissertation noted that the term 'stuxnet' (as Boo and Lee frequently use it in their assessment of North and South Korean cyber capabilities) is a misnomer, and implies that that particular malware is still a threat. The actual stuxnet virus itself was decoded and most major antivirus protocols were adapted to identify it shortly after its discovery in 2011 (Zetter 2013). A more appropriate term would be "stuxnet-like", or "complex zero-day" virus, malware or technology.

Boo and Lee concede that these two sides of the cyber security debate (neorealism versus neoliberalism) are irreconcilable. However they see this as unimportant, as solutions lie with pragmatic ideas based mainly on sharing the responsibility for cyber security. The authors are careful to note that there is a place in cyber security for aspects of neorealism, and supports this by with the argument that North Korea is the most prevalent threat to Korean cyber security:

“Among the cyber security issues in South Korea’s infrastructures, North Korean cyber threats are regarded as the highest priority. Its efforts to harm South Korean cyber assets have increased. As previously mentioned, nations with well-developed ICT infrastructure are considerably exposed to the risks from cyber attacks. South Korea is no exception. Considering the South Koreans’ impatience and love for ICT devices, they are more likely to quickly panic when a large-scale cyber attack occurs. Therefore, it is safe to assume that South Korea is one of the most vulnerable countries against cyber threats.” (Boo and Lee, 2012 p. 99)

To construct their pragmatic model, Boo and Lee end up agreeing with Clarke and Knake’s (2009) main contention that cyber strategies (if and when these need to be neorealist strategies) should be more defensive than offensive, however without the need for militarization of cybersecurity:

“We have to focus on what the rational choice is for ROK Armed Forces. In short, South Korea must invest and prepare of defensive measures rather than offensive options. Furthermore, South Korea must delve into nonmilitary options first because there are inherent limitations of countering cyber attacks by employing military assets. Thus, enhancing multi-national cooperation and establishing solid inter-organizational cooperation in the domestic level should be considered since others may fall in the realm of technology.” (Boo and Lee, 2012 p. 100)

This vulnerability that is based on a society's dependence on technology describes almost word-for-word Clarke and Knake's concept of the asymmetric nature of cyber warfare. However in doing so, Boo and Lee possibly overestimate North Korea's cyber capabilities:

“Some experts even estimate that North Korea's cyber warfare abilities are almost equal to that of the CIA. According to a report by the Korean Times, South Korea's intelligence agencies now believe that North Korea has the capability to ‘paralyze the U.S. Pacific Command and cause extensive damage to defense networks inside the United States.’

Among the most frequent visitors to U.S. military websites, according to the U.S. Defense Department, are computers traced to North Korea. According to estimates from Washington and Seoul, their abilities rival those of the CIA.” (Boo and Lee, 2012 p. 97)

Most recent and reliable sources report that although there is a concerted effort by North Korea to swiftly achieve a high degree hacking acumen, it lacks the computing and knowledgeable man power to commence an attack at the level of stuxnet, nor would they be capable of the damage described by Boo and Lee (Rozenweig, 2013, p. 68). Such overestimations may be the evolutionary result of early fear campaigns to garner support for greater cybersecurity efforts, and extend from the state’s attempts to frame attacks within its national security narrative. The possibility of North Korea’s possession of stuxnet-like technology is irrelevant. If employed correctly, even simplistic DDoS attacks can have disastrous consequences for South Korea. It would be more prudent to focus less on fuzzy inconsistent reports on the size and capabilities of North Korea’s cyber command, and instead focus more on how non-state actors (individuals and corporations) contribute to the success of these attacks.

Boo and Lee answer their initial questions by concluding that securing cyberspace sometimes requires a neorealist approach using defensive measures with current networks based, non-aggressive cyber deterrents, such as resilience. In addition, they adequately support their claim that strategy must evaluate and

attempt to predict when provocative measures are necessary (Boo and Lee, 2012). This dissertation finds no fault in that assessment, and would add to their conclusions by arguing that these defensive measures also partially lie with the technical characteristics and behavior of end-users and the motives and capabilities of hackers.

The search for a purely technological solution to software uniformity or any problem with cyber security is tempting. However, to do so would not necessarily provide the security intended, and overlooks other alternatives that do not involve technology. As was the case of the SEED encryption mandate, legislating technology can often have a negative effect on cyber integrity. Such phenomena and the security problems with browsers and operating systems are explained by Kim, in the context of internet banking.¹⁹ Although software by definition is technology, the forces that led to its uniformity also reside outside of technology.

This dissertation addresses the abilities and motives of hackers. Hackers working as state agents are under the orders and direction of their respective state governments, and therefore have no personal motives for their actions. Although software uniformity may make the execution of those orders easier, it has no bearing on the acquisition of targets, as those political motives belong to the state. However, individual hackers not affiliated with any government or formal organization, choose their targets and plan their attacks independently or in

¹⁹ Ibid 15, p. 95

concert with other like-minded independent hackers. It is these hackers that may be attracted to the software characteristics of South Korea. For that reason, it was important to understand the culture from which such decisions come from. The culture of bravado in the hacking community and the public alarm that hackers incite is examined closely in Douglas Thomas's book, *Hacker Culture*.

The word "hacker" has an interesting double-meaning: a vastly more widespread connotation of technological mischief, criminality, and an original meaning amongst the tech-savvy as a term of highest approbation. Both meanings, however, share the idea that hackers possess superior ability to manipulate technology according to their will. This book mainly concerns itself with the former meaning. For Thomas, this simultaneously mystified and vilified, elusive set of individuals exemplifies "the performance of technology" (Thomas, 2002 p. xx), showing the way in which "the cultural, social and political history of the computer...is fraught with complexity and contradictions" (ibid, p. ix). In fact he claims that hacking is more a cultural than a technological phenomenon, citing Heidegger's, "the essence of technology is not anything technological" (ibid, p. 56). In part one of the book, Thomas claims secrecy to be the defining issue of "hacker culture". Society has an ambivalent, contradictory relationship to secrecy, which the pranks of hackers highlight in paradoxical and/or "supplementary" ways. For instance, "Secrets can preserve an institution's identity, but...they can also prevent a hacker from being identified" (ibid, p.xi). Thomas seeks a

“genealogy of secrecy” in the Foucauldian sense. To this end, Thomas retells much of hacking’s history, from its little-known origins in phone “phreaking”, through the hacker Eden of the 1960s. During this period in the computer labs of MIT, Cornell and Harvard information and equipment were shared and it was accepted that any person had the right to tinker with anything that they could improve upon (ibid, p. 15).

Thomas also examines literature produced by hackers themselves, and the way they are represented by non-hackers, and the complex interplay between the two. For instance, hackers are “prone to precisely the same kind of overstatement and mischaracterization of their activities that the media and government officials are” (ibid, p. 117). Hackers are revealed in this section as superb wielders of irony. As an example, Thomas cites the editors of the underground magazine *Phrack*. Aware that their publication was assiduously studied by law enforcement agencies and corporations, they formally copyrighted their work, stating that it was available free of charge to “the amateur computer hobbyist”, but that any “corporate, government, legal or otherwise commercial usage” was forbidden without “prior registration”, costing \$100. Thomas’s analysis of this act is somewhat utilitarian. Editor Chris Goggan’s own words, however, speak more of an intrinsically glorious act

“I named several people who were not only getting the magazine but in one case, they were spreading it around and, of course, none of them even contacted me for registration. I had a riot with it. It was a lot of fun” (ibid, pp. 128-9).

As exemplified by this research, the media, national governments, and even hackers themselves present a narrative of the ‘cyber-omnipotence of hackers’. While this may be true for large groups of state-sponsored hackers collaborating towards a single goal or mission, the reality of the typical hacker is quite different. Hackers seek to compromise systems by the simplest means required. When bugs in system’s programming are seemingly absent, the attackers often resort to socially engineered or alternative methods to access the target.²⁰ In well-defended systems, these alternative methods often require a great deal of resources or physical access to the system, as was the case with the stuxnet hack. Such endeavors fall beyond the resources and capabilities of most hackers. However as the complexity and integrity of a system’s defenses decrease, the opportunity for more hackers to successfully penetrate systems increases.

The covert nature of interstate cyber warfare often means that national and international law, its enforcement and resulting punishment are little deterrent to state-sponsored hackers. The same cannot always be said of individual hackers, and such consequences often channel such activities towards the systems most

²⁰ Interview with Bright Gameli on 12/10/13

easy to hack. Thomas mentions this in his exploration of “the juridical construction of the hacker” (ibid, p. 177). Thomas suggests that much of the fierceness of such penalties arises from hackers being “made to stand in for an issue of great cultural anxiety”, i.e. the increasing role of technology and attendant surveillance in governance (ibid, p. 216). The hacker spirit is curious in that despite being so apparently irresponsible, it is also robustly practical. It is just such practicality that may encourage hackers to choose easy targets well within their range of capabilities, than to take up the challenge of compromising systems with complex and sound defense.

Using the previously mentioned works, this dissertation contributes to the body of literature in its unique approach to South Korea’s cyber security. The current discussions in the field approach problems from paradigms of traditional national security, such as military responses, intelligence, corporate security and international cooperation. Such discussions of traditional strategies and their implementation are important as they address the threat from North Korea, and actively seek to detect, defend against, and recover from enemy attacks. However while necessary for cyber defense given the geopolitical state of the Korean Peninsula and East Asia, these strategies often require vast resources, are labor intensive and in the end may still not provide adequate protection to all South Korean systems against the many threats. For example, one very logical response to strengthen vulnerable areas of cyber defense would be to allocate more men

and materiel to those areas of vulnerability. However despite a steady increase in resources dedicated to cyber security, the overall number of successful cyber attacks has grown dramatically.²¹ Furthermore, the frequency and scope of successful large-scale attacks has also increased.²² Therefore, it is reasonable to assume that at least part of the problem may not simply be a matter of resource allocation, but may also be a product of alternative factors, such as the diversity and proportionality in the software characteristics of a nation's systems.²³ Acknowledging these alternative factors may provide a simpler, across the board solution that is less expensive, but more politically adroit, socially tolerable and would provide added protection against all types of attackers. However, the author does not imply that such suggestions are mutually exclusive with current cyber strategies, and could be used in concert with existing conventional and cyber defensive strategies.

1.4 *Taxonomy*

Due to the nascency and perpetually evolving nature of cyber security studies, many concepts within the field are often obfuscated by ambiguities in

²¹ Chang, Jenifer. 2014. "US, South Korea Join Forces To Prevent Cyber Attacks from North Korea." *PC World*. January 14, 2014. Accessed August 9, 2014.

²² For the purpose of this dissertation, a 'large scale attack' is defined as a successful cyber attack against government or corporate-wide systems with intention of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

²³ Kim, Seungjoo. "How South Korea Invests In Human Capital For Cyber Security". Korea University Department of Cyber Defence. SANE Lab. 2015. Presentation.

language. New technical terms, descriptions and categorizations are constantly being added to the field's lexicon and can have multiple interpretations depending on the context involved. NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) concedes there are no common definitions for cyber terms, "...they are understood to mean different things by different organizations, despite prevalence in mainstream media and in national and international organizational statements."²⁴ Such obfuscations become more prevalent as works in cyber security studies relate to other nontechnical fields and theories.

To avoid such ambiguities in this dissertation, the final portion of this chapter is dedicated to defining several key terms and concepts used in this study. The author calls upon Revision II of the US National Institute of Standards and Technology's Glossary of Key Information Security Terms, NATO CCDCOE's "Cyber Definitions", commercial cyber security firm glossaries, generally accepted reference materials, the author's own nomenclature, and the body of existing literature that this paper is built upon to lay the linguistic and conceptual foundation for the main argument of this dissertation. To that end, the definitions of terms and language related to this work have been organized into three categories; technical, conceptual, and normative.

²⁴ "Cyber Definitions." CCDCOE. 2014. Accessed January 22, 2016. <https://ccdcoe.org/cyber-definitions.html>.

1.4.1 Technical Terminology

Technical terminology refers to general technology and related jargon used throughout this dissertation.

1. *Antivirus software/Virus protection*: A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.²⁵
2. *Cyberspace*: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers.²⁶
3. *The internet*: A single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).²⁷
4. *Malware*: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim; a virus, worm, Trojan horse, or other

²⁵ Ibid 24

²⁶ "NIST - Glossary Of Key Information Security Terms | Maximus Impact." Maximus Impact. Accessed. <http://www.maximusimpact.com/national-institute-of-standards-and-technology-glossary-of-key-information-security-terms.>, p. 62. January 16, 2016

²⁷ Ibid 26, p. 103

code-based malicious entity that successfully infects a host.²⁸

5. *Trojan horse*: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.²⁹
6. *Virus*: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.³⁰
7. *Worm*: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself; a malicious code.³¹

1.4.2 Conceptual Terminology

Conceptual terms are those used in this dissertation to describe general, intangible elements in the cyber security field. Many of these words may be used differently outside this dissertation.

1. *Cyber attack*: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or

²⁸ Ibid 26, p. 122; Information Audit and Control Association (ISACA): Cybersecurity Fundamentals Glossary, 2014, p. 19

²⁹ Ibid 26, p. 202

³⁰ Ibid 26, p. 212

³¹ Ibid 26, p. 215

- destroying the integrity of the data or stealing controlled information.³²
2. *Large-scale cyber attack*: a successful cyber attack on either any government or corporate-wide system.
 3. *Cyber dynamic*: the social, political and economic forces affecting the operation of the internet.
 4. *(South Korean) Cyber environment*: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.³³
 5. *Cybersecurity*: The ability to protect or defend the use of cyberspace from cyber attacks.³⁴
 6. *Cyber incident*: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.³⁵
 7. *Cyber threat*: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.³⁶ Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other

³² Ibid 26, p. 57

³³ Ibid 24

³⁴ Ibid 26, p. 62

³⁵ Ibid 26, p. 57

³⁶ "Glossary of Security Terms." SANS.. <http://www.sans.org/security-resources/glossary-of-terms>. Accessed February 6, 2016

organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; the potential source of an adverse event.³⁷

8. *(Cyber) Vulnerability*: A weakness in an information system, system security procedures, internal controls, or security implementation that could be exploited or triggered by a threat source³⁸; a weakness in a system, application, or network that is subject to exploitation or misuse.³⁹
9. *Cyber-specific theory (of international relations)*: a theory unique to cybersecurity that explains the relationship between systems integrity, national security and international politics, and is not an interpretation of a traditional school of thought in international security.

1.4.3 Normative Terminology

The following terms define agents relevant to this dissertation:

1. *Hacker*: An unauthorized user who attempts to or gains access to an information system.
2. *Black hat hacker*: A hacker who breaks into a computer system or

³⁷ Ibid 26, p. 198

³⁸ Ibid 24, p. 216

³⁹ "Cybersecurity Fundamentals Glossary." Information Audit and Control Association (ISACA). 2014.. P.34.

http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf. Accessed February 6, 2016

network with malicious intent.⁴⁰

3. *White hat hacker*: A hacker who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach.⁴¹
4. *Grey hat hacker*: a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.⁴²
5. *Non-state actor*: a person, persons or entity that is acting independent of direct government control.

1.5 Organization of This Dissertation

In order to provide a logical narrative to this study, this dissertation organized the following chapters in such a manner as to illustrate the author's comprehension of this field of study in general, and more specifically the problem being discussed, as well as to express the adroitness by which the problem is defined, tested, measured and analyzed. In the next chapter, the author provides the theoretical context from which the study was derived. Several

⁴⁰ WhatIs.com . "What Is Black Hat? - Definition from WhatIs.com." SearchSecurity. Accessed March 12, 2016. <http://searchsecurity.techtarget.com/definition/black-hat>.

⁴¹ "What Is White Hat? - Definition from WhatIs.com." SearchSecurity. Accessed March 12, 2016. <http://searchsecurity.techtarget.com/definition/white-hat>.

⁴² De, Chu: "White Hat? Black Hat? Grey Hat?"; *ddth.com*. Jelsoft Enterprises, 2002: <http://www.ddth.com/showthread.php/200-ENG-White-Hat-Black-Hat-Grey-Hat>

relevant theoretical concepts are discussed as well the author's reasons for selecting them. In Chapter Three, the author lays the empirical design of the study with coinciding explanations of the relevance of the methods employed. Chapter Four analyzes the data collected. First, a statistical analysis is provided for comparison of South Korean data with similar data previously collected on the United States and worldwide.⁴³ Also provided is expert testimony on aspects of the subject and data. This is followed by an examination of the software uniformity in chapter five. This includes examinations of problems associated with software uniformity, the actors involved, the environment in which the problem resides, as well as its implications and possible solutions. Ultimately in Chapter six, the author draws his conclusions, both empirical and analytical, and discusses the theoretical implications and impact on policy of the findings, as well as the need for future research, the limitations of the study and the author's own closing remarks.

⁴³ Usage data for the U.S was provided by *Statista.com*, and global usage rates were retrieved from *Stack Overflow* and reflect the 2013-2014 time frame.

CHAPTER TWO:

THE THEORY OF INTERSECTIONALITY: AN INTERSECTION OF THEORY

As national governments scramble to deal with a growing number of large-scale covert and public acts of cyber warfare, cybercrime and cyber espionage, IR scholars also find themselves in a dilemma as well. National security strategies designed to stem the tide of these attacks has become increasingly less effective. One possible reason for this could be the disconnect between traditional IR security theories that are based on real-world responses to kinetic threats, and the vastly different and complex environment of cyberspace. This theoretical rift has been a major problem in the field of cybersecurity, leading many to advocate aggressive offensive policies, or policies of containment in an attempt to preempt threats. Maintaining the spirit, if not the tenets of traditional security theories when applied to cybersecurity is often difficult or impossible. Furthermore, when applied to cybersecurity concern, the strategies spawned from IR theories tend to focus on only select aspects, actors, and/or one type of solution to the problem. This may be why the first reaction of a great power is to launch a cyber attack, or to give a threat of such. In response, they often employ offensive strategies through the military, directed at another great power or state actor from which they feel threatened. Examples of such theoretical single-mindedness can be found in the corporate world. Firms tend to view cybersecurity through a lens of immediate profit and loss rather than

viewing it in terms of long-term cost versus benefits. Accordingly, they weigh the possible short-term profits from not acting, against the substantial financial cost and logistical difficulties in implementing better security. When a major attack happens, it is already too late. Strict adherence to such profit models often make corporate security more myopic.

Fortunately, governments seem share a greater concern over the integrity of their information, mostly due to modern society's dependence upon it. However, governments are also regularly guilty of myopia when it comes to cyber strategy, its implementation and administration. National cyber security is often disproportionately constructed on a macro level. This tends to simplify defenses to only stratagem that can be implemented across a broad, consistent spectrum. Ironically, it is this broad spectrum that limits governments' scope of those threats to only encompass competing nation-states, or large militant groups. States accordingly dedicate their resources almost exclusively to what very well may be their great threat, but certainly not the only one. And in doing so, states often neglect alternative solutions. The gradual, yet consistent militarization and centralization of authority over national cybersecurity often prioritizes security over logistics, as well as over the effects these government actions may have on the behavior and security of its citizens. It is possible that the net negative effect of ignoring these narrower aspects of cyber strategy is greater than that of the threats presented by state actors or large international groups. This drive towards

centralizing and militarizing cybersecurity is greater in countries that are prime targets for cyber attacks, such as the U.S. or China, and most certainly South Korea. Therefore, it is not surprising that in these countries the perspective on cybersecurity and resultant strategies most closely resemble those of the neorealist perspective. From the neorealist perspective, the level of analysis is focused on states, and where power and security are viewed as functions of relative gains against competing adversaries. This seems most logical as attacks from state entities are real, most apparent, and present grave danger to national security. As a total cyber strategy however, neorealism fails to recognize the threats against and opportunities for greater systems integrity presented by non-state actors and technology.

Security theories that focus solely on non-state actors, such as individuals and groups, and the power dynamic they share with states, are also insufficient to encompass the entirety of threats to cybersecurity. Groups with shared identities and goals often view cyberspace and the balance of power only in the context of those shared norms. This idea tends to clash with the goals of national security, which gives supremacy of the state over the constructed identities of individuals and collectives. Nonetheless, social constructivist security theories are adept at analyzing shared perceptions both inside and outside of a society, and are proficient at recognizing both the function of identity within the national security dynamic, and how those perceptions effect security. However, it is neither

practical nor feasible to implement an entirely social constructivist-based national security strategy in the middle of a cyber war zone, like the Korean Peninsula. Under such conditions, the concerns of the state must be recognized, and to a certain extent, so must the need for the coordination of cyber security and conventional security strategies and plans.

Neorealist and social constructivist perspectives on cyber security, however, share a similar problem. They both developed as interpretations of conventional international security, and at their core, neither one includes information technology to any great degree, which is the very *raison d'être* of cybersecurity. Despite the convenience of framing digital technologies within a traditional international security theorem, doing so is insufficient at best, especially for the subject of this study. There is, however, a growing community of IR scholars attempting to frame cyber security in largely digital, not kinetic dimensions. Among these theories, the one that is most explicit about the incongruent nature of unique national technologies, such as SEED encryption, and the extreme centralization of the internet and its security, is the theory of a “Cyber Westphalian” system. This theory is predicated on the development of possible or likely future technologies, and posits that state centralization of the internet in many countries, in concert with the development of these future technologies, will give rise to national “cyber borders”. Upon first inspection, this theory appears to be inclusive of technology, the state and its national security,

international aspects of the cyber environment, and both state and non-state attackers. What is missing in this model, however, is the role that benevolent or unwitting individual citizens and their behavior play. Neglecting to include these actors overlooks the benefits they can bring to national cyber security, and ignores the unfeasibility of sequestering the internet activity of individuals in a democratic society. Cyber Westphalianism is also limited somewhat in its scope (cyberspace), and in its approach towards a solution (technology). It also does not consider the economic, political and military dynamic between great, middle and regional powers. For these reasons, this theory is also an insufficient perspective from which to form a singular framework for the problem of software uniformity.

Rather than straining to fit one existing security theory to the software uniformity problem in South Korea, the author endeavored to find a theory that could encompass all facets of the problem, and that could allow the inclusion of aspects from neorealism, social constructivism, and cyber Westphalianism. Therefore, the argument of this dissertation is largely framed within the context of ‘intersectionality’ as it pertains to cyber security. Identified first by Kimberlé Crenshaw in 1989 to explain racial diversions in feminism, the theory of intersectionality explains problems in terms of the intersection of individual factors.⁴⁴ The idea was expanded to address other issues in the social sciences (Collins 1998, p. 71; McCall 2006, p. 1790). This theory holds that problems such

⁴⁴ Crenshaw, Kimberlé. 1989. “Demarginalizing The Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics.” *University of Chicago Legal Forum*. p. 140

as social injustice, are not caused solely by one aspect, event or system, rather they are the result of a convergence, or intersection, of multiple factors on different levels and from different environments that require multiple types of analyses. Recently, this theory has been applied to the field of cyber security by scholars such as Ben Fitzgerald (2015) and Tara Davenport (2015). Through this perspective, problems in cyber security are not viewed as solely policy-based, social or technical, but are the intersection of all three factors.⁴⁵ When applied to the uniformity of software in South Korea, intersectionality may provide clearer, more appropriate solutions to the problem of software uniformity in South Korea.

Similar to the convergence of phenomena that arises to cause social problems, it is the contention of the author that the solution of many cyber security problems, and specifically the problem of software uniformity, may also involve the convergence of particular traditional and non-traditional cybersecurity strategies, or an "intersection of theory". An intersection of theory for the problem of software uniformity would therefore have to analyze cyber security theories that address factors germane to this unique problem, namely a national security strategy, individual actors (*i.e.*, South Korean end-users and non-affiliated individual hackers), and technology (*viz.*, operating systems, browsers, and security software). For those reasons, the next three sections of this chapter are

⁴⁵ FitzGerald, Ben. 2015. "The Theory Of Intersectionality Can Make Cybersecurity Collaboration&Nbsp;Real." *TechCrunch*. <http://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/> (January 10, 2016).

dedicated to analyzing the theories connected by this intersectionality.

In this chapter, the concept of intersectionality and how it connects the other three relevant theories is explained at length. Neorealism is then examined in the context of national security and the state actors involved with software uniformity. This analysis is followed by an assessment of social constructivism in terms of the collective identities of end-users and hackers and their behavior. Lastly, the cyber Westphalian theory approach to software uniformity is elaborated upon.

2.1 *The Theory of Intersectionality*

The term “intersectionality” was first used in 1989 by American scholar Kimberlé Williams Crenshaw (1989) to explain social injustices committed against black females. Soon other legal scholars and social scientists utilized the idea of intersectionality in their work, due to its flexible nature. As intersectionality’s popularity grew, so did its uses (*e.g.*, as a theory, methodology, paradigm, lens or framework) and definitions. According to Olena Hankivskyan, under an “intersectionality perspective, inequities are never the result of single, distinct factors. Rather, they are the outcome of intersections of different social locations, power relations and experiences. Intersectionality promotes an understanding of human beings as shaped by the interaction of different social locations (*e.g.*, ‘race’/ethnicity, indigeneity, gender, class, sexuality, geography,

age, disability/ability, migration status, religion). These interactions occur within a context of connected systems and structures of power (*e.g.*, laws, policies, state governments and other political and economic unions, religious institutions, media). Through such processes, interdependent forms of privilege and oppression shaped by colonialism, imperialism, racism, homophobia, ableism and patriarchy are created.” (Hankivskyan, 2014 p. 9)

Hankivskyan claims that intersectionality is based on several key tenets:

1. Human lives cannot be explained by taking into account single categories, such as gender, race, and socio-economic status. People’s lives are multi-dimensional and complex. Lived realities are shaped by different factors and social dynamics operating together.
2. When analyzing social problems, the importance of any category or structure cannot be predetermined; the categories and their importance must be discovered in the process of investigation.
3. Relationships and power dynamics between social locations and processes (*e.g.*, racism, classism, heterosexism, ableism, ageism, sexism) are linked. They can also change over time and be different depending on geographic settings.
4. People can experience privilege and oppression simultaneously. This depends on what situation or specific context they are in.

5. Multi-level analyses that link individual experiences to broader structures and systems are crucial for revealing how power relations are shaped and experienced.
6. Scholars, researchers, policy makers, and activists must consider their own social position, role and power when taking an intersectional approach. This “reflexivity,” should be in place before setting priorities and directions in research, policy work and activism.
7. Intersectionality is explicitly oriented towards transformation, building coalitions among different groups, and working towards social justice. (Hankivskyan, 2014 p. 3)

According to intersectionality, human lives cannot be reduced to a single category, and policy analysis cannot assume that any one social category is most important for understanding people’s needs and experiences. Intersectionality also does not promote an additive approach (*e.g.*, examining the collective impact of gender, ‘race,’ sexuality, age and class) as the sum of their independent effects (*e.g.*, gender, class, race, etc.). Instead, intersectionality conceptualizes social categories as interacting with and co-constituting one another to create unique social locations that vary according to time and place. These intersections and their effects are what matters in an intersectional analysis. This multi-level, multi-faceted approach is concerned with understanding the effects between and across

various levels in society, including macro (*i.e.* global and national-level institutions and policies), meso or intermediate levels (*i.e.* provincial and regional-level institutions and policies), and micro levels (community-level, grassroots institutions and policies as well as the individual or ‘self’). Attending to this multi-level dimension of intersectionality also requires addressing processes of inequity and differentiation across levels of structure, identity and representation (Dhamoon and Hankivsky, 2011 p. 35; Winker and Degele, 2009 p. 66).

One way that intersectionality pays attention to power is through reflexivity. Reflexivity acknowledges the importance of power at the micro level of the self and our relationships with others, as well as at the macro levels of society. Reflexive practice recognizes multiple truths and a diversity of perspectives, while giving extra space to voices typically excluded from policy ‘expert’ roles (Bolzan, Heycox, & Hughes, 2001 p. 54). Practicing reflexivity requires researchers, policy makers and stakeholders to commit to ongoing dialogue about “tacit, personal, professional or organizational knowledges,” and their influences on policy (Parken, 2010, p. 85). Reflexivity can help transform policy when the people involved bring critical self-awareness, role-awareness, interrogation of power and privilege, and the questioning of assumptions and ‘truths’ to their work. For example, reflexive practices should help people consider their individual connections to colonization, and facilitate questioning

about policy and practices that accompanied the colonization of indigenous peoples in Canada (Hankivskyan, 2014 p. 9).

Consideration of resistance and resilience is integral to intersectionality because these can disrupt power and oppression. Even from so called ‘marginalized’ spaces and locations, oppressive values, norms, and practices can be challenged. One mechanism of resistance from subordinated groups has been to use collective actions to destabilize dominant ideologies. Conversely, policies and discourses that label groups of people as inherently marginalized or vulnerable undermine the reality that there are no ‘pure victims or oppressors’. Categorical policy approaches obscure similarities between groups and their shared relationships to power. It also prevents coalitional work by reinforcing conceptions of difference based upon specific categories.

Leslie McCall (2005), outlines an “intracategorical complexity” approach to intersectionality that “begins with a unified intersectional core, a single social group, event, or concept, and works its way outward to analytically unravel, one by one, the influences of gender, race, class, and so on” (McCall, 2005, p. 1787). It recognizes the shortcomings of existing social categories, and questions the way they draw boundaries of distinction.

Until recently, intersectionality had only been explained in the context of political, legal, or social issues. However, there are those who have begun to apply the multifaceted approach to cyber security. Ben Fitzgerald (2015) explains

the connection between the two thusly:

“Government outreach efforts often talk about collaboration and working together but usually in a vague, aspirational, kumbaya kind of way. However, for cybersecurity the need for collaboration is pragmatic and pressing. The ubiquity and power of information technology means that the biggest security risks exist at the intersection of disciplines and communities. Collaboration is the only way to mitigate these risks. An intersectional perspective allows us to better understand why certain cyber attacks occur and are so damaging.

The recent attacks on Sony have accelerated the Obama administration's efforts on cybersecurity. But why was the Sony attack such an unmitigated disaster for the moviemaker? While this was definitely a cyber attack, it was also an international relations incident, a state sponsored terrorist attack on freedom of expression, and an example of Hollywood being ridiculous. The damage occurred at the intersection of the actions of a sophisticated hacking group (or 'advanced persistent threat'); poor cybersecurity practices by Sony; the leaking of damaging private corporate data; the use of terrorist threats to block the release of “The Interview” and the incompetent responses from Sony (including canceling then digitally releasing the movie, threats to sue Twitter and an

alleged denial of service attack on servers hosting Sony's leaked data). The attack and its fallout could absolutely have been mitigated if Sony had a better IT department. But Sony would also have benefited from better leadership, a less toxic corporate culture and a crisis management team with the ability to call on government support.

Other factors beyond Sony's control also played a critical role in this attack including, a poor relationship between the United States and China on cybersecurity, a lack of international protocols for dealing with cyberattacks and limited means for the United States to impose further political costs on North Korea. Sony was on the receiving end of a sophisticated attack but simple attacks can also have outsized impact when they occur at the right set of intersections.” (Fitzgerald, 2015 pp. 1-2)

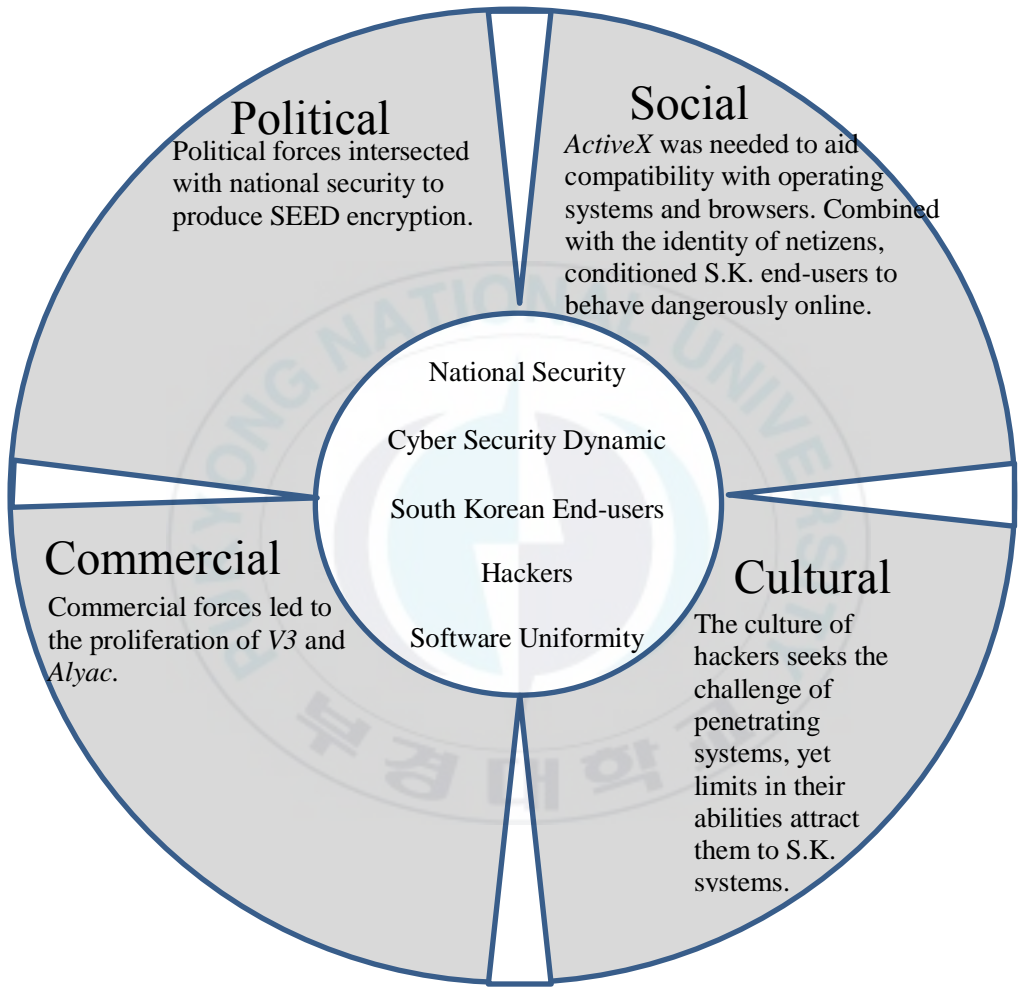
It is these “right set of intersections” that may have occurred in the past fifteen years during the major South Korean cyber attacks. Politically, past administrations chose domestic encryption policies that seemed sound and promoted national security. Such policies can be examined in the context of political science, where political motivation, power politics and legislative factors are examined. Alternatively, investigations on said policy could be examined through the lens of international relations and neorealism. Such an approach

would look at the loss or gain of South Korea's relative power via its national public-key policy. It could also be viewed by cyber-Westphalians as a defense mechanism that serves as a type of cyber border. On another level entirely, the problem could be studied as a function of group or cultural identity of South Korean end-users, hackers, or both. Many chose to view any problem associated with cyber security as a technical problem, and would suggest that an answer rooted in technology. All of these premises, events, and actors intersect with each other at different point along the timeline. It is the author's contention that these radically different viewpoints and approaches all contribute to the explanation of the problem, and to its solution.

Logistically, these policies made many South Korean systems incompatible when they intersect with the international cyber environment. Commercially, these intersections decrease the diversity of software used in South Korea. Socially, the nature of *ActiveX*, the use of which was proliferated by the first intersection, may have intersected with cultural identity, conditioning end-users to download files in a manner that can have deleterious effects. All of the independent factors involved in software uniformity and its exploitation intersected to have a negative impact on South Korean cyber security. The intersection of hacker culture and South Korean software uniformity may have, and may continue to attract larger numbers hackers, and lower the threshold on the range of abilities necessary to penetrate South Korean systems. Figure 2-1

conceptualizes such a model of intersectionality.⁴⁶

Figure 2-1: Intersectional Model for Software Uniformity



Crenshaw identifies the issue of a singular analysis that separates of

⁴⁶ Mason, C. Nicole. *Leading at the Intersections: An Introduction to the Intersectional Approach Model for Policy & Social Change*. New York: NYU Wagner, 2010. p. 6. Accessed January30, 2016.

social injustice into different challenges facing specific groups (race, gender, sexual orientation or socioeconomic status) (Crenshaw, 1989 p. 158). Individually, these analyses miss the bigger picture, creating competition and division between issues, and rifts in perspectives that obfuscate important problems. A single-axis analysis of South Korean cyber attacks might suggest that they were merely an issue of poor network security or the inevitable outcome of focused, state sponsored hacking. Cybersecurity and social justice are markedly different fields but the core insight of intersectionality holds true for both. The field of cybersecurity must move beyond discussions over whether a core issue is about Problem A or Problem B, or theory A or theory B. Instead cybersecurity must understand the relationships among all problems, and utilize all relevant theories in approach those problems (Fitzgerald, 2015 p. 4). In that vein, the remaining sections of this chapter highlight the unique and applicable aspects of neorealism, social constructivism. It also explains each theory's relevance to the problem of software uniformity in South Korea.

2.2 *Neorealism*

The neorealist perspective on international relations, famously put forth by Kenneth Waltz in the late 1970's, outlines the actions of nations as reactions to structural constraints of relative power (Waltz, 1979 p. 218). Waltz's theory on the relative balance of power is quite comprehensive in determining how states

interact with one another in an international system that is decentralized and anarchic. It is therefore understandable why many current cyber security scholars and policy makers find it useful in framing the international cyber dynamic similarly to Waltz's model. Power consequently coalesces towards one, two or several great nations. Driven by their own survival in this structure, states develop capabilities to either increase or protect their relative balance of power (Waltz, 1979 p. 102; Mearsheimer, 2001 p. 13).

On the surface, cyber security seems to fit well within the neorealist model for several reasons. The internet by its nature is anarchic. This decentralization of cyberspace makes it difficult to coordinate efforts internationally, or to enforce international laws across oceans or continents. This allows for security strategies that are more self-interested and less cooperative. A state can militarize their capabilities both defensively and offensively. Governments can also attempt to control their citizenry's access to outside information when that information is political, undermines state authority, or threatens national security. Such control can extend outside the state, as was the case of Russia and Estonia.

In April of 2007, protests broke out among the ethnic Russian population over the Estonian government's removal of a Soviet war monument. Supported by a protesting Kremlin, anti-government sentiment in the region grew beyond the streets and into cyberspace. What initially started out as defacing Estonian

government websites, soon escalated into cyber war. State-affiliated hacker groups based in Russia were able to utilize millions of computers infected with 'zombie' malware to launch denial of service attacks that shut down communication and banking networks in Estonia. These groups were believed to be supported and utilized by the Russian government, and were part of a growing community of underground hackers in Russia who use their skills for illegal gains. This was a way for Russia to punish its former satellite which had joined the EU, and was moving towards stronger ties with NATO. (Clark and Knake, 2010 pp. 12-16; *The Economist*, 2007) In essence, the Russian government used the protest as an excuse to protect their national security and secure or even extend their sphere of influence in the region. Protecting national security and international influence in a zero-sum model (usually associated with resources, military power and relative economic advantage), and is a common idea among offensive realists such as John Mearsheimer.⁴⁷ In offensive realism, states project power internationally to pre-empt encroachment on their relative power in a manner consistent with the idea of “the best defense is a good offense”. These states will engage in conflict only when the result is a net gain for the state and a net loss for its adversary. Such strategies can be observed in international cyber conflict. As was the case with Russia and Estonia, great powers will launch preemptive and retaliatory cyber attacks (often covertly), as their disproportionate

⁴⁷ In Mearsheimer's Tragedy of Great Power Politics, he explains that great powers avoid a 'status quo bias' by acting offensively and "look for opportunities to alter the balance of power by acquiring additional increments of power at the expense of potential rivals" (Mearsheimer, 2001)

power advantage, in the form of greater resources, skilled manpower and more advanced technology, will most likely result in relative gains. However, great powers also attack other great powers, despite the lack of any advantage. Such attacks occur frequently on a small scale, because it is feared that an attack from the other is imminent, and not preemptively attacking represents a net loss of relative power.

Richard Clark, succinctly characterizes the militaristic aspect of the neorealist argument when describing the 2009 North Korea cyber attack on South Korea:

“The new ‘cyber warriors’ (in North and South Korea) and much of the media herald these incidents as the first public clashes of nation states in cyber space. There are other examples, including operations by China, Taiwan, Israel, and others. Some have called the Estonia case ‘WWI’, that is, Web War One.” (Clark and Knake 2010 p. 15)

However, there are potential pitfalls to viewing cyber security strictly from a neorealist perspective. First, the only level of analysis are states and national interest. Many cyber attacks are often initiated by individuals with motives outside of national interest and financial gain. Hactivist groups such as ‘Anonymous’ often have political agendas not affiliated with a single government

or state, and are usually done without state support.⁴⁸ Hackers often coordinate activities across borders and social groups to achieve goals that have little to do with the balance of power in the international system. Unlike a nation's military and other government-run entities used to protect or increase relative balance of power, access to the internet is not limited only to the state. Additionally, actors using the internet that are not included in neorealist observations (*i.e.* individuals, political groups and corporations) are also not necessarily motivated by national security interests.

Secondly, neorealism assumes that states with the greatest resources have the greatest power, and are therefore more secure than those states with less resources and relative power. However, vast armies, cutting edge technology and large GDP's are not necessary to wage cyber warfare. All any nation would need to inflict severe damage are computers with access to the internet and dedicated individuals with the expertise to carry out the attacks. We have seen this already in countries like North Korea. In general, North Korean infrastructure and society are less dependent on cyber space. Lack of cyber infrastructure prevents more technologically advanced nations from disrupting the weaker nation's operational logistics through the internet, and therefore makes less advanced, developing nations more secure against cyber attacks. Conversely, a high dependency on the internet and a complex, computer integrated infrastructure in nations such as the

⁴⁸ 'Anonymous' is a loosely organized group of international hackers who have claimed responsibility for disrupting the computer systems of governments and corporations.

U.S., China and South Korea, make them more vulnerable to electronic attacks (Clark and Knake 2010, p. 218). The asymmetric and decentralized nature of cyber capabilities in developing countries, makes it difficult to adapt an entirely neorealist philosophy towards cyber defense.

Despite the discrepancy between power and security in cyberspace, Seoul seems to favor a neorealist strategy towards cyber defense. Government policy on cyber security is of a top-down nature that focuses on the military and intelligence agencies as the main conduit for control and implementation. The 2008 Korean National Defense White Paper listed cyber security as an important component of National Defense. In 2011, Presidential Directive 141 created the National Cyber Security Center.⁴⁹ The Lee Myoung Park administration regarded cyberspace as an operational domain (in addition to land, air and sea) that needed a state-level defense system. This militarization of cyber security has centralized much of the decision-making power over the security of the internet. These strategical decisions not only show the emphasis that is placed on cyber security in South Korea, but also show that the government treats cyberspace as the new international battleground for national security. Therefore, in order for a framework for studying software uniformity in South Korean to be comprehensive, it must reflect these strategies. It must include an analysis of states-level threats and attacks, primarily from North Korea, and suggest policy to

⁴⁹Defense White Paper. Seoul: Ministry of National Defense, Republic of Korea, 2008.

defend against those attacks. The unintentional consequences of implementing these strategies on unacknowledged or low-priority aspects of the national cyber environment must also be examined, but from different more appropriate perspectives and methods.

2.3 *Social Constructivism*

As this dissertation deals with the capability, motives, and behavior of individual non-state actors, it is important to examine the elements of social constructivism as they pertain to cyber security and South Korea. Constructed identities of both computer hackers and South Korean end-users play a part in the South Korean cyber security dynamic. However, choosing such a theoretical framework from which to interpret the data from the cyber attacks on South Korea, has been the subject of debate. Some see what happened in South Korea as a top-down problem in which the government is not the problem's only source, but the main agent of change. South Korean policy makers, security analysts and corporate decision-makers are more hesitant to embrace a wider focus on the problem. Their solutions focus around state-level actors (*e.g.*, the North Korean government, the Chinese, etc.), and are firmly embedded in neorealist perspective. There has not been much of an attempt by anyone to search for a constructivist solution to the problem of cyber integrity in South Korea.

South Korean cyber security studies may only focus on the cyber threats and state actors of neorealism or power-sharing, and to a much lesser extent, the international cooperative dynamic of neoliberalism (Valeri, 2010 p. 144). However, within the field cyber security theory, constructivism has been discussed at length. Constructivists generally view the internet as a conduit for groups of people with shared regional, cultural or normative identities to propagate ideation (Onuf, 1999, p. 23). Eriksson, Giacomello and Ransport have all written about how cyber attacks are affected by constructed identities (Eriksson and Giacomello, 2010 p. 181). Although it mentions nothing of cyber security per se, the theory of 'securitization', developed by the 'Copenhagen School', offers an analysis on threat politics based on perceptions and constructed identities. Matters of security are framed by political actors based on their perceptions of threats. These shared perceptions form around how and when threats occur and with what consequences (Waeber 1995, p.210; Buzan 1998 p.79; Williams, 2003 pp. 523-6). In the Copenhagen view, perceptions are formed by 'speech acts', and studies therein rely on examinations of the language used to frame threats. In this way, reports prematurely blaming North Korea for a cyber attack can be viewed as explicit government 'speech acts', designed to frame perception around the national security narrative. This is very useful when examining the political rhetoric that accompany attacks. When studying cyber threats presented by individual state actor however, a framework more

appropriate for collective actions and behaviors of individuals in cyber space is also required.

Johan Eriksson takes the Copenhagen School concept a step further and relates it to cyber security in his study of securitization of IT in Swedish Politics. However, rather than uncovering weaknesses in Swedish IT behavior or Swedish policy concerning IT, his analysis focused on who or what is to blame, and how responsibility for dealing with the threat is allocated (Eriksson 2001, pp. 211-212). Again, language becomes important as responsibility for ‘cyber crime’ and ‘cyber warfare’ fall under different purviews. Cyber crime must be handled by police, making the criminals the actors of analysis. Power rests partially in civilian hands. Whereas cyber warfare is the responsibility of the military, and states then become the actors analyzed. This makes sense in terms of organizing vast amounts of cyber threats, trying to identify the attackers and delegating responsibility for defending against them. However, the solution seems rather post hoc, as it does not address inherent weaknesses in a social system. The construction of identities are outward (towards the criminal, state or institution), not collective identities of self (Wæver, 1995 p. 187). An analysis of cyber actions against South Koreans and how they can be prevented must first start with the individual’s action vis-a-vis the collective understanding of the internet. It would be difficult to fix systemic problems by chasing individual events and the different motivations of individual actors. However, there have been

constructivist based theories which focus on collectivism with regard to specific cyber events. Giacomello describes a constructivist approach to international cyber security which does involve the method of attacks (Erikson and Giacomello, 2010 pp. 18-19). In his analysis, Giacomello focuses on individual and collective perception as they relate to IT. However it is still language-centered and looks at how terms like ‘virus’, ‘malware’, ‘bugs’, ‘firewalls’ etc. are used:

“The use of terms such as ‘information warfare’ and ‘electronic Pearl Harbor’ convey a special meaning: that which is digital by nature has, nonetheless, a physical consequence comparable to those of conventional war. Constructivist analysis can contribute to revealing and understanding the significance of such rhetoric and symbolic actions.”

(Erikson and Giacomello, 2010 p. 21)

Although perhaps mired in terms and symbolism, Giacomello does make a compelling case for the use of a constructivist framework in studying cyber attacks and their impact on international relations. His analysis can be taken beyond symbolism to include other kinds of actions, namely social norms and internet behavior. In South Korea, individual and collective perceptions of cyber security not only have their root in South Korean ‘online world’ terms, but also in

‘off-line world’ culture and actions.

Magnus Ranstorp mentions these actions when analyzing the success of Al-Qaeda recruitment across territories and its link to IR theory (Erikson and Giacomello, 2010 p. 35). He describes how Al Qaeda was able to fuse collective ideas into a belief that unified behavior into a call for action. He also refutes Fiona Adamson’s claim that there is a ‘lack of theory’ regarding the relationship between individual agents and international security (Adamson 2005, 547-8). He states that, “Constructivism seems to offer a valuable pathway out of this conundrum (i.e. the disconnect between the structural theories of the international system and the micro-practices of individual actors engaged in the promotion of normative agendas). Actions can be conceptualized as a series of arguments about Muslim identity” (Erikson and Giacomello, 2010, p. 32). In the case of South Korea, ‘normative actions’ are already fused (through government action or by South Korean culture), and we can readily judge its impact not only on cyber security, but also how it relates to the international system.

South Korea is a somewhat unique country to study in terms of constructivism and international relations. First, it has only one ethnicity and culture. To be Korean means to be ethnically Korean and to have been raised in Korea. This identity as ‘Korean’ goes beyond what those in the West view as citizenship. South Korea does have a growing population of naturalized citizens, but they are not viewed as ‘Korean’ ontologically by the rest of South Korean

society (Lee, 2013 p. 201). There are also many ethnic Koreans who have been raised outside of South Korea. Perhaps closer to Koreans in identity, Koreans born and raised abroad, called “Gyo po” (교포) in Korean, are also considered ‘others’ for their lack of knowledge of Korean culture and/or its language (Zur, 2003 p. 15). Koreans have a shared history going back almost 3,000 years. For most of that time, Korean society and its political system evolved around Confucian beliefs; mainly a hierarchy of allegiances and strong emphasis on humility and collective congruence. (Jiang, 2006 p. 9406) The collective identity of South Koreans and the idea of ‘the other’ being non-Koreans was cauterized during the 50 year occupation by the Japanese in the late nineteenth and early twentieth century (Bayliss, 2013 p. 171). South Korean society and behavior is a product of that history.

Amongst South Korean people there are numerous economic, social, political, religious and cultural divisions, yet when it comes to South Korean identity and the perceptions of threats from the outside, South Koreans are often unified. Mixed views on foreign policy towards North Korea give way to a singular demand for action from South Korean people in the face of an incident like the sinking of the naval vessel the Cheonan in disputed waters off the Yellow Sea coast in 2010. The South Korean legislature is notorious for its heated debates and infighting, however even low-level challenges to national security stemming from territorial disputes with Japan are met with a seemingly unified

national response, galvanized across political aisles. Disputes like the possession of Tok-do island⁵⁰ bring back the collective wounds of the Japanese occupation, to which many Koreans still identify. These disputes threaten South Korean identity, much like the occupation itself did.⁵¹

Collective behavior is also evident in how things are done or how one learns to do things. With its early origins in the Confucian system, the education system in South Korea is designed to teach all students the same way with an extremely high degree of standardization. Students are then arranged in a hierarchy based on rank and age (Chung, 1995 p. 111). Students (and later adults) do things because that is what their elder, more informed classmate or friend told them to do. When that behavior is pervasive, people begin doing things because that is the way it is done in South Korea. This is especially true when South Koreans use the internet. The sites they go to, the social media platforms they use, the types of software and browsers employed are all products of how things are done. Unknowingly perhaps, Korean people are defining their identity through this behavior.

Age and position are also strong elements of South Korea collective behavior. The more senior a colleague is in terms of age or position, the more respect that colleague commands, the more his or her actions and commands are

⁵⁰ *Tok-do* is a group of islets (located 37°14'30"N 131°52'0"E") currently under Korean possession, but is disputed by the Japanese government (known as *Takashema* in Japanese) (Wiki Atlas).

⁵¹ During the occupation, the Japanese government carried out a campaign to exterminate Korean culture, language, names and identity. Koreans were forced to take Japanese surnames, forbidden to speak or write Korean and were encouraged to think of themselves as Japanese.

followed, and the greater share of responsibility he or she has for how things are done. This can be seen in the corporate hierarchy in South Korea. Input from subordinates is rarely used or accepted and therefore is not given (Lam, 2015 p. 18). Decisions and protocols concerning computer use follow along the same lines. A Korean employee does not question the logic of cyber security protocols, they simply follow the orders that have been sent down from above, and come to accept the validity of the behavior simply because it is the rule. Whether viewing the ‘top-down’ formation of collectivization as with the educational and corporate structure or ‘bottom-up’ formation in response to outside threats, any constructivist framework around cyber security must consider such cultural phenomena and be able to link it to the international system.

Alexander Wendt’s ‘Social theory of International Politics’ can be adapted to encapsulate the cyber threats and the prevention thereof. Although the theory does not specifically address cyber security, it does incorporate both the cultural and international parameters prevalent in the cyber attacks of 2013. Collective identity and social norms and practices are connected to the international structure through the society’s perceptions of the elements of that structure (Wendt, 1999 pp. 313-336). His theory also fits nicely with dynamics of South Korean culture and society. Observable, collective behavior can be used to explain not only South Korean perception of outside cyber threats (that they are negligible), but also its perception of and connection to the international system.

In this analogy, collective behaviors based on identity, such as using *Microsoft's Internet Explorer* exclusively and using only *Ahnlab* and *ActiveX* software, make South Koreans more prone to cyber attacks, and how South Korean society reacts are all based on its perceptions of the international system

Wendt defines this collective identity as the collective identification of shared characteristics of the self (in this case South Koreans) from others (non-Koreans). Identities are arranged hierarchically based on the degree of commitment to them (Wendt, 1999, p. 122), and Koreans have an unmoving commitment to that identity. Wendt argues that the salience of the collective identity to the individuals determines the strength of society's commitment to it (Wendt, 1999, p. 230). For South Koreans, the salience of being Korean (*e.g.*, Korea's history, culture and norms), are instilled in them through their education and observation of collective behavior. Collective identity creates structures in the form of governments and corporations that reinforce identity and behavior through centralization and internalization (Wendt, 1999, p. 219). These self-reinforcing structures of collective identity are apparent in the centralization and internalization of internet norms and behaviors by South Korean corporations and the South Korean government.

How is collective behavior connected to identity, theoretically? Wendt believes that engagement in public activity connects the community to events and practices. These practices are reinforced through internalization. Therefore,

behavior like identity can be communal (Wendt, 1999 p. 178). In South Korea, the public engagements of individuals are pursued in the same manner, and practices have become monolithic. It is these practices that leave South Korea vulnerable to cyber attack, and where a solution can be found.

The connection of collective identity to the international system depends not only on the structure of the international system, but also on how you view the goals of the individual actors in the system. For neorealism, this means an anarchic system with state actors whose ultimate objective is material (*e.g.*, economic, power, hegemonic, military etc.). For neoliberals, this means a structured international system also with state actors, but whose objective is to cooperate for a greater, more stable, collective reward. Wendt argues that IR theorists have to think about the connection to the international system in social, not materialistic terms. Even anarchy can be broken down into its elements that the actors (i.e. nations, individuals, society) perceive (Wendt, 1999, pp. 246-8). He writes, “The structure of anarchy varies with changes in the distribution of ideas” (Wendt, 1999 p. 310). The manner in which ideas are distributed in South Korea, changes very little. Therefore, the structure of anarchy to South Koreans and their behavior towards it also change very little. Wendt continues to explain that these actors internalize these identities more deeply over time. In that manner, South Korean identities have been solidifying under such conditions since 1945, and since the late 1990’s in cyberspace. There is an argument for

collective behavior being a product of policy and not identity. Koreans have a strong cultural (and national) identity. In many circumstances, that identity, transcends intra national politics and international norms. In general, Korea is a conformist society where age and position often dictate the behavior towards other Koreans. This identity often opposes the state view its national security narrative and directives.

The best example of this can be seen in the South Korean concept of ‘the netizen’. The South Korean government has seen a surprising reaction from its self-proclaimed ‘netizens’ towards restrictive cyber policy. Such reactions are often unexpected in a country renown for conformity. In 2008, policy makers felt Korean netizens posting on the internet were acting irresponsibly by circulating rumors over the dangers of contracting mad cow disease from American beef imports and posting malicious comments about celebrities under pseudonyms. Public fervor ignited when actress Choi Jin-sil committed suicide. There was wide speculation by Korean people that negative comments posted on the internet led to her suicide, and demands were made on legislators to prevent users from posting comments anonymously. In 2008, the so-called “real-name internet” law was passed, which required people to use their real name, verified by their national identification number when posting comments on the internet.⁵² At first, internet users tolerated the restrictions on their freedom of expression. But as

⁵² Article 44-5 (Authentication of Online Bulletin Board User) of the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (정보통신망 이용촉진 및 정보보호 등에 관한 법률). Accessed December 15, 2015.

cases of retribution for message board postings grew, and after a system hack that downloaded millions of South Korean identification numbers, South Korean netizen opinion on the real-name law soured. There were massive protests against the law and public outcry from mostly younger Koreans sparked a movement that eventually spilled over into the mainstream. Finally in 2012, the constitutional court overturned the law finding that it “is unconstitutional, and such provisions are in violation of the principle of less restrictive alternative expression, and the freedom of speech of both users as well as ISP’s in cyberspace, and the self-dissemination of personal information.”⁵³. If internet behavior was only the product of limitations set down by the government, then change in such behavior (and directives) would also have to come exclusively from the state. However, as the ‘real-name-internet-law’ and the netizen backlash showed, that change can also occur through actions of collective identity. In the case of software uniformity, the argument that download behavior is a product of SEED/ *ActiveX*, is not mutually exclusive with idea that end users disregard the dangers of active downloads due to the ideation of their netizen, end user or national identity. There are those within South Korea who do not identify with that ideation, and thus simply refuse to download. Their behavior is motivated by information outside of the collective knowledge.

Given the large role that individual and collective identity and behavior

⁵³ Constitutional Court Decision 2010.Hun-Ma47.decided on August 23, 2012. Accessed May 3, 2014.

play in the problem of software uniformity, it is crucial that these aspects be measure and analyzed through a constructivist perspective. Behavior and identity must be measured at the source, and must also measure the effects of policy on them and vice versa must be analyzed. However, a constructivist analysis can only explain technology in terms of how it affects collective identities, and not the effectiveness of those technologies as a cyber defense.

Despite constructivists' compelling description of the cyber dynamic, its actors, and the connections to the international system, it would be difficult to convince those outside constructivism (especially those in the government) that cyber infrastructure can be adequately defended solely through recognizing identities an ideation. To them, the problems with constructivist identity arguments are compounded by the difficulties in attributing these attacks to their sources. Furthermore, constructivism fails to explain the technological gaps between South Korean end users, and does not explain how technology can affect the problem or offer a solution. Those explanations require elements from other more appropriate theoretical perspectives.

2.4 *Cyber Westphalian Theory*

Chris C. Demchak and Peter Dombrowski state in their paper "Rise of a Cybered Westphalia", that the relatively ungoverned frontier of cyber space, like all frontiers, does not last forever when human societies are involved. Eventually

nation-states will extend their sovereignty to the internet and exert control over the electronic information that comes in and out of their national domains. In essence, nations will create electronic borders. Demchak and Dombrowski cite the recent developments in the cyber security policies of developed nations as evidence that states are already moving towards a bordered internet (Demchak and Dombrowski, 2011 p. 13). This theory constructs conditions of national cyber security and a process by which nations will create cyber borders through the use of technology. It is important to this dissertation for two reasons. First, it builds an alternative theory predicated on technology and exclusiveness. Secondly, an analysis of the theory provides clear examples of the deleterious and often unintended consequences of a national restriction of access through the use of technology.

According to Demchak and Dombrowski, “the transformation from frontier to substrate across cyberspace” began with the discovery of the stuxnet virus in 2010. Stuxnet was a virus planted in the systems of Iran’s nuclear centrifuge. It eventually destroyed those centrifuges and set the Iranian nuclear program back years. The malicious software was believed to be uploaded to the Iranian secure off-line system via USB flash drives. Ingeniously crafted, the virus employed many new sophisticated techniques and codes that were designed with specific knowledge of its target. Such an endeavor required the resources of an advanced country with an extensive intelligence network, and have led some to

believe that it was created by the United States, Israel or both.⁵⁴

Without remote directions, stuxnet meticulously sought and destroyed a predetermined section of the centrifuge and demonstrated that heavily secured systems not connected to cyberspace are still vulnerable to cyber attack (Zetter, 2011) (Langer, 2013). For Demchack and Dombrowski, this was a turning point in cybersecurity policy. Developed nations now had a concrete example of a cyber threat with real world catastrophic potential. More importantly, they now have a reason to draw lines and establish sovereignty over the internet.

Demchack and Dombrowski maintain that the response will be to move further towards a closed, bordered internet system that can more thoroughly scrutinize foreign data and thereby prevent potential threats to national security. This can be seen in how states are administering cyber security. Cyberspace is no longer only under the jurisdiction of state-run communications and commercial agencies. Many industrialized nations are now treating cyberspace as another operational domain of the military. Countries like China and the United States are developing technology and defense strategies that would create borders in cyberspace and allow nations to deal with threats; even when those threats come from their own citizens. These nations have already demonstrated their willingness to go on the offensive to protect national interest. Through each nation's 'cyber command', the militaries of technologically advanced countries

⁵⁴ Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force.'" *PC*, March 25, 2013.

have engaged in cyber warfare that goes beyond simple espionage or vandalism, as they seek to extend their regional and international security paradigm to the realm of cyberspace. Such actions have forced less technologically advanced countries to push their more developed allies to secure their cyberspace through traditional security arrangements and organizations such as NATO and the U.N., as the cyber Westphalian map begins to take shape (Demchak and Dombrowski, 2011 p. 7).

The concept of a partitioned, defined, organized and controlled cyberspace runs contrary to how most people perceive the internet. It is not a distant, sparsely populated region of the country, nor is it an isolated no man's land. The frontier of cyberspace is a network of billions of systems in virtually every part of the world, and has an equal number of diverse actors. The exponential acceleration of the technological evolution and innovation therein, has formed an environment in which the aggressors manage to outpace defensive strategies and systems. Software and hardware designed to steal information, subvert systems, disrupt public policy, and mask the user's identity are freely shared among hackers. Also, computer users in liberal democracies have become accustomed to the freedom that a borderless cyberspace provides. Attempts by governments to close Pandora's Box are often met with resistance that spills over into the political arena, and has a significant effect on policy. Unlike a physical frontier, reining in cyberspace would seem to be impossible. However Demchak

and Dombrowski assert that reclaiming sovereignty over the internet is technologically possible, psychologically comfortable, and systemically and politically manageable.

It is Demchack and Dombrowski's contention that the new map of cyberspace complete with borders, boundaries, and frontiers that are accepted by all states is inevitable. The beginnings of which can already be seen in countries such as the U.S., China, South Korea and the E.U. to varying degrees (Demchack and Dombrowski, 2011 p. 22). However, examining not only the cyber military policy of these states, but also their public and commercial internet policies reveals that it will be difficult for liberal democratic nations to execute and enforce even many basic restrictive cyber policies. Furthermore, creating cyber borders depends on a partitioning of cyberspace through technology and national public standards. Although states can have shared agendas on cybersecurity, they rarely have common standards when it comes to executing cybersecurity. Such disconnects in cyber policies will impede the flow of cyber traffic necessary for many forms of international communication and commercial interaction. Forrest Hare agrees with the basic concept of cyber borders, but cautions policy makers not to disrupt the connectivity between nations. Kunrether and Heal apply a game-theory approach to binary choices (known as the interdependent security investment decision)⁵⁵ to international cyber security, which alluded to two

⁵⁵ Heal, G., and H. Kunruther. "Self-protection and Insurance with Interdependenci." *Journal of Risk and Uncertainty* 36 (2008): p. 117. Accessed January 4, 2016.

points. First, the probability of a state investing adequately in cyber security is directly related to the threat level at which it perceives cyber incursions. Secondly, in order for cyber borders to be effective, all nations must participate. Hare uses his own model for interdependent liberal democracies to show that in order for cyber borders to be effective all relevant nations must participate. The less states participate, the greater the probability of a successful attack. If only one state or a few participate, the system is compromised.⁵⁶ There is little or no benefit for states to construct cyber borders, if they maintain a connection with allies who do not pursue such borders (Hare, 2011 p. 39). As the utility of the internet expands its reliance on internet-driven communications, and as commerce created in a borderless cyberspace increases, states may be less inclined to participate. Thus more obstacles to cyber borders are created making a Cyber Westphalian system less probable.

South Korea can be seen as a litmus test for liberal democracies following a closed internet strategy. It has already experienced the difficulties of limiting cyberspace from its initial forays in cyber security policy. In addition to early policy mandating SEED technology, the government also began to limit anonymity, content and access to foreign sites in an attempt to save the moral and social integrity of its cyberspace. However, these actions had the unintended consequences of limiting the commercial potential of the internet, and facilitating

⁵⁶ Hare uses the analogy of two airplanes from different airlines, boarding at the same time. Both airlines must inspect all of their passengers' luggage. If one of the airlines fails to do so, a malicious actor may be able to plant a bomb on the secured plane through the unsecured airport.

the theft of personal information of its citizens. Ironically, this new security coding ended up actually making South Korean systems more vulnerable to incursions. During the past fifteen years, South Korea has been the victim of many successful large-scale attacks, and has seen its carefully laid plans to partition and defend national cyberspace slowly unravel.

As was the case with South Korea, nations who pursue borders in cyberspace will have to either drastically change the nature and scope of plans for a nationalized cyberspace or abandon the concept all together. Also, Demchack and Dombrowski's model is predicated on the assertion that virtual borders are technologically possible, psychologically and politically manageable. However, there is evidence that suggests for liberal democracies this may not be the case. The following represent obstacles to the cyber Westphalian theory.

Technologically speaking, there have been a number of innovations that make borders in cyberspace possible. However they are not without their logistical limitations. Although cyber borders may well be desired by developed nations, the implementation of such might not be feasible. Collectively, hackers have historically had an advantage over those defending national systems. Within the parameters of the current architecture of the internet, it is still not possible in some cases to detect new malicious codes, locate and identify attackers or fully secure vital, off-line systems. Even if future technological advances were to allow nations to sequester their national cyber infrastructures, there is no guarantee that

such actions would make systems more secure.

Technologies securing borders in cyberspace must be able to scan all information coming through its networks in order to detect malicious or illegal codes, distinguish between national and international content, and identify and locate their sources. The conventional wisdom has been that such security measures are simply impossible, and that no defense is impenetrable. No matter what kind of defensive strategy or technologies states may devise, given enough time, every system can be hacked (Cisco 2012, p. 4). Current technology cannot scan all incoming data to determine its national origin and threat potential, nor can modern forensic techniques always track the source of the hack and the identity of the hacker. Demchak and Dombrowski argue against this (Demchak and Dombrowski, 2011 p. 2).

The way citizens perceive their government's role in cyberspace varies greatly from state to state. Culture, history and demographics are all determinant factors of a nation's psychology on issues such as privacy, freedom of information, intellectual property, libel and trust in the government. Cyber borders may be psychologically acceptable in one society, but not in another. These sui generis elements of the national psyche may also impede the transition to a Westphalian internet.

In China for example, the government has felt very little resistance to its restrictive internet policies. Beginning in the mid 1990's, successive regulations

have increasingly limited what Chinese citizens can say or access online. This led to creation of Section Five of the Computer Information Network and Internet Security, Protection, and Management Regulations approved by the State Council on December 11, 1997. This law criminalizes the use of the Internet to create, replicate, retrieve, or transmit anything that incites not only criminal and treasonous actions, but anything harming national unification, and promoting of untruths, vices and slander (Abbot 2004, pp. 110-113).

In addition to censorship of government criticism online, many commercial and social networking sites, such as Google and Facebook, are banned and replaced by their domestic counterparts. There are as many as 18,000 websites that are blocked by the Chinese government (Zittrain, 2006, p. 1982). Penalties for violating these rules or using virtual private networks to circumvent policy can be harsh. But despite the threat of imprisonment there is still a subdued counter reaction to government actions, often through satire and sarcasm. “Chinese websites made subtle grievances against the state’s censorship by sarcastically calling the date June 4 (the anniversary of the 1989 Tiananmen Square massacre) as “Chinese Internet Maintenance Day.”⁵⁷ Perhaps this type subtle acknowledgement of censorship that still complies with government policy, would be psychological manageable. But it would most likely be an atypical reaction to a government restricting the internet.

⁵⁷ Johnson, Bobby. "Chinese Websites Mark Tiananmen Square Anniversary with Veiled Protest." *The Guardian*, June 4, 2009. Accessed November 13, 2014

Then there are those nations that have sought to control the flow of certain sensitive foreign and domestic information only to find their efforts undermined by a citizenry not willing to conform to state standards. The best example of this is the Arab Spring. Despite the ban on social networking and outside media sites, citizens of Tunisia, Egypt, Libya, Yemen, Syria and Bahrain were all able to utilize banned sites to organize protest movements, disseminate censored information, and eventually bring down many of those regimes.

Given the nature of civil societies in liberal democracies, it is not certain that cyber borders would be politically manageable either. In some societies, freedom of expression supersedes issues of cyber security within the politic. For these countries, cyber borders are not politically manageable. Furthermore, the democratic process in many countries often impedes the formation of the political consensus required to expedite new cyber policy. The speed of technological development, relative to that of policy formation, also makes it extremely difficult for governments to legislate technology. In South Korea, this problem is exemplified by the constraints and vulnerabilities mentioned in the previous chapter.

However, there have been attempts by the South Korean government to effect change in this area. In 2011, after pressure from makers of alternative technologies such as smart phones forced the government to rethink their 10 year-old cybersecurity strategy, the government created a bylaw calling for the support

of at least three different web browsers on government websites. Even if varying the browser support for government websites could change the now embedded online behavior of developers and users, implementing change is very difficult. In order for websites to stop using *ActiveX* plug-ins, a government appraisal committee must evaluate the new technology to ensure it has the same level of security. So by moving farther away from the rest of world, the South Korea government actually put its country's cyber infrastructure closer to harm's way.

Stuxnet is a key element in this Cyber Westphalian model. It not only shifts policy makers' focus towards a radically new method of cyber defense, but it also serves as the fulcrum by which public opinion is swayed towards cyber borders. But is that a fair representation of stuxnet's salience? It is not entirely certain whether or not stuxnet conforms to Demchak and Dombrowski's characterization as a catalyst for a new internet paradigm. Stutnex was a large, densely-coded computer virus designed specifically to attack the synchronization mechanisms of the uranium centrifuge at the Iranian nuclear facility. The virus replicated itself and spread throughout the targeted system by utilizing a zero-day exploit, a very rare and dangerous code.⁵⁸ Malware appropriately named "zero-day" are types of pernicious coding previously unknown in cyberspace. It is unique in code and structure, and therefore can be undetectable and indefensible. Zero-days take advantages of vulnerabilities in the software of its host that are

⁵⁸ Less than one in 1,000,000 malicious code that are uncovered are 'zero days'. They require the creator to meticulously test every part and line of a software's code; a process that can take years. (Zetter, 2011, p. 3)

unknown to the software's designer at the time of the incursion. With no defensive obstacles to confront, nor any possibility of detection, the exploit spreads very rapidly making containment extremely difficult if not impossible. Stuxnet's first zero-day exploit spread itself to other sections of the centrifuges systems through infected USB sticks introduced to the facility's system by its workers (Zetter, 2011). This exploit was necessary as the different sections of the centrifuge system, like that of many highly secured systems with catastrophic potential, were not connected to each other nor to cyber space.

It is worth noting that today the main mission of the stuxnet virus' coding is essentially dead. It had one specific goal, and that goal was achieved. Although residual effects from stuxnet were felt by systems in cyberspace for some time afterwards, the coded commands would only have its intended effect on the Iranian centrifuge. Once the virus was discovered and deconstructed cyber security firms were able to tag its specific characteristics allowing most security programs and firewalls to detect and block the virus. The entirety of stuxnet's code has since been open sourced, however the fear that an international actor could employ the same or similar techniques found in stuxnet still remains.

However, stuxnet's effectiveness has not gone unnoticed by South Korean cyber security policy makers, especially in light of their ongoing cyber war with North Korea. Many cyber attacks originating in North Korea have wreaked havoc on its neighbors to the south, especially the previous two attacks

in 2013. South Korea's cyber command has publicly stated that it is actively seeking to develop a stuxnet-like weapon that could disable North Korea's Young Ban nuclear facilities. The development of such a weapon is the first half of a two stage strategy. The first part of South Korea's plan, which is ongoing, is to conduct online propaganda operations by posting to North Korean social networking and social media services. The development of weapons capable of physically damaging North Korean nuclear plants and missile facilities would be the second phase of a strategy that began in 2010. The completion of the second stage would culminate in regular cyber missions against North Korea.

However such a strategy would most likely be unsuccessful due to lack of cyber infrastructure and dependency on the internet in North Korea. Lack of cyber infrastructure prevents more technologically advanced nations from disrupting the weaker nation's operational logistics through the internet, and therefore makes less advanced, developing nations more secure against cyber attacks. Conversely, a high dependency on the internet and a complex, computer integrated infrastructure in nations such as the U.S., China and South Korea make a nation more vulnerable to electronic attacks (Clark and Knake, 2010 p. 16). The asymmetric and often decentralized nature of cyber capabilities in developing countries makes it difficult to adapt an entirely neorealist philosophy towards cyber defense.

It can be inferred from the stuxnet experience that cyber borders would

be ineffective against such a sophisticated zero-day threat. The virus showed that connectivity is not necessary to infiltrate secure, closed systems. After all, the virus' success was dependent upon the intelligence gathered for its creation and implementation. It is not unrealistic to assume that the distribution of such a cyber weapon could just as easily be distributed in a national cyber domain, given the intelligence and resources by the attacks.

Although the cyber Westphalian theory does approach cybersecurity threats from a technical perspective, it fails to account for the international cyber dynamic, or the social and political norms of individuals. Additionally, the end result of a national internet is a narrower, more limited, and perhaps more vulnerable national cyber environment.

2.5 *The Intersection of Theory: An Integrated Approach*

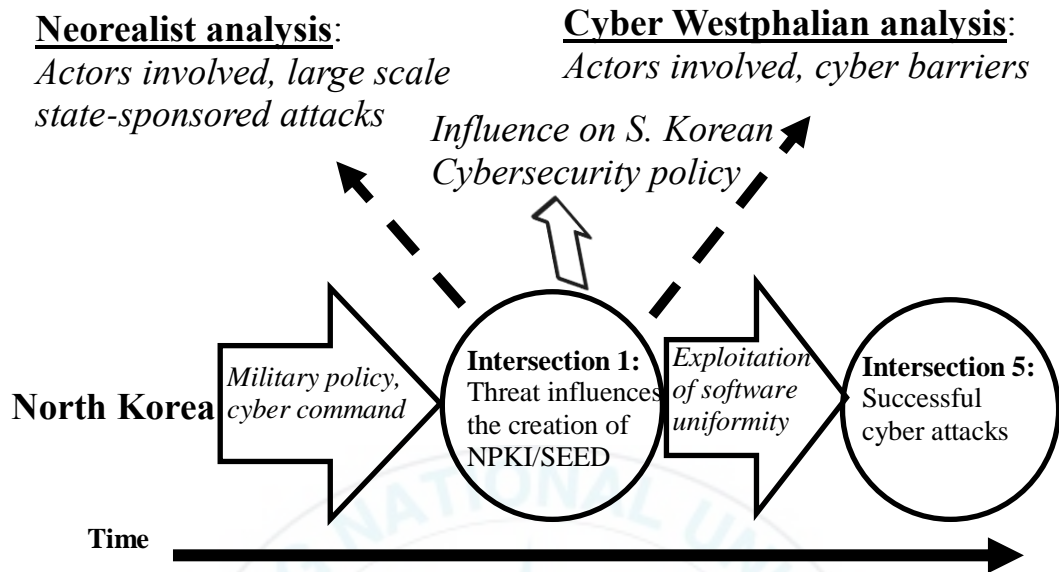
In order for intersectionality to be a viable model for explaining phenomena in cybersecurity, it is important to understand, to the extent possible, when and how separate actors, events, actions, characteristics of the cyber dynamic, and all other relevant factors on every level of analysis intersect to bring about such phenomena. It also requires that researchers know all or most of these factors intimately, and approach the problem with an open mind so that they can design a comprehensive and integrated methodology which employs multiple perspectives. Actors (states, individuals, groups, etc.) take actions (enact policy,

follow policy, attack, defend against attack, project power, etc.) that intersect with elements of the cyber environment (infrastructure, technical limitations, culture, policy, identity, etc.) and give rise to cyber security phenomena, such as vulnerabilities, system integrity, deleterious behavior, identities and motivations.

It can be confusing and difficult to conceptualize a model that includes four different types of actors, three different security theories, ten separate phenomena interacting at six intersections. Therefore, the rest of this chapter organizes and explains the different inputs in such a model. To avoid confusion, the author explains each actor individually and its corresponding actions, phenomena, intersections and relevant security theories.

The first actor to participate in this model is North Korea (Figure 2-2). The North's cyber command and traditional military strategy intersect with South Korea by influencing their cybersecurity policy at 'Intersection 1'. State level actors and competition for relative gains call for a neorealist approach to that aspect of the problem. To a lesser extent, elements of cyber Westphalianism can be employed in the analysis. As events unfold, North Korea can exploit the vulnerabilities of South Korea's software uniformity, and thus intersect with the phenomena at 'Intersection 5'.

Figure 2-2: Intersectional Analysis of North Korea

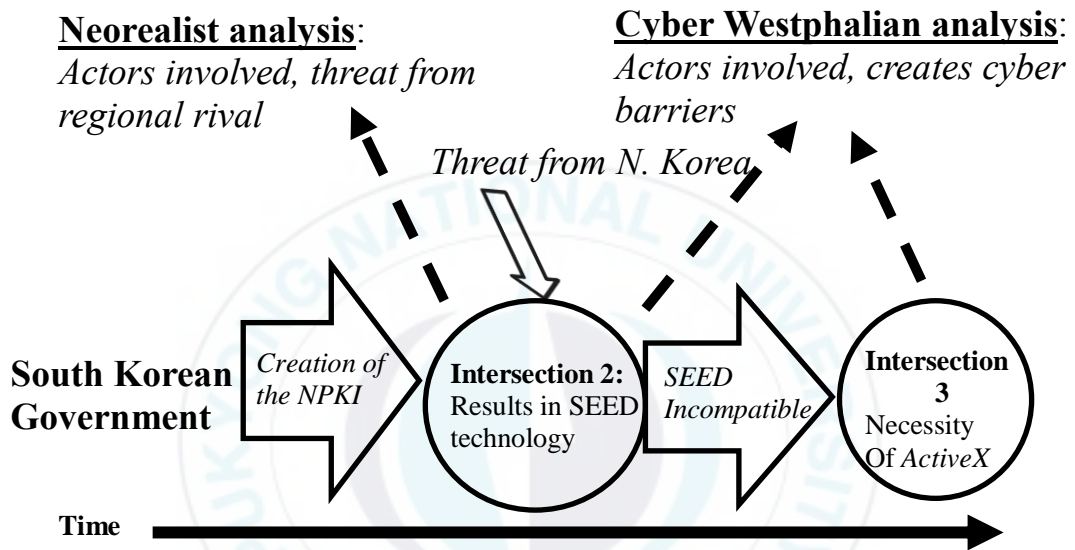


Another level of analysis employed by this dissertation is that of the South Korean government. In order to protect its new digital infrastructure, the South Korean government initiated its national public key infrastructure (NPKI). As a response to the threat of cyber attack from North Korea and possible digital fraud, policy makers created required SEED technology (Intersection 2). This intersection of the South Korean government, its actions and North Korea can be analyzed from a neorealist perspective due to actors involved and their motives. It can also be approached using cyber Westphalianism, as the actors are appropriate for such, and because it is the beginnings of a type of cyber barrier based on technology. As a result of these actions, *ActiveX* became necessary to read and download operation and security plugins (Intersection 3). Therefore, this

intersection of the South Korean government and *ActiveX* can be investigated using a cyber Westphalian approach for similar reason as the first intersection.

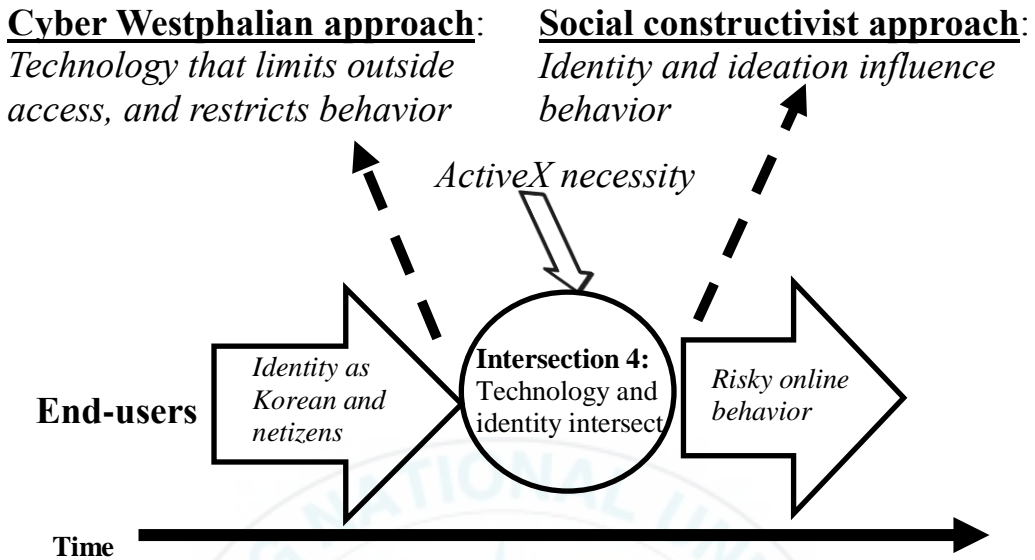
Figure 2-3 illustrates this level of analysis.

Figure 2-3: Intersectional Analysis of the South Korean Government



The next level of analysis involves South Korean end-users. End-users and their behavior is a product of their identity as both Koreans and netizens. This intersects with the necessity of downloads and digital signatures through *ActiveX* at 'Intersection 4'. At this intersection, technology and identity produce the risky online behavior of the end-user. Thus, this intersection can be analyzed by both a cyber Westphalian approach (limiting technology) and social constructivism (identity/culture). Figure 2-4 illustrates this concept.

Figure 2-4: Intersectional Analysis of South Korean End-users

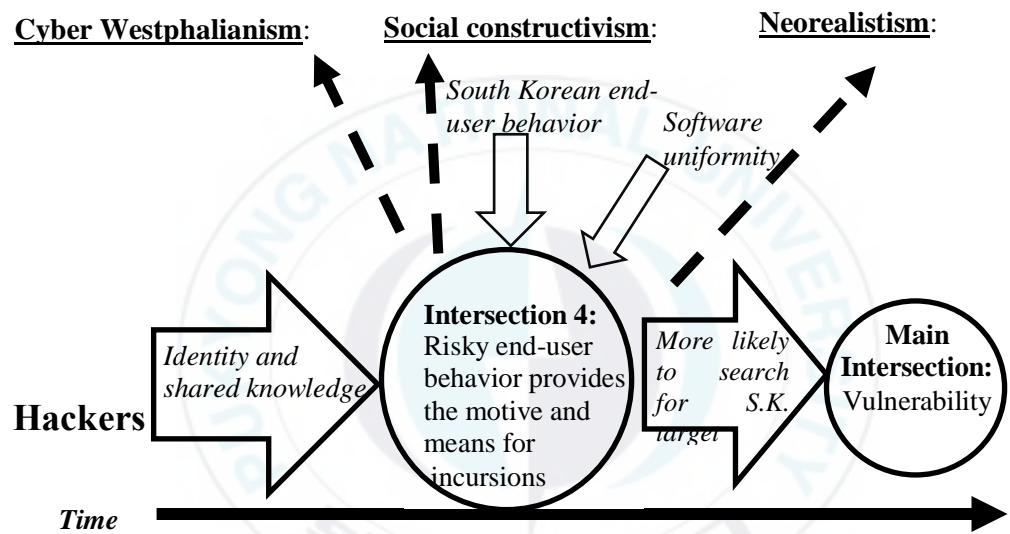


The final level of analysis involves hackers. The intersection of hackers' collective identity and culture (knowledge, behavior, ideation, etc.) and the risky online behavior of end-users represent the main vulnerability of South Korean cybersecurity. For it is here that South Korean end-users' risky online behavior provides the motivation and means for hackers to compromise South Korean systems. Since that behavior is a result of technology, identity and state-level threats and policies, all three theoretical approaches must be used to investigate the problem. Figure 2-5 illustrates this main intersection.

Lastly, Figure 2-6 integrates all these levels of analysis in to one schematic. Represented on the far left of Figure 2-6, are the levels of analysis necessary to understand the intersectionality of software uniformity, and how this phenomenon contributes to vulnerabilities in South Korean cyber security. The

broad, two-dimensional arrows going from left to right represent the action of the actors, and other factors within the cyber environment. The circles represent the intersection of these factors, and the dashed-line arrows, indicate the corresponding theoretical approaches listed horizontally at the top.

Figure 2-5: Intersectional Analysis of Hackers



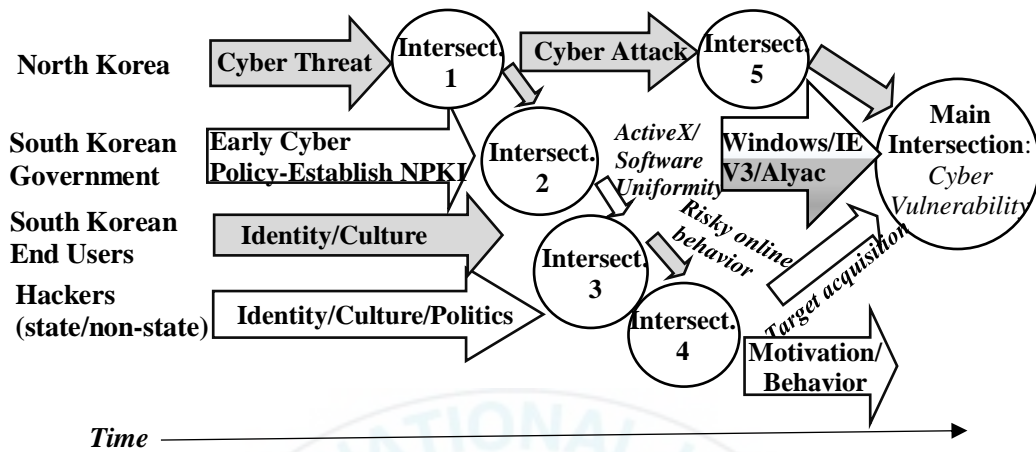
Moving forward in time, the persistent security threat from North Korea intersects with the South Korean NPKI (Intersection 1). These factors and their resultant intersection are best analyzed by both a cyber Westphalian and a neorealist approach. South Korean policy requiring the download of embedded technologies intersects with technical limitations (Intersection 2) which creates a dependency on *ActiveX*. The analysis of this intersection, and its related factors, is also best served by the technical aspects of the cyber Westphalian approach. *ActiveX* dependency intersects with end users, as it conditions to them to

disregard security warnings (Intersection 4). As this intersection deals with the identity and behavior of individuals, specifically the risky online behavior of end users, a social constructivist approach is most appropriate for its analysis. *ActiveX* also contributes to the lack of variation of operating systems and browsers, which in turn is a contributing factor to overall cyber vulnerability.

Meanwhile, hackers create their various identities and cultures online. In the schematic, state hackers branch off early, and use the computers of end users to launch attacks against South Korea (Intersections 1 and 5), and are analyzed through neorealism. These attacks also contribute to overall vulnerability. However, individual hackers do not intersect with South Korea on a national level or with end users until South Korea becomes dependent on *Windows* and *Internet Explorer*, and the risky online behavior of end users, attract the hackers' attention and influences their target acquisition (Intersection 4). The behavior and motivations of these individual hackers lend themselves best to the social constructivist perspective.

In this case of the vulnerabilities in South Korean cybersecurity, intersectionality provides a good comprehensive model to explain, in detail, all the factors contributing to vulnerabilities with a broad, multi-discipline perspective, and deeper understanding of the problem.

Figure 2-6: *A Multi-tier, Integrated Schematic for the Intersectionality of South Korean Software Uniformity's cyber vulnerability.*



If the author's interpretation of the theory of intersectionality is correct, a solution to South Korea's software uniformity may be simple, but it is drawn from the intersection of political, social, and technological factors unique to South Korea and the time frame examined: namely, the dismantling of the NPKI, or at least the abolition of authorization plug-in requirements for all types of transactions and the indirect requirement of any one browser or operating system, and the promotion of national and foreign security software variation. The methodology, analyses and conclusions of this study are all framed within this context and provide the foundation for the following hypothesis:

1. The limited technical characteristics of systems in South Korea are a threat to the integrity of South Korean cybersecurity.

2. These technical limitations increase the range of knowledge and capabilities of those able to successfully penetrate South Korean systems, and thus allow more perpetrators to compromise a larger number of such systems.

3. Greater ease in accessing South Korean systems surreptitiously, results in greater motivation for hackers to target these systems.



CHAPTER THREE

METHODOLOGY: A MIXED APPROACH

This dissertation's hypothesis makes the supposition that the limited technical characteristics of systems in South Korea constitute a threat to the integrity of South Korean cyber security, and that such factors increase the range of knowledge and capabilities of those able to successfully penetrate South Korean systems. This would potentially allow more perpetrators to compromise a larger number of systems than if those characteristics did not exist. The author further posits that these characteristics could increase the motivation of hackers to target these systems. These claims make two basic assumptions. The first assumption is that an inordinate uniformity of operating, browsing and security software does indeed exist in the systems of South Korea. The second and perhaps more important assumption is that such uniformity makes South Korean systems both easier to infiltrate, and more attractive to hackers. Testing these assumptions requires a methodology in which all relevant variables are defined and measured accurately.

To that end, this chapter attempts to delineate the software characteristics of South Korean users, separate the relevant variables, and measure the qualifying components. The author then correlates these components with the users' rates of incursions on his/her system, and then verifies the potential threat level through qualitative analyses. It must be understood that the author cannot and does not

make any claims of direct causation between major cyber attacks and software uniformity. Although a lack of software diversity may have indeed made it easier for hackers to perpetrate major cyber attacks, there is no definitive evidence supporting such a categorical claim in either this dissertation or the body of literature. However, the author does suggest that a correlation would infer that these characteristics are contributing factors to cyber vulnerabilities. The author also attempts to similarly measure the proficiency and inducements of hackers as they relate to different types of software. Unforeseen complications with this part of the study prevented the author from claiming direct correlation with any high degree of confidence.

To answer the basic research questions of this study, the author first devised a quantitative method to measure the technical aspects, behavior, motives and capabilities of the subjects in question. Once this was established, qualitative methods were employed to highlight the security risk each variable may pose. This data is then used in the following chapters to analyze and predicate its implications.

In order to test the assumptions made in this dissertation, the author employs both quantitative and qualitative methods. Quantitative data was collected in the form of two surveys to measure specific variables of the subjects being examined. An online survey was given to South Korean end-users to gauge what types of operating systems, browsers and security software they used, and

how the respondents act under certain conditions. Another survey was distributed online to hackers to measure their abilities and motives.

Using this data, the author then utilized qualitative methods in its interpretation to uncover linkages between the variables. Experts on coding, malware, and the technical parameters of cyberspace and the South Korean cyber dynamic contributed their expertise to this research. Experts in the behavior, culture and methods of hackers were also interviewed to provide a more salient understanding of the South Korean cyber dynamic. Throughout this section, the author also considers mitigating factors that may have also affected the accuracy of surveys results.

3.1 *Quantitative Methodology*

Quantitative data was collected by administering two online surveys. One survey targeted South Korean computer users, and the other survey targeted computer hackers. The information gained from these surveys represents a significant portion of the total evidence presented in this dissertation, and therefore establishing the validity of their design, distribution and collection is paramount.

3.1.1 **Validity of Online Surveys**

Although there is currently some skepticism of the validity of online

survey methods in academia, the use of such methods in modern research is growing. The digital format of this type of survey has distinct advantages in terms of cost, speed, and often coverage. Such advantages are often negated by those critical of its validity and reliability. However, there is a preponderance of evidence to suggest that online surveys, such as those used in this research, not only contain less bias than their off-line counterparts, but may be more valid for certain research goals. It is the author's contention that this dissertation conforms to such goals.

Traditionally, coverage of the target audience was the largest hurdle for online sampling to overcome in achieving valid reliable results. U.S. President Harry Truman's 1948 victory over Thomas Dewey, a seemingly standard technology may appear to provide comparable coverage to previous methods, but actually may skew the results dramatically. Just prior to the 1948 presidential election, a Gallup poll conducted by telephone erroneously predicted that New York Governor Dewey would defeat incumbent president Harry Truman. At the time, many households did not have a phone, or used a shared phone line with multiple households. This lack of coverage drastically affected the accuracy of the sample. Using this poll and spurned on by leading pundits of the day, *The Chicago Tribune* released its November 3, 1948 edition with the front-page banner headline of "Dewey Defeats Truman", which led to the iconic photograph

of Truman holding a copy of the paper after his victory.⁵⁹ Sampling methods using technology only become more representative as the total population's adoption of the technology increases. In 1998 for example, only 6% of the South Korean population had regular access to the internet.⁶⁰ Despite what was arguably one of the most prolific rises in the national internet adoption rate, the total number of households with internet connections was only 65.5% five years later during the height of the internet boom.⁶¹ At the time this research was conducted in 2014, coverage was far less of a problem for online surveys in South Korea, as the connectivity rate of the population was 83.4%.⁶² In fact, the potential coverage of some online surveys has even surpassed that of their off-line counterparts. However, the issues of validity and reliability are more complex than just the coverage of a survey, and require a greater level of scrutiny for any such research to produce meaningful results.

In order for any population sampling and questionnaire to claim validity, they must be both externally and internally valid. External validity requires that the sample is indeed representative of the population being studied. This can be affected by response rates, distribution channels and the population's interest in the researcher's topic. A greater response rate generally indicates a more accurate representation of the population. Response rates for online surveys have been

⁵⁹ Groffin, Ken, Fred Lekme, and Ursala Koners. *Identifying Hidden Needs: Creating Breakthrough Products*. Springer, 2010. p. 28.

⁶⁰ World Bank Data. "Internet Usage as a Percentage of Population." Accessed January 22, 2016.

⁶¹ Ibid 57. p. 10.

⁶² Ibid 11.p. 2

shown to be lower by a significant margin than telephone, mail-in or paper surveys. However depending on the channels by which the digital survey is disseminated, its total distribution may be much larger than off-line alternatives, and its response rates vastly more difficult to calculate.⁶³ The survey must be distributed in a manner that could potentially reach all of the selected population. In other words, every member of the target population must have an equal chance of being selected to participate. For traditional survey methods, this is done by a random selection of those solicited to participate from the entire target population. This is not always an easy endeavor, as randomization of large populations requires vast databases and legitimate randomization methods. For many online surveys such randomization is impossible, but that does not always mean that the entire target population does not have the potential to be chosen as a participant. When researchers target online populations, such as users of a particular website, users in a particular geographic region, etc., traditional methods could yield much less representative samples than those distributed directly through the medium being studied. It has also been observed that interest in the topic of the survey amongst the target population, specific segments of that population, or the population at-large are key factors in the response rates of questionnaire recipients.⁶⁴ Given these external characteristics that can potentially invalidate traditional surveys, it would be impossible to say with absolute

⁶³ Weirisma, Weibo. "The Validity of Surveys: Online and Off-line." *Oxford Internet Institute*, 2009, 3-23. p. 11. Accessed January 7, 2016.

⁶⁴ Ibid 60, p. 13

certainty that such surveys are more representative than those distributed through the internet, especially with regard to online populations.

The pendulum of academic perception swings in the opposite direction on the question of which type of survey is more internally valid. Internal validity demands that the conditions of the survey itself and the questions within are accurately measuring what they were intended to measure. The two main impediments to a survey's internal validity are question bias and testing bias. Bias born of poorly worded questions can appear in all types of surveys equally, regardless of the survey's expedition, and are therefore irrelevant in a comparison between traditional and online surveys. The types of questions used can also affect the internal validity of both kinds of surveys similarly. For example, open-ended questions, such as fill-in-the blank or essay questions are more subject to interpretation by participants and researchers than close-ended questions, such as multiple choice or numerical questions. The more specific and easily quantifiable the question is, the more accurate the measurement of the intended variable will be. However, in regard to a self-administered survey, the likelihood that the questions are presented to the participant in a random order, thus ensuring participant's previous answers will not have a statistical effect on her or his answer to the current question. The possibility of randomization is actually greater with online surveys or any computerized survey method that has the

ability to randomize questions⁶⁵. Testing bias occurs in the administration of the survey and the interpretation of its answers. As was the case with question bias, open-ended questions are less valid internally, because the answers are at greater risk of being misinterpreted by the researcher than are quantitative answers. Again, this is true both online and off-line. Generally speaking however, testing bias is lower in online surveys simply due to the absence of a human moderator or administrator, and the influence he or she may have on the respondent. There is evidence to suggest that the aesthetics of an online survey questionnaire may also influence a respondent's answers, however that effect may be negligible.⁶⁶

3.1.2 KISA Survey Methodology

As this dissertation concerns South Korean cybersecurity and online populations, it would seem appropriate to investigate the methodology of surveys conducted by KISA as a standard for comparison. KISA's 2015 survey on national internet usage targets the same population as the user survey in this dissertation. The nation-wide survey was conducted using face to face interviews of 63,200 participants in 25,000 households, during a 10-week period (08/01/15 - 10/15/15). Post-stratified multi-stage cluster sampling was then employed to improve the accuracy of the sample.⁶⁷ Cluster sampling divides the population into groups, or 'clusters' based on a selected demographic that each cluster

⁶⁵ Bryman, Alan. *Social Research Methods*. Oxford: Oxford University Press, 2015. pp. 206, 173

⁶⁶ Ibid 60 p. 605

⁶⁷ Ibid 11 p. 1

member shares. One of the clusters is then randomly selected to be sampled. This is done to reduce administrative costs by improving the efficiency of the sampling, and only when the population is deemed to be homogeneous (the mean of each cluster is similar). Multi-stage cluster sampling repeats the simple cluster technique producing a smaller population to randomly sample after each stage. In the case of KISA's survey, the population was clustered in multiple stages by type of living quarters and occupancy, rooms in use, age group and educational attainment of household head. After each stratum of clustering, the sample is weighted by current estimates of changes in the population.⁶⁸

The methods employed by KISA are not without statistical drawbacks. Cluster samples are less accurate than simple random sampling, and each stage of clustering negatively affects the external validity of the survey.⁶⁹ Furthermore, there are those that would argue that the degree of a population's homogeneity and the selection of post-stratified weights can be arbitrary, possibly further skewing results.⁷⁰ However, such sampling methodologies are necessary given the cost and manpower required to accurately sample the entire population through face to face interviews. Apart from the sampling method, the face to face format itself is at a much greater risk of being internally invalid. The interviewer

⁶⁸ Ibid 63

⁶⁹ Ahmed, Saifuddin. "Methods in Sample Surveys: Clustering." *Journal of the School of Public Health, John Hopkins*, 2009, 1-45. p. 2. Accessed January 15, 2016.

⁷⁰ Bryan, Paul D., and Thomas M. Conte. "Combining Cluster Sampling with Single Pass Methods for Efficient Sampling Regimen Design." *2007 25th International Conference on Computer Design*, 2007. doi:10.1109/iccd.2007.4601941. p. 23. Accessed January 16, 2016.

and the interviewee both have the potential to bias the results. The greater number of interviews conducted, the greater chance there is for such errors to occur.

Despite the afore mentioned drawbacks, post-stratified multi-stage cluster sampling is a widely accepted practice in both industry and academia, and the data compiled in KISA's survey on internet usage should not necessarily be treated as suspect. Due to practical constraints, this method was used, but it would appear that KISA has done its due diligence to be as accurate as possible. In that same vein, the methodology of this dissertation, while not also without statistical drawbacks, reflects the author's commitment and effort to ensure that the results are accurate.

3.1.3 South Korean End-user Survey

This survey was designed specifically to measure which types of operating system, browsing and security software were used at home and work, as well as the number of incursions on those computers, if any. If the target of this survey were the entire population of South Korea, its online distribution would call into question its coverage. As mentioned in section 3.1.1, only 83.4% of the populace regularly uses the internet, so more than one sixth (16.6%) of the country would not be represented.

The author used the online research tool *Survey Monkey*, and solicited participants online through advertisements on subject-specific message boards,

face-to-face distribution, Naver, Facebook, KaKao, and email trees.⁷¹ From January 1, 2013 until December 31, 2014, these solicitation remained posted and led respondents to the questionnaire through a link. All collection and collation of data was done by *Survey Monkey*, and the identities of the respondents were kept anonymous.

However since the target population is South Korean internet users, coverage is theoretically 100%.⁷² This also adds to the survey's external validity as the entire population has a chance to be a participant.⁷³ The 2,570 participants in this survey represent a sample size of South Korean internet users with a $\pm 1.97\%$ margin of error (See Figure 3-1). The author was careful to distribute this survey through as diverse an array of South Korean internet channels as possible, so as to reach a broad variety of demographics. The fact that the survey was self-administered, quantifiable, randomized the order of the questions, and recorded and compiled responses digitally, added to its internal validity.

The Korean-language survey consisted of one qualifying question and 24 Korean-language multiple choice questions pertaining to the following aspects of

⁷¹ An 'e-mail tree' is a generic term used to describe distribution of an e-mail in which the recipient has the ability and authority to send the contents of an email to whomever he or she chooses. In this study specifically, respondents were asked both before and after participation to invite at least one person to participate in the survey by sharing the link with any qualified person they wish.

⁷² There is always the possibility that a small number of the target population could not access this survey for any number of unforeseen reasons, however with less than a 2% margin of error the effects of such a possibility would be minimal.

⁷³ Although the total target population would all have a chance to participate in the survey, the probability that each member of the population will participate is not necessarily equal across the population.

participants (*For a copy of the full questionnaire in Korean, with its English translation, see Appendix A*):

1. Demographics (four questions).
2. Frequency and location of internet access (one question).
3. Type and version of operating software (four questions).
4. Types of browsers used at work and at home (two questions).
5. Antivirus software used (two questions).
6. Frequency of specific internet behavior (three questions).
7. Cyber incursions on the participant's personal computer (seven questions).

Table 3-1: The Statistical Parameters of South Korean Internet Users Survey⁷⁴

Population Size	41,110,000 (83.4% of the population) ⁷⁵
Sample Size	2,570
Confidence Level	95%
Confidence Interval	1.93
Standard Error	.00985
Relative Standard Error	1.97

Usage data for the U.S was provided by *Statista.com*.⁷⁶ Global usage

⁷⁴ Statistical parameters were partially calculated by the *Australian National Statistical Service*

⁷⁵ (KISA, 2015 p. 4)

rates were retrieved from *Stack Overflow*.⁷⁷

3.1.3.1 *Demography of Participants:*

Originally, it was the author's intent to cross-reference segments of the end-user population by demographics. However, there was not a great deal of discernible distinction in the responses from the participants along these different segments. Also, the goal of this study was to find potentially vulnerabilities to cyber security originating from all end-users, thus there was no need for a deep examination of these characteristics. In the future, this data could be helpful to cyber security research that is more demographically focused.

3.1.3.2 *Operating System*

The survey participants were asked a series of questions regarding the type of operating system software that he or she used both at home and at work. The multiple choice questions allowed users to choose between four commonly used operating systems (Apple *Macintosh*, OS/X, *Windows*) and "Other/I don't know". *Windows* users were further asked to clarify which version of *Windows* they used. Participants were given the choice between all five versions of *Windows* still being supported by Microsoft at the start of the survey.

⁷⁶ "2014 U.S. Software Usage/P.C.," *Statista.com*, 2015

⁷⁷ "Survey 2014 Desktop Software (World)"; *Stack Overflow*, 2015

3.1.3.3 *Browser Software*

Participants in the survey were also asked which browser they used at work and at home. Similar to the questions on operating systems, participants could choose between Microsoft's *Internet Explorer*, Google's *Chrome*, Apple's *Safari*, Mozilla's *Firefox*, and "other".

3.1.3.4 *Security Software*

Survey participants were also asked which security software they used on their computers at home and at work. They were asked to choose one of seven widely used Korean and international security software services, or "none".

3.1.3.5 *Frequency and Location of Internet Access*

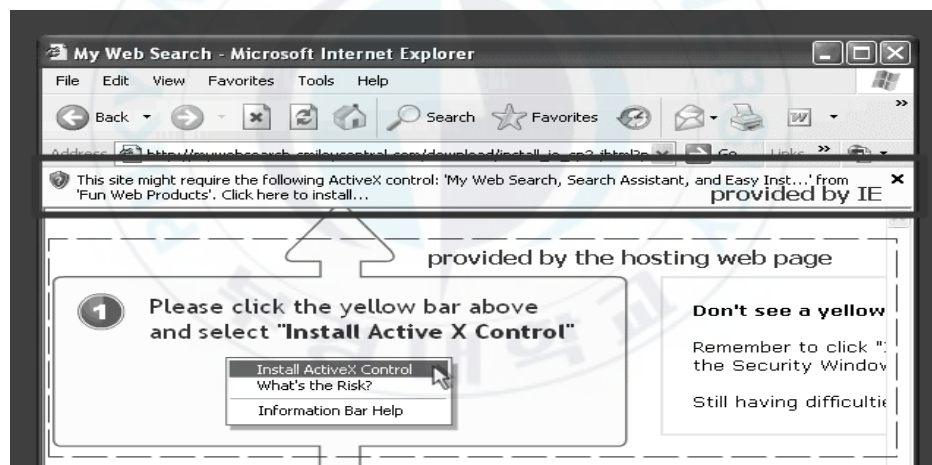
The next question was designed to ascertain the locations where South Korean end-users access the internet, and the frequency with which they use those locales. Participants were given five locations (*home, work, public computer, and other*) and asked to rate the frequency (*daily, weekly, monthly, less than one a month, or never*) with which they access the internet from each location.

3.1.3.6 *Response to ActiveX Warnings*

Several questions were designed to measure the degree to which the

survey participants engage in online behavior that would increase their system's exposure to malware, and thus may also increase the probability of an incursion to said system. The first of these questions asks the sample population to assess, with relative certainty, their response to an *ActiveX* warning prompt (Figure 3-2). The multiple choice question asks the respondent if she or he would accept the download after *ActiveX* prompt warns the user of the risks, and if so, with what regularity do they do it (*always*, *usually*, *sometimes*, *rarely*, *never*).

Figure 3-2: ActiveX Download Warning Prompt



3.1.3.7 Behavior towards Unknown Website Links

This survey also measures the behavior of users when presented with links to sites of interest. Again, participants were asked to gauge their response to a given situation. However, this time the response is to a link to an interesting or informative post sponsored by an unknown or untrusted third-party website. The

multiple choice answers vary in degree of trust (implicitly trust, occasionally skeptical, usually skeptical, always skeptical) of the link, and the frequency (*always*, *usually*, *sometimes*, *rarely*, *never*) of the user opening such a link.

3.1.3.8 Behavior Towards E-mail Links

The final question concerning the online behavior of South Korean end users also measures their response to links of interest and importance. However, this link is distributed through an e-mail received by the user. The participant is asked to evaluate the frequency (*always*, *usually*, *sometimes*, *rarely*, *never*) with which she or he would open such a link.

3.1.3.9 Occurrence, Location and Mode of Incursions

The next set of questions measures whether or not users have experienced an incursion on their system, how many times they have been hacked, and where the incursion occurred. Participants were asked if their e-mail or a social network account had ever been compromised. They were also asked if their home PC or mobile device had ever been rendered inoperable due to malware. The same questions were posed to participants regarding their PC or mobile device used for work or school.

3.1.3.10 *Connectivity between Home System and Work/School Network*

The final question posed to South Korean users measures what portion of the sample population that has access to his or her work or school's computer network from their home or personal device.

3.1.4 **Hacker Survey**

In order to test the assumption that the uniformity of software in South Korea may incentivize hackers to try and penetrate South Korean systems, an online questionnaire was designed to gauge certain capabilities of the respondents, and to quantify his or her behavior under hypothetical circumstances. Information on the survey was distributed at several computer security conferences, and links to the questionnaire were posted on the message boards of several known hacker sites. This research originally intended to poll a sample pool of hackers that was representative of the total population of national and international hackers. However, the author of this dissertation could find no verifiable data on hacker population from which to calculate an appropriate sample size (see Figure 3-3). This obstacle, combined with a low response rate, makes the external validity of this survey statistically suspect. Therefore, the data collected from the respondents of this survey was used purely as anecdotal evidence and not as objective statistical information.

Participants were asked 10 scaled and multiple choice questions

pertaining to the following aspects of their behavior, capabilities and perceptions:

1. Orientation (one questions)
2. Target selection/motivation (five questions)
3. Knowledge, experience and familiarity with the South Korean

cyber

environment and software (nine questions)

Table 3-2: Statistical Parameters of Hacker Survey

Population Size	Unknown
Sample Size	167
Confidence Level	Unknown
Confidence Interval	Approaching 100
Standard Error	Unknown

3.1.4.1 Question about Orientation

The sole question regarding orientation asked respondents to characterize themselves as either a ‘white hat hacker’, a ‘black hat’ hacker or a ‘grey hat’ hacker. As mentioned in chapter one, white hats attack a system solely to find its vulnerabilities, and help eliminate them. Black hats attempt to penetrate systems for either personal gain, criminal and/or political reasons, or as random acts of vandalism or mischief. Grey hats infiltrate systems for reasons that are not always altruistic, or participate in both black hat and white hat activities.

3.1.4.2 *Questions about Target Acquisition and Motives*

Participants were asked about their impressions and actions upon encountering various types of operating systems and browsers. These questions attempt to ascertain the respondent's perceptions as to the level of difficulty in penetrating these systems, given certain software conditions (*viz.*, *Windows 7 or lower* and *Internet Explorer*), and whether it has any bearing on the behavior of hackers. Respondents were also asked to choose which operating system and browser they found easiest to compromise, from among a list of most frequently used software.

3.2 *Qualitative Study*

In order to confirm the implications of the author's hypothesis on South Korean cybersecurity, it was necessary to find a consensus of experts in various disciplines outside of the available literature. To that end, this dissertation utilizes qualitative methods in the form of interviews of leading experts in the study of technology and national cybersecurity, the motives and culture of national and international hackers, and the legal and social aspects of South Korea's NPKI. Such interviews were conducted either in person, or through the telephone and focused on aspects related to the goals of this research. These interviews were used to help answer the main research questions of this paper, namely, whether or not software uniformity constitutes a threat to cyber security, and if uniformity

effects the range of capabilities necessary to compromise South Korean systems or not.

3.2.1 Dr. Kim Keechang

Dr. Kim is a professor of law at Korea University, as well as an expert in the legal and technical and social limitations of South Korea's NPKI. In addition, he is also the director and one of the founders of *Open Net* (오픈넷), a non-governmental organization which aims for freedom and openness of South Korea's internet.⁷⁸ Kim has researched extensively on the effects of South Korea's cybersecurity laws on national e-business. Dr. Kim's explanations of national cyber policies and law, as well as their evolution and effects on e-business and corporate security were invaluable in this dissertation's interpretation of data collected.

3.2.2 Jim Jackson

In addition to being a 23-year veteran of the military, Mr. Jackson is a team leader for U.S. Army Cyber Integrity. He is an expert on national cybersecurity, security software programing, de-bugging systems and hardware engineering. Jackson provided this research with much needed support in

⁷⁸ "Open Net: Mission Statement." Open Net. <http://opennetkorea.org/en/wp/about-opennet>. Accessed June 8, 2014

reference to the science of cyber attacks, attack attribution, attack prevention, programming and cyber agendas of state actors.

3.2.3 Bright Gameli

Mr. Gameli has worked as a corporate information security consultant and engineer in South Korea for the past five years, and is also the director of the annual *Africa Hackon* conference. Much of his formative years were spent with the online hacking community learning about coding malware, socially engineered cyber attacks, hacking and sharing his exploits and expertise with fellow hackers of all capabilities and orientations. His interview provided insight into the behavior and technical characteristics of South Korean end-users, cyber policy in South Korea, and the culture and motives of the hacking community.

CHAPTER FOUR:

A STATISTICAL ANALYSIS

Similar to the preceding chapter, this chapter is organized into two distinct parts. The first part contains a statistical analysis of the quantitative data collected from South Korean internet users and hackers, in the author's attempts to find evidence of statistical significance to either prove or refute the assumptions made in the hypothesis. In the latter half of this chapter, the author analyzes all relevant statistical inferences and the qualitative data from expert opinions, the body of literature, evidence from both the cyber environment and the cyber power dynamic, as well as the unique historical narrative of South Korean cybersecurity in the context of software uniformity and systems integrity

4.1. *Overview*

In this section the author reports on the statistical data gathered from both the South Korean end-user survey, and the hacker survey. However, since the statistical relevance of the sample pool used in the hacker survey could not be verified, it would be a misnomer to categorize the data collected therein as 'statistical'. Therefore, a strong argument can be made that the data obtained from the user survey was the only real statistical data gathered during the course of this dissertation. While statistically this may be true, the data itself still has value to this study. Used anecdotally, a preponderance of answers given by participating

hackers may highlight the vulnerability of software uniformity and the South Korean NPKI system. Also, it may provide a foundation for further, more comprehensive investigations into the relationship between these factors and hackers.

4.1.1 User Survey

4.1.1.1 The Security of Software:

The end-user survey and this section of questions, in particular, are of paramount importance to the validity of this research. All secondary and tertiary research goals are predicated on concept that the operating systems, browsers and anti-virus software in use in South Korea display an inordinate amount of uniformity. Before beginning this dissertation, the author had only seen anecdotal evidence of such uniformity, albeit in copious amounts. As the purpose of this study is to find any unexplained disproportionate groupings of any one particular software program, the multiple choice answers of the respondents were quantified, measured and compared with both U.S. and world averages.⁷⁹ Any significant statistical derivations between South Korea, the U.S. and the world, provided data for further analysis.

⁷⁹ Usage data for the U.S was provided by *Statista.com*, and global usage rates were retrieved from *Stack Overflow* and reflect the 2013-2014 time frame of this dissertation's survey.

4.1.1.1.1 Operating Systems

For operating systems, there was a statistically significant difference in the dispersal of software in regards to *Windows*. South Koreans use *Windows* at home over 8% more than the world average and over 18% more than their counterparts in the U.S. (Figure 4-1). It should be noted that a majority of users in the U.S. and internationally use windows, but not quite at the rate of South Koreans. For institutional use, South Korean *Windows* users lie outside the U.S. range with a 14.28% higher usage rate for *Windows*, and a rate 9.93% above the world average (Figure 4-2). Again, the world and U.S. averages also show a majority of *Windows* users, but but nowhere close to the usage rates of South Koreans. Also, usage rates for the remaining operating systems is much more evenly dispersed outside of Korea.

However this research's investigation into which version of *Windows* was being used at home, discovered that although South Koreans on average, use higher versions of *Windows* (*Windows* 7 and up) in their home at relatively the same rate as the rest of the world (Figure 4-3), their rate was 13% lower than American home users. This gap increases at the office, as South Korea lags over 10% behind the rest of the world and 23% behind American offices using versions of *Windows* 7 and higher (Figure 4-4). However, what is also quite noticeable is the percentage of Koreans still using *Windows XP*. Usage of *XP* was 7.4% higher than the rest of the world and 17% higher than the U.S. Again this

discrepancy increases at the workplace where almost of third of those surveyed in Korea are still using the decade old operating system as compared to 10.49% in America, and 19.22% everywhere else.

Table 4-1: Type of Operating Systems (Home)

Type of Operating System	% S.K. Usage	% U.S. Usage	%Global Usage
Apple/Mac	7.8%	12.85%	9.68%
OS/X	0%	14.84%	7.98%
Linux	0.79%	2.03%	1.43%
Windows	89.05%	70.28%	80.91%
Other/I don't know	2.36%	N/A	N/A
Total	100%	100%	100%

Table 4-2: Type of Operating System (Work)

Type of Operating System	% S.K. Usage	% U.S. Usage	%Global Usage
Apple/Mac	5.66%	9.03%	8.15%
OS/X	0%	14.84%	11.47%
Linux	0.79%	2.03%	1.93%
Windows	88.38%	74.1%	78.45%
I don't know	5.17%	N/A	N/A
Total	100%	100%	100%

Table 4-3: *Version of Windows (Home)*

Version of Windows	% S.K. Usage	% U.S. Usage	%Global Usage
XP	21.77%	10.49%	14.22%
Vista	5.74%	4.33%	13.61%
Windows 7	54.1%	52.29%	47.31%
Windows 8	14.29%	20.71%	16.38%
Windows 8.1 and up	4.1%	12.18%	8.48%
Total	100%	100%	100%

Table 4-4: *Version of Windows (Work)*

Version of Windows	% South Korea usage	% U.S. Usage	%Global Usage
XP	32.76%	10.49%	19.22%
Vista	4.31%	4.33%	8.47%
Windows 7	47.39%	42.29%	42.26%
Windows 8	14.43%	25.71%	20.7%
Windows 8.1 and up	1.11%	17.18%	9.35%
Total	100%	100%	100%

Based on the data, it is quite apparent that a much greater degree of software uniformity of operating systems exists in South Korea than internationally. Incidentally, *Windows XP* has been largely disregarded elsewhere due to the greater risk from cyber attacks on its relatively archaic architecture and outmoded security.

4.1.1.1.2 Browser Software:

In regard to browsers, the data shows that South Korean usage rates both at home and in the workplace for *Internet Explorer* far exceed those of the U.S. and the world. Despite the fact that almost a quarter (24.41%) of South Korean users browse with *Google Chrome* at home (Figure 4-5), they still have a higher percentage of people using *Internet Explorer* by more than 14% over the world, and more than three times the rate of users in the U.S. (Figure 4-6). Inversely, the total percentage of South Koreans using a browser at home other than *Internet Explorer* is only 5.49%, highlighting the uniform nature of browsers in the country. At the work place, the disparity is much worse as 78.33% of office workers in Korea are browsing with *Internet Explorer* (Figure 4-7). Uniformity in the types of browsers regularly used in South Korean offices follow along the same lines, as less than 6.7% of users in South Korea browse the internet on a consistent basis with a program other than *Internet Explorer* or *Chrome*.

Table 4-5: Type of Browser (Home)

Type of Browser	% S.K. Usage	% U.S. Usage	% Global Usage
Internet Explorer	69.29%	21.7%	55.83%
Google Chrome	24.41%	47.48%	25.68%
Safari	3.15%	14.8%	5.12%
Mozilla Firefox	2.25 %	13.6%	11.7%
Other	0.9%	2.42%	1.67%
Total	100%	100%	100%

Table 4-6: *Type of Browser (Work)*

Type of Browser	% S.K. Usage	% U.S. Usage	% Global Usage
Internet Explorer	78.33%	20.5%	57.66%
Google Chrome	14.96%	47.39%	27.24%
Safari	2.85%	15.64%	6.62%
Mozilla Firefox	2.36%	16.3.%	7.3%
Other	1.5%	.17%	1.18%
Total	100%	100%	100%

4.1.1.1.3 *Anti-virus Software*

In terms of Antivirus software, South Korea is somewhat of an enigma as less than on-tenth of one percent of both U.S. and international users run security software produced in Korea on their home computers (Figure 4-7). The two most popular security programs in Korea, *V3* and *Alyac* however, make up over 75% of the virus protection installed on South Korean home computers, and with the small exceptions of Microsoft (9.45%) and Avast (6.3%) only a small percentage use any type of international security software. Once again, South Koreans appear to be even less diverse in their choice of office security software than home users, as 79.85% of workers reported using one of the two South Korean security software giants (Figure 4-8).

Table 4-7: Antivirus Software (Home)

Type of Antivirus Software	% S.K. Usage	% U.S. Usage	%Global Usage
Microsoft	9.45%	25.8%	19.4%
Avast	6.30%	13.6%	21.4%
Ahnlab/V3	32.28%	>.01%	>.01%
Esoft/Alyac (알약)	43.31%	>.01%	>.01%
Kaspersky	0.79%	15.8%	7.5%
Nortons	1.1%	17.3%	9.1%
McAfee	2.36%	23.1%	26.2%
None	4.41%	N/A	N/A
Total	100%	100%	100%

Table 4-8: Antivirus Software (Work)

Type of Antivirus Software	% S.K. Usage	% U.S. Usage	%Global Usage
Microsoft	11.02%	30.2%	21.4%
Avast	3.45%	23.6%	18.07%
V3	34.65%	>.01%	>.01%
Alyac (알약)	45.2%	>.01%	>.01%
Kaspersky	0.47%	5.6%	3.5%
Nortons	2.10%	11.1%	6.3%
McAfee	3.11%	20.6%	23.8%
None	0%	N/A	N/A
Total	100%	100%	100%

The responses to these questions also showed a statistical significance in software uniformity, as distribution of the usage of these programs are grouped

around *Windows* (specifically *Windows 7* and *Vista*), *Internet Explorer* (and to far lesser extent *Chrome*), *V3* and *Alyac*. There are also several types of internationally produced security software that a majority of user in the U.S. and internationally enjoy. But the usage rates of any single ‘preferred’ programs is generally lower than was observed in South Koreans’ very limited preferences. Therefore, the diversity along different types of programs is smaller in our sample of South Korean users than it is in either the United States or the world.

4.1.1.2 *Online Behavior*

These questions were designed to ascertain where South Korean internet users access the internet, and measure the degree to which they engage in online behavior that can potentially infect the computers they use with malware, or compromise their e-mail and social networking accounts. In addition, due to the danger from hackers when connecting to public servers and wi-fi, the first question inquires as to the frequency and mobility of participants’ internet use. The last three questions pertain to certain techniques known for being conduits of cyber attacks, and participants’ responses should be a cause for concern to South Korean cyber defense strategists. Almost half (45.9%) of the subjects indicated that they access the internet at public places daily (Figure 4-9). For most, such access has become a common daily occurrence, and by itself would certainly not be cause for alarm. However in concert with questionable online behavior such

as downloading multiple unknown programs from unknown and untrusted sources, it could increase the likelihood of incursions. This concept will be illustrated statically later in this section. Half (54.33%) ‘always’ or ‘usually allow’ the down load of plug-ins, routinely exposing themselves to cyber threats (Figure 4-10). At the top of that group, 17.32% percent use little to no precaution or forethought when downloading such files as responded that they “always allow” files to be downloaded when prompted. The author of this dissertation does not believe that these end-users would willingly give up almost complete control over the security of their computer out of an intense desire to acquire the file or program, rather they view going through the motions of such protocols, as the price of using the internet in South Korea, much like those who click the “I accept” button automatically when forced to accept the “terms of use” information in order to establish an account.

Perhaps the most surprising statistic revealed by this group of questions, is the percentage of end-users who regularly click on links posted in social networking sites leading to third-party websites (48.81%), despite this being a preferred method of cyber criminals (Figure 4-11). However considering the prevalence of these links on such sites, it is easy to understand how being on a network with trusted friends and family members could mislead someone into thinking he or she will not be harmed by these actions. What did not pass scrutiny amongst the respondents of this survey, however, were the now-dated phishing

techniques using email links (Figure 4-12). Over 69% of subjects showed little interest in clicking links provided through e-mails. Although as indicated by the responses to these question, there are many factors in end-user behavior that could lead to a precarious cyber security environment.

Table 4-9: Frequency and Location of Internet Access

Location	Daily	Weekly	Monthly	Less than once/month	Never	Total
From home	81.89%	9.45%	4.72%	3.15%	.79%	100%
From work	58.33%	15.83%	2.5%	1.67%	21.67%	100%
From a school	49.12%	14.04%	6.14%	8.77%	21.93%	100%
From a public terminal (e.g. library, cafe, etc.)	45.9%	9.84%	9.84%	19.67%	14.75%	100%
From other places	52.89%	7.44%	7.44%	12.4%	19.83%	100%

Table 4-10: Reaction to Warning Prompt

Action	%
Always “allow” to view the website?	17.32%
Usually “allow” to view the website?	37.01%
Sometimes “allow” to view the website?	29.92%
Seldom “allow” to view the website?	12.6%
Never “allow” to view the website?	1.57%
Investigate further	1.57%
Total	100%

Table 4-11: Linking to Unknown or Untrusted Third-Party Websites

Action	%
If I know the person or company who posted the link, I click every time I want to see it.	22.83%
I usually click on the links, but I am occasionally skeptical.	25.98%
I rarely click on the links to a third - party website.	33.07%
I never click on the links to a third - party website.	18.11%
Total	100%

Table 4-12: Behavior towards Email Links

Action	%
I always click on links that I find interesting or important.	8.66%
I usually click on links that I find interesting or important.	9.45%
I often click on links that I find interesting or important.	11.81%
I seldom click on links that I find interesting or important.	32.28%
I never click on links that I find interesting or important.	27.8%
Total	100%

4.1.1.3 Occurrence, Location and Mode of Incursions

The last section of questions in this survey was designed to reveal if any of the respondents had actually been a victim of a cyber attack. If so, through what locus were they attacked? Unfortunately for the respondents, the rate of single and multiple incursions on their home and workplace computers was surprisingly high. Despite the respondents' trepidation to click on e-mail links, 34.7% have had their e-mail account hacked once and 53% experienced the same on multiple occasions (Figure 4-13). Generally speaking, penetrating SNS

accounts is more difficult than penetrating email accounts due to greater common understanding of how such sites operate and the vulnerabilities of member accounts. However, 92.9% of responding South Koreans had their SNS account hacked (Figure 4-14), and 89% had their email accounts hacked (Figure 4-15). CPU incursion rates were also high. For devices used outside of work, incursion rates were 15% higher for home devices than for those used for work purposes (Figure 4-16).

Table 4-13: *Compromised E-mail Accounts*

Has your email account been hacked before, and if so how many times?	%
Yes, only once.	34.7%
Yes, more than once.	54.3%
No, my email has never been hacked.	11.0%
Total	100%

Table 4-14: *People Who Have Been Hacked through SNS*

Has your SNS account been hacked before, and if so how many times?	%
Yes, only once.	24.4%
Yes, more than once.	68.5%
No, my SNS has never been hacked.	7.1%
Total	100%

Table 4-15: *Compromised CPU or Mobile Device (Home)*

Has your personal mobile device or PC been rendered inoperable by malware? If so, how many times?	%
Yes, only once.	32.2%
Yes, more than once.	63.5%
No, my home computing device has never stopped working due to malware	4.3%
Total	100%

Table 4-16: *Compromised CPU or Mobile Device (Work)*

Has your office mobile device or PC been rendered inoperable by malware? If so, how many times?	%
Yes, only once.	34.6%
Yes, more than once.	45.7%
No, my email has never been hacked.	19.7%
Total	100%

4.1.1.4 *Accessibility of Organizational Networks*

The purpose of this question was to gauge how connected the respondents are to their institutional (*e.g.*, school, work, etc.) network. The author was trying to establish a correlation between South Korean users' connectivity and cyber intrusions at the work place. It seems that over half (55.3%) of those polled had access to their professional network (Figure 4-17). Such connectivity could also be a contributing factor to institutional cyber security. However, further investigation needs to be conducted for such inferences to be made.

Table 4-17: Home Access to Work or School Network

Do you have access to your work/school network from home?	%
Yes.	55.3%
No.	44.7%
Total	100%

4.1.1.5 Most Vulnerable User Characteristics:

In order to more clearly define what characteristics, if any, put South Korean users at greater risk of incursion, this study cross-referenced certain responses with incursion rates to see which of the characteristics measured, in particular, displayed a correlation with incursion rates. The results were interesting.

In regard to user actions when using the internet, two types of behaviors showed strong correlation with incursion. 96.3% of respondents who answered that they “always accept” downloads when faced with notifications from *ActiveX* prompts had experience one or multiple incursions on their computer that left it inoperable, as opposed to only 6.8% of those who “seldom” or “never” such downloads. Perhaps not surprisingly, 81.4% of those who “always or “usually” clicked on links sent to them by email had experienced multiple e-mail account hacks with another 7.2% having only experienced one e-mail account hack.

When examining the types of software associated with incursions, the data showed that those using *Windows* were more than ten times more likely to

have experienced multiple crashes due to incursions (28.2%) than were Apple users (2.6%). Data collected on browsers used, indicated that 54% of *Internet explorer* users had at least one crash, and another 8.4% experienced multiple crashes, whereas only 28.1% of *Chrome* users experienced a such a crash once with another 3.5% having more than one such incident. The most visible difference of software's used in South Korea in terms incursion, was in the version of windows being used. 78.8% of *WindowsVista* users and 94.7% of *WindowsXP* users experienced one more debilitating incursion, as opposed to only 19.2% of those using *Windows7* of higher. Although incursion rates for those using Microsoft or Avast security software was much lower than those who relied on their Korean counterparts *V3* and *Alyac*, the disparity was discounted by the research due to their relatively low usage in South Korea. These statistical anomalies in and of themselves do not in any way prove causation.

4.1.2 Hacker Survey

As stated in the previous chapter, any evidence garnered from this particular survey's data is regarded as purely anecdotal, as the author failed to establish a representative sample of hackers. That being said, statistically strong responses could indicate the possibility of a relationship between the variables that is worthy of further, perhaps more appropriate investigation.

The author's intent in conducting this survey was to measure the

motivations and self-perceived capabilities of the respondents. Therefore, the questions were designed so that the participants' answers could be quantified and reflect the category and scope of their inducements. Reports claiming hackers enjoy the challenge of hacking into highly secure systems may be correct, as 42% indicated that they would continue to attempt to hack a system, despite the difficulties.⁸⁰ However, the inverse was not true. Respondents overwhelmingly (72%) indicated that the ease of a hack would not stop them. Of those polled, 71% saw *Internet Explorer* as the easiest type of browser to hack and 61% chose *Windows* as the easiest browser to penetrate. Therefore, since hackers prefer easier targets, and indicated that *Windows* and *Internet Explorer* platforms are easiest to hack, those using *Windows* and *IE* would present more attractive targets

4.1.2.1 Hacker Orientation

On the surface, this question was designed as a kind of interesting demographic of the participants. However, how a hacker behaves and perceives themselves is relevant not only to possibility that he or she may choose to surreptitiously access a network, but also what they will do with that access. According to the survey only 20.6% of respondents classified themselves as 'black hat' (Figure 4-18). Over one-third of those who answered described themselves as 'white hats', and a majority of respondents believed themselves to

⁸⁰ Thomas, Douglas. 2002. *Hacker Culture*. Minneapolis: University of Minnesota Press. p. 18

be ‘grey hats’. If a future study of hackers were to be statistically valid, and had these results, it would indicate that there is approximately a one in three chance that a network intruder would simply be exploring the network, with no nefarious intent. Perhaps they are accessing the network as a personal or public challenge, or even looking for security flaws with which to share with the administrator. There would also be a one in five chance that the hacker who has gained illegal access to the system would most certainly be there to do some kind of damage, and a 45% chance that such a hacker could not be able to say or certain that he or she is not there to cause harm.

Table 4-18: Hacker Orientation

Orientation	%
White Hat	34.2%
Black Hat	20.6%
Grey Hat	45.2%
Total	100%

4.1.2.2 Target Selection

Given all the bravado of the hacker community, it would stand to reason that more difficult targets would be more prized by the hacker themselves and in their community, and therefore would elicit more effort to penetrate. However, among those who responded to the survey the opposite appeared to be true, as 74.2% would more likely try to gain access a to a target, if its defenses were less

formidable (Figure 4-19). For our small pool of participants the inverse would seem to be slightly true, as 65.3% responded that they would be less likely to attempt accessing a network with better security (Figure 4-20).

Table 4-19: Hackers Response to Easy Targets

If an unknown system is easy for you to penetrate, will that make you:	%
More likely to try to access it?	74.2%
Less likely to try to access it?	17.6%
It has no bearing on whether you will try to access it.	8.2%
Total	100%

Figure 4-20: Hackers Response to Difficult Targets

If an unknown system is difficult for you to penetrate, will that make you:	%
More likely to try to access it?	25.7%
Less likely to try to access it?	65.3%
It has no bearing on whether you will try to access it.	9.0%
Total	100%

Had this sample been more representative, the author had hoped to correlate the monolithic software programs in South Korea with how secure hackers perceived these programs to be. The results were compelling anecdotal evidence that South Korea's dependence on these programs represents a vulnerability at all levels using these software. In total, 75.4% believed *Windows* to be the most easily compromised among the four programs listed (Figure 4-21).

Similarly, 72.9% thought *Internet Explorer* was the easiest browser to hack (Figure 4-22). This study declined to pose similar questions about *V3* and *Alyac*, as the author believed respondents to the English-language survey would mainly come from outside of Korea, and therefore be unfamiliar with those programs, invalidating the question internally.

Table 4-21: Operating System Viewed by Hackers as the Easiest to Compromise

Which of the following operating systems are easiest to compromise?	%
Apple/Mac	11.6%
OS/X	7.7%
Linux	4.3%
Windows	75.4%
Other	1%
Total	100%

Table 4-22: Browsers Viewed by Hackers as the Easiest to Compromise

Which of the following browsers are easiest to compromise?	%
Internet Explorer	72.9%
Google Chrome	11.6%
Safari	5.1%
Mozilla Firefox	10.4%
Other	0%
Total	100%

4.2 Qualitative Analysis

This study required qualitative methods in the form of expert interviews

in order to provide a better context for the defensive nature of the international cyber dynamic, technical details, and the culture of hackers. The author therefore took the opportunity to speak with three such experts: Dr. Kim Keechang (Korea University), Jim Jackson (U.S. military) and cyber security expert, Dr. Bright Gameli.

The author's choice of these three experts was very deliberate. In order to conduct an intersectional investigation into software uniformity, it is essential that each person contributing to it has a very unique skills set, background and approach to the problem than the others, in order to give specific insight into his or her field and be able to relate it to the insights of the others involved. Most importantly, every person contributing to the investigation must have an intimate knowledge of at least one aspect germane to subject being studied, so that he or she is able to trace it back to one or more of the intersections of other, perhaps seemingly unrelated, aspects within the problem more clearly understood by other members of the investigative team.

The contributions of these three researchers accomplishes the goals of intersectionality. Including the author, there are four individual cybersecurity researchers from different fields, with vastly differing academic, geographic, professional, cultural and perhaps even political backgrounds, contributing their expertise on different actors, behaviors and phenomena within a shared environment to achieve one goal; understanding if and how software uniformity

and other related concepts and phenomena affect the integrity of cybersecurity.

Dr. Kim is a Korean law professor with vast knowledge on the construction, legality and effect on individuals and e-commerce of South Korea's NPKI. He was perhaps the first, if not the most vocal, person to produce work detailing the pernicious effects of the social constructions of his fellow internet users. Although perhaps not a constructivist theoretically, Dr. Kim's knowledge of these constructs allowed the author to broaden his perspective to consider a constructivist approach as part of his methodology.

Mr. Jackson is a West Point graduate who has been in two wars, and risen through the ranks of military IT experts to his position as team leader. He knows intimately the constraints of the state when defending against a remote enemy, and the methods and motivations of state-sponsored attacks, as well as how to defend against them. His explanations of North Korea, their capabilities, and South Korea's past cyber vulnerabilities helped the author to understand the state's need to construct a national cybersecurity narrative around state-level enemies, specifically North Korea. It also allowed this research to reflect the importance of a strong national defense that is capable of defending itself against a state-level attack. Furthermore, due to Jackson's vast technical knowledge, he was able confirmed the infeasibility of a national public key system, especially when defending against state-level threats. His input greatly influenced the author to include aspects of neorealism in his approach to the problem.

Dr. Gamelli, by contrast, is an information security engineer, who in his youth, engaged with Africa's hacking community. He learned many tricks of the hacking trade, but perhaps more importantly to this research, his first-person perspective of hacking and hackers, and his time spent in South Korea, allow him the unique ability to delineate the motivations and capabilities of hackers as they relate to South Korea's cyber environment, and software uniformity in particular. As a former hacker and a security engineer, he knows the methods employed by hackers, and understands the potential danger that a seemingly innocuous threat, such as a disgruntled IT employee, can pose to public and private systems. However, his most surprising contribution to this research was his explanation of how important social engineering often is to hacking individuals, corporations and government systems. Most people think hackers rely solely on technology and computer codes to infiltrate systems. But in reality, most people with connections to the hacking community can receive or purchase the appropriate malware for a job, but introducing that malware to the intended target requires extensive knowledge of the psychology and behavior of the victims. Hackers spend a great deal of time studying the target both online and in person to determine the most effective way to introduce a virus, or get the victim to click on the desired link, or to present their security credentials unwittingly to the hacker. Dr. Gamelli's experience and knowledge in this area, helped the author to understand how user behavior is, partly a function of software uniformity, and the

NPKI.

4.2.1 Dr. Kim Keechang

Dr. Kim elucidated on the behavior of South Korean internet users and their reticence to execute downloads from untrusted websites:

“Here in Korea you have a situation where every online banking site, or internet shopping mall requires you to download additional software in order to use the site, not just once, but every time you visit a site. They [South Korean computer users] must download this type of software again and again. This leads to people [in South Korea] to be overly accepting of downloads. Most of these people have no idea what that software can do, or perhaps what it will do in the future [at the behest] of the programmer. It’s very dangerous. The number of crimes...crime, like cyber theft, that are committed in Korea alone is increasing.”

Dr. Kim also explained corporations’ lack of diligence in ensuring secure transaction via the internet.

“It is partially based on Korean commercial or banking laws.

When a company has fulfilled their obligation to the law... that is to say, met the minimum level of security requirement by the government, and a crime occurs, the business is not held responsible for that lapse in security. This is true even when the bank or business knows through experience that the customer is not secure. There are many criminals that will take advantage of this. What [the criminal] will do is call up a customer, pretending to be an employee at the bank, and will say...I don't know... that there is a problem with their account, or that they qualify for some kind of bonus program. Then they get simply the user's ID number and some [qualifying] information, and then that [customer's] money is all gone. And the bank, although technically complicit, has no responsibility to the client."

As to why corporations large and small would risk being victims to the kinds of major attacks that have taken place recently in Korea, Dr. Kim explained it thusly:

"They think that they have met the minimum requirement by law, why should I spend tens of thousands, hundreds of thousands, and in the case of large banks millions of dollars, because when something suspicious happens they are protected, or so they think. And then you

have a situation like Sony or the banking industry in 2013.”

Dr. Kim warns of the deleterious effects of these types of plugins (similar in nature to *ActiveX*) that are still being required by the government long after President Park mandated that 90% of e-commerce businesses, financial firms and educational institution rid themselves of the outdated technology.⁸¹

“I’m trying to point out that requiring the installation of additional software, that in itself is a very risky technology, a very risky business approach that is outdated now and should be replaced with the kind of technology that is used prevalently around the world. Make the transaction without downloading additional software. Use the web browser and nothing more. Unfortunately, the financial regulatory commission requires the installation of additional software.”

Although not familiar with how Esoft and Ahnlab came to dominate the market, Dr. Kim did speak to *V3*’s performance as an antivirus defense, and how they and corporations have propagated a revolving system of software requirements with the government’s complicity:

⁸¹ "South Korea to Remove 90 Percent of ActiveX by 2017 | ZDNet." ZDNet. Accessed July 1, 2013. <http://www.zdnet.com/article/south-korea-to-remove-90-percent-of-activex-by-2017/>.

“That is another very serious problem. The antivirus software industry in Korea used to be a very thriving business in Korea. There are many antivirus products in Korea, but no one really knows how effective they are. Ahnlab in particular has been repeatedly rated very poor. But they do a large percentage of the business based on this mandatory requirement, selling solutions to these banks and business. The business or banks, in turn, require the same software to be used by their customers. Everyone thinks that these antivirus softwares (sic) are doing their job, when in fact, they may not even be performing any type of anti-virus job.”

Dr. Kim confirmed the author’s suspicions that the South Korean government’s policy mandating special security plugins that require numerous downloads every time the user wants to make a simple transactions or perform a task online, has desensitized users in South Korea to the potential disasters that malware hidden in these downloads can cause. It seems that when it comes to cybersecurity and security plugins less is more. Mandating technology is a slippery slope that locks all users into a paradigm that is quickly outdated and completely unnecessary. For some unknown reason the government insists it is making cyberspace in Korea more secure, despite overwhelming evidence to the contrary.

4.2.2 Jim Jackson

Mr. Jackson contributed to this dissertation by bringing a detailed technical perspective on cyber security that was previously absent, and succinctly broke-down the difficulties of using exclusivity of coding or public keys as a cyber defense using the Chinese IP6 plans as an example. Also due to his military and international cybersecurity background, he was uniquely qualified to speak on international cyber security.

“There is no perfect security system, and even those organizations that take information security extremely seriously may find that attackers have been successful. And while the Target and JP Morgan breaches differed greatly, what they shared is that both their IT teams were well respected by the cybersecurity industry, and yet they still got hit. Companies should therefore expect that the bad guys will get in, and, indeed, should plan for it. Security isn't just about detecting malware -- it's about preventing it from succeeding in stealing data once it's on your system. Large organizations have to understand the new responsibilities that come with storing large amounts of sensitive information.”

When pressed about the role of non-state individuals in the international cyber security dynamic, Jackson replied thusly:

“Differentiating between these kinds of threats is critical, because different risks require different types of responses. The claims some have made that the Sony hack is an act of ‘cyberterrorism’ are a case in point. The FBI definition of cyberterrorism requires ‘an act that results in violence,’ which stealing scripts about James Bond carrying out acts of violence wouldn’t meet. This also applies to the recent threats by the hackers to create 9/11 style events at any movie theater that shows the film. Rapidly becoming an illustration on how not to handle online threats, virtually all the major U.S. theater companies have now said they won’t show the movie. Yet the ability to steal gossip celebrity emails is clearly not the same as having the capacity to undertake physical attacks at thousands of movie theaters across the country. So, at least based on their actions so far, the ‘bitter fate’ the hackers promised moviegoers is most likely to be the price they pay for popcorn.”

Different types of cyber crime, have different types of goals. The hack of Sony has often been lumped in with stories ranging from run of the mill online credit card theft, to the Target, Home Depot and JP Morgan breaches, to the time that Iranian-linked hackers allegedly "erased data on three-quarters of Aramco's corporate PCs." In fact, most of these crimes have little more in common than the

fact that they were committed using computers. It is similar to lumping together every incident in New York that involves a gun, be it a bank robbery, a murder, or a football player accidentally shooting himself.

4.2.3 Dr. Bright Gameli

Dr. Gameli's testimony gave insight on several major aspects of importance to this dissertation. His career and experiences brought him in close contact with both of the independent variables of this study. As a former hacker, he was able to provide a detailed context for the motives and capabilities of this mysterious and often elusive subculture. Furthermore, in his time on the Korean Peninsula, he has worked intimately with virtual every part of the cyber security dynamic. His personal narratives on corporations, South Korean end users, and both civilian and military government officials illuminate the interesting relationships they have with one another, particularly the relationship between governments and hackers:

"They (non-state hackers and South Korean government officials) certainly know of each other, but seem to know nothing about each other. And neither side respects the other...The corporate and government officials I've work with view hackers as an annoyance, like someone who wandered off the tour and went to some rooms they weren't

suppose go to. They certainly don't perceive them as a threat, at least not as the dangerous threat that they are, or can be. Even a hacker with the most modest of skill sets, with the right codes, can crash the systems of large institutions whose systems were believed to be secured. But hackers are equally blind to the intelligence of the other side. They perceive corporate and government security experts as bumbling fools. They have no idea how meticulous and well-informed many of these experts are...until it's too late. Who's dumber: the idiot, or the guy that got caught by the idiot?"

Gamelli addressed the concerns of this research on the risky online behavior of South Korean end-user by confirming that there is a rampant disregard by Koreans of their risky behavior online.

"To security consultants familiar with this country, Koreans are notorious for their unsafe practices. I can't tell you how many times I consulted with a company on a sometimes month-long investigations when they had been hit by an attack, and had to spend massive amounts on response and prevention, only to find out that it was caused by someone using 'password' as their password. When we find the bug it almost always came from an employee who, despite rules to the contrary,

clicked on a bad link while on Facebook, or through a phishing scam while accessing their work network from home. Your email privacy will not be respected, so act like it.”



CHAPTER FIVE

UNIFORMITY AND VULNERABILITY

In order to understand how uniformity affects cyber security, it is first important to understand the nature of malware. For each task that is to be carried out by any type of virus or malware, there must be a series of corresponding instruction codes encrypted in the program. Multiple algorithms dictate each step the virus takes, and often begins with recognizing the target platform and uploading itself.⁸² Therefore, malware designed to infect only one type of operating platform or browser requires fewer codes with less complex encoding than those designed to work across multiple platforms. The entire code required for one virus to infect systems using two completely different types of operating systems can often be geometrically denser than codes designed to infiltrate only one type of operating software. Also, the less complex or older a virus is, the easier it is to understand, alter, encode or obtain through the underground networks of hackers. It would stand to reason that if a majority of the computer users in a population uses only one type of software, a larger portion of the systems in that population would be vulnerable to attacks made by hackers using a simpler coded virus. Similarly, if a large portion of users in a population utilize older versions of operating systems and browsers, those networks would also be more vulnerable to attack. The availability of many

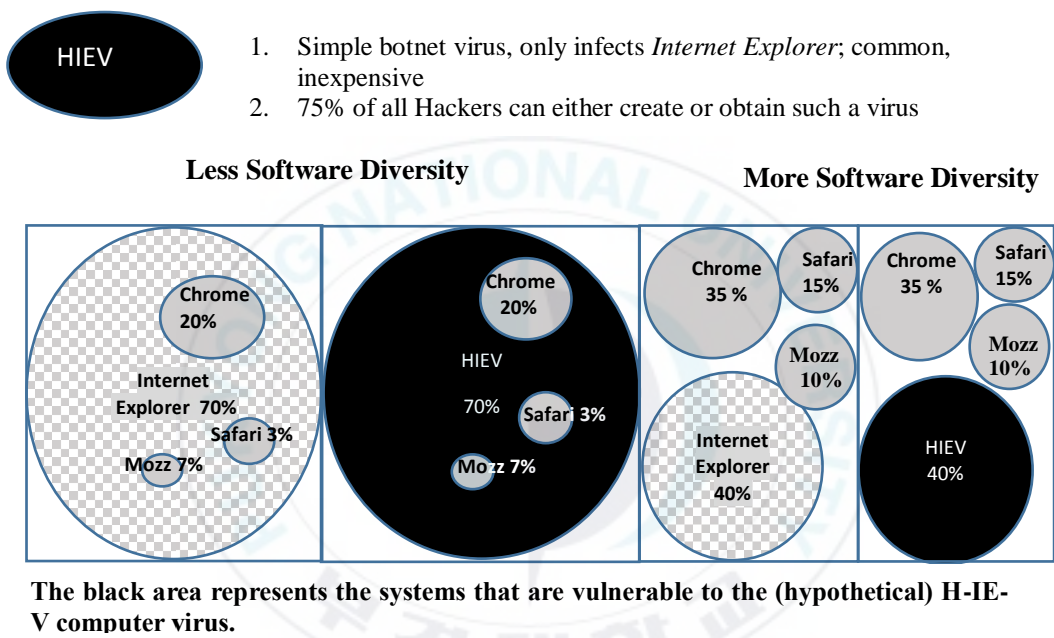
⁸² Skoudis, E./Zeltser, L.: *Malware: Fighting Malicious Code*; Prentice Hall, 2014 pp. 31-33

different types of viruses designed to infect these software is greater because they have been around longer, and their coding has been exposed to much more scrutiny and alterations from hackers than have newer versions of the same software. Eventually, the outdated programs become so vulnerable or obsolete, that the manufacturer stops supporting (creating security add-ons or plug-ins) the program altogether, which was the case with Microsoft and *ActiveX*. This means that a greater number of hackers with fewer capabilities and less resources to code or obtain malware can infiltrate large numbers of systems in such a population.

The diagram in Figure 5-1 represent two different hypothetical cyber environments. The environment on the left is less diverse in terms of the type of browsers its population uses. Seventy percent of computer users in that population use *Internet Explorer*, with the remaining 30% split between Google's *Chrome* (20%) Mozilla (Mozz 7%), and *Safari* (3%). In the more diverse environment on the right, *Internet Explorer* also has the most usage among the population. However, the proportions of each browser used are more balanced. A hypothetical virus (HIEV) containing relatively simple coding that can only be uploaded through *Internet Explorer* is represented in black. The simplicity of the code means that it can be reproduced, altered or obtained by 75% of hackers. When the HIEV virus is introduced to both systems, a larger portion of the less diverse environment is at risk. In the less diverse environment, 70% of all

systems are potential targets for 75% of all hackers. In the more diverse environment, however, only 40% of the systems can potentially be hacked. The security protocols of operating systems are similarly affected by variation.

Figure 5-1: Effect of Software Diversity on Browser Integrity



Like operating systems and browsers, lack of variation in the types of antiviral software and services used in a national environment can also create the potential for a greater number of successful cyber attacks. Unlike operating systems and browsers however, this potential vulnerability is not due to the degree of complexity in the malware necessarily, but the process by which these cyber security services discover and identify malware, devise solutions to defend against and eliminate these threats, and also to disseminate this information.

Some viruses are designed to infiltrate and spread to systems all over the world. For example, botnet attacks usually disseminate throughout cyberspace by surreptitious downloads hidden on links posted on trusted websites, or by phishing attacks with the intention of forcing the infected computers to execute preset or remote command without the user's knowledge. These infected systems are then orchestrated by the hacker for attacks that require a large number of computers, such as a distributed denial of service (DDoS) attack. There is no specific region, country or physical location targeted in this attack. The attacker simply needs to infect a certain number of computers, regardless of locale. Eventually, the malware in one or multiple locations is detected by anti-virus software (*e.g.* Norton's), reported back to its security service, and this information is disseminated to other security software firms via formal and informal channels. Since this kind of attack is done internationally, it is likely to be detected by one or more of the major international anti-virus companies, and information about it will likely be made available to many of its counterparts. In countries where there is very little variation in anti-virus software, the major security firm or firms in those countries can add the detection and solution protocols for this malware that it has possibly received from the foreign security firm that discovered it. However, if a such a virus were targeted only in that nation, and that country happens to have only one or two types of antivirus software in general use, it becomes the sole responsibility of those major antivirus

companies in that country to detect and eliminate the virus. Figure 5-2 further illustrates this point.

Figure 5-2: Effect of Software Diversity on Antivirus Software Integrity

X = Systems infected with virus *X*
O = Systems not infected with virus *O*

<i>Antivirus A</i> (55%)	<i>Antivirus B</i> (35%)	<i>Antivirus C</i> (3%)	<i>Antivirus D</i> (7%)
OOOXOOOOOOOO	OOXOOO	O	OO
OOOOOXOOXOOO	OXOOXO	O	OO
OOXOOOXOOOXO	OOOXOO	O	OX
OXOOOOOOOOOO	XOOOOO	O	
OOOOOOOOOXOOO	OOOOOX		

Assume that in a hypothetical country neither of the two major security protocols *Antivirus A* nor *Antivirus B* is able to detect virus *X*, which has been introduced to 5% of all the computers nation-wide. *Antivirus A* is used by 55% of all of the systems in that country and *Antivirus B* is used 35% of those systems, with the remaining 10% being shared by two smaller firms (*Antivirus C* and *D*). *Antivirus C*, however, can detect the virus and report the anomaly for further investigation, but it is only used in 3% of computers and therefore has a very small probability of gaining access to it. *Antivirus D* cannot detect the virus, and is used by the remaining 7%. The probability of virus *x*'s early detection are low, as there is only a 0.45% chance that virus *X* will end up infecting a computer that is equipped with antivirus *C* software. As antivirus software is distributed more

evenly across all systems, the probability that it will be detected and eliminated increases.

It should be noted that South Korea's variation problems in each of the three types of software examined in this dissertation, are only represented in pc-based systems accessing the internet. Smart phones, tablets and other non-pc devices constitute a significant portion of internet access, and may not be affected by a lack of variation. Furthermore, most if not all acts of cyber warfare and espionage conducted by state actors with access to vast resources, as well as advanced technology and capabilities may not be limited by the complexity of codes, and therefore fall outside the scope of this research. Such attacks may represent a greater threat to cyber security than a lack of variation in operating systems, browser and antivirus software. However, when the uniformity problems in these individual types of software are compounded, the potential for a successful large scale attack increases geometrically.

For every type of software measured in this study, South Korea's usage of software is less diverse than the United States and often the world, and is even denser than the world average for computer users at work. Although South Korea's technology usage rate dispersal is wider than the world averages for technology used at home, its anti-virus software usage for institutions is twice as dense as the world average. It is possible that the restrictive internet policies may have contributed to this dispersal. Many industrialized nations have comparably

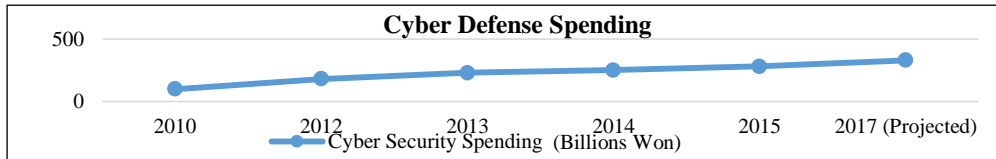
fewer restrictions on software compatibility and encryption technology, allowing inventors, entrepreneurs and corporations to innovate, develop and promote new technologies for financial gain, and vicariously creating a broader diversity of options in the market. This also has the added effect of requiring hackers who want to attack larger areas of the cyber environment to have a great number of techniques and more skill sets. This chapter has provided evidence that the types of software antivirus programs used in South Korea is much more uniform than elsewhere.

5.1 Major Cyber Attacks

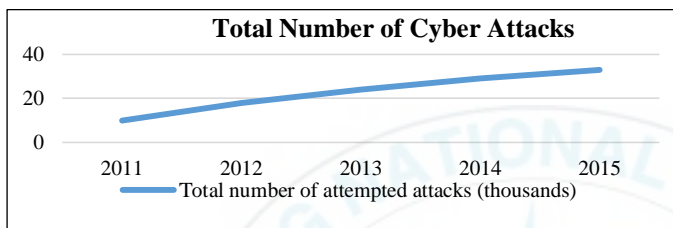
The upward trend of attempted and successful small scale cyber attacks in South Korea could reflect alternative factors influencing the cyber dynamic, such as an increase in total internet traffic in South Korea, greater exposure of South Korean corporations and entertainment in the international media (Figure 5-3). Therefore, to fully investigate failures in cyber security, this research examined all major cyber attacks from 2009 to 2014 and gives an analysis of the methods, motives and alleged identities of the perpetrators. Many of these attacks were designated as acts of cyber warfare by the state. For the purposes of this study, cyber warfare is defined as a large scale, state-sponsored, coordinated attack motivated by espionage or other political agendas. In order to properly analyze severe threats to the integrity of government and industrial system as they

relate to individual non-state actors. This paper examines six major cyber attacks in South Korea fitting such parameters. Namely, the attacks occurring in July 2009, June 2010, March 2011, July 2012, and on March 20th and June 25th of 2013 are all analyzed in terms of the methods, motives, government attribution for the attacks and the identity of the attacker. Although James A. Lewis argues that these attacks do not rise to the level of cyber warfare, as there was no violence or destruction. He instead characterizes them as annoyances and criminal acts. He suggests that true cyber warfare is only one part of a larger military campaign with the same goals as conventional warfare: destruction, loss of territory, human casualties, or serious disruption of critical services (Lewis 2009, p. 3). However, the goals of conventional warfare are not always among the aforementioned conditions. Cyber warfare should also not be confined to such a limited definition. Martin Libicki defines cyber warfare as “actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks” (Libicki, 2009 p. 23). Andy Manoske gives a similar definition of cyber warfare as “the use of hacking to conduct attacks on a target’s strategic or tactical resources for the purposes of espionage or sabotage” (Manoske 2013 p. 1). The attacks analyzed in this section fall under the two latter definitions and are therefore helpful in finding vulnerabilities in South Korea’s current cyber deterrence strategy.

Figure 5-3: Spending on Cyber Defense vs. Number and Frequency of Cyber Attacks



Source: Ministry of National Defense



Source: National Computing & Information Agency (NCIA), National Assembly's Report

Frequency of Major Cyber Attacks

Year	Number of Major attacks
2010	1
2011	1
2012	2
2013	2
2014	3

Source: Center for Strategic and International Studies

5.1.1 July 4-7, 2009

What is often referred to as the 'Independence Day' attack, the first successful major cyber attack on South Korean systems actually began as an attack on government websites in the United States (including the White House and the Pentagon) on American Independence Day, July 4th. The second wave of the three-wave attack targeted government sites in South Korea, namely the Blue house, the Ministry of Defense, the Ministry of Public Administration and Security, the National Intelligence Service and the National Assembly. Apart from being the first successful major cyber attack in South Korea, this attack was significant in that it shaped the formation of the state's perception of cyber threats

and set a precedent for the attribution of cyber attacks and the strategic decisions made in response to them. In the view of the Lee Myoung Park administration, this was cyber warfare perpetrated by the one actor that would stand to gain the most in terms of regional power: North Korea. The malicious codes, albeit rudimentary, were an extension of conventional warfare and politics that fit conveniently within the national security narrative. It also supported the strategy of ultimately putting virtually all cyber policy potentially under the umbrella of national defense. To the state, this was not a disgruntled employee seeking revenge, nor was it the work of bored vandals with an ax to grind against the government. Hundreds, even thousands of computers with IP addresses from China, South Korea and elsewhere were hi-jacked by what appeared to be multiple cyber agents acting in concert at the behest of Pyongyang. Thus began a predominance of the government to attribute cyber attacks to a state power and design the appropriate defense against it, often despite evidence to the contrary or the plausibility of alternative explanations.

Many were not convinced that these attacks were the actions of North Korea. The DDoS (Distributed Denial of Service) attack was executed by botnets infected through the "MyDoom" worm, a malicious code first discovered five years previously in 2004. It was originally designed to spread through the KAZAA peer-to-peer network, but had one interesting adaptation relevant to South Korean systems. Somewhere along the way, the worm's code was altered to affect the

win.exe files of older versions of *Windows*, released between the years 2002-2005.⁸³ Bound by the restrictions of SEED technology and *ActiveX* at the time of the attack in 2009, a majority (96%) of South Korean systems were in fact using these versions of *Windows*.⁸⁴

The lack of sophistication of the attack also led many experts to believe that the Independence Day attacks were not carried out by state actors, but by individual hackers with very limited skills, capabilities and destructive ambition. The attack took advantage of a port vulnerability on *Windows*. Director of malware research at SecureWorks, Joe Stewart noted:

*“Usually you see a DDoS attack against one or two sites and it will be for one of two reasons; either they have some beef with those sites or they are trying to extort money from those sites. To just attack a wide array of government sites like this, especially high-profile, just suggests that maybe the entire point is just to get attention to make some headlines rather than to actually do any kind of damage.”*⁸⁵

Denial-of-service attacks are one of the least sophisticated kinds of attacks a hacker can launch and have been around for nearly as long as e-commerce. However, their strength and reach has increased since the advent of

⁸³ Choe, Sang-hun, and John Markoff. "Cyber Attacks Jam Government and Commercial Websites." *The New York Times*, July 9, 2009. Accessed March 14, 2014.

⁸⁴ StatCounter. "Top 7 Desktop, Tablet & Console OS in South Korea from July to August 2009" - <http://gs.statcounter.com/#os-KR-monthly-200907-200908> Accessed January 29, 2016.

⁸⁵ Zetter, Kim. "Lazy Hacker and Little Worm Set-off Cyberwar Frenzy." *Wired*, July 8, 2009, 12-18: <http://www.wired.com/2009/07/mydoom/>

botnets, where hackers take control of thousands of machines by getting users to inadvertently click on files containing malware that allows them to remotely control the machines. The hackers then use the machines to launch attacks on websites. The only reason this one seems to have caught the public eye is because so many government sites were targeted at once. Although Stewart concedes that the breadth of targets was "unusual", the attacks caused no damage and would produce no comparative advantage for North Korea in the power dynamic. An argument could be made that the leaders of North Korea have often threatened and even attacked the South causing little or no damage as part of one of its many saber-rattling campaigns, or to better its position at the bargaining table. However, when Pyongyang acts provocatively, it usually is not shy about taking credit for it. In this case and in every similar case to come, North Korea has not accepted any responsibility for any cyber incursions.

The overt nature of the codes and the attack may also be evidence that the operation was not state-run. Cyber warfare is predicated upon stealth. Attacking your opponent successfully requires that the target not be made aware that you have accessed its systems. There are very good legal and political reasons for keeping such activity under wraps. Not the least of which being that a cyber-attack could lead to a counter-attack with conventional weapons. When a state has gained access to a pathway leading to an enemy's sensitive information, logically it would want to conceal that access for as long as possible. What

purpose would revealing the incursion serve? It is doubtful that North Korea would risk revealing its first (publicly known) access to South Korean and American government and military databases in such a fashion. The codes themselves were easily detected and systems resolved very quickly. According to Dean Turner, director of Symantec's Global Intelligence Network, "The fact that it's using older threats isn't a terribly stealthy attack...and the fact that it's re-using code could indicate that somebody put it together in a hurry or that, as with most DDoS attacks, their purpose is mostly to create a nuisance. It didn't require a degree in rocket science to pull that stuff together."⁸⁶

Stewart and Turner's remarks brings up another point arguing against this attack being the work of state actors. The dated, simplistic nature of the codes make them vulnerable to detection, eliminating this method for any attack in the future. If North Korea had only one chance to breach these systems and inflict as much damage as possible, why would they choose such a low-impact method of attack? A more reasonable explanation is that the attack was perpetrated by individual, non-state actors with limited capabilities, but exceptional knowledge of South Korean systems parameters.

After de-bugging and repairing the affected systems, the government's immediate response was to convert the Internet Crimes and Investigation Center to the Korea Cyber Emergency Response Team (KrCERT), and absorb it along with the National Internet Development Agency (KIDA), and the Korean IT

⁸⁶ Ibid 82 p. 6

International Cooperation Agency (KIICA) into the Korea Internet Security Agency (KISA). Despite evidence to the contrary, the NIS declared on October 30th of 2009 that the North Korean Ministry of Telecommunications was indeed behind the Independence Day attacks. The growing centralization of cyber security was just the beginning of a larger move to make cyber defense a sole function of national security and the military. At the beginning of the following year, cyberspace would become a domain of the military as published in the 2010 Defensive White Paper along with a greater emphasis on oversight of the public sphere by the military and related intelligence agencies.⁸⁷

5.1.2 June 10th, 2010

South Korea experienced its second major cyber attack less than a year later. Like the previous attack, this was a DDoS attack and once again targeted a government website. This also utilized malware designed specifically for *Windows*.⁸⁸ However the effects of this attack were even smaller than the Independence Day attack. The attack target only one website (www.korea.go.kr), and lasted only three and a half hours. During that time traffic was merely slowed down on the website meant to inform visitors on public policy.

This was a far cry from the three and a half week-long attack of the previous July, and would have probably not come to the public's attention had it

⁸⁷ 2010 *Defense White Paper*. Seoul: Ministry of National Defense, Republic of Korea, 2010.

⁸⁸ "South Korean Government Website Hit by Cyber Attacks." *Phys.org*, June 10, 2010. 2010-06-skorean-website-cyber.pdf.

not been curiously announced by the Ministry of Public Administration and Security. In a report released by the ministry, it was revealed that hackers had used about 120 China-based internet servers, and the government took immediate measures to thwart the "distributed denial of service" (DDoS) attacks.⁸⁹ Once again, blame for the attack fell swiftly and squarely on the shoulders of North Korea. What was even more curious was the series of announcements made by the military after the attacks were attributed to the North. Amidst fierce denial of any responsibility from Pyongyang, Major General Bae Deuk-Shik, chief of the Defense Security Command and the head of South Korea's military intelligence unit warned that the North may follow up its ship attack⁹⁰ with cyber attacks to disrupt the Group of 20 summit that took place in Seoul in November of that year, and added that the North had an army unit of elite hackers.⁹¹ It is not the contention of this dissertation that the attacks were misattributed to North Korea. It is possible that North Korea did indeed perpetrate this attack. However, South Korean intelligence definitely went out of its way to use these attacks as evidence to reinforce the national security narrative.

⁸⁹ "South Korean government website hit by Cyber Attacks," *Yonhap News*. June 10, 2010. Accessed March 12, 2014.

⁹⁰ Earlier that year, North Korea was blamed for the sinking of the "Cheonan", a navy corvette sunk near the North/South Korea boundary.

⁹¹ *Ibid* 82 p. 1

5.1.3 March 4th, 2011

If the follow up attack on South Korean systems in 2011 lacked the breadth and sophistication of a state actor like North Korea, the next attack only 18 months later would certainly provide that. Beginning on March 4th, 2011, operations of multiple commercial government and military websites, were halted due to another DDoS attack dubbed ‘the ten days of rain’. Although another DDoS attack, the length, scope and level of complexity of this operation were all increased. The 10 day-long attack targeted 40 websites, and among the 29 systems that were effected included government ministries, the National Assembly, the military headquarters, US Forces in Korea and major banks. This was also the first major attack involving commercial and government websites. The 11,000 personal computers that were hijacked through two corrupted peer-to-peer networks and used in the attack, far surpassed the number of any previous major attacks in South Korea (BBC, 2011). Major banking and financial trading institutions were hit, although some targets were hit worse than others. The complexity of the code was outlined in McAfee’s White Paper report on the incident to the South Korean government:

“While the attack itself seems fairly generic at first glance, there are several things that make this particular combination of targets, malware, and botnet activity different from many we’ve analyzed, warranting our investigation. The DDoS attacks had clearly defined

targets and a finite window of operation preconfigured as 10 days. Once that time expired, the bot on the compromised hosts would halt DDoS activity and render the host inoperable, thus requiring a full rebuild of operating systems, applications, and user data. While highly destructive code like this was common with early malware, it has long since given way to bots that allow for long-term command and control. Cybercriminals realized that compromised computers under their full control are much more valuable to them for sending spam, proliferating malware, and for harvesting valuable data from the compromised device. While there is some temporary satisfaction from an act of vandalism that renders the machine inoperable, this outcome has given way to financial motivations. The bots in these attacks, however, were configured to only perform DDoS attacks instead of having multiple capabilities and allowing for a wider range of nefarious uses. There was a high degree of cryptographic diversity: many disparate algorithms were utilized with the goal of slowing analysis and ultimately increasing time to mitigation. In addition to the bots themselves, a multitier botnet architecture, optimized to mitigate takedowns, was employed to ensure operational resiliency. In short, several steps were taken to ensure that the mission was executed without interruption, within the predefined attack window—and

*following, ensuring that all vehicles of attack would be destroyed, thus limiting forensic analysis.”*⁹²

After a week-long investigation, intelligence agencies reported to the media that once again the culprit was North Korea, and was not only a military attack, but was an attack against South Korean capitalist society. Along with Korean language-based prompts, the nature of the codes gave credence to their argument. Although not very stealthy, this attack did require a great deal of effort, and even perhaps manpower to accomplish. However, even though this attack inflicted a greater amount of damage than the two previous attacks, it was still easy to detect and repair. Why would North Korea go to these lengths for an attack that in the end did relatively little damage? A new explanation for this question would appear. North Korea was testing the South's response to cyber attacks and looking for vulnerabilities. The explanation was difficult to refute and gained traction amongst international media who cited 'expert sources' outside the South Korean government. Chief among these experts voicing their opinion was also McAfee, who had studied the virus extensively at the government's request:

⁹² "White Paper Report: Ten Days of Rain, Expert Analysis of Distributed Denial-of-service Attacks Targeting South Korea." McAfee. March 15, 2011. <http://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf>. P. 4. Accessed September 1, 2013

“This wasn’t a surgical strike; it was more like a sledgehammer, as most DDoS attacks are. As such, it was noisy, making it easier to detect than a stealthy attack that might be used to steal sensitive data. Knowing this, the attackers relied on the encryption to buy them more time against reverse engineering until the DDoS attack window expired. But what was their motivation? A number of theories can be entertained to address this question, and while a definitive answer isn’t always available, based on our technical analysis and investigation, we feel that the following scenario captures the likely actors and motives behind these attacks. This attack was engineered by multiple individuals with varying insight into the overall architecture of the code. This may have been a test of South Korea’s preparedness to mitigate cyberattacks, possibly by North Korea or their sympathizers. While the code and botnet architecture were advanced, the attack itself was very limited and may have been utilized to test and observe how quickly the attack would be discovered, reverse engineered, and mitigated. Armed with this knowledge, the aggressor could launch cyberattacks, possibly in conjunction with kinetic attacks, with a greater understanding of South Korea’s incident response capabilities. As such, the attackers could better understand their own requirements for a successful campaign...DDoS, malware-leveraging encryption, and multitier botnet

architectures are not new. Nor are attacks against South Korea that suspiciously align with North Korea's agenda. However, the combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome is analogous to bringing a Lamborghini to a go-cart race. As such, the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe response capabilities.”⁹³

It is worthy to note that McAfee's well-publicized findings contain a great deal of political speculation for which the cyber security firm may not be qualified to make, and no other outside firms were given such access. An argument could be made that McAfee was finding what the South Korean government wanted them to find. In any case, the media blitz worked, and now it is generally accepted among those in the cyber security field that North Korea was responsible for the 10-days of rain. Attention for any and all major cyber attacks was put on North Korea, and any previous focus on strategies involving non-state individual actors was fading. A subsequent attack a month later at the farm cooperative Nonghyup Bank crippled the institution for three days and credit card account information was lost as the malicious code was instructed to delete data, or 'wipe' the system. For this reason, they are called 'wiper codes'. This attack and two other smaller DDoS attacks in 2011 were again attributed to North Korea probing its enemy's response for weaknesses.

⁹³ Ibid 89. p. 3

5.1.4 June 11th, 2012

The June 11th attack on conservative newspaper Jung-Ang Ilbo's Korean and English websites that was again attributed to North Korea was unique for two reasons. First, it was the first major attack attributed to North Korea that was not a DDoS attack. The attack accessed the employee login site to shut down the servers and replaced them with a message reading, "Hacked by IsOne."⁹⁴ Secondly, this was the first time that the motives for a cyber hack were presented as retaliation by the North. A week prior to the attack, statements released by the North Korean government warned of retaliation against Jung-Ang and all the major daily newspapers in South Korea for their negative coverage of a mass-children's event. The argument for North Korea as the perpetrator was compelling, and the mass media reports on the incident in South Korea certainly reinforced the point. Major print media reported that North Korea was behind the attack. An IP address of one of the computers used in the attack was found to be identical to a computer involved in the 2009 attack. This was given as forensic evidence linking this new attack to the earlier attack and to North Korea. However, nothing was mentioned about the differences in the two attacks or the

⁹⁴ Sydney Morning Herald. "Hacked by IsOne'...Or by Kim? Newspaper Hit by Cyber Attack." *Sydney Morning Herald*. June 11, 2012. <http://www.smh.com.au/technology/technology-news/hacked-by-isone--or-by-kim-newspaper-hit-by-cyber-attack-20120611-205cn.html>. Accessed June 2, 2014.

fact that only one newspaper was targeted out of the many mentioned in Pyongyang's threat.

Several months later, KISA released definitive evidence of North Korean involvement. According to police, North Korean hackers infiltrated the Joongang Ilbo's administrator computer on June 7, and used malicious codes to access the daily's production system two days later. Investigators traced "IsOne" to an IP address at North Korea's Ministry of Posts and Telecommunications, from where hackers had repeatedly accessed the daily's main server since April 21 of that year. The North evidently collected information about the newspaper for more than a month and planted malicious codes. A statement by KISA read:

*"The first hacking attack on the server was nearly timed with the North Korean Army's warning on April 23 last year of provocation that a 'revolutionary force will take action soon.' It seems that the North made meticulous preparations once it singled out a particular media outlet for the cyber attack."*⁹⁵

If true, it would seem that in this case the national security narrative was the correct one.

⁹⁵ "North Korea Fingered in Cyber Attack on South Korean Daily." *Chosun Ilbo*, January 13, 2013. Accessed February 18, 2014.

5.1.5 March 20th, 2013

At approximately 2:20pm on March 20th, 2013 computer systems at television broadcasting networks MBC, KBS and YTN as well as Shinhan, Jeju and Nonghyup banks simultaneous shut down. System administrators attempted to reboot the systems' servers to no avail. These large institutions had all been hit by the same malware attack. Cyber response teams began investigations as the individual corporations tried feverishly to get their systems back on line. Although the details of the attack would not be uncovered for several days, all seven institutions were hit in a coordinated attack employing what is known as a 'dropper' malware, or code.

Dropper codes are called such because they 'drop' malicious code on the back of a downloaded application on servers within the system. Once the application is downloaded, the dropper code infects the computer, and later the servers, with remotely controlled or timed commands that spread the code throughout the entire system. The code can force the system to do anything the hacker wants. The dropper codes in the March 20th attacks specifically targeted the systems at these companies. However the codes dropped at the different corporations were all designed around the same parameter: *Windows* platform (replete with *ActiveX* controls) (NSHC, March 2013 p. 2). This code could have very easily been planted in over 90% of all the computers in South Korea.⁹⁶ Once dropped, this particular malware was not recognized by the *ActiveX* controls.

⁹⁶ Over 90% of Computers in South Korea run on a *Windows* platform.

After it was activated, it immediately executed its remotely controlled command to erase all data on every hard drive and then delete the *Windows* operating system making any reboot of the system impossible (NSHC, March 2013 p. 3). In other words, all the data and operating systems for a third of the banking systems in South Korea and two-thirds of its major broadcasting networks had been completely wiped clean in a matter of moments. This particular dropper code embedded itself within the *Internet Explorer* exe. file, and it was suspected that it was planted by an insider.⁹⁷

It would seem that an event like this could cripple a company, or at the least put it out of working order for some time. However in South Korea, corporations and government institutions have been fighting smaller yet similar attacks for several years, so the response efforts were swift and encompassing. Also, the nature of the code itself helped repair efforts in the aftermath. The malware only infected systems in the headquarters of these institutions. Local stations, branches and office operating systems were not affected. The data bank that was lost was pieced together with data from remote locations and backups at their headquarters. Systems at the banks and broadcasters were back online within days (Martin, 2015 p. 13). This time it seems that the damage could have been much worse.

⁹⁷ Kwaak, Jesup S. 2013. "Seoul Suspects South Korean Tech Executive of Helping North in Cyberattacks." *The Wall Street Journal*.
<http://www.wsj.com/articles/sb10001424127887324136204578639540757695644> (February 18, 2014).

The South Korean government's suspicion for the attack began to fall on North Korea.⁹⁸ If true, this would be the biggest hacking effort attributed to Pyongyang since a 10-day denial of service attack in 2011, dubbed the "Ten Days of Rain". South Korean officials stated that the attack was a bid to test the South's computer defenses in the event of a real conflict.⁹⁹ The Associated Press quoted an official close to the investigation as saying that these attacks were retaliation from the North for what it believes was a joint U.S.-South Korean cyber attack on its websites for two days of the previous week.¹⁰⁰ The level of sophistication of this attack was quite low, so it is possible that North Korea, which has merely the skeleton of a national network infrastructure, could have had the resources and know-how to pull it off. Both the U.S. and South Korea have made mention of a North Korean "cyber unit" staffed by "around 3,000 people handpicked for their computer literacy" (Carr, 2013, p.1). Regardless of who actually committed this attack, it shows that hackers from anywhere with little resources can exploit the cyber vulnerabilities of Windows and its *ActiveX* plug-in.

5.1.6 June 25th, 2013

Three months after the attack on South Korean banking and broadcast industries, South Korea was besieged once again by hackers. But this time the

⁹⁸ "Government Confirms Pyongyang Link in March Cyber Attack." Yonhap News Agency. April, 10, 2013. Accessed February 2, 2016.

⁹⁹ "South Korea Says Chinese IP Behind Cyber Attack." Al-Jazeera. March 21, 2013. Accessed September 11, 2014.

¹⁰⁰ "South Koreans Blame North Korea for Recent Cyber Attack." March 21, 2013. Associated Press. Accessed September 12, 2014.

target of the cyber attacks was the South Korean government. At around 9am on June 25th (which was the 63rd anniversary of the Korean War), the websites of 18 government-linked agencies, departments and political parties were simultaneously compromised by a mix of malware codes. The attack codes varied based on their effect. Some attacks altered websites, while others revealed personal information about government officials and soldiers on websites. The last group froze the websites all together.

The website of South Korea's Presidential Palace, or *Chong Hwa Dae*, was hacked into, and aspects of the site were altered in an attempt to embarrass the Park Geun Hae administration. A video was also posted alleging wrongdoing by Park and her cabinet members. The attackers used a mix of Trojan horse malware on the presidential website's servers, in concert with a timed DDoS attack, and were able to escape initial identification through a TOR network.¹⁰¹ The virus was encoded to hijack an auto update function on window-based servers, such as those dedicated to Chong Hwa Dae's site.¹⁰²

In addition to these alterations, personal information about 200,000 federal government workers were posted on the Chong Hwa Dae site. In a similar fashion, the personal information of 10,000 U.S. 3rd Division marines, 15,000

¹⁰¹ Celestino, Oscar, and Abendan, Angelo. "Trend Micro Investigates June 25 Cyber Attack in South Korea." *Trend Micro*. July 01, 2013. <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/124/trend-micro-investigates-june-25-cyber-attacks-in-south-korea>. Accessed September 15, 2014.

¹⁰² Delete-removevirus.com. "How to Remove TROJ_DIDKR.A Completely From Windows, Information about TROJ_DIDKR.A." http://www.delete-removevirus.com/post/How-to-Remove-TROJ_DIDKR.A-Completely-From-Windows_14_258622.html. Accessed June, 3 2016.

Army 1st Division soldiers, 15,000 U.S. Army 25th Division infantry men, 300,000 South Korean military personnel and 2.5 million New Frontier Party (Park Geun Hae's party) members were all posted on their respective websites (NSHC, June 2013 p.3). Scrawled across every page of every altered website were supposed notices by the hacktivist group "Anonymous" claiming responsibility.

Investigators found similar coding in this new attack to those of the March 20th attack. Like the first attack, the malicious code was meant to circumvent *ActiveX* security protocols. This "dropper" containing one of several similar, malicious payloads that were extracted from the PE Resource section of the dropper into the Windows %Temp% directory, and again required the unsuspecting user to accept the often legitimate plug-in, piggy backed with the surreptitious malware.¹⁰³ This meant that users across all of these government-affiliated institutions at least once, maybe multiple times had to download the virus via *ActiveX* controls. The websites of Chong-Hwa Dae, the Office for Government Policy Coordination, The Ministry of National Defense, The NIS (formerly the Korean Central Intelligence Agency), The Chosun Daily, Tae-gu Daily, and Maeil Shinmun newspapers, The Korean Press Foundation, eToday online journal and The New Frontier Party's Seoul, Busan, Ulsan, Gyung-gi Do, Jeju, Incheon, Kyung Sang Buk Do and were all frozen by 5:00pm. They had all

¹⁰³ Martin, David M. *Tracing The Lineage of DarkSeoul*. Technical paper. November 20, 2015. <https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787.p.15>.

been hit by a denial of service (DDOS) attack from IP addresses located in South Korea (NSHC, June 2013 p.1).

Although the computers that attacked South Korean systems on June 25th were located in South Korea, it does not mean that perpetrators were necessarily all South Korean. The computers were infected with a botnet virus that commanded these zombie computers located in South Korean to overwhelm the servers at these websites, and then began to alter them through a timed command. At first glance it would appear that the culprit was the hacktivist group Anonymous due the anti-government rhetoric, videos and copy plastered on the sites claiming responsibility by Anonymous. This was determined not to be the case as the low level of sophistication of the hack as well as the coding was not congruent with the group's typical methods (NSHC, June 2013, p.4). Furthermore, similarities between this newest malware and that of the March 20th and previous attacks attributed to North Korea, led South Korean investigators to conclude that this was once again the work of Kim Jung Eun's cyber unit.¹⁰⁴

The two major incursions that took place in 2013 were not of the caliber of the 'electronic Pearl Harbor' that pundits warned of in the late 1990's, however they did show that South Korea's *ActiveX*, *Windows* and *Internet Explorer* policy has left them extremely exposed to malicious attacks against their systems. Had response teams not acted quickly and thoroughly to contain the damage the

¹⁰⁴ Choe, Sang-hun. "South Korea Blames North For June Cyber Attacks." *The New York Times*. http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0. Accessed March 14, 2014.

effects could have been much worse. If either attack had been of the caliber of the Iranian stuxnet attack, it is possible that the financial sector and vicariously the South Korean economy could have been permanently damaged. Such an attack would have also wreaked havoc on many of the country's communication and broadcasting infrastructure.

Regardless of who was actually behind these attacks, strategy should be more focused on the methods of the attacks, but more importantly, what technical and behavioral vulnerabilities were exploited by these methods. It is the contention of this dissertation that the outdated platforms, security programs and social conditioning of end-users contributed to the execution of this and other hacks, and that these conditions still exist and still potentially leave South Korean systems vulnerable.

5.2 *Cyber Dynamic*

South Korean cyber security does not operate within a national vacuum. Cyber policy decisions are influenced by a broad dynamic of regional and international forces in addition to domestic ones. This 'cyber dynamic' is effected not only by threats from North Korea, but by traditional security alliances, individual and collective groups of hackers attacking for an array of political and non-political reasons, as well as other state and non-state actors. Although all of these forces deserve the attention and resources to combat threats, and to take

advantage of security opportunities, cyber policy reflects very little, if at all on the potential problems associated with software uniformity in South Korea. It is also the contention of the this dissertation that depth of the crisis of the recent cyber attacks and South Korea's national security position have obfuscated opportunities to protect against the vulnerabilities to which software uniformity contributes.

There are many state actors to consider in the South Korean cyber security dynamic, chief among them being North Korea. The antagonizing actions, threats and decisions Pyongyang has made in the past decade, coupled with their determination to wage cyber war with the South, has made the rogue nation the preeminent threat to South Korean cyber security. Several major cyber attacks were confirmed to have been the work of North Korea's growing cyber division, and therefore do deserve a great deal of consideration when making strategical cyber security decisions. In response, Seoul has created its own cyber command, and has taken a more aggressive posture towards cyberwar. It has actively sought out a cyber alliance with Washington, and is in the planning stages of joint cyber exercises with the U.S.¹⁰⁵ In addition, South Korea has also asked its American ally for help in developing a zero-day cyber weapon similar to the stuxnet virus.¹⁰⁶ Although antagonistic, this aggression seems reasonable and necessary

¹⁰⁵ Ibid 91

¹⁰⁶ Wood, Anthony. "South Korea Pushes for Cyber Weapon to Undermine North Korean Nuclear Facilities." *Gizmag.com*, February 24, 2014. <http://www.gizmag.com/south-korea-stuxnet-cyber-weapon/30977/>.. Accessed March 12, 2015

given the recent string of major attacks against its public and private cyber infrastructure. However, what may need further consideration is the means by which North Korea carried out the attacks. Most were botnet, DDoS or other unsophisticated attacks requiring simple algorithmic encryption. They were designed to penetrate a limited amount of operating platforms and software, such as those used in South Korea, and ultimately uploaded by end-users. This implies that cyber security, even as it pertains to North Korea, is related to the diversity of the technical characteristics of systems and the behavior of end-users in South Korea.

Regional powers also constitute a large portion of South Korea's cyber security dynamic. From a neorealist perspective, an alliance with the U.S. represents a bedrock strength, and presents opportunities for South Korea to preserve or increase its regional power. Cyber defense in South Korea has the resources, technology and intelligence of the United States at its disposal, for a relatively minuscule loss of operational control and military sovereignty. However, for the added cyber defense options that an alliance with the U.S. provides come with it limited strategies for cyber defense outside of the alliance. In America, the White House participates in a shared power structure for civilian cyber defense with corporations and non-governmental organizations, sanctioned by congress under roles defined by the federal body of laws, much of which falls under some form of bureaucratic oversight. However, even in the

United States where privacy, due process, and search and seizure laws are clearly defined, successive administrations have pushed the constitutional boundaries of surveillance in the name of national security. After the wars in Iraq and Afghanistan, and the passing of the Patriot Act, this line continued to blur culminating in embarrassing Snowden scandals involving surveillance of American allies and American citizens en-masse.¹⁰⁷ However, any power-sharing the U.S. does within its borders, certainly does not pertain to its operations overseas. Outside of the U.S., Washington holds a very neorealist perspective on cyber strategy. As was evident by the disregard for agreements with its allies and even its own laws when caught spying on German officials, the United States views the international cyber security structure as anarchic, and therefore it is not beholden to agreements therein when national security is at stake.¹⁰⁸ Furthermore, the U.S. has employed a very aggressive offensive realist strategy to protect and increase its cyber power in relation to China.

The covert cyberwar raging between the two superpowers has put South Korea in between its most powerful military ally and its largest trading partner. Yet despite the economic influence China wields in the region, and despite the overt diplomatic agreements and greater understanding on North Korea, Seoul has chosen to rely on its neorealist-based, traditional security strategies in regards

¹⁰⁷ Andrews, Suzanna, Bryan Burroughs, and Sarah Burroughs. 2014. "The Snowden Saga: A Shadowland Of Secrets and Light." *Vanity Fair*.

¹⁰⁸"White House on the Back Foot over CIA Role in German Spying Scandal." *The Guardian*, July 7, 2014. Accessed January 12, 2015.

to cyber security. Any active US-ROK alliance of cyber commands precludes cooperative cyber security efforts with China. This does affect cyber integrity as 44% of all international cyber attacks on South Korean systems have IP addresses originating in China.¹⁰⁹ Many of those attacks may be at the behest of North Korea. However with South Korea firmly allied with the Beijing's regional cyber rival, China has little motivation to cooperate in any investigative efforts.

South Korea's current strategy for cyber security within the international security paradigm and cooperation with international institutions and other states should not be considered mutually exclusive. South Korea has participated with many international cyber security groups and agencies, as well as the UN's International Telecommunications Union (ITU) which held their 2014 congress in Busan, South Korea. The government has also pursued relationships in the field of cyber security with individual states. However well-intentioned, most international agreements have only committed Seoul to the general pursuit of shared goals and norms, and memos of understanding on the need for cooperative cyber efforts. At the time of this research, a cyber crime policing agreement with the U.K. and the cyber defense pact the U.S. were the only international cyber agreements binding South Korea to certain protocols in cyber space.¹¹⁰

¹⁰⁹ Im, Su-Kyung; Report to the National Assembly on: The South Korean National Computing & Information Agency (NCIA) collected data on hacking attempts over the period of June 2011 to June 2015. Accessed September 18, 2015

¹¹⁰ Trimm, Peter. *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership*. Edited by Heung Youl Youm. Report Submitted to the Korean Government and the UK Government. 2013. Accessed January 15, 2015

Corporations play a role in the South Korean cyber dynamic also. The government and corporations have a particularly close relationship. The government set up and paid for the infrastructure that powers the South Korean information super highway, and has supported private internet providers, telecommunications, software and security companies in its promulgation (Oh and Larson, 2011, p. 39). It also works directly with large conglomerates within the banking, manufacturing and media industries. But to say these are all equal partnerships for policing and defending against cyber attacks would be a misnomer. Although corporations do hold sway with the government when greater economic good is at stake, national security more often than not takes precedence over corporate rights of privacy and intellectual property (Boo and Lee, 2012 p. 90).

One element of the South Korean cyber dynamic that is underrepresented in government security strategy consists of individual actors. There have been many major cyber attacks that have been committed by errant unaffiliated individuals, many with connections to targeted systems. Preventing these 'inside attacks' is often difficult due to the level of access of the attacker, and does require a concerted effort by corporations, public and private entities, and government agencies. There has been progress in regards to delegating responsibility for monitoring cyber space to government agencies. Both the Lee Myoung Bak and Park Geun Hye administrations have created new government

ministries and bureaucratic agencies responsible for cyber oversight.¹¹¹ Despite these new mechanisms for sharing power over securing the internet, the National Intelligence Service (NIS), formerly the Korea Central Intelligence Agency (KCIA), has supreme jurisdiction in all public and private matters concerning cyber security. However effective at combating these inside attacks the government may be, they fall short when combating individual hackers with no connection or prior access, due to the technical constraints of the software of systems in use in South Korea. Given enough time and information, the best coders nationally and internationally have the expertise and ingenuity to hack most if not all systems connected to the internet in South Korea. International and South Korean hackers will compromise systems. The lack of diversity of operating platforms, browsers and security software only increases the range and likelihood of potential attacks.

The strategical focus on outside state actors and national, mainly civilian individuals with insider access, intending to secure the overall cyber infrastructure, has drawn attention away from the threats and opportunities presented by other individual, non-state actors, and the problem of software uniformity. Therefore, the dependent variables in this study lie within two types

¹¹¹ Over the past two administrations, as cabinet ministries have been renamed and reorganized, responsibility for cyber security has gradually been coalesced through a series of administrative mergers. In 1999, The Korean Internet Security Agency (KISA) subsumed the not for profit Korean Network information center, and later merged with National Internet Development Agency of Korea (NIDA) and the Korean IT International Cooperation Agency (KIICA) in 2009. KISA now work in conjunction with the NIS and cyber military command in the event of an attack. On March 31st, 2015, the Blue House announced a new Ministerial Post directly in charge of cyber security.

of individual non-state actors: international hackers and South Korean end-users. It is within these two demographics that we can measure, to a certain degree, the effects on both the motives and capabilities of international hackers, as well as the technical characteristics and online behavior of South Korean end-users. The results of these measurements support the author's contention that strategical decisions limiting the technical characteristics of end-users (operating systems, browsers, anti-virus software), and a lack of user-based, identity-focused and ground-up policies have the potential to both attract international hackers, and lower the level of expertise needed to penetrate South Korean systems. Furthermore, these conditions have the unintended consequence of altering national end-user behavior deleteriously. The author also notes that individual Korean hackers are also most likely affected by such strategical decisions, and do play a large role in the South Korean cyber security dynamic. Further research on individual non-state actors should also include South Korean hackers, the outline of which is presented in the discussion section of this dissertation.

The skill sets and capabilities of attackers being equal, the range of potentially vulnerable computers is larger relative to the number of systems that could be compromised in the U.S. or internationally. For example, if a hacker attacked systems in South Korea using malware design to penetrate the software in the afore mentioned groupings, the number of possible victims would be significantly higher than if the same attack were used in the U.S. or against the

world on average. Therefore, hackers would need to know how to attack many fewer types of software, using less complex methods, while still targeting a significant number of systems in South Korea.



CHAPTER SIX: CONCLUSIONS

6.1 *Empirical Findings*

The goal of this research was to test certain assumptions made about the nature of operating systems, browsers, and security software in South Korea, the behavior of South Korean internet users in cyberspace, and the capability and motivation of hackers. More specifically, the author's hypothesis contends that a select few browsers, operating systems and anti-virus software enjoy abnormally high usage rates among South Koreans, to the mutual exclusion of similar competing software. The author's specific contention is that internet users in Korea, disproportionately support the use of *Windows*, *Internet Explorer*, and either Ahnlab's *V3* or E-soft's *Alyac* security program, and that this disproportionality affects national cybersecurity in a negative manner. Also, it was suspected that Korean internet users were engaging in dangerous behavior online, namely accepting unknown downloads and opening links from unknown or untrusted third parties. The results gathered from the survey confirmed these assumptions.

The novel insight gained from examining the intersection of the Korean state, its NPKE, South Korean internet users' perceptions and learned behavior, the regional security dynamic and technology are all very significant in understanding the gaps in the integrity of the nation's defenses, seemingly

overlooked by state and even outside experts on the matter. As such, it could be argued that this research achieved and perhaps even went beyond the goals originally undertaken. However, this knowledge in and of itself may not improve the state of South Korean cybersecurity as a whole, because the goals, motivations and rationale of the actors involved with the problem appear incongruous with one another. National intelligence, for example, rarely employs the talents and insights of foreign or even non-state domestic hackers. This is especially true of South Korea. Dr. Gameli often expressed his frustration at the Korean government's inability to trust outsiders, especially former members of the opposing team, so to speak. However frustrating it may seem at times, it is understandable that those responsible for the protection and safety of every one within their borders would have a difficult time entrusting anyone outside the military, especially those whose cultural background and intentions may not be completely understood in the context of the core engine of their society, namely its cyber infrastructure integrity. In regard to domestic actors involved with the problem of software uniformity, there are many who may argue that as citizens of the same country, working on the same problem with the shared goal of cyber integrity that they should be able to work with another towards that goal. However, the competing minutiae of politics, identity and many levels of differing perceptions often make such cooperation impossible, whatever their shared goals may be. Dr. Kim Keechang, for example is one of the founders of

‘Opennet’, a citizens’ action group, with the goal of promoting a freer and more open internet in Korea. As was illustrated in this dissertation, aspects of this goal of greater liberty in cyberspace can benefit national cybersecurity, so there would be a logical argument for the South Korean government to contribute to this goal. However, this is not the case. In fact, Dr. Kim has even brought suit against the government for possibly violating the civil liberties of netizens. KISA would have to be hard pressed to ask for his help, despite his clear expertise on the subject, and most likely in possession of sound ideas. Other discordant objectives among those seeking to solve the problem will similarly impede the resolution of this dilemma.

This researcher sees more promise in finding a solution through understanding the perceptions and processes, both formal and informal that drive the government’s cybersecurity decisions, strategy and stances. Doing so may resolve existing problems, and the research with a greater foundation of mutual understanding and trust between the government, its citizens and the major parties involved.

6.2 *Theoretical Implications*

The author’s adaptation of the theory of intersectionality provides an alternative to the state-centered, neorealist approach to cybersecurity. All too often cybersecurity scholars and government officials look for the simplest cause

of network vulnerability. Often it is a rival state or in the case of South Korea, it is North Korea who provides a simple enemy around which a national narrative and cybersecurity strategy can be made. Outside of South Korea and outside of national governments as well, the same phenomena can be observed, for example, attributing an attack to Anonymous without a thorough investigation, or vilifying Edward Snowden. At times, researchers may incorporate more than one phenomena when trying to discover the root of a cybersecurity problem. But this usually only involves two or more factors that are often already related. Many would see this broad scope as exhaustive, but the further one goes from his or her original suspicions, the more collaborators one may find, as well as a greater number of connections involved. These seemingly unrelated connections may ironically provide a much simpler solution than those more singularly focused, and provide a more well-rounded understanding of the problem. The singular method of investigation lacks the wealth of evidence provided by numerous inputs from completely unrelated sources, often in a very counterintuitive way.

It is the cross-disciplinary aspect of intersectionality that provides a fresh perspective for the diversity of researchers involved in cybersecurity. Consider the case at hand for a moment. Information spanning the cybersecurity related disciplines could only be fully organized and analyzed through an intersectional model. Legislation was designed to secure internet activity by limiting the manner in which computers and users are recognized (the public-key infrastructure). This

infrastructure required users to always act within protocols when interacting with a sight requiring identity authentication. However, the repetitive nature and frequent requirement of these protocols, made them reflexive actions to users who were being conditioned through their identity to accept any and all downloads as a price of doing business online in Korea, and to conform to the status quo. It was these actions that allowed computers to be compromised. The strategy of public keys actually had the exact opposite effect on cyber security than policy makers had intended. It would seem that all the actors involved with this problem lie within a relatively small domain of Korea and are connected through the internet. However, that connection is dubious at best as 83% percent of the country could potentially be connected to the problem. Also state, individual, and corporate actors, from everywhere all affect each other in ways they may not even know or understand. Intersectionality would serve only to broaden the field of cyber security.

What the author found most surprising about the intersectional approach was the lack of cybersecurity researchers and policy makers using it. Given the nature of the disciplines involved however, its absence does make sense. Researchers in international security studies, international relations and political science tend to group together and against one another over theoretical perspective. In part, this dissertation shows that the inclusion and acceptance of different perspectives in an investigation of this nature can serve to enhance the

understanding of the problem, and improve the veracity of its conclusions.

6.3 *Policy Implications*

Further investigation into the origins of South Korea's software uniformity traced its beginnings to the NPKI system. Aside from the problem of software uniformity, there is a deluge of indications that NKPI policies negatively affect cybersecurity. First and foremost, is the fact that cyber incursions continue to happen in relatively the same way year after year, over the course of the last decade. Also, the frequency and scope of these breaches have increased over time when compared to countries with similar populations, economies and internet access, despite NPKI policies often becoming more restrictive. In addition, no other free nation in the world uses such restrictive technology nationally. The use of an NPKI also has the unintended consequence of limiting the commercial potential of e-commerce in Korea. Foreign sites are far easier to navigate than their Korean counterparts, drawing Koreans away from the domestic e-market and making it very difficult for foreigners to spend money in Korea through the internet. North Korea's cyber attacks (if they were indeed such) are a sign that the government must try a new approach to cyber policy.

Outside of the South Korean government and those who benefit financially from the NPKI's implementation and maintenance, none of the parties involved seem to support South Korea's NPKI. It would seem that policy makers

prefer to amend the system when such localized or logistical problems arise, further complicating and slowing down what should be an efficient process. Continually amending the NPKI, as opposed to abandoning it for other alternatives, suggests that there are clear security, social, or economic benefits to its continued existence. However, there is no evidence supporting this suggestion. In fact, there is a preponderance of evidence supporting the opposite conclusion. The South Korean government even has compatibility issues with its own intranet version of the NPKI, making logistics less efficient. Despite this, the government continues to support the NPKI, and is now even promoting its implementation abroad. In the last two years, the government has been in talks with or signed memorandums of understanding with India, Kenya, South Africa, on developing NPKI in those countries, and promoted the benefits of its own NPKI at the UN's 2014 ITU conference in Busan. Perhaps the South Korean internet's reputation for speed has overshadowed the major security breaches, or the growing number of small successful attacks in the republic. Defending against North Korea becomes a less justifiable reason for keeping this system.

However, it would be foolhardy to suggest that the greatest threat to national security (including cyber security) is not North Korea. The government has the responsibility of protecting its citizens from a very real kinetic threat that is only kilometers away from the capital, as well as protecting cyber infrastructure from Pyongyang's growing cyber command. With that

understanding, it is not the contention of the author that the problem of software uniformity and internet behavior should be the overriding concern for those involved with cybersecurity in Korea. However, this research does support the notion that better education of the public to the risks of their online behavior, and eliminating software uniformity, to the extent that the government could or would encourage software diversity and international inclusiveness, would mitigate two key factors of the problem, and strengthen systems integrity without the need for complex strategies, policies or exhausting vast amounts of resources.

6.4 *Recommendations for Future Research*

The author was disappointed that the hacker survey could not be conducted in a quantitative and representative manner. In retrospect, doing so would require resources and man-power that go far beyond those available to the researcher. However, this dissertation did break new ground in addressing the problem of software uniformity with objective evidence and quantitative methods. There is indeed much more to be discovered about the relationship between South Korea's cyber security and its software.

Also, bringing cybersecurity under the umbrella of intersectionality with a scope such as the one in this dissertation was rather unique. It allowed more freedom with respect to investigative tools and pragmatism, and had less obfuscation from unrelated aspects of the theoretical perspectives used. Should a

cyber security researcher be so inclined, he or she may find such a distinctive application of intersectionality as intellectually stimulating as the author did. The author, in particular, wishes to integrate more intersectionality in future research endeavors.

6.5 *Limitations of the Research*

There were several limitations encountered by the author during the course of this research. As previously revealed in chapter 3, the vast and covert nature of hackers, and their distrust of institutions, made designing and implementing a statistically valid survey seem impossible. Perhaps this was the researcher's shortcoming. If the author were to attempt such a project again, it may be better to use a more hermeneutical approach. However, this would lack the desired statistical validity.

Another major limitation encountered in this study, and as is often true of many such studies, was a relative lack of confidence in the analyses involving the attribution of cyber attacks. The author lacked the technical knowledge to entirely comprehend highly technical reports detailing the cryptographic nuances of the attacks, and mainly relied on the interpretation of trusted colleagues, and public sources more versed in cryptography. Greater first-hand knowledge may have allowed the author to make more distinct and interesting connections or challenge perceptions that were not evident in this dissertation's findings. Furthermore, a

crucial factor of this study was the manner in which malware is introduced to a system. Although many after action or post incident reports explain in great detail the damage done and methods of the attackers, this highly relevant information is rarely addressed publicly. This type of skewed reporting only gets worse as it receives more attention. Authorities seem obsessed with allocating blame, often when such allocations are completely without merit.

6.6 *Closing Remarks*

South Korea is the eleventh largest economy in the world, with one of the most highly educated populations on the planet. However this was not something that happened overnight, or as a matter of routine. This nation's emerged from occupation, rising out of the third world and established a democracy by the will of its people to overcome adversity. South Korea has gone on to accomplish great things. It has become a regional hegemon, and has saved itself from the brink of extinction more than once, entirely due to the intelligence, collective actions, indomitable spirit and superior work ethic of the South Korean people. As sloth, opportunity, and brainpower are not at issue, it is unfathomable that the growing logistical problem of software uniformity and the national public key infrastructure are treated with more electronically restrictive policy and mandated technology. No sooner will the latest state encryption become widespread, than it will become obsolete. Once again there will be collateral damage, while policy

makers tout and force the newest old idea on Korean computer users as the underlying issues fester. It is my hope that this research is received as it was intended: an alarm bell for encryption key-obsessed cyber policy wonks to focus on what they are doing and the potential disastrous results that their actions can have. It is true that the focus of this dissertation was on individual, mostly international hackers. However, the conduit through which they breached South Korean systems (national software uniformity, cavalier online behavior, and public key policy) remains open for individual, or state actors alike. The next hacker to exploit the weakness of these characteristics could as easily be a North Korean cyber soldier as a teenager hacking Korean systems from his bedroom in Springfield, Missouri. The government seems to concern itself greatly with the ‘who’ of cybersecurity. Perhaps they should worry a little more about the ‘how’.

REFERENCES

- 2008 Defense White Paper. Seoul: Ministry of National Defense, Republic of Korea, 2008.
- Ahmed, Saifuddin. "Methods in Sample Surveys: Clustering." *Journal of the School of Public Health, John Hopkins*, 2009, 1-45. p.2. Accessed. January 15, 2016.
- Al-Jazeera. "South Korea Says Chinese IP Behind Cyber Attack." *Al-Jazeera*. March 21, 2013. Accessed September 11, 2014.
- Andrews, Suzanna, Bryan Burroughs, and Sarah Burroughs. "The Snowden Saga: A Shadowland of Secrets and Light." *Vanity Fair*, May 2014. Accessed June 7, 2015.
- Associated Press. "South Koreans Blame North Korea for Recent Cyber Attack." March 21, 2013. Associated Press. Accessed September 12, 2014.
- Atkinson, Robert D., Daniel K. Correa, and Julia A. Helmund. *Explaining International Broadband Leadership*. Report. May 2008. http://www.itif.org/files/ExplainingBBLeadership.pdf?_ga=1.108746948.731530544.1462898497. Accessed March 13, 2012.
- Baylis, John, and Steve Smith. *The Globalization of World Politics: An Introduction to International Relations*. Oxford: Oxford University Press, 2006.
- BBC News. "North Korea Behind South Korean Bank Cyber Attack." BBC Asia Pacific News. May 3, 2011. <http://www.bbc.co.uk/news/mobile/technology-12646052>. Accessed July 7, 2015.
- Boo, Hyeong-wook, and Kang-kyu Lee. "Cyber War and Policy Suggestions for South Korean Planners." *International Journal of Korean Unification Studies* 21, no. 2 (2012): 85-106. Accessed March 11, 2013.
- Bryman, Alan. *Social Research Methods*. Oxford: Oxford University Press, 2015.
- Bryan, Paul D., and Thomas M. Conte. "Combining Cluster Sampling with Single Pass Methods for Efficient Sampling Regimen Design." *2007 25th International Conference on Computer Design*, 2007. doi:10.1109/iccd.2007.4601941. p. 23. Accessed January 16, 2016.
- Buzan, Barry, Ole Waever, and Jaap H. De. Wilde. *Security: A New Framework for Analysis*. Boulder: Rienner, 1998.
- Carr, Jeffrey. *Inside Cyber Warfare Mapping the Cyber Underworld*. Sebastopol: O'Reilly Media, 2009.
- CCDCOE. "Cyber Definitions." *CCDCOE*. 2014. <https://ccdcoe.org/cyber-definitions.html>. Accessed January 22, 2016.
- Celestino, Oscar, and Abendan, Angelo. "Trend Micro Investigates June 25 Cyber Attack in South Korea." *Trend Micro*. July 01, 2013. <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/124/trend-micro-investigates-june-25-cyber-attacks-in-south-korea>.

- Accessed September 15, 2014.
- Chang, Jenifer. "US, South Korea Join Forces to Prevent Cyber Attacks from North Korea." *PC World*, January 14, 2014. Accessed August 9, 2014.
- Choe, Sang-hun. "South Korea Blames North for June Cyber Attacks." *The New York Times*. http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?_r=0. Accessed April 25, 2014.
- Choe, Sang-hun, and John Markoff. "Cyber Attacks Jam Government and Commercial Websites." *The New York Times*, July 9, 2009. Accessed March 14, 2014.
- Chosun Ilbo. "North Korea Fingered in Cyber Attack on South Korean Daily." *Chosun Ilbo*, January 13, 2013. Accessed February 18, 2014.
- Chung, Edward Y.J. *The Korean Neo Confucianism of Yi T'oegye and Yi Yulgok: A Reappraisal of the 'Four-Seven Thesis' and Its Practical Implications for Self-Cultivation*. SUNY Press, 1995.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010.
- Collins, Patricia Hill. "It's All In the Family: Intersections of Gender, Race, and Nation." *Hypatia* 13, no. 3 (1998): 62-82. doi:10.1111/j.1527-2001.1998.tb01370.x. Accessed January 4, 2016
- Crenshaw, Kimberlé. "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics." *University of Chicago Legal Forum*, 1989.
- Davenport, Tara. "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis." *Catholic University Journal of Law and Technology* 24 (2015) Accessed January 4, 2016.
- De, Chu: "White Hat? Black Hat? Grey Hat?"; *ddth.com*. Jelsoft Enterprises, 2002: <http://www.ddth.com/showthread.php/200-ENG-White-Hat-Black-Hat-Grey-Hat>. Accessed March 15, 2016.
- Defence White Paper 2008. Seoul: ROC Ministry of National Defense, 2008. Accessed July 5, 2014
- Defending Cyber Borders: Beyond the Virtual Maginot Line. *Cisco Systems*. October 25, 2012. Accessed June 15, 2013. Interactive video cast.
- Deibert, Ronald. "Militarizing Cyberspace." *MIT Technology Review*, June 22, 2010. doi: <http://www.technologyreview.com/notebook/419458/militarizing-cyberspace>. Accessed September 9, 2013.
- Delete-removevirus.com. "How to Remove TROJ_DIDKR.A Completely From Windows, Information about TROJ_DIDKR.A." http://www.delete-removevirus.com/post/How-to-Remove-TROJ_DIDKR.A-Completely-From-Windows_14_258622.html. Accessed June, 3 2016.
- Demchak, Chris, and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly*, March 2011. Accessed January 28, 2013
- Eriksson, Johan. *Threat Politics: New Perspectives on Security, Risk, and Crisis*

- Management*. Aldershot, Hants, England: Ashgate, 2001.
- Eriksson, Johan, and Giampiero Giacomello. *International Relations and Security in the Digital Age*. London: Routledge, 2007.
- FitzGerald, Ben. "The Theory Of Intersectionality Can Make Cybersecurity Collaboration Real." TechCrunch. May 17, 2015.. <http://techcrunch.com/2015/02/17/the-theory-of-intersectionality-can-make-cybersecurity-collaboration-real/>. Accessed January 10, 2016
- Groffin, Ken, Fred Lekme, and Ursula Koners. *Identifying Hidden Needs: Creating Breakthrough Products*. Springer, 2010.
- Hankivsky, Olena, and Sarah De Leeuw. *Health Inequities in Canada: Intersectional Frameworks and Practices*. Vancouver: UBC Press, 2011.
- Hankivsky, Olena. "Intersectionality 101." *The Institute for Intersectionality Research & Policy SFU*, April 2014. Accessed January 4, 2016.
- Hare, Forrest. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 88-105. Vol. 3. Cryptology and Information Security Series. IOS Press, 2009 DOI: 10.3233/978-1-60750-060-5-88. Accessed March 21, 2013.
- Heal, G., and H. Kunruther. "Self-protection and Insurance with Interdependencies." *Journal of Risk and Uncertainty* 36 (2008): 101-23. Accessed January 4, 2016.
- Iglaur, Phillip. "South Korea's Government Hit with 114,000 Cyberattacks in 5 Years." CNET. September 20, 2015. <http://www.cnet.com/news/south-korea-hit-with-over-114000-cyberattacks-in-five-years/#!> Accessed September 25, 2015.
- Im, Su-Kyung; Report to the National Assembly on: The South Korean National Computing & Information Agency (NCIA) collected data on hacking attempts over the period of June 2011 to June 2015. Accessed September 18, 2015.
- Information Audit and Control Association (ISACA): Cybersecurity Fundamentals Glossary, 2014. Accessed February 12, 2016.
- Jiang, Rui, Tu Zhidong, Ting Chen, and Fengzhu Sun. "Network Motif Identification in Stochastic Networks." *Proceedings of the National Academy of Science* 103, no. 25 (June 12, 2006): 9404-409. doi:10.1073/pnas.0507841103. Accessed April 11, 2015.
- Johnson, Bobby. "Chinese Websites Mark Tiananmen Square Anniversary with Veiled Protest." *The Guardian*, June 4, 2009. Accessed November 13, 2014.
- Jun, Jenny, Scott Lafoy, and Ethan Sohn. "The Organization of Cyber Operations in North Korea." *Korea Chair Platform - Center for Strategic and International Studies*, December 18, 2014, 1-3 Accessed January 9, 2015.

- Karyotis, Vasileios, and M. H. R. Khouzani. *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*. Morgan/Kaufman, 2016.
- Kim, Dongcheol. *Korean Experience of Overcoming Economic Crisis through ICT Development*. Technical paper. UNESCAP Information and Communications Technology and Disaster Risk Reduction Division, 2009. Accessed January 9, 2015.
- Kim, Hyoungh Shick, Jun Ho Huh, and Ross Anderson. *On the Security of Internet Banking in South Korea – A Lesson in How Not to Regulate Security*. Publication. Oxford University Computing Laboratory, 2011.
- Kim, Keechang. "Recent Changes in the Regulatory Landscape for E-Commerce in South Korea." *The Asian Business Lawyer* 16 (Fall 2015): 87-103.. file:///C:/Users/user/Downloads/04. Keechang Kim_article (3).pdf. Accessed December 24, 2015
- KISA. "Public Key Authentication Service." Public Key Authentication Service. http://rootca.kisa.or.kr/kor/popup/foreigner_pop1_en.html.. Accessed February 15, 2016.
- Kuo Chung-Chieh, Jay Cong, Bellingham, Bill. *Proceedings of SPIE - The International Society for Optical Engineering. Digital Image Storage and Archiving Systems. Held in Philadelphia, PA, 25-26 October 1995. Volume 2606*. By, WA: Spie-the International Society for Optical Engineering Bellingham Wa, 1995. Accessed January 22, 2015.
- Kwaak, Jesup S. "Seoul Suspects South Korean Tech Executive of Helping North in Cyberattacks." *The Wall Street Journal*, July 31, 2013. Accessed February 18, 2014. <http://www.wsj.com/articles/SB10001424127887324136204578639540757695644>.
- Lam, Jeanne, Kwang Keung Ng, and Simon K.S. Cheung. *Technology in Education. Technology-Mediated Proactive Learning*. Proceedings of Second International Conference, ICTE Hong Kong, China, July 2-4, 2015. Accessed April 8, 2016.
- Langer, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. Publication. Langer Group, 2013.
- Lazarus, Arnold A., and Ofer Zur. *Dual Relationships and Psychotherapy*. New York, NY: Springer, 2002.
- Lee, Yong-Ro, Byong-Cho Kim, Seong-Wook Nah, and Jung Hwae Hu. "Analytic Study on Korea's IT Infrastructure Development Policies." *Informatization Policy*, September 2013, 277-304. Accessed January 9, 2015.
- Lewis, James A. "Korean" Cyber Attacks and Their Implications for Cyber Conflict". *Center for Strategic and International Studies*. October 2009. Accessed January 13, 2015.
- Libicki, Martin C.: "Cyber Deterrence and Cyber War". *Rand Corporation*.

- October 7, 2009.
- Manoske, Andy. "How Does Cyber Warfare Work?"; *Forbes*. July 18, 2013: <http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/#3239797b33c3> Accessed August 18, 2014.
- Martin, David M. *Tracing The Lineage of DarkSeoul*. Technical paper. November 20, 2015. <https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787>. Accessed December 23, 2015.
- Mason, C. Nicole. *Leading at the Intersections: An Introduction to the Intersectional Approach Model for Policy & Social Change*. New York: NYU Wagner, 2010. Accessed January 30, 2016.
- Maximus Impact. "NIST - Glossary Of Key Information Security Terms." *Maximus Impact*. <http://www.maximusimpact.com/national-institute-of-standards-and-technology-glossary-of-key-information-security-terms>. Accessed January 16, 2016.
- McAfee. "White Paper Report: Ten Days of Rain, Expert Analysis of Distributed Denial-of-service Attacks Targeting South Korea." McAfee. March 15, 2011. <http://www.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf>. Accessed September 1, 2013.
- McCall, Leslie. "The Complexity of Intersectionality." *Signs: Journal of Women in Culture and Society* 30, no. 3 (2005): 1771-800. doi:10.1086/426800. Accessed January 14, 2015.
- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: Norton, 2001.
- Moody, Glen. "South Korea Still Paying the Price for Embracing Internet Explorer a Decade Ago." *Tech Dirt*, May 2012. Accessed June 14, 2014.
- NSHC Securities. *Red Alert Research Report: 3.20 South Korea Cyber Attack. 03/21/13*, [http://training.nshc.net/KOR/Document/virus/20130321_320CyberTerrorIncidentResponseReportbyRedAlert\(EN\).pdf](http://training.nshc.net/KOR/Document/virus/20130321_320CyberTerrorIncidentResponseReportbyRedAlert(EN).pdf). Accessed June 5, 2014.
- NSHC Securities. *Red Alert Research Report: 6.25 South Korea Cyber Attack. 06/25/13*, http://training.nshc.net/ENG/Document/virus/20130625_6.25_CyberTerrorAnalysis_Report.pdf. Accessed June 5, 2014.
- OECD. "Broadband and Telecom." *OECD Broadband Statistics Update*. June 2015. Accessed October 3, 2015. <http://www.oecd.org/sti/broadband/broadband-statistics-update.htm>.
- Oh, Myung, and James F. Larson. *Digital Development in Korea: Building an Information Society*. London: Routledge, 2011.
- Onuf, Nicholas. "Worlds of Our Making: The Strange Career of Constructivism in International Relations," in Donald J. Puchala, ed., *Visions of International Relations*
- OpenNet: Mission Statement." Open Net. <http://opennetkorea.org/en/wp/about-opennet>. Accessed June 8, 2014.
- Columbia: University of South Carolina Press, January 2002.

- Paik, Jin-hyun, Seok-Woo Lee, and Kevin Tan. *Asian Approaches to International Law and the Legacy of Colonialism and Imperialism: The Law of the Sea, Territorial Disputes and International Dispute Settlement*. London: Routledge, 2012.
- Park, Hun Myoung. *2012 45th Hawaii International Conference on System Sciences: (HICSS 2012) Maui, Hawaii, 4-7 January 2012*. Proceedings of The Web Accessibility Crisis of Korea's Electronic Government: Fatal Consequences of the Digital Singature Law. New York: IEEE, 2012. 2319-328. Accessed July 7, 2013.
- Parken A: "A Multi-strand Approach to Promoting Equalities and Human Rights in Policy Making"; *Policy Politics*, 2010.
- Phys.Org. "South Korean Government Website Hit by Cyber Attacks." *Phys.org*, June 10, 2010. 2010-06-skorean-website-cyber.pdf. Accessed June 5, 2014.
- Republic of Korea. Korean Internet Security Agency. MSIP(Ministry of Science, ICT and Future Planning), KCC (Korea Communications Commission), MSPA(Ministry of Security and Public Administration),. *2013 Korea Internet White Paper*. Seoul, Republic of Korea, 2013. Accessed May 5, 2014.
- Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Santa Barbara, CA: Praeger, 2013. Accessed May 9, 2014
- SANS "Glossary of Security Terms." SANS.org <http://www.sans.org/security-resources/glossary-of-terms>. Accessed February 6, 2016.
- Siddiqui, Muazzam, Morgan C. Wang, and Joohan Lee. "A Survey of Data Mining Techniques for Malware Detection Using File Features." *Proceedings of the 46th Annual Southeast Regional Conference on XX - ACM-SE 46*, 2008. doi:10.1145/1593105.1593239. Accessed February 13, 2013.
- Skoudis, E./Zeltser, L.: *Malware: Fighting Malicious Code*; Prentice Hall, 2014.
- StatCounter. "Top 7 Desktop, Tablet& Console Oss in South Korea from July to August 2009" - <http://gs.statcounter.com/#os-KR-monthly-200907-200908> Accessed January 29, 2016.
- Sydney Morning Herald." "Hacked by IsOne'...Or by Kim? Newspaper Hit by Cyber Attack." *Sydney Morning Herald*. June 11, 2012. <http://www.smh.com.au/technology/technology-news/hacked-by-isone--or-by-kim-newspaper-hit-by-cyber-attack-20120611-205cn.html>. Accessed June 2, 2014.
- Tech Times. South Korea's Government Hit with 114,000 Cyberattacks in 5 Years". *Tech Times*, September 22, 2015. Accessed January 15, 2016.
- The Constitution of the Republic of Korea. Cong. Seoul: Office of Public Information, Republic of Korea, 1956. Accessed August 4, 2014.
- The Economist. "Estonia and Russia: A Cyber Riot." *The Economist*. May 10th, 2007 Accessed January 12, 2014.

- The Guardian. "White House on the Back Foot over CIA Role in German Spying Scandal." *The Guardian*, July 7, 2014. Accessed January 12, 2015.
- The Korea Times. "Korea Paying Price for Microsoft Monoculture". *The Korea Times*. September 23, 2009. Accessed June 9, 2012.
- Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002.
- Trimm, Peter. *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership*. Edited by Heung Youl Youm. Report Submitted to the Korean Government and the UK Government. 2013. Accessed January 15, 2015.
- Valeri, Lorenzo. "Securing Internet Society: Toward an International Regime for Information Assurance." *Studies in Conflict & Terrorism* 23, no. 2 (2000): 129-46. doi:10.1080/105761000265566. Accessed March 3, 2014.
- Wæver, Ole. *Concepts of Security*. København: Institute of Political Science, University of Copenhagen, 1997.
- Waltz, Kenneth N. *Theory of International Politics*. Reading, MA: Addison-Wesley Pub., 1979.
- Weirsmas, Weibo. "The Validity of Surveys: On-line and Off-line." *Oxford Internet Institute*, 2009, 3-23. Accessed January 7, 2016.
- Wendt, Alexander. *Social Theory of International Politics*. Cambridge: University Press, 1999.
- WhatIs.com. "What Is Black Hat? - Definition from WhatIs.com." SearchSecurity.. <http://searchsecurity.techtarget.com/definition/black-hat>. Accessed May 15, 2016.
- WhatIs.com. "What Is White Hat? - Definition from WhatIs.com." SearchSecurity. <http://searchsecurity.techtarget.com/definition/white-hat>. Accessed March 12, 2016.
- Williams, Michael C. "Words, Images, Enemies: Securitization and International Politics." *Int Studies Q International Studies Quarterly* 47, no. 4 (2003): 511-31. doi:10.1046/j.0020-8833.2003.00277.x. Accessed May 18, 2014.
- Winker, Gabriele, and Nina Degele. *Intersektionalität: Zur Analyse Sozialer Ungleichheiten*. Bielefeld: Transcript, 2009. Accessed October 22, 2014.
- Wood, Anthony. "South Korea Pushes for Cyber Weapon to Undermine North Korean Nuclear Facilities." *Gizmag.com*, February 24, 2014. <http://www.gizmag.com/south-korea-stuxnet-cyber-weapon/30977/>. Accessed March 12, 2014.
- World Bank Data. "Internet Usage as a Percentage of Population." Accessed January 22, 2016.
- Yang, Söng-ch'öl. *The North and South Korean Political Systems: A Comparative Analysis*. Boulder, CO: Westview Press, 1994.
- Yonhap News. "Government Confirms Pyongyang Link in March Cyber Attack." Yonhap News Agency. April, 10, 2013.

<http://english.yonhapnews.co.kr/northkorea/2013/04/10/49/0401000000AEN20130410007352320F.HTML>. Accessed February 2, 2016

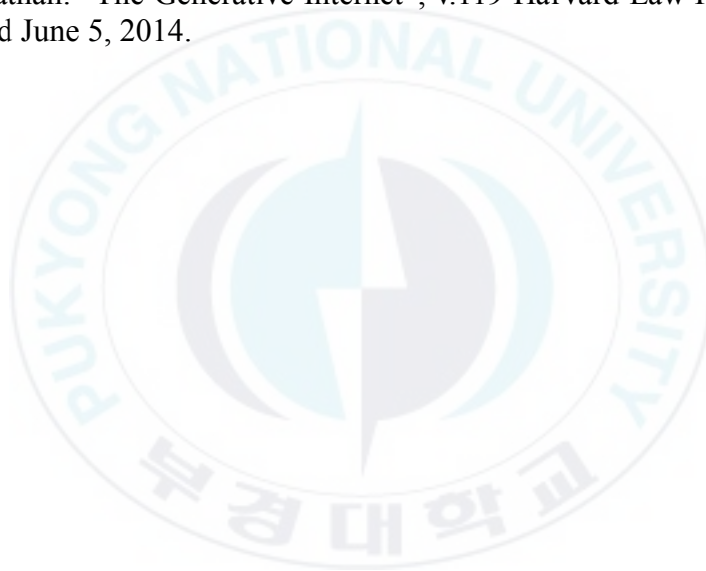
Yonhap News. "South Korean Government Website Hit by Cyber Attacks," *Yonhap News*. June 10, 2010. Accessed March 12, 2014.

ZDNet. "South Korea to Remove 90 Percent of ActiveX by 2017." *ZDNet*. [http://www.zdnet.com/article/south-korea-to-remove-90-percent-of-activex-by-2017/..](http://www.zdnet.com/article/south-korea-to-remove-90-percent-of-activex-by-2017/) Accessed July 1, 2013.

Zetter, Kim. "Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force.'" *PC*, March 25, 2013. *Wired*. March 25th, 2013: <http://www.wired.com/2013/03/stuxnet-act-of-force/> Accessed October 4, 2014.

Zetter, Kim. "Lazy Hacker and Little Worm Set-off Cyberwar Frenzy." *Wired*, July 8, 2009, 12-18. Accessed January 22, 2013.

Zittrain, Jonathan: "The Generative Internet"; v.119 *Harvard Law Review* (2006) Accessed June 5, 2014.



Appendix A:

South Korean end-user Survey (Korean)

당신은 한국인 입니까?

a. 네 b. 아니요

당신의 연령대는?

a. 21 세 이하 b. 22 세~34 세 사이 c. 35 세~44 세 사이 d. 45 세~54 세 사이

e. 55 세~64 세 사이 f. 65 세 이상

당신의 성별은?

a. 남성 b. 여성

당신의 직업이나 산업은?

1. 주부
2. 학생
3. 실업자
4. 농업, 임업, 어업, 수렵
5. 교육자 - 단과대학, 종합대학, 성인교육
6. 교육자 - 초등학교, 중,고등 학교
7. 정치학, 행정학
8. 금융업, 보험업
9. 보건의료, 사회 복지

10. 호텔, 음식서비스
11. 정보 - 서비스, 데이터
12. 정보(그밖의)
14. 법률 서비스
15. 방송
16. 제조업(컴퓨터, 전자공학)
17. 기타
18. 광업
19. 출판업
20. 부동산업
21. 종교업
22. 소매업
23. 도매업
24. 과학, 기술 서비스
25. 소프트 웨어
26. 전기 통신
27. 수송, 창고
28. 에너지
29. 학생
30. 교육
31. 군인
32. 건설
33. 유틸리티



직장에서 당신의 역할은?

1. 경영진
2. 중간 관리자
3. 하위 관리자
4. 관리 직원
5. 지원 직원
6. 직업 훈련
7. 학생
8. 숙련 노동자
9. 컨설턴트
10. 연구원
11. 임시 고용인
12. 자기 직원
13. 해당사항 없음

당신이 일하는 조직은?

1. 공공 부문
2. 민간 부문
4. 모른다.

당신은 다음과 같은 장소에서 얼마나 자주 인터넷을 사용합니까?

매일 매주 매달 한 달에 한 번 이하 사용 안함

집에서

(홈오피스 포함)

직장에서

학교에서

공공 터미널

(도서관, 사이버카페 등)

기타 장소에서

모바일 장치

어떤 유형의 운영 체제를 집에서 사용하십니까?

1. Apple/MAC
2. OS2
3. Unix
- 4.
5. PC running Unix
6. Windows
7. 모른다.

어떤 버전의 윈도우를 실행하고 있습니까?

1. XP
2. Vista
3. Windows 7
4. Windows 8
5. Windows 8.1

어떤 유형의 브라우저를 집에서 사용하십니까?

1. 인터넷 익스플로어

2. 구글 크롬
3. 사파리
4. 모질라 파이어 폭스
5. 넷스케이프
6. 기타(지정해 주십시오)

당신의 컴퓨터는 어떤 유형의 바이러스 백신 소프트웨어를
사용하십니까?(집에서)

1. Microsoft
2. Avast
3. AhnLab
4. 알약
5. 시만텍
6. ESET
7. Avira
8. Kaspersky
9. McAfee
10. 기타

당신의 컴퓨터는 어떤 유형의 바이러스 백신 소프트웨어
를 사용하십니까?(직장에서)

1. Microsoft
2. Avast
3. AhnLab
4. 알약



5. 시만텍
6. ESET
7. Avira
8. Kaspersky
9. McAfee
10. 기타

(인터넷 익스플로워를 사용하는 사람들을 위해) 활동 제어 경고가 날 때;
당신은 다음과 같은 프로그램이 당신의 컴퓨터를 변경 하는 것을
허락합니까? 혹은 이 소프트웨어를 다운로드하면 손상을 입을 수
있습니다. 당신은 어떻게 하십니까?

Appendix B:

South Korean End-User Survey (English)

Would you describe yourself as:

- a. Korean b. non-Korea

Please specify your age group:

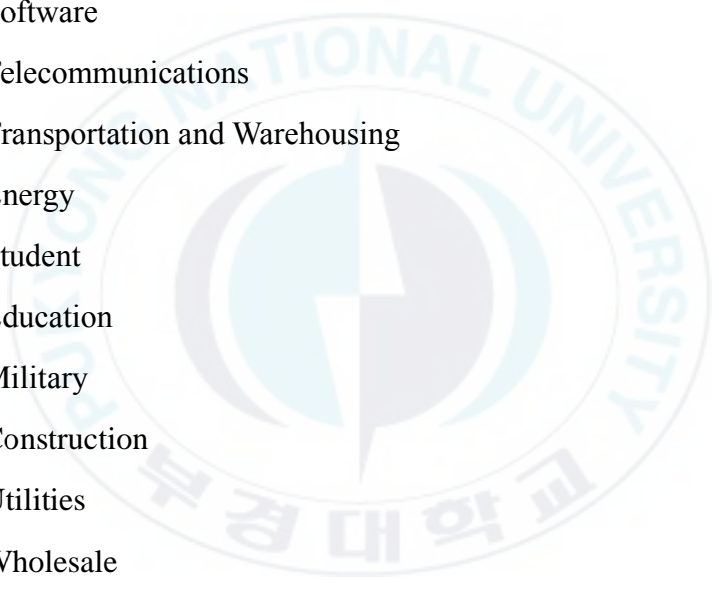
- a. (21 and under) b. (22 - 34) c. (35-44) d. (45-54) e. (55-64)
f. Over 65

What is your sex?

- a. Male b. Female

How would you characterize your job or industry?

1. Homemaker
2. Student
3. Unemployed
4. Agriculture, Forestry, Fishing, or Hunting
5. Education - College, University, or Adult
6. Education – Primary or secondary (K-12)
7. Government and Public administration
8. Finance and Insurance
9. Health care and social Assistance
10. Hotel and food services
11. Information – Services and data
12. Information (other)
13. Processing
14. Legal Services
15. Broadcasting

16. Manufacturing (Computer and Electronics)
 17. Other
 18. Mining
 19. Publishing
 20. Real Estate
 21. Religious
 22. Retail
 23. Scientific or technical services
 24. Software
 25. Telecommunications
 26. Transportation and Warehousing
 27. Energy
 28. Student
 29. Education
 30. Military
 31. Construction
 32. Utilities
 33. Wholesale
- 

Which of the following best describes your role at work?

1. Upper management
2. Middle Management
3. Junior management
4. Administrative staff
5. Support Staff
6. Trained professional
7. Student

8. Skilled laborer
9. Consultant
10. Researcher
11. Temporary employee
12. Self employed
13. None of the above

How would you describe the organization you work for:

1. Public Sector
2. Private Sector
3. Not-for-profit
4. Don't know

How frequently do you access the internet from the following places?

	Daily	Weekly	Monthly	Less than once a month	Never
From home (including a home office)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
From work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
From school	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
From a public terminal (e.g. library, cybercafe, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
From other places	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A mobile device	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

What type of operating system do you use at home?

1. Apple/MAC
2. OS2
3. Unix
4. Linux
5. PC running Unix
6. Windows
7. Don't know

(if Windows) What version of windows are you running?

1. XP
2. Vista
3. Windows 7
4. Windows 8
5. Windows 8.1

What type of browser do you use at home?

1. Internet explorer
2. Google Chrome
3. Safari
4. Mozilla Firefox
5. Netscape
6. Other (please specify)

What type of antivirus software do you use on your computer at home?

1. Microsoft
2. Avast
3. AhnLab

4. 알약
5. Symantec
6. ESET
7. Avira
8. Kaspersky
9. McAfee
10. Other

What type of antivirus software do you use on your computer at work?

1. Microsoft
2. Avast
3. AhnLab
4. 알약
5. Symantec
6. ESET
7. Avira
8. Kaspersky
9. McAfee
10. Other

(For those using Internet explorer) When the *ActiveX* control warning indicates, “Do you want to allow the following program to make changes on your computer?” or “Downloading this software may be damaging to your computer.” do you:

1. always “allow” to view the website?
2. usually “allow” to view the website?
3. sometimes “allow” to view the website?
4. seldom “allow” to view the website?

5. never “allow” to view the website?
6. investigate further

How often do you click on interesting, informative or commercial links to a third party website on your social networking site?

1. If I know the person or company who posted the link, I click every time I want see a link.
2. I usually click on the links, but I am occasionally skeptical.
3. I rarely click on links to a third party website.
4. I never click on links to a third-party website.

How often do you click on links sent to you by emails?

1. I always click on links that I find interesting or important.
2. I usually click on links that I find interesting or important.
3. I often click on links that I find interesting or important.
4. I seldom click on links that I find interesting or important.
5. I never click on links through email.

Has your email account ever been hacked?

1. Yes, more than once.
2. Yes, once.
3. No, never.

Has your social networking account ever been hacked?

1. Yes, more than once.
2. Yes, once.
3. No, never.

Has your computer or mobile device at work been infected with a virus?

1. Yes, more than once.

2. Yes, once.
3. No, never.

Has your home computer or mobile device been infected with a virus?

1. Yes, more than once.
2. Yes, once.
3. No, never.

Do you access your school or company network from home?

- a. Yes
- b. No

Has your computer at work or school ever become inoperable due to malware?

1. Yes, more than once.
2. Yes, once.
3. No, never

Has your home computer become inoperable due to malware?

1. Yes, more than once.
2. Yes, once.
3. No, never

Appendix C: Hacker Survey

1. Would you characterize yourself as a:
 - a. White hat hacker
 - b. Black hat hacker
 - c. Grey hat hacker

2. If a system is easy for you to penetrate, will that make you:
 - a. more likely to try to access it?
 - b. less likely to try to access it?
 - c. It has no bearing on whether you will try to access it.

3. If a system is difficult for you to penetrate, will that make you:
 - a. more likely to try to access it?
 - b. less likely to try to access it?
 - c. It has no bearing on whether you will try to access it.

4. How often are your political beliefs the main reason for selecting a target?
 - a. Always
 - b. Usually
 - c. Sometimes
 - d. Rarely
 - e. Never

5. Please rank the following operating systems in terms of their difficulty to hack (1 is most difficult to hack).
 - a. OS2
 - b. Linux
 - c. Windows
 - d. Apple/MAC

6. Please rank the following Web browser in terms their difficulty to compromise (1 is most difficult to hack).
- a. Internet explorer
 - b. Google Chrome
 - c. Safari
 - d. Mozilla Firefox

