Cyberterrorism: Trends and Responses

윤해성
Researchers

<table>
<thead>
<tr>
<th>Principal Researcher</th>
</tr>
</thead>
</table>
| **Yoon, Hae-sung**  
  (Associate Research Fellow, Korean Institute of Criminology) |

<table>
<thead>
<tr>
<th>Joint Researcher</th>
</tr>
</thead>
</table>
| **Yun, Minwoo**  
  (Professor, Department of Police Science and Security, Gachon University) |
| **Joshua Freilich**  
  (Professor, John Jay College of Criminal Justice, City University of New York) |
| **Steven Chermak**  
  (Professor, School of Criminal Justice, Michigan State University) |
| **Robert G. Morris**  
  (Assistant Professor, Criminology Department, School of Economic, Political and Police Science, The University of Texas at Dallas) |

<table>
<thead>
<tr>
<th>Editor</th>
</tr>
</thead>
</table>
| **Sohn, Hee Jun**  
  (Researcher, Korean Institute of Criminology) |
| **Lee, Suk Yian**  
  (Assistant Researcher, Korean Institute of Criminology) |
After the 911 attacks, terrorism is becoming increasingly networked, diversified and complex. In terrorist cases such as the recent DDoS attacks, hacking of Korean government institutions by hackers in China, Stuxnet attacks and the Norway terrorist attack, it can be observed that cyberspace is used as a key asset in terrorist methods. With the advent of the information age, this is a reality that can no longer be ignored in consideration of the fact that many types of cyberterrorism that occur in cyberspace directly affect our everyday lives. Also, the UNODC recognizes cyberterrorism as an important problem by separately categorizing ‘Terrorist Use of the Internet’, attesting to the global importance of cyberterrorism.

In this context, this research examines the most current trends in cyberterrorism in this information age and proposes efficient and systematic response measures. This research is significant in that it conducts a comparative legal analysis of legal systems on the new threat of cyberterrorism and proposes measures for the legal system of South Korea along with its implications. This research makes valuable contributions in increasing the awareness of cyberterrorism among the people, and furthermore provides a basis to for proactive and preventive countermeasures against cyberterrorism.

In particular, this research, to reflect upon the trends of the 21st century where globalization is rapidly facilitated by the expansion of cyberspace and its close connections to real space, examines cyberterrorism on its aspects of inter-

Foreword
national trends and policies, conducts international joint research to seek countermeasures, introduces and analyzes methods of terrorist use of the internet and acts of cyberterrorism by terrorists, makes use of interview results from international cyberterrorism experts and institutions, publishes the research in not only Korean but also English. In this regard, this research not only opens the potential of the Korean Institute of Criminology to internationally disseminate its research, but also in leading this research, the Korean Institute of Criminology confirms the potential to act as a hub of international exchanges and make contributions to the world.

I sincerely hope that this research can contribute to efficient and systematic countermeasures against cyberterrorism, and research from the Korean Institute of Criminology can contribute to not only to South Korea, but also the world. In final words, I would like to congratulate the hard work of assistant researcher Yoon Hae-sung in faithfully performing this research to the end, and acknowledge the valuable contributions by joint researchers Professor Yun Minwoo, Professor Joshua Freilich, Professor Steven Chernak and Professor Robert G. Morris. Furthermore, I would like to appreciate the efforts of those who provided consultations to this research and to all others who helped this research come to fruition.

December, 2012

Korea Institute of Criminology
President

[Signature]
Table of Contents

Executive Summary ................................................................. 13

Chapter 1. Introduction ............................................................. 21
   I. Research Purpose ............................................................ 21
   II. Research Scope and Content .............................................. 22
   III. Research Method .......................................................... 29

Chapter 2. General Issues of Cyberterrorism ............................... 33
   I. Definition of Cyberterrorism ............................................... 33
      1. Introduction ............................................................ 33
      2. What is Cyberterrorism? ................................................ 34
      3. Definition of Terrorism, Cybercrime and Cyberterrorism ...... 36
      4. Typology and Threats of Cyberterrorism ............................ 41
      5. Case Studies of Cyberterrorist Attacks .............................. 50
      6. Typology of Cyberterrorism ............................................ 54
      7. Conceptual Overview from an Overall Perspective ............... 58
   II. International Cooperation System in Cyberterrorism Response .... 65
      1. International Characteristics of Cyberterrorism .................. 65
      2. Rules, Conventions and Laws regarding International Cooperation ................................................ 68
      3. International Conventions .............................................. 75
      4. Conclusion .................................................................. 77
III. Analysis of Cyberterrorism Response System of Major Countries

1. Cyberterrorism Response System of the United States of America

2. Cyberterrorism Response System of the United Kingdom

3. Cyberterrorism Response System of the Federal Republic of Germany

4. Cyberterrorism Response System of the French Republic

5. Cyberterrorism Response System of Japan

6. Cyberterrorism Response System of India

7. Implications

8. Conclusion

Chapter 3. Terrorist Use of the Internet and Counterterrorism Measures

I. Introduction

II. Theoretical Discussions

1. Terrorist Use of the Internet and Cyberterrorism

2. Physics and Strategic Advantage of Cyberspace

3. Threats from Cyberspace and Existential Crisis of Nation-State

III. Terrorist Threats through Cyberspace: Terrorist Use of the Internet

1. Terrorist Use of the Internet

2. Types of Terrorist Use of the Internet

3. Terrorist Use of the Internet

IV. Transformation of Mode of Warfare: Marriage between Terrorism and Cyberspace
1. Overview .............................................................................................................. 158
2. Marriage between Terrorism and Cyberspace ................................................. 160
3. Qualitative Changes on Mode of Warfare ....................................................... 161
4. The Fifth Generational Warfare ..................................................................... 163

V. Counterterrorism Measures: C&C (Communication & Cooperation) and Infiltration ................................................................................................................................. 168
1. Overview .............................................................................................................. 168
2. Counterterrorism Measures against Terrorist Use of the Internet .................. 169

VI. OSINT (Open Source Intelligence) as a Counterterrorism Measure .......... 172
1. Overview .............................................................................................................. 172
2. The Concept of OSINT ....................................................................................... 173
3. OSINT practices ................................................................................................. 174
4. Things to Consider for the Use of OSINT ....................................................... 176

VII. Conclusion ........................................................................................................ 179

Chapter 4. Terrorist Use of the Internet: an Analysis of Strategies, Objectives and Law Responses ................................................................. 183

I. Introduction ........................................................................................................... 183

II. The Strategies Used to Harness the Power of the Internet ............................ 187

III. Understanding the Rationale for Using the Internet ..................................... 196
1. Propaganda ......................................................................................................... 196
2. Recruitment and Radicalization ...................................................................... 200
3. Strategic Tactics ................................................................................................. 204

IV. Law Enforcement Response to Terrorism on the Internet .......................... 209

V. Conclusion ........................................................................................................... 216
Chapter 5. Current Status and Legal System of Cyberterrorism in the Republic of Korea

I. An Overview of the Republic of Korea’s Penal Measure and Cases pertaining to Cyberterrorism

   1. Overview
   2. Case Study of Cyberterrorism in Korea
   3. Analysis on Cyberterrorism Penal Measures in Criminal Law
   4. Analysis on Cyberterrorism Penal Measures in Special Law

II. Response System and Conditions on Cyberterrorism in the Republic of Korea

   1. Cyberterrorism Cases
   2. Overview of Response System on Cyberterrorism
   3. Problems Confronted by Response System on Cyberterrorism

III. Countermeasures for Cyberterrorism

   1. Intelligence
   2. Expert System and Founding National Digital Evidence Research Institute
   3. Improvement on Cyberterrorism Legislation
   4. Examination on Cybercrime Investigation Cooperation System

Chapter 6. Conclusion

Reference

Abstract
# Table of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Typology of Cyberterrorism</td>
<td>49</td>
</tr>
<tr>
<td>2</td>
<td>Information System Attacks</td>
<td>50</td>
</tr>
<tr>
<td>3</td>
<td>Typology of Cyberterrorism of Korea National Police Agency’s Cyber Terror Response Center</td>
<td>55</td>
</tr>
<tr>
<td>4</td>
<td>Categorization of Attacks against National Security by National Intelligence Service’s Cyber Safety Center</td>
<td>56</td>
</tr>
<tr>
<td>5</td>
<td>Typology of Cyberterrorism</td>
<td>58</td>
</tr>
<tr>
<td>6</td>
<td>Major Cases of Cyberterrorist Arrests</td>
<td>78</td>
</tr>
<tr>
<td>7</td>
<td>Statutory Punishment on Cyberterrorism in Criminal Law based on Behavioral Types</td>
<td>230</td>
</tr>
<tr>
<td>8</td>
<td>Statutory Punishment on Cybercrime in Special Law based on Behavioral Types</td>
<td>241</td>
</tr>
<tr>
<td>9</td>
<td>Major Cyberterrorism Cases of South Korea</td>
<td>245</td>
</tr>
<tr>
<td>10</td>
<td>Legislation relative to Cyberterrorism Reporting Rate</td>
<td>254</td>
</tr>
</tbody>
</table>
Table of Figures

(Figure 1) Fifth Generational Warfare ......................................................... 166
(Figure 2) Structure of Cybercrime Initial Detection Response

   Expert System ................................................................. 259
After the 911 attacks, terrorism has evolved to become more networked, diverse and complex. Cyberspace, which pervades many aspects of our everyday life, both real and imaginary, is in the center of this evolution, increasingly used as a means of terrorism. This new form of terrorism, cyberterrorism, threatens our lives in a variety of ways, attested by multiple cases of cyberterrorist attacks such as DDoS attacks and the Stuxnet worm. Other forms of cyberterrorism are utilization of the Internet to facilitate terrorist activity, which is defined by the UNODC as “use of the Internet for terrorist purposes". Cyberterrorism is now globally recognized as a fundamental threat to national security. To face this emerging threat of cyberterrorism, this research seeks a more strategic approach to cyberterrorism and considers more systematic and inclusive policies and responses.

This is a joint research lead by Yoon, Hae-sung, with eminent professionals in terrorism, Joshua Freilich, Steven Chermak, Robert G. Morris and Yun, Minwoo as joint researchers.

Yoon, Hae-sung, as the principle researcher, organized the joint research effort, analyzes and discusses conceptualization of cyberterrorism, legal systems of different countries regarding cyberterrorism, South Korea’s penalty code regarding cyberterrorism and the current status of cyberterrorism in South Korea, and sums up joint materials provided by joint researchers to discuss overall proposals on countermeasures against cyberterrorism.

Joint researcher Professor Yun, Minwoo empirically analyzes interviews of professionals on activities of law enforcement and intelligence agencies on use of the
Internet for terrorist purposes in the United States and European countries. Also, he tries to suggest solutions on problems regarding cyberterrorist acts by traditional terrorists. Joint researcher Professor Joshua Freilich categorizes cyberterrorist cases after the 911 attacks into a typology, explicates the characteristics of each type of cyberterrorism and discusses their implications, and along with joint researcher Professor Steven Chermak, a research is conducted on enforcement of the law on the use of the Internet for terrorist purposes in the United States. Joint researcher Professor Robert G. Morris’s research proposes counter-cyberterrorist policies based on legal responses and cyberterrorism trends in the United States.

The main aim of this research is to categorize cyberterrorist cases and profile their characteristics by analyzing open information and interviews. To achieve this goal, international joint research with eminent foreign terrorism agencies and professionals is conducted. First, literature review is conducted to analyze existent domestic and overseas legal systems and suggestions for improvement are proposed. Second, a joint research to synthesize theoretical model of counter-cyberterrorist policies is conducted along with foreign specialists. Third, feedback between internal and external joint researchers is exchanged to discuss and propose effective counter-cyberterrorist policies.

With this methodological framework in place, this research mainly focuses on facts and realities by analyzing existent discussions on counter-cyberterrorism and existent cyberterrorism response systems. Along with research materials from foreign joint researchers, consultations with domestic professionals and practitioners are also analyzed as qualitative data. There is also theoretical review on conceptualization and typology of cyberterrorism. A workshop was conducted to collect information on the current status of cyberterrorism, cyberterrorism response systems, countermeasures and their typology, and legal systems. Empirical analysis was also conducted on cyberviolation, by types and categories, mostly by the foreign joint researchers.

With regards to conceptualization of cyberterrorism, it is indicated that the defi-
nition of cyberterrorism cannot be fully justified due to the reason that the nature of the cyberterrorist crime being too comprehensive. New methods and technology are constantly emerging through the characteristic of cyberspace. It is recommended to implement a legal measure that accommodates variant forms of cyberterrorism, which is broad and mutating in its nature.

With regards to international cooperation, the necessity of multilateral cooperation is emphasized in consideration to extradition and judicial assistance. To facilitate this process, minimization of administrative procedures and cooperation, both official and unofficial, is recommended. Among various organizations and agencies taking important role in facilitating cooperation at international and national levels, organizations such as CERT and FIRST can serve instrumentally in formal, informal, bilateral and multilateral cooperation. In the field of cybercrime and cyberterrorism, informal activities between the public and private sectors lead to formal cooperation. Therefore, it is recommended to establish organizations or agencies such as a coordination center for cooperation and coordination at every level.

With regards to legislation on cyberterrorism, the UN Security Council Resolution 1368 and 1373 after the 911 attacks urged the Member States to enact counterterrorism laws. To meet the demands of the UN, most of the states modified their policies, including South Korea. Most importantly, amending and consolidating the existing legislation pertaining to cyberterrorism is an international priority. It is recommended to accept counterterrorist legislations, discuss new provisions on cyberterrorism, integrate cyberterrorist response and crisis management systems and diversify operating system software. Also, implementation of a reporting procedure for the private sector is recommended for public-private cooperation and coordination in cyberterrorism prevention and response efforts.

With regards to the use of the Internet for terrorist purposes, results indicate terrorist organizations were using the Internet for various purposes. Accessibility to uncensored information on the Internet has made it more cost-effective and enabled aggregation of dormant members through websites, chat rooms and online
discussion sites. In addition, the Internet served as a valuable tool for collecting information on tactics, information about the target victim, and ways to avoid getting arrested. In response, law enforcement agencies bolstered their surveillance capabilities and inter-agency coordination and cooperation. Also, results indicate oppressive management and strategy had the paradoxical effect of augmenting efficacy of terrorist organizations. It is recommended for law enforcement agencies to develop an understanding of the relationship between technology and terrorism, develop investigation techniques, collect information on terrorist organizations, identify potential terrorists, and use technical tools to disrupt terrorist plans.

The academia should also participate in this endeavor with further research. Research thus far has not been able to provide any practical results on what responses work against terrorism, and the fact is that there is no empirical evaluations of counterterrorist strategies on the Internet used thus far. This study indicates only a state-lead response can understand the terrorist use of the Internet and execute countermeasures. Therefore, there should be further research on the terrorist use of the Internet and its future trends, along with further research on related subjects.

As terrorist organizations evolve continuously through constant acquisitions of new technological methods, cyberterrorism is unavoidable and inevitable. The best response to this type of threat is security provisions that continue to change and improve to minimize the cyberterrorist threat. Due to lack of research on this topic, researchers should start from cyberterrorist attitudes, acts, methods and targets and apply innovative research methods to produce new knowledge on cyberterrorism. At the same time, a major finding in this research is that in order to prevent cyberterrorist attacks and bolster cyberspace security, there needs to be innovative and meaningful interaction between the government, the private sector, and the citizens. Therefore, this is where the discussion should start on finding the most optimal approach to respond to cyberterrorism and minimize its impact.
In conclusion, the most pressing matter for South Korea is establishment of safety measures for cyberterrorism and further research on the topic. Furthermore, individuals and private companies should prepare security measures and reporting protocols. Also, with regards to investigations in cyberspace, a cooperative system should be created to promote information exchange between law enforcement agencies and cyberviolation response institutions. Considering the current trend of terrorist using the Internet as a means, it is imperative to establish a cooperation system between law enforcement agencies and internet service providers, and also between public and private sectors, government agencies, and furthermore, an international cooperation system between nations. These cooperation systems should be given priority to prepare a prudent and effective response system against the threat of cyberterrorism,
Chapter 1

Introduction
I. Research Purpose

After the 911 attacks on the 11th of September, 2001, terrorism has evolved to a new form of terrorism and this new form of terrorism has become more networked, diverse, and complex. In the center of this evolution is cyberspace being used as a means of terrorism. With the coming of the information age, cyberspace pervades many aspects of our everyday life, both real and imaginary, and directly influences our life and society. Thus, it is hard to simply ignore cyberterrorism and threats to cyberspace, which is already deeply ingrained into our everyday life.¹)

Cyberterrorism threatens our live in diverse ways. For example, recent DDoS

¹) In 2003, in the so-called ‘1.25 internet disaster’, major telecommunication networks all around South Korea went to a halt. In 2004, an attack from what is assumed to be an organized hacker group from China incapacitated security systems in major South Korean institutions such as the Parliament, the Korea Institute for Defense Analyses and the Korea Atomic Energy Research Institute, resulting in leaks of classified information and e-mails of key figures. In 2009, in the so-called ‘7.7 DDoS disaster’, major government agencies, website portals and bank websites in South Korea and the United States were temporarily disrupted. These series of cyber-emergencies are a wake-up call to the threat of cyberterrorism and the necessity for a systematic response.
attacks and hacking of national government agencies initiated from China prove these threats are real. Examples of direct forms of cyberterrorism are DDoS attacks, the Stuxnet worm, hacking and use of botnets. Other forms of cyberterrorism are utilization of the Internet for logistics of traditional terrorist activity, recruitment, propaganda, training, education, financing, command & control, and procurement of supplies. UNODC defined this type of activity as “the use of the Internet for terrorist purposes” and classified this as issues with special concerns.

In particular, after the 911 attacks, there is no systematic analysis of the characteristics and the level of threat of various types of cyberterrorism, and most of the existent policies are narrow and solely focus on technical matters. UNODC recognizes cyberterrorism as a fundamental risk to national security and takes comprehensive approaches on cyberterrorism. Cyberterrorism is globally recognized as fundamental threats to national security as well. Therefore, there is a need to look into the topic with a more strategic approach, and consider more systematic and inclusive policies and responses.

In this regard, this research aims to introduce cyberterrorism as a new form of threat to our society, which reflects the distinctive characteristics of information society of the 21st century. By promoting public awareness of this threat, mass confusion can be prevented in case of a real cyberterrorist attack. Also, through analysis of new trends of cyberterrorism, this research intends to propose effective and systematic responses to cyberterrorism.

II. Research Scope and Content

This research is an international joint research conducted as a part of UN

Cooperation. Foreign agencies and experts participate in this research. This research intends to come up with effective, systematic, legal and political countermeasures by conducting scientific research on cyberterrorism, which threatens not only our everyday lives, but also national security. Primary research method is review of legal systems and documentary evidence.

The study is conducted cooperatively with foreign counter-cyberterrorist agencies and professionals whose empirical methodologies use qualitative data such as interviews with specialists and professionals in the fields and press release. Also, the most important theme dealt by UN agencies and international society, use of the Internet for terrorist purposes, is included in the study. As terrorists use the Internet as a means to committing terrorist acts, there is necessity to conduct research on this emerging issue. Thus, this study aims to analyze trends of cyberterrorism and propose countermeasures.

For this purpose, Yoon, Hae-sung(Associate Research Fellow, Ph.D. in Law) jointly conducted this research with eminent professionals in terrorism fields namely Joshua Freilich(Associate Professor, John Jay College of Criminal Justice, Director of START program), Steven Chermak(Professor, Michigan State University), Robert G. Morris(Assistant Professor, The University of Texas at Dallas), and Yun, Minwoo(Professor, Department of Police Science and Security, Gachon University). The joint researchers from different specializations divide their roles as follows,

First, Yoon, Hae-sung, as the principal researcher, i) organizes contents of the joint researchers’ study to avoid repetitions and gives feedback to improve quality of this research by complementing and amending the materials within researchers’ initial intention, ii) tries to conceptualize cyberterrorism and suggest ideas to facilitate international cooperation after reviewing response systems with other joint researchers, iii) analyzes and compares legal systems of different countries to find drawbacks in the system, and discuss implications of the findings, iv) analyzes South Korea’s penalty code regarding cyberterrorism and the current status of cy-
berterrorism in South Korea, and reviews response and cooperation systems against cyberterrorism, v) sums up joint materials and discusses overall proposals on countermeasures against cyberterrorism. This covers chapter 1, chapter 2, chapter 5, and chapter 6.

In chapter 3, Professor Yun, Minwoo empirically analyzes interviews of professionals on activities of law enforcement and intelligence agencies on use of the Internet for terrorist purposes in the United States and European countries. Also, he tries to suggest solutions on problems regarding cyberterrorist acts by traditional terrorists.

According to Yun’s research, Terrorism can be categorized by the type of support activities conducted for an attack and the organization itself. Such activities can be intelligence, human resources, recruitment, training, education, propaganda, instigation, financial support, weapon supplies and other forms of support activities. The advent of cyberspace has made such support activities easier, more clandestine, less costly and faster. This allows terrorists to act with more destructive impact with less resources and capabilities. On the other hand, it makes counter-terrorist activities, such as detection and elimination of terrorists and prevention of terrorism, more difficult for government agents.

As such, this research discusses the terrorism of today that occurs not only in the real space consisting of sky, ocean and earth, but a new form of real space consisting of cyberspace. Also, against the backdrop of convergence of national security, public security, crime and warfare, this research discusses the threat against national security of complex terrorism, and presents the relevant counter-terrorist response systems in major international institutions and countries. For this purpose, this research synthesizes materials from observations, training sessions, seminars, conferences during visits to the United States, the Russian Federation, Israel and Austria during the last several years, and materials from interviews with various professionals on the subject through various opportunities such as personal contact, and materials from official reports and academic papers.
from various national security think tanks and government agencies, and also media reports. Through this synthesis of materials from diverse sources, this research describes the reality of the threat of a more complex form of terrorism of today observed in various major countries around the world and integrative counter-terrorist response systems in international institutions and individual countries.

Joint researcher Professor Joshua Freilich categorizes cyberterrorist cases after the 911 attacks into a typology, explicates the characteristics of each type of cyberterrorism and discusses their implications. Also, with another joint researcher Professor Steven Chermak, he conducted a research on enforcement of the law on the use of the Internet for terrorist purposes in the United States. This research material is covered in detail in chapter 4.

In this research, a review was conducted on previous research on how the Internet is used by terrorists, political extremists and their supporters, and three major issues are extrapolated for discussion, which are as follows. First, the research examines how internet is being used by terrorist organizations, and discusses the contents posted on websites of terrorist organizations. Second, the research discusses purposes of terrorist organizations for using the Internet, and emphasizes the reason why terrorist organizations use the Internet as one of their resources. Third, the research examines how law enforcement agencies respond against terrorist threats from the Internet.

Results from Freilich’s research indicate terrorist organizations use the Internet for various purposes. Accessibility of prohibited information on the Internet makes it a useful propaganda tool for terrorist organizations, and another advantage of the Internet for terrorist organizations is that they can contact potential recruits through websites, chat rooms and online discussion pages. Also, information on tactics, ways to collect information on targets, ways to avoid capture can be found on the Internet, making it a valuable tool in performing certain operations.

Meanwhile, law enforcement agencies are aware of the emerging threat of use of the Internet by terrorists, and police response to this threat is mainly strategic,
focusing on establishing the necessary infrastructure and policy mechanisms. Furthermore, emphasis is given to the importance of understanding the relationship between terrorism and technology in the evolving information society.

Results from Chermak’s research indicate law enforcement agencies attempt to monitor use of the Internet by terrorists, and this involves several tasks in the process. First, law enforcement agencies must expand their technological capability to monitor targeted terrorist organization. As strategies to disseminate information via internet keep evolving, understanding implications from the information is getting harder. Second, it is difficult to focus on a specific target, because interactions in cyberspace is almost exclusive. Third, while there are positive changes in law enforcement agencies such as establishing information reception capabilities and improving information sharing across all agencies, but there is still room for improvement. Most major terrorist organizations pose a threat to the world, and this requires international cooperation between government agencies. The point is that significant time and effort is needed to establish relations and trust to develop a cooperative relationship.

Joint researcher Professor Robert G. Morris’s research proposes counter-cyberterrorist policies based on legal responses and cyberterrorism trends in the United States. This research material is covered in detail in chapter 2. In this research, it is pointed out that in case of the United States, although there is no definitive evidence that there was a cyberterrorist attack against her citizens, nevertheless there were a political cyberattacks in the past, and therefore a real cyberterrorist attack is only a matter of time. Thus, efforts at all levels of law enforcement agencies are necessary to deal with cyberterrorist attacks and prevent them. Also, it is of utmost importance that threat and impact of cyberterrorism be minimized through education programs on cybersecurity for the general public and the private sector. In light of this, the research examines law enforcement response systems, international cooperation, and education and training programs for the general public and the private sector on the cyberterrorist threat,
Furthermore, the research examines trends in academic research in the United States on cyberterrorism, and discusses the future prospect of this trend in chapter 6.

The basis of this research scope is first the difficult task of conceptualizing cyberterrorism, and second the important consideration that this is an international joint research. Conceptualization of cyberterrorism affected the entire organization of this research, and the efforts to integrate research materials was an almost impossible task due to different thoughts and research materials from different joint researchers. Furthermore, this was a multidisciplinary research, with researchers specializing different fields of expertise such as the law, criminology and international law. This diversity inevitably lead to different arguments and conclusions from different joint researchers, each with their own conceptualization of cyberterrorism. To integrate this diverse research material, the principle researcher took a broad approach to the conceptualization of cyberterrorism.

Another important factor in the decision to use the broad conceptualization of cyberterrorism is that it includes the ‘Terrorist use of the Internet’ of the UNODC as an aspect of cyberterrorism. Despite the logical fallacies in dealing with cyberterrorism in general and use of the internet by terrorist organizations as the same subject matter, this field is rapidly emerging, and the current trend of the conceptualization of terrorism is becoming more inclusive and broader after the 911 attacks, and thus the same trends in the conceptualization of cyberterrorism is an issue that cannot be ignored. Broadening of the conceptualization of terrorism is inextricably linked to the broadening of the conceptualization of cyberterrorism. Therefore, terrorists use of the Internet should be examined as a form of cyberterrorism. With these considerations in mind, the broad conceptualization of cyberterrorism was necessary for setting the scope of this research, integrating research materials on trends of terrorist use of the Internet, counterterrorist measures, strategy and objectives on the use of the Internet by terrorist organizations and law enforcement response to cyberterrorism. With this re-
search scope, this research is organized as follows.

Chapter 1 examines trends of cyberterrorism and responses to cyberterrorism and discusses necessity and purpose of this research.

Chapter 2 reviews general issues of cyberterrorism. This chapter is divided into 3 parts, which are definition of cyberterrorism, international cooperation system in cyberterrorism response, and analysis of and implication from cyberterrorism response system of major countries.

Chapter 3 explains terrorist use of the Internet and counterterrorism measures. The discussions go through part 1 and part 2. In relations to terrorist use of the Internet, terrorist threats though cyberspace is reviewed in part 3. In following parts 4 and part 5 transformation of mode of warfare and counterterrorism measures are reviewed. Lastly, in part 6, Open Source Intelligence is suggested as a counterterrorism measure.

In Chapter 4, strategies, objectives, and legal responses revolving around terrorist use of the Internet is analyzed. This chapter consists of 5 parts, which are introduction, the strategies used to harness the power of the Internet, understanding the rationale for using the Internet, law enforcement responses to terrorism on the Internet, and conclusion.

Chapter 5 introduces current condition and legal system of cyberterrorism in the Republic of Korea. In part 1, the author overviews the Republic of Korea's penal measures and cases pertaining to cyberterrorism. Part 2 introduces response system and conditions on cyberterrorism in the Republic of Korea, and countermeasures for cyberterrorism in the Republic of Korea is referred in Part 3.

Last in chapter 6, core issues from each chapters are summarized, and implications from the research are suggested. Also, trends in academic study on cyberterrorism and importance of further research are pointed out.
III. Research Method

The main aim of this research is to categorize cyberterrorist cases and profile their characteristics by analyzing open information and interviews. To achieve this goal, international joint research with eminent foreign terrorism agencies and professionals is conducted. First, literature review is conducted to analyze existent domestic and overseas legal systems and suggestions for improvement are proposed. Second, a joint research to synthesize theoretical model of counter-cyberterrorist policies is conducted along with foreign specialists. Third, feedback between internal and external joint researchers is exchanged to discuss and propose effective counter-cyberterrorist policies.

With this methodological framework in place, this research mainly focuses on facts and realities by analyzing existent discussions on counter-cyberterrorism and existent cyberterrorism response systems. Along with research materials from foreign joint researchers, consultations with domestic professionals and practitioners are also analyzed as qualitative data. There is also theoretical review on conceptualization and typology of cyberterrorism. A workshop was conducted to collect information on the current status of cyberterrorism, cyberterrorism response systems, countermeasures and their typology, and legal systems. Empirical analysis was also conducted on cyberviolation, by types and categories, mostly by the foreign joint researchers.
Chapter 2

General Issues of Cyberterrorism
I. Definition of Cyberterrorism

1. Introduction

The domain created by computer system networks is defined as Cyberspace. Cyberspace is an important space for social activities, and such social activities are sustained by computer systems and networks. If a computer system and network that have important functions for a nation, an enterprise or a person are damaged or disrupted by domestic or international attacks, severe damage is incurred on the victimized nation, enterprise or person. Therefore, in this modern age of information society, a violation of safety of cyberspace, comprising computer systems and networks, can be seen as a threat as serious as an attack on territory, maritime territory and territorial airspace.3)

In research regarding cyberviolations, various terms and concepts are used akin to cyberviolations, such as cybercrime, cyberterrorism, cybersecurity and cybersafety. Among these related concepts, cybercrime is the most frequently used, whereas the most commonly used concept is cyberterrorism. This study intends to focus on cyberterrorism. Here, cyberterrorism is a type of cyberattack, and conceptualization approach of this concept of cyberterrorism is objective and realistic, discarding policy or legal considerations such as national security and crime. Therefore, a cyberattack can either be cyberterrorism or cybercrime, depending on the circumstances concerning national security or the social norm.

As this indicates, there is no clear academic definition of cyberterrorism, but ‘cyberterrorism’ can be generally seen as an ‘act of disrupting critical infrastructure such as energy, transportation and public facilities by using cyber tools for the purpose of threatening the government or its people.’4) In other words, the concept of ‘cyberterrorism’ differentiates from the conventional definition of ‘terror’ in that unlike terror, which utilizes physical methods, cyberterrorism utilizes software and networks in cyberspace to commit an act of terror.5) In what follows, definition of cyberterrorism will be discussed in detail.

2. What is Cyberterrorism?

Technological development has always been an indicator of progress for human


5) Meanwhile, National Security Management Act(Presidential Decree 267) Article 2 uses the term ‘cyberattack’, and defines it as an act of aggression of illegally trespassing, disrupting, destroying national informations network or stealing or damaging information by means of electronic methods such as hacking, computer virus, logic bomb, mail bombing and denial of service.
beings. Such improvements have resulted in ease of movement, enhanced safety and security, healthier lives, more fruitful economies, and enhanced communication. However, with any development, there is generally the potential for it to be exploited or misused.

More specifically, digital computing technology is easily one of the most profound technological developments in terms of impacting the daily lives of most human beings. Modern societies use this technology in both unsecure and secured formats for everything from communication (e.g., computer networks, the Internet, telecom systems) to the control of critical infrastructure components (e.g., hydro control, electrical power grids, homeland defense). While the results of these developments are far more positive than negative, the fact is that individuals and/or groups that wish to disrupt or exploit an adversary, whether that might be an individual person, a business corporation, or a government, may use secured or unsecure formats of digital technology to their advantage, just as would those with good intentions.

For example, terrorist organizations may use unsecured formats of digital technology, such as the Internet, to share information or intelligence, garner political support for their cause, organize a social movement or even an attack can potentially find a way to exploit cybersecurity vulnerabilities to reach their goals. Such events remain a serious threat to society. This introductory chapter outlines cyberterrorism in general, including variation in defining cyberterrorism and distinguishing it between information warfare, outlines different threats from cyberterrorism (i.e., attacks on a nation’s critical infrastructure versus attacks on specific information systems whether operating under the auspices of a nation or of a private corporation), and explores the current state of the literature surrounding cyberterrorists along with recent events that may be considered acts of cyberterrorism. At the close of the chapter, an overview of some of the more famous cyberterrorist attacks are presented, along with their analogs, that have occurred across the planet in recent years.
3. Definition of Terrorism, Cybercrime and Cyberterrorism

A. Comparison between Related Concepts

In order to fully understand cyberterrorism, it is important to consider the intersecting roles between cybercrime and traditional terrorism. Each have no single definition and both have been the source of considerable debate, regarding how to define them, respectively. Many related concepts exist that may cause some confusion, example of which are cybercrime, cyberwarfare and cyberattack. Here, various related concepts will be examined in order to differentiate them from the concept of cyberterrorism.

Cybercrime can be generally defined through criminal behaviors that utilize some aspect of cyberspace or computing technology. This involves many different types of cyber-related behaviors, These behaviors can be sub-divided into four primary categories. Important thing is that although there is overlap between forms of results and acts of cybercrime and cyberterrorism, cybercrime does not mean cyberterrorism in its broad conceptualization. Particularly, when cyberterrorism is seen as a form of terror, it can be seen as an international crime under the longitudinal aspect of international criminal law (therefore principle of aut de clere aut judicire and principles of universalism can be discussed), whereas cybercrime is seen as either domestic or extraterritorial international crime (crime under latitudinal aspect of international criminal law). For these reasons, cyberterrorism and cybercrime should be seen as different types of crimes.

Also, cyberwarfare means an act of aggression by use of the Internet by a state,

The fact that a state is the aggressor can mean much more serious consequences, and while it is very similar to cyberterrorism in form, the aggressor and purpose of the act is different from cyberterrorism. With regards to these differences, there is an ongoing discussion on whether regulations that apply to law of war and armed conflict under traditional international law can be applied to cyberwarfare.

Additionally, cyberattack can be differentiated from cyberterrorism in that it is not a legal concept, but rather an expression focusing on a phenomenon.

Cyber-trespass involves an encroachment on the use of copyrighted materials or online ownership. When a computer hacker gains access to a secured system through illegitimate means, they are using networks that do not belong to them, and would thus be considered cyber-trespass.

Cyber-deception/theft involves the theft of intellectual property, trade secrets, money, etc., via malicious computer hacking, or unauthorized access with the intent to steal. Cyberporn is self-explanatory and is not directly related to cyberterrorism for the purposes of this report. Cyberviolence, however, involves the use of the Internet to send or relay injurious, hurtful, or dangerous materials over the Internet. For example, this might involve sending threatening messages or videos via email or through a social networking site. Cyberviolence may also involve the transmission of materials online that could be used in a physically or virtually violent manner. Such might involve the sharing of bomb-making guides, warfare strategies, or information to help an individual learn hacking techniques that could later be used in a criminal or violent capacity.

As noted by Holt (2012), the breadth of cybercrime makes it somewhat difficult to define cyberterrorism in any consistent manner. This reality is primarily driven by the fact that many people who engage in cybercrime are not terrorists, do not have radical ideological goals, and do not communicated with extremists in any regard. However, many of the crimes that they might commit, were they committed by a terrorist, would constitute cyberterrorism. In short, there are considerable differences in the motive of the cyber criminal and the cyberterrorist,
To more fully understand cyberterrorism, it is important to have a firm grasp of physical terrorism. Across the globe, nations do not fully agree on what constitutes a terrorist event occurring in the physical world. This is due to differences in cultural norms, religious beliefs, and politics in general. In fact, scholars have identified little consensus across hundreds of different definitions of physical terrorism. Terrorism can be defined as “the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change.” In this sense, terrorism is intended to generate fear within a population with the hope of resulting in some form of political change. The primary difference between a terrorist and an ordinary criminal is that the terrorist acts as a sub-national entity.

Cyberterrorism has been defined in many ways and may sometimes be confused with information warfare, electronic warfare, or information operations. While perhaps consisting of equivalent techniques, cyberterrorism is primarily distinguished by intimidation of civilian enterprises via the destabilization of critical infrastructure data and/or information. The Center for Strategic and International Studies (CSIS) defines cyberterrorism specifically as:

"The use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population."


Alternatively, the National (US) Conference of State Legislatures has defined cyberterrorism as:

“… the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically…”

Between this variation in definition, cyberterrorism encapsulates many forms of cybercrimes, which may or may not constitute cyberterrorism. Such include any type of criminal activity that transpires in cyberspace including general forms of malicious computer hacking and/or cyberattacks (e.g., denial of service attacks, spam, spyware, phishing, virus attacks, cyber squatting, etc.). Such acts of terrorism may be direct (e.g., attacks on infrastructure) or indirect through the generation of revenue via cybercriminal techniques (e.g., credit fraud and identity theft).

B. Cyberterrorism vs. Information Warfare

In all, it is important to consider differences between cyberterrorism and information warfare\(^{12}\) as well as between terrorist use of the Internet and actual cyberterrorism.\(^{13}\) FBI Director Robert Mueller, among many academics, distinguishes between cyberterrorism and terrorist use of the internet, Denning's more recent definition of cyberterrorism\(^{14}\) may be the best-known definition of


cyberterrorism,

“[Highly damaging computer-based attacks or threats of attacks by non-state actors against information system when conducted to intimate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction or disruption against digital property].”

As discussed by Ballard et al. (2002), there are four main categories of attack that surround both cyberterrorism and information warfare,\(^1\) These include: Infrastructure Attacks; Information Attacks; Technological Facilitation; and Promotion. Each of these components is defined below. In the following sections, each component of cyberterrorism is discussed in greater detail.

Infrastructure Attacks include those that are designed to disable or destroy a system that contains critical data.

Information Attacks involve those whereupon the goal is to damage, destroy, manipulate, or otherwise compromise the content of electronic files or media.

Technological Facilitation involves the use of cyber technology or digital communication to coordinate and/or communicate plans for a terrorist attack, to incite an attack, or to assist in a terrorist event in general.

Promotion involves any use of cyber communications technology to promote the cause of a terrorist group, to recruit members, to solicit information, or to generate revenue (e.g., fundraising).

\(^{124}\)

C. Cyberterrorism and the Terrorist Use of the Internet

Another ongoing discussion is whether to consider the use of the Internet for terrorist purposes as cyberterrorism. The UN adopts a broader concept of cyberterrorism in defining the use of the Internet for terrorist purposes as a form of cyberterrorism. However, from the perspective of international law, if this broadest concept of cyberterrorism is adopted, an act under such definition of cyberterrorism cannot be always considered an international crime from a longitudinal aspect. However, adopting the most broadest concept of cyberterrorism has the advantage of defining an act with more detail, but because it is ambiguous in issues and criteria concerning human rights (e.g., freedom of speech), it is vulnerable to controversy concerning the principle of legality.

4. Typology and Threats of Cyberterrorism

A. Cyberterrorism Threats to Critical Infrastructure

The USA Patriot Act of 2001 (and subsequent updates) defines the critical infrastructure as "system and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, national health or safety, or any combination of those matters." The US Government identifies 12 areas as critical infrastructures requiring some form of protection from potential threats. These include Agriculture and Food, Water, Public Health, Government, Defense Industrial Base, Information and Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry and Hazardous Materials, and lastly, Postal and Shipping.

A cyberattack disrupting or disabling any of the above mention components could potentially have devastating effects, ranging from the loss of human life to
financial harm to both private and federal agencies. As an example, the 9/11/2001 attacks on the World Trade Center buildings in New York City were devastating primarily in the loss of innocent life and property damage, but the mass transportation industry was harmed due to disruption of service in the wake of the attacks. The vulnerabilities underlying critical infrastructure systems make them attractive targets for terrorist organizations as a successful attack could result in large-scale operational and economical damage.\textsuperscript{16}

Each critical infrastructure has its own specific vulnerabilities to cyberterrorism, the shared issue being reliance on digital communication and network access to operations control. Banking and financial institutions may be less vulnerable as a whole due to most operating on private networks, however, as noted by Taylor et al. (2011), a successful attack on a particularly important financial organization, such as a stock exchange, could have devastating effects with a single cyberattack from a terrorist group.\textsuperscript{17} Alternatively, water and electrical components too rely on digital communication networks to maintain safe operations. One successful attack here could have immediately devastating effects resulting in the loss of life. It is important to note, however, that such components may be at a greater risk of vulnerability from inside employees, rather than a terrorist group,\textsuperscript{18} however, recent reports suggest that outside hackers have penetrated critical infrastructures in China and North Korea.\textsuperscript{19}

Across the globe, transportation networks rely on networking technology to ensure safe and secure commerce. Many have raised concern about a cyberattack on transportation networks, however, many of these systems, such as air traffic

\textsuperscript{18} Institute for Security Technology Studies, 2012. (http://www.ists.dartmouth.edu/)
control, are largely custom designs with built-in redundancy protocols to protect against system failures, along the lines of what could potentially happen in a cyberattack from a terrorist group.\textsuperscript{20} The primary vulnerability of transportation infrastructures, regardless of how secure their particular systems are, is that they rely heavily on other critical infrastructures. If power and communications networks are disables, so too would be any transportation network that relied on other infrastructures to operate.\textsuperscript{21}

In the United States, there is concern of a surprise cyberattack on the critical infrastructure that would, with a single event, be catastrophic. In fact, there may have already been cyberattacks on the critical infrastructure in the United States, but none have been linked to terrorist organizations, As noted, much of the critical infrastructure that relies on dedicated digital programming to operate has built in redundancy protocols in order to operate in the case of a systems failure. Such failures are not uncommon normally and have only minor effects on the population at large. Furthermore, different components of the critical infrastructure are not linked directly, thus a successful attack on a large portion of the critical infrastructure by a terrorist organization would unlikely be catastrophic, though some systems rely upon one another to operate. In the end, much of the fear of cyberterrorism on the critical infrastructure is believed to be driven by and large by a lack of education about the topic and media portrayals of terrible events.\textsuperscript{22}

The critical infrastructure and be broken down into three subsequent categories


of assets including 1) physical, 2) human, and 3) cyber assets.

Physical assets involve tangible property as well as intangible information. This includes facilities, real estate, products, and information. In the United States, the bulk of physical assets are privately owned, The US federal government owns approximately 15% of physical critical infrastructure assets in the country, which makes securing those assets somewhat challenging.

Human assets refer to the people involved in the legitimate operation of the critical infrastructure as well as those who pose a threat (e.g., by having access to control systems).

Cyber assets refer to all information hardware, software, data, and networking that are used to maintain and operate the assets.

B. Debate on the Threat of Cyberterrorism towards Critical Infrastructure

Some have suggested that the cyberterrorism threat to the critical infrastructure may not be as big of a concern as once thought. In fact, a study conducted in 2007 suggests that the cyber prowess of violent terrorist organization members is not superior to that of the general population, thus the threat of cyberterrorism should be downplayed. This study, based on a random sample of over 400 members of Islamist groups identified as violent, found that less than 2 percent jihadists had a computing background. Of those, the study reports that far fewer had a mastery of the high level skills needed to carry out an act of cyberterrorism, However, an act of cyberterrorism does not have to come from a terrorist organization directly.

An additional threat of cyberterrorism not yet considered is that of the cyber-mercenary. If terrorist organizations do not possess members who have the capability of successfully carrying out a cyberterrorism attack, what is to stop them...
from contracting with an outside party? Some have argued that while possible, this is unlikely. Conway (2011) suggests that by contracting out to hackers with the requisite capabilities would compromise the operational security of the terrorist organization, opening up the door for infiltration by the opposition.24) Further, if a terrorist organization does not have the technological skillset to fully understand how to carry out such an attack, then how are they to know how to gauge the capabilities of the hired help?

C. Cyberterrorist Threats to Information Systems

Cyberterrorist attacks on information systems may not have the potential for mass destruction as to threats toward critical infrastructure components, but disruptions to information systems have the potential for major economic damage to both governments and private corporations.25) Further, considering the complex skillset required to successfully carry out an attack on the critical infrastructure, attacks on specific information systems (e.g., a website), such are probably more likely candidates for success.

Attacks on information systems, whether from a terrorist organization or from a warring nation, are intended to damage, destroy, or alter digital content stored within a particular system. In such attacks, only information is compromised, physical hardware remains undamaged, in general.26) These attacks vary considerably in design. For instance, they might involve the use of malicious programming, typically associated with cybercrime, such as Trojans, viruses, or worms, denial of service attacks (DoS), and virtual computer takeover/intrusion to name a

few. Or, they may involve the defacement of a public or private webpage. Such behavior is typically referred to as malicious computer hacking. An overview of computer hacking is provided by Morris and Blackburn (2009) who discuss how the term “hacking” has changed over the decades and is now commonly associated with criminal or malicious activities.\footnote{Morris, R. G. & Blackburn, A. G., Cracking the code: An empirical exploration of social learning theory and computer crime. Journal of Crime and Justice 32, 2009, pp. 1-34.}

Though much additional research is warranted, the research to date suggests that computer hackers are more commonly male, though some female hackers exist,\footnote{Morris, R. G. & Blackburn, A. G., Cracking the code: An empirical exploration of social learning theory and computer crime. Journal of Crime and Justice 32, 2009.} are generally younger adults with little to no history of traditional criminality (e.g., theft, burglary, etc.). In the U.S., they tend to come from middle- to upper-class families, and no longer have to have a dedicated education in computer science in order to carry out hacking attacks.

Of particular concern, as noted by Taylor et al. (2011), is the use of a cyberterrorist attack in conjunction with a physical attack. Taylor et al. refer to this cyber event as a “force multiplier” to a general terrorist attack.\footnote{Taylor, R. W., Fritsch, E. J., Liederbach, J, & Holt, T. J., Digital Crime and Digital Terrorism, 2\textsuperscript{nd} Ed. ,NewYork: Prentice Hall, 2011.} As an example, if a terrorist organization were to successfully implement an attack on the ground, and were successful in disabling various components of the critical infrastructure, then the effectiveness of the attack would be amplified (e.g., emergency response delays due to loss of communication).

Hildreth (2001) discusses the potential for information warfare to be used by China and that country’s outright acknowledgement of the potential for its use in military operations. Reports have also been made that China has attempted to assemble a unit of computer hackers with the intention to launch cyberattacks against the United States. It is believed that China has already launched successful
attacks against U.S. information systems in recent years.\textsuperscript{30)}

D. Other Threats from Cyberterrorism

Digital technology has also enhanced terror organizations in their ability to share information whether in support of an attack, for purposes of recruiting, or for purposes of generating revenue.

Discussed in detail by Taylor et al. (2011), cyberterrorism via Technological Facilitation involves the use of cyber technology or digital communication to coordinate and/or communicate plans for a terrorist attack, to incite an attack, or to assist in a terroristic event in general. In terms of coordination on the ground, cyber communication technology has dramatically shortened transmission time from one member/s to the next, Web forums, social networking sites, video conference chatting software, and voice-over-internet-protocol (VIOP) can all be used by terror organizations to enhance their efficiency in communication.

Digital cryptography has in recent years become very easy to learn. It is now very easy for a person to hide information into a digital file (e.g., an image) that appears to be harmless. Many freely available software programs now exist that can easily encrypt messages and information, which can then be accessed via the Internet, decrypted, and utilized for the purposes of a terrorist attack. In fact, reports of data encryption use by terrorist organizations were reported in conjunction with the September 11, 2001 attacks on the United States.\textsuperscript{31)} One report suggested that al Queda used intelligence hidden via encryption on pornographic websites and sports chat rooms. Such information could have been accessed by any person at any time, but the shear vastness of the files stored digitally make


it near impossible to search for terrorist related information,

Terrorist groups also use digital technology for purpose of disseminating propaganda intended on garnering support from individuals. Promotion involves any use of cyber communications technology to promote the cause of a terrorist group, to recruit members, to solicit information, or to generate revenue (e.g., fundraising). Most major terrorist organizations have an Internet presence and can use digital technology as a tool, just as would any legitimate business.

E. Fear of Cyberterrorism

Another consideration, discussed by Stohl (2007) is the role of fear within cyberterrorism. Most cyberterrorism experts tend to consider cyberterrorism (in the form of a major attack) as less of a threat compared to conventional terrorism simply for the fact that a successful cyberattack is either beyond the reach of terror organizations or that naturally occurring systems failures provided industrialized nations with a means to respond to such an event were it to stem from a terrorist group. However, the fear generated by the threat of a massive cyberterrorist attack, akin to the bombing of Pearl Harbor, may be more a tool for public and private sector organizations to generate a continuous revenue stream, such as in the solicitation and sale of protection software.

The fear generated by the threat of terrorism stems from public and media confusion regarding the reality of the threat itself, Conway (2011) discusses the basis of this fear as stemming from two modern fears: fear of technology and the fear of terrorism. The fear of terrorism was modernized in the wake of the 9·11 attacks in New York. The fear of technology is more innate and has to do with a lack of public understanding on the inner workings of modern technologies, particularly computer programming. In general, people have no idea how complex

computing technologies work, or how to combat them. The arcane nature of technology, as perceived by those who do not understand it, is a source of anxiety. When this anxiety is tethered to a more understandable fear component, here terrorism, the product is an amplified or heightened sense of fear, which is intensified further by fears of random violence, Conway argues that journalists have become quite fearful of cyberterrorism for this very reasons which is why the topic receives the attention it does in the news media.33)

The types of cyberterrorism can be classified as the table below.

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition and Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information attacks</td>
<td>Cyberterrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various material therein.</td>
</tr>
<tr>
<td>Infrastructure attacks</td>
<td>Cyberterrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programming in a computerized environment.</td>
</tr>
<tr>
<td>Technological facilitation</td>
<td>Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.</td>
</tr>
<tr>
<td>Fundraising and promotion</td>
<td>Use of the Internet to raise funds for a violent political cause, to advance an organization supportive of violent political action, or to promote an alternative ideology that is violent in orientation.</td>
</tr>
</tbody>
</table>


5. Case Studies of Cyberterrorist Attacks

There have been many attempted cyberterrorist attacks across the globe in recent years. Most are not successful, but many are, and others may not even be detected. However, their effect size varies considerably. Successful attacks on the critical infrastructure are rare, having never occurred in the United States, but several of such have been seen in other countries though some debate may exist as to whether they were actual terrorist events. Attacks on cyber information systems, on the other hand, are much more common and also vary considerably in magnitude of effect. This section will provide a brief outline of some of the more famous successful and attempted cyberterrorism attacks that have occurred in recent years around the world.

A. Information System Attacks

There has been several attacks against information systems around the world, including cases in South Korea. The table below shows major cases suggesting that cyberterrorism is not only a problem exclusive to developed or highly technologically vulnerable countries but a threat to any countries.

<table>
<thead>
<tr>
<th>Date and Country</th>
<th>Attacker</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003, United States,</td>
<td>Titan Rain</td>
<td>A series of coordinated computer attacks against the US Department of Defense and several defense contracting organizations (e.g., Lockheed Martin) that included zombie attacks, spyware use, and viruses. Some speculate that the origin of the attacks were from China.</td>
</tr>
<tr>
<td>2009–present, S. Korea</td>
<td>Unnamed</td>
<td>Cyberattacks on computer systems in the US and South Korea stemming from North Korea. In June, 2012, a...</td>
</tr>
</tbody>
</table>
### General Issues of Cyberterrorism

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Name</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011, US</td>
<td>Unnamed</td>
<td></td>
<td>In 2011, 24,000 files were hacked from Pentagon from an &quot;unknown&quot; country.</td>
</tr>
<tr>
<td>2001, Sri Lanka</td>
<td>Unnamed</td>
<td></td>
<td>In 2001, the terrorist organization called the Tamil Tigers, of Sri Lanka, successfully carried out an act of cyberterrorism to disrupt government computer networks in Sri Lanka.</td>
</tr>
<tr>
<td>October, 2007, Estonia</td>
<td>Unnamed</td>
<td></td>
<td>A series of successful DOS attacks disabled the websites of many Estonian organizations. The origin of the attacks is argued to be from Russia. Denial of service attacks sometimes disrupted the public’s access to internet sites. <em>DOD classifies cyberspace as an active battlefront, just like land, sea, and air.</em></td>
</tr>
</tbody>
</table>

#### B. Logic Bomb Case

The oldest case of destruction of a critical infrastructure by a computer program is the explosion of a pipeline in Siberia during the Cold War. Cause of the explosion was confirmed to be a logic bomb stored in a software stolen by a Soviet spy from a Canadian software company. This explosion was known to be the most powerful explosion of the time, nuclear explosions being exceptions.

#### C. Conficker Worm

The Conficker Worm was a malware that affected computers around the world.

---


D. Stuxnet Worm

The Stuxnet Worm, found in the Fall of 2010, is theorized to have originally developed as a ‘cyber weapon’, intended to attack the centrifuge in Iran’s nuclear reprocessing plant at Natanz, Iran. The Stuxnet Worm used an exploit in the Microsoft Windows operating system to spread and attack Siemens industrial control systems and disrupt its operations. Unintentionally, the Stuxnet Worm had spread to about 44,000 computers and caused damage, including many computers in the United States and Germany.35)

Due to the complexity of this computer virus, there were suspicions that there was state intervention(United States and Israel) in its creation.36) James Lewis of the Center for Strategic and International Studies defined the Stuxnet Worm incident as the first case of cyberwarfare.

E. Distributed Denial-of-Service(DDoS)

Denial of Service attack is to attack a computer system or a network, If this attack succeeds, the victimized computer system or network is rendered


General Issues of Cyberterrorism

inoperable. This attack overloads computer resources or stops a network by exhausting bandwidth of the network.\(^{37}\)

**F. The Use of the Internet by Al Qaeda**

The infamous terrorist group Al Qaeda uses the Internet in a variety of ways to achieve their purpose. In fact, since 2005, Al Qaeda has made a strategic move to cyberspace from the real world as their main domain of activities.\(^{38}\) Al Qaeda uses cyberspace for communications and political acts to earn more supporters. Terrorists such as Al Qaeda uses the Internet to disseminate and acquire information on specific methods to achieve terrorist purposes, and also uses the Internet as a medium where terrorist groups can share their political views.

Al Qaeda uses the Internet to reach out beyond state boundaries to people who share their ideology and expect that when the time comes, those people will carry out terrorist activities. Since 2008, civic groups against terrorism in the United States saw this kind of Al Qaeda activities on the Internet as a problem and started making official complaints. Al Qaeda’s internet activity includes Facebook, YouTube and various blogs.\(^{39}\)

First, Al Qaeda uses the Internet to express their anger and frustration persistently. For terrorists, use of expression in cyberspace is a weapon. For example, Awais Younis, a 25 year old man born in Virginia Arlington, was arrested for disseminating threatening messages throughout the United States for terrorist purposes. At that time, Younis threatened on his Facebook account that he will deploy explosives. According to a document from Joint Terrorism Task Force of FBI, Younis had written technical details of making pipe bombs, and expressed

\(^{37}\) Stein Schjolberg, Terrorism in Cyberspace - Myth or Reality? (http://www.cybercrimelaw.net/documents/cyberterrorismism.pdf.)

\(^{38}\) Jarret Brachman, Watching the Watcher, Foreign Policy, 2010. 11. 10.

\(^{39}\) Jarret Brachman, Policing Al Qaeda’s Army of Rhetorical Terroists, 37 Wm. Mitchell L. Rev. 5225, 5228-29 2011.
his intentions to deploy three to four pipe bombs in subway cars of the
Washington D.C. rapid transit system. Selection of these particular targets was be-
cause these locations are where most commuters are and deployment of the
bombs may not be conspicuous.40)

Another example is Chesser, who was prosecuted for expressing threats in
cyberspace. One of the charges of the prosecution was that Chesser not only ex-
pressed threats, but also solicited terrorist acts from others. This solicitation was
posted on his blog and Internet bulletin boards, and he uploaded 200 books re-
lated to “Jihad, Islam and War” on Internet bulletin boards and his blog, and also
uploaded a book about “making preparations” for terrorism.41) The prosecution al-
so found in evidence discovered from the Internet that Chesser had connections
to Al Qaeda, and this charge was also added to his case,

6. Typology of Cyberterrorism

A. Basic Typology

In South Korea, cyberterrorism is categorized mainly by type of method used
or type of consequent damage.42) ‘Cyber Terror Response Center of the Korean
National Police Agency’ categorizes illegal attacks on computer systems and in-
formations network using electronic equipment such as hacking, virus dissem-
ination, e-mail bombs and DoS attacks as cyberterrorism, differentiating it from
hacking, which is simple security intrusion, identity theft, deleting or disseminat-

40) Affidavit in Support of Criminal Complaint at 2-5, United v. Martinez No. 10-4761-JKB (D.
Md. Dec. 8, 2010).
41) Jarret Brachman, Policing Al Qaeda’s Army of Rhetorical Terrorists, 37 Wm. Mitchell L.
42) Cyberterrorism is usually categorized from a practical point of view rather than an academic
point of view.
General Issues of Cyberterrorism

Table 3 Typology of Cyberterrorism of Korea National Police Agency’s Cyber Terror Response Center

<table>
<thead>
<tr>
<th>Type</th>
<th>Act of Violation</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simple Intrusion</td>
<td>Without legitimacy,</td>
<td>① Without access authorization or in excess of given access authorization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>② Intruding into an information network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i Access authorization: Authorization for a person to access resources of an information network at will</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ii Intruding into an information network: A person does not go through the recognition process necessary to use resources of an information network, in other words, the situation where a person is able to use resources of an information network at will can be considered as a violation.</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Using user accounts and passwords given to others without their consent for the purpose of intruding into an information network,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>※ Conceptually it is merely a form of simple violation, but it is separately categorized due to its pervasiveness.</td>
<td></td>
</tr>
<tr>
<td>Deletion and Dissemination of Data</td>
<td>A secondary consequence violating an information network, it is usually only possible after an intrusion of an information network has been committed</td>
<td></td>
</tr>
<tr>
<td>Mail bombing</td>
<td>Using executive commands and other means to send massive amounts of e-mails at once, so that a mail server cannot withstand, causing either disruptions in the mail server or the computer that which receives the email. This is a form of denial of service attack.</td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Sending massive amounts of data to an information network at once to cause an overload, disrupting normal operations.</td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trojan</td>
<td>Actively executing a precoded function in a program for a hacker to access information or control a system. It is hard to identify infections due to their disguise as useful utility programs.</td>
<td></td>
</tr>
<tr>
<td>Internet Worm</td>
<td>Expands throughout the Internet by means such as attached files in e-mails for the purpose of overloading</td>
<td></td>
</tr>
</tbody>
</table>

systems. When infected, legitimate files may be attached to outgoing e-mails, endangering disclosure of privacy.

Spyware
Implanted in open-source, share-ware or trial programs, any program with the capability to disclose information.

National Intelligence Service categorizes any cyberattacks that may cause much harm to national security or national interests as “Attacks against National Security,” typology of which are as follows.

<table>
<thead>
<tr>
<th>Type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks against State Confidential Documents, Resources, Facilities and Areas</td>
<td>In accordance with, National Intelligence Law article 3 and security task provisions, an attack against someone who manages state-confidential documents, resources, facilities and area.</td>
</tr>
<tr>
<td>Attacks by anti-State Groups, International Crime Organizations and Terrorist Groups</td>
<td>Cyberattacks by Anti-state groups, as defined by National Security Law article 2, and international crime organizations and terrorist groups defined by National Security Law article 3.</td>
</tr>
<tr>
<td>Attacks against critical informations infrastructure related to national security</td>
<td>Cyberattacks against managers of critical information infrastructure related to national security as defined by Act on the Protection of Information and Communications Infrastructure article 7.2항</td>
</tr>
<tr>
<td>Attacks against Critical National Technology</td>
<td>Cyberattacks against people who work with national critical technology as defined by the Act on Prevention of Divulgence and Protection of Industrial Technology</td>
</tr>
</tbody>
</table>

As such, cyberterrorism can be either defined as illegal attacks on computer systems and informations network using electronic equipment such as hacking, virus dissemination, email bombs and DDoS attacks, or as cyberattacks that may cause much harm to national security or national interests.

‘Operatory Regulations on Information and Communications Cyber Security Center, Article4(4).
B. Detailed Typology

Traditionally, cyberterrorism can be categorized by method of attack, in which case there are hacking, dissemination of malware, DoS attack and others.

Hacking means the act of obtaining illegal access, either physical access or electronic access, on network, system, application program, data and other information resources by someone who does not have authorized access. Dissemination of malware means the act of installing malware into a computer without the owner’s consent to steal user information, disrupt computer operations and network. DoS attack means the act of disrupting services and system performance by overloading the computer resources. Other types of attack include a complex attack that combines multiple methods of cyberattacks, such as those mentioned above.

Also, considering that Stuxnet Worm, which recently caused much disruptions around the world, was specifically designed for the purpose of destroying critical infrastructures such as power plants, airports and railroads, there is a need for specialized safety measures for each types of critical infrastructures.

As such, all types of cyberterrorism considered as a whole, including their attack methods, damages incurred, target of attacks and attackers, it can be conceptual differences between cyberwarfare, cyberterrorism(attacking critical informations infrastructure), ordinary violation of information systems and information, but under South Korean law, cyberterrorism is legally seen as an electronic act of violation. By this legal definition, cyberterrorism is an illegal act

45) Stuxnet, first discovered in June of 2010, is a virus programmed to destroy infrastructures such as power plants, airports and railroads. It easily infects other computers via a USB stick without network access, and once it infects programmable logic controllers(PLC) of certain Siemens SCADA systems, it can cause failures in the infected SCADA system such as malfunctions in electric currents, hydraulic pressure, temperature and valve intake.

of attacking informations network itself, an electronic act of violation against critical informations network that could cause major harm to national security and national interests by means of using electronic equipment for hacking, virus dissem-ination, logic bomb, and DoS attack.

<table>
<thead>
<tr>
<th>Type</th>
<th>Attacker</th>
<th>Attack Target</th>
<th>Attack Methods</th>
<th>Damages</th>
<th>Attack Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-warfare</td>
<td>State</td>
<td>Critical informations infrastructure - military facilities - infrastructure</td>
<td>hacking, dissem-ination of malware, denial of serve attacks, and others</td>
<td>Disruption of State-func-tions and Ability to wage war</td>
<td>Extra-territorial</td>
</tr>
<tr>
<td>Cyber-terrorism</td>
<td>State Terrorist Group</td>
<td>Critical informations infrastructure - military facilities - infrastructure</td>
<td>hacking, dissem-ination of malware, denial of serve attacks, and others</td>
<td>Disrupting social func-tions and spreading terror</td>
<td>Domestic Extra-territorial</td>
</tr>
<tr>
<td>Violation of Information System and Information</td>
<td>Crime organization Individual</td>
<td>- Ordinary in-formation sys-tem - information</td>
<td>hacking, dissem-ination of malware, denial of serve attacks, and others</td>
<td>Disrupting particular work and disclosure of information</td>
<td>Domestic Extra-territorial</td>
</tr>
</tbody>
</table>

7. Conceptual Overview from an Overall Perspective

A. Introduction

Although there is already is a cyberterrorism concept, people in ordinary society and the academia, particularly related fields such as security and intelligence professionals, use the concept of “cyberterrorism” indiscriminately. However, under international criminal law, the global consensus is that there is no legal concept that is recognized internationally as cyberterrorism. Due to this global consensus
that there is no legal concept, internationalization of crime of cyberterrorism can be seen as an impossibility from the principle of legality aspect. Therefore, the realistic alternative is to define a concept of cyberterrorism for domestic use by legislating domestic laws, although this would have very limited effect in establishing and preventing cyberterrorism. Otherwise, the appropriate way to deal with issues regarding cyberterrorism and principle of legality is to first decide whether a concept of cyberterrorism that includes both the narrow and broad definitions can conform with criteria of the principle of legality set by the European Court of Human Rights.

Additionally, if an internationally recognized conceptualization of cyberterrorism is an impossibility, an emphasis can be put on the act of cyberterrorism to avoid controversy concerning principle of legality. If there are conceptual differences among different countries and without adequate legislations, international cooperation on judicial assistance, especially with regards to extradition, is proving to be very difficult.

Concerning freedom of speech and use of terrorism on the Internet, as mentioned above, it seems obvious that there should be legal safeguards against terrorists such as Al Qaeda using the Internet to propagate and share political messages and rally supporters, but articles on the freedom of speech in the First Amendment of the United States Constitution can make complications. Currently, the First Amendment guarantees safety against violation of essential elements of freedom of speech, but expressions on the Internet that express provocation, propagation, inducement and conspiracy of terrorism are exempted from First Amendment protections.

47) In should be noted that in CR v. United Kingdom and Cantoni v. France of the European Court of Human Rights, even if the concept of crime is ambiguous and in the grey area, it has been judged that as long as there is a degree of foreseeability to the extent that anyone can perceive which act is a crime in terms of current concepts of crime, there is no violation of the principle of legality.
If terrorists are restricted to the point that they are unable to express themselves over the Internet, they will simply go underground to circumvent the restrictions set in place. This will make terrorists only more unpredictable. Also, openly recognizing propaganda and provocations of terrorists while allotting more resources to countering these propaganda and provocations is seen as a way of allowing least limitations of the First Amendment.\(^{(48)}\)

**B. International Conceptualizations of Cyberterrorism**

With regards to conceptualizing cyberterrorism, there are generally two opposing sides, one supporting a “narrow” concept and the other supporting a “broad” concept. Each position will be explained in what follows.

First, the narrow concept of cyberterrorism is defined as an act of attack using information systems, computers and particularly the Internet, that results in disruption of society in the real world and critical infrastructure, and real harm to life. The narrow concept of cyberterrorism prioritizes its concept as a “crime” and sees primary targets as computer systems, but it emphasizes that there should be some violation of law in the real world. Of course, there is some overlapping part with the broad concept of cyberterrorism, but they differ in that “real harm to life” is requisite in the narrow concept of cyberterrorism. Also, the narrow concept of cyberterrorism tends to have support from legal experts, but as mentioned above, the possibility of a narrow concept of cyberterrorism actually occurring is low, and requiring harm in the real world makes the narrow concept more conforming to the principle of legality, and as it necessitates enough punishment, it is a concept more consistent with the traditional concept of terrorism.

The broad concept of cyberterrorism defines cyberterrorism as an act of dis-

---

ruption or threat against a computer or a network to cause damage for social, ideological, religious or other similar purposes. The broad concept of cyberterrorism tends to be supported by policy makers, politicians and intelligence and security experts. This is because with regards to controversies concerning the definition of traditional terrorism, cyberterrorism can be treated as an exceptional form of crime. In other words, there is much possibility of occurrence, and there is no definitive harm or damage in the real world. In that it considers the Internet both as a means and an end to cyberattacks, the broader concept may generate legal controversy, and under the principle of disclosure, it can be seen as a rather broad concept.

Aside from the above controversy, there are several other smaller problems. Some experts on cyberterrorism express “terrorism” as a concept with a firm definition, but this is not true. In other words, “terrorism”, as an international crime, does not have an “internationally recognized” concept. For instance, in 2002 the EU defined terrorism as (1) Act committed with the aim of intimidating a population, (2) or compelling a government or international organization, (3) to perform or abstain from performing any act, but this definition has the disadvantage of being too broad a concept. In other words, even an act of arson on a bus during the course of a strike advocating changes in pension recipient qualification can be defined as terrorism. Also, there is no mention of “intent of spreading terror”, and this kind of broad conceptualization of terrorism could lead to violation of human rights. Moreover, the 1937 Geneva Conventions on deterrence and punishment of terrorism defines terrorism as (1) crime against the state, (2) intentionally promoting condition of terror, (3) in which part of that intention is against a person, a group or the general public, but there’s been controversy over the exact definition of the term “general public.”

In addition, Antonio Cassese defined terrorism as (1) Deliberately targeting civilian populations, (2) To spread terror amongst the general public, (3) with international crime perpetrated to achieve this end, (4) for a political purpose, but the
Hijacking Convention (Hague Convention) makes no mention of “political purpose” and rules of the International Criminal Court, which despite not mentioning terrorism nevertheless has the power to punish an act of terror as a crime against humanity, in most cases do not require “political purpose” as an actus reus. Under these circumstances, there was discussion over a draft of a comprehensive counterterrorism convention, but the draft did not pass due to differences of opinion between different states on the definition of terrorism.

C. Discussion

Terror and terrorism are generally used without strictly distinguished meanings as if they are the same. Generally, “terror” is understood as “an act of an individual or a group with political, religious, ideological or nationalistic purposes, which is a planned act to further such purpose, by means of kidnapping or assassination of a state VIP, destruction of critical infrastructure, hijacking or destruction of transports such as an airplane, large scale mass murder using explosives or chemical weapons, to influence national security or international relations, or cause social unrest.”

From the perspective of distinguishing terrorism from terror, ‘terrorism’ is understood as a ‘policy or political ideology using methods of terror such as assassination or assault to achieving any political purpose’ or ‘method of force or coercion that systematically uses terror to achieve a revolutionary, political or ideological purpose, which is one of the forms of illegal political extremism that threatens or disrupts individuals, societies or governments to destroy liberal democracy’, which distinguishes it from the concept of ‘terror’.

Likewise, cyberterrorism also currently lacks a single common concept backed

by consensus, Cyberterrorism has various definitions and the concept is constantly changing to this day. The broadest concept of cyberterrorism can be defined as an attack against an electronic communication network.\footnote{WordNet: A Lexical Database for English, (http://wordnetweb.princeton.edu/perl/webwn)} Furthermore, many experts consider attack against social infrastructure by using a computer network to be a common element of the definition of cyberterrorism. Here, ‘social infrastructure’ refers to infrastructure in the real world such as ports, airports, medical facilities and powerplants, but they can also mean the system itself consisting of operating software running on computer networks of large scale online markets, governments and public or private institutions.\footnote{J.F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyber Terrorism 4, Citadel Press 2003; Embar-Seddon, Cyber Terrorism: Are We Under Siege? 45:6 Am. Behavioral Scientist 1033, 1034, 2002.}

FBI provides a more specific definition, which is “The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”\footnote{Mudawi M. Elmusharaf, Cyber Terrorism: The New Kind of Terror, Computer Crime Research Ctr. 2004 .04. 08 (http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism)} The National Infrastructure Protection Center provides the most detailed and clear definition, which is “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.”\footnote{Clay Wilson, Computer Attack and Cyber Terrorism; Vulnerabilities and Policy Issues for Congress, 2003. 10. 17. (http://www.fas.org/irp/crs/RL32114.pdf)}

Here, infrastructure of a society refers to banking, finance, information, airport, port, health and health care, transportation, religious places of worship, government service, education centers, power and energy generation and distribution, manufacturing, agriculture and food, electricity and water supply, military defences and etc.\footnote{Among the definitions of cyberterrorism, an act which causes}
extensive and destructive outcomes is called cyberwarfare.

As discussed above, “cyberterrorism” is generally used without a commonly defined concept. This may lead to controversies, thus it is necessary to define detailed forms of act along with specific description of harm by that act. However, controversy is inevitable if the concept of terrorism is used, and there will be criticism that the difference between terrorism and cyberterrorism is ambiguous.

To respond to transnational crimes such as cyberterrorism, it is important to have a common definition. Defining crimes according to their characteristics will not only make crime investigation easier but also enable cooperation with other countries. Therefore, countries should put their effort to come up with internationally accepted definitions of terrorism, cyberterrorism, and cybercrime.\(^{56}\)

In this study, cyberterrorism is an act of disrupting computer systems, violation of informations or violation of electronics to spread terror or anxiety in a state or society. Thus, the premise in this study is that cyberterrorism can ‘spread terror or anxiety in a state or society’. Also the UN uses the broad concept, which includes using of the Internet by a terrorist group for terrorist purposes in the concept of cyberterrorism. For the reasons above, this study adopt the broad concept of cyberterrorism, because this allows effective preventive strategies against cyberterrorism, and it has the advantage of making extensive regulations on detailed forms of acts possible in international treaties should this come to pass.

The definition of “cyberterrorism” cannot be complete, because the very nature of cyberterrorism is inclusive. Also, because of the characteristics of “cyberspace”, new method and techniques keep coming out and some even suggest not making a definitive conceptualization of cyberterrorism. By not doing so, it allows the

\(^{55}\) Ruwantissa Abeyrantne, Cyberterrorism: The Next Great Threat to Aviation, 24 No. 1 Air $ Space Law. 4 .2011.

courts to liberally interpret definition of cyberterrorism, granting them the discretion to strictly punish and take care of cyberterrorism. Nevertheless, because of technological developments, laws governing cyberterrorism cannot keep up with the ever-changing methods and techniques of cyberterrorists, therefore it will be very difficult and meaningless to clearly define forms of cyberterrorism. Therefore, because cyberterrorism is in its nature inclusive and open-ended, it is necessary to enact laws in accordance to recent trends so that future forms of cyberterrorism can also be dealt with.\(^{57}\)

### II. International Cooperation System in Cyberterrorism Response

#### 1. International Characteristics of Cyberterrorism

Due to the international characteristics of cyberterrorism as explained above, limitations are inevitable for domestic legal response to cyberterrorism within the United States. Most literature on cyberterrorism takes an international legal perspective rather than domestic legal response within the United States. This international legal perspective on cyberterrorism can also be analyzed from various aspects. There is a discussion on whether cyberterrorism with catastrophic losses should be governed under the legal principles of war in international law, as it is close to an act of war. Foremost, with regards to cyberattacks, most brought up issues have to do with jurisdiction. In particular, most effective legal response against cyberterrorism is securing universal jurisdiction.\(^{58}\) Literature also often point out that a more expansive international convention should be ratified for co-

---


operation in investigation and judicial assistance of cyberterrorism.\textsuperscript{59} In fact, there is much cynicism against stricter punishment or domestic criminal law response within the United States.\textsuperscript{60}

In summary, the question lies in whether cyberterrorism exists in the real world, and whether terrorist groups or members of such groups can use information technology for the purpose of terror. With regards to this question on the reality of terror, there are those who take on a positive position and those who take on a negative position. If the negative position is valid, discussions by various parties including states on cyberterrorism are based on a false premise, and therefore it is inevitable that such discussions are nothing but political acts fearmongering terror among the public. On the other hand, if the positive position is valid, discussions on regulating cyberterrorism are well timed and an urgent matter for the safety and peace of the international community.

A. International Perspectives on Cyberterrorism

There were various arguments from the negative position. They are i) that in actuality there was no “notable” case of a terrorist attack using hacking or cracking methods on a government or a civilian company that could amount to achieving a terrorist purpose, ii) and that although cyberterrorism is said to incur losses greater than the 911 attacks as former president George W. Bush had stated, considering today’s technological systems, it is a false premise that there can be losses of human life or physical destruction through hacking or cracking methods, iii) and that for the terrorist groups, cyberterrorism is not a very feasible alternative compared to physical terrorism in terms of costs and techniques, iv) and that con-


sidering the differences between ideologies of hackers, crackers and cyberterrorists, it is very unlikely for a hacker to participate in a cyberterrorist attack and at most a hacker will do nothing more than merely providing necessary hacking techniques to the terrorists.

On the other hand, those on the positive position argue i) that there are allegations that terrorist groups such as Al Qaeda used significant amount of time on the Internet in acquiring methods to destroy critical infrastructure, and there is significant probability that such a scenario could occur, ii) that convergence between information technology and everyday life in cyberspace is proceeding rapidly, and recently there was a case of cyberattack groups known as the Elderwood gang and Comment Crew which attacked the security firm RSA in 2011, and another case called 'Stuxnet' that attacked Iran's nuclear power facilities in 2010. Reflecting upon these cases, the probability of is high for a cyberattack to result in actuality of social chaos(spread of terror) and losses in human life and property. iii) That a cyberterrorist attack can originate from any place in the world and because it is easier for the terrorists to hide behind the anonymity of cyberspace, it is an attractive method for the terrorists.

B. The Experiments on Cyberterrorism

Despite contrasting views on reality and premises, it cannot be denied that both positions have significant validity.

In this regard, there was an interesting experiment that used a simulation to test the strategic, technological and economic appeal to terrorists of a terrorist attack using the Internet. This simulated experiment, which was conducted by the United States Naval War College in 2002, the terrorist conducts a "digital Pearl Harbor" cyberterrorist attack. According to the results of the simulation, a single hacker cannot incur significant damage to the American informations system, but there is probability that a terrorist group can conduct a cyberattack that could
damage a specific part of the American informations system. However, consider-
ing that a significant amount of planning and funds are needed for such a cyber-
attack to succeed, it may not yet be appealing to terrorist groups. Nonetheless,
it seems such a cyberattack is possible if significant amount of funds are procured,

Whichever the case, the following aspects of cyberterrorism cannot be ignored.

First, facilitated by the development of information technology costs and man-
power needed for the commitment of a “cyberterrorist crime”, such as cracking
or disrupting access using increased traffic, targeting a government institution or
at least a financial institution, is decreasing. Second, high profile terrorist groups
started to use the Internet actively to spread their propaganda and for recruitment
and communications, and such use of the Internet is increasing qualitatively.

Third, considering the significant amount of cyberattacks by crackers or hackers,
the possibility of similar attacks by terrorist groups cannot be ignored. Fourth,
such an attack against a state without a well developed informations system like
the United States can be done with more ease and far more serious consequences.

2. Rules, Conventions and Laws regarding International Cooperation

   A. Establishment and Operation of International Rules

   There were various international efforts regarding international cooperation on
legal control and effective judicial assistance of cybercrime. However, efforts to
deal with cyberterrorism alone is very rare, and there were few cases when cy-
berterrorism was discussed along with cybercrime. Therefore, it is necessary to
first examine how international rules regarding cyberterrorism are established and
operated,

   To this end (1) regarding definition, selecting a concept that is considered ap-
propriate by individual states and regional organizations should be encouraged,
General Issues of Cyberterrorism

and legislation of domestic laws and establishment of monitoring institutions to combat terrorism should be encouraged (Security Council Resolution 1373). During the process, there is ample possibility that there will be problems from discussing *actus reus*, but since in most part there is some common element, it seems that this problem can be alleviated. (2) Major international acts of terrorism are prohibited by international conventions that specifically describe particular acts without a generalized conceptualization of terrorism. Such examples are the Hague Convention (Hijacking Convention / Convention for the Suppression of Unlawful Seizure of Aircraft) of 1971 that deal with illegal hijacking of airplanes, the Montreal Convention (Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation) of 1971 that deal with illegal acts that compromise safety of civilian airplanes, the International Convention against the Taking of Hostages of 1979, the Rome Convention (Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation) of 1988 that deal with illegal acts compromising safety of maritime navigation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents of 1974, International Convention for the Suppression of Terrorist Bombings of 1998 and International Convention for the Suppression of the Financing of Terrorism of 1999. It is important to point out that these international conventions can be considered as precedent cases for establishing a legal system regarding cyberterrorism, which is currently under discussion. It is also possible to use these conventions as a backdrop for seeking alternative concepts for future conventions. Suppose, should the term "Illegal Act against Cyber Safety" be used, (1) the international conventions approach on terrorism can be adopted, (2) and there is the advantage of determining detailed forms of acts.

**B. Relationship with Cybercrime**

Representative case of international regulation system through international con-
ventions is the Budapest Convention on Cybercrime, but there are the following limitations. First, there are only 29 member states and 45 signatory states, and while non-EU member states such as the United States has joined, their main purpose of joining is to regulate cybercrime originating from Europe. The Budapest Convention, with regards to jurisdiction, clarifies exercise of jurisdiction through domestic legislations, and states the principle of *aut dedere aut judicare*; but there are suspicions on their actual effectiveness. Such suspicions come from difficulties in investigation and law enforcement despite existence of the Convention, which is because there are limitations to cooperation in criminal matters based on this Convention for cybercrimes that originate from non-EU member states. Another problem is that the Convention only regulates matters pertaining to “cybercrime”, and there is no mention of cyberterrorism in the Convention. Also, there is no mention of applying the Convention on cyberterrorism in the negotiation documents concerning the Convention. Therefore, it seems there will be legal complications in applying the Budapest Convention on matters regarding cyberterrorism.

C. International Cooperation and Jurisdiction

1) International Cooperation

The Council of Europe has made it compulsory to 1) establish measures for swift and smooth international cooperation on criminal cases for effective punishment regarding cyberterrorism, 2) international and domestic support for investigation, prosecution and detection of cyberterrorist acts, and 3) swift and fair international cooperation. Currently South Korea deems it necessary to join the Convention, but due to various issues in substantial and procedural law in order to adopt the provisions of the Convention, there are still issues to resolve for South Korea to join the Convention.

The United Nations Convention Against Transnational Organized Crime is intended to regulate serious crimes that have some degree of organization, such as
hacking and DDoS attacks, and use threat and extortion for economic profit. There are up to 147 countries that completed the signature and ratification process. In case of cyberterrorism, a close cooperation system is necessary between the involved states in order to track down the suspect of hacking or DDoS crimes. The suspect of either hacking or DDoS attack is an intelligent criminal who can delete all traces of his involvement, and there is also the possibility that various system access logs and service user logs can be deleted after a certain duration of time, thus immediate tracking of the suspect is very important. Despite this urgency, Act on International Judicial Mutual Assistance in Criminal Matters is criticized for stipulate a cooperation process that is too complex for investigating cyberterrorist crimes.

Also, the G8 High Tech Crime 24/7 Network is a multinational network of law enforcement agencies established for the purpose of constant cooperation regarding investigations in transnational cybercrimes, of which a total of 49 countries are a member. Recognizing that the formal system of international cooperation process through official diplomatic channels takes too much time and is inappropriate for investigations in transnational cybercrimes, this system adopts a cooperation process that uses informal contacts (phone, email, fax) to request judicial assistance first and then go through the official channels later, which gives it the unique advantage of swiftness. Currently 50 states participate in this network, and in South Korea the Supreme Prosecutor’s Office is the only member of this network, but because the Korean National Police operates Interpol’s I-24/7 Network, this causes problems in overlap or dispersion of operations.

63) Lee, Dong Hee Jang, Yoon Sik., Kim, Seok Bum., and Pyo, Chang Won., Development of
Therefore, in order to proactively prevent and suppress an act of crime that the international community commonly recognizes as harmful, these countries of the international community should provide a basis of rule and punishment of this particular act of crime through the establishment of a convention, and each member states should legislate domestic laws to implement an organizational and systematic investigation process that is appropriate to the realities of the member state, so that the convention may be effectively executed.  

It is important to recognize that despite all the differences and incongruities of law and treaties, one things that all countries share in common with regards to cyberspace is the private sector. As much as cyberspace is a borderless wildland where jurisdictional problems make it a security agency’s nightmare, this cyberspace is built from its very foundations by hardwares and softwares made by a few multi-national companies, and these hardwares and softwares, with some variation, are a common element of cyberspace. This common element creates a bond between the perpetrators and the protectors - they use the same tools. No matter where the perpetrator is, the tools that they use to commit cyberterrorism is the same as those as the tools that security experts use and software developers create. 

In light of this fact, international cooperation on sharing known flaws and exploits in hardwares and softwares with the appropriate officials and security experts become one of the most essential safeguard against cyberterrorism. In other words, the security experts and IT developers can convene and share the means to hack and compromise their own computer systems, and fix them up before any cyberterrorists or cybercriminals can exploit them for their purposes. 

There are many venues through which IT developers, security experts and government officials can convene and share flaws and exploits, and prevent their use.
by those with malicious intent.

Arguably the largest of such conferences, the Black Hat Briefings is a computer security conference held regularly around the world, mainly in Las Vegas, but also have been held in Barcelona, Amsterdam, Tokyo and Dubai. Black Hat Briefings is privately owned by UBM plc, a multinational media company located in London, and it takes private sponsors, mainly software and security companies such as Microsoft, IBM and RSA. It consists of a conference of computer security experts, government officials and individual hackers, and also offers training courses in hacking and computer security.

2) Jurisdiction

As discussed so far, there is not enough international consensus on cyberterrorism, and the reality is that there is absolutely no international system(particularly multilateral system) to control terrorism. As long as an international system regarding cyberterrorism and an international cooperation system in judicial assistance don’t exist, problems may occur regarding jurisdiction, which are as follows. i) While domestic control and law enforcement can be achieved by domestic legislations through the six principles(personal, territorial, universal, etc) that determine domestic legislative jurisdiction, such legislations cannot be of much help for effective and efficient investigation and law enforcement, regardless of which determinant principles of legislative jurisdiction is applied. In other words, in law enforcement, the basic principle of executive jurisdiction based on consensus between involved states is applied. ii) In the above situation, there will be some political pressure to apprehend a suspect, particularly if the suspect is currently in another country, but under influence of political circumstances and diplomatic relations between the involved states, there is the limitation that predictability cannot be guaranteed. iii) Measures that apply the existent extradition treaties and judicial assistance treaties can be considered, but there can be complications from
applying such measures. For instance, concerning extradition, one country may have domestic legislations on cyberterrorism while the other country may not, and in such case there may be problems from principles of international law that apply to extradition, such as the principle of double criminality and the principle of speciality. In such a case, circumstances could lead to rejection of extradition.

iv) Based on the majority consensus of international criminal law experts that certain forms of terrorism can amount to crime against humanity, the argument that cyberterrorism can be seen as a crime against humanity and be brought to trial at the International Criminal Court is being claimed, particularly among American scholars. In reality, however, considering the differences between terrorist forms of crime and cyberterrorist forms of crime, and that to be brought to trial at the International Criminal Court, requisites of objective actus reus and subjective actus reus should be satisfied, and also considering the existence of basic principles of jurisdictional exercise of the International Criminal Court, which are the principle of complementarity and the trigger mechanism, this argument can be evaluated as having no merit or prospect. v) There are discussions whether the principle of aut dedere aut judicare can be applied to cyberterrorism, but in accordance to international law, the principle of aut dedere aut judicare is merely a conventional obligation rather than a principle of customary international law. Therefore, without a separate international convention on cyberterrorism, legal limitation to claiming this principle is inevitable.

Then there is the problem of whether international cooperation on cyberterrorism is necessary, and how cyberterrorism should be dealt with. In this regard, those with a negative opinion point out the negative position on the possibility of occurrence of cyberterrorism and ambiguity of conceptualization. They also point out the problem that terrorist acts can be committed not only by terrorists or terrorist groups (when the terrorist crime satisfy actus reus), but also by individuals and anarchists. In such cases, differences between cyberterrorism and cybercrime can only be based on subjective actus reus, but in reality, criteria for
the differences are ambiguous. Another issue they point out is whether a separate treaty for cyberterrorism is necessary when punishment of cybercrime is possible by existent system of domestic laws and international treaties. If use of the Internet is only considered as a means and not an end, there are many systems of domestic laws and international treaties where such an act is punishable.

On the other hand, those with a positive opinion point out that cyberterrorism is a new form of terrorism, treaties that reflect the unique characteristics of cyberspace is necessary, although cyberterrorism cases so far is rare, there is increasing probability that they will occur in the future, They also point out that as much as universal jurisdiction for terrorist crimes is controversial, they should at least establish the principle of *aut declere aut judicare* obligatory by treaty, which can make prohibition and punishment of cyberterrorism take actual effect.

On the question of whether new treaties can effectively apply and enforce its provisions, the answer is negative when human rights in cyberspace is considered, Especially with regards to “the use of the Internet for terrorist purposes” as stated by the UN, concerns for human rights is especially true when looking at the precedents of drafting process of the UN Convention against Terrorism, Also, the fact that countries are establishing their own response systems against cyberwarfare makes it even more difficult to effectively apply the provisions.

3. International Conventions

As noted above, attention in the literature has been given to the application of traditionally terrorism laws as they may apply in cases of cyberterrorism.65) However, there

does not appear to be, at present, an international legal instrument that deals with cyberterrorism specifically. Therefore, the prosecution of a cyberterrorist would be based in large part on laws developed for “normal” or “traditional” terrorist activities, This of course would depend on the nature of the cyberterrorism event (i.e., whether it were an attack on the critical infrastructure or on information systems). Several examples of such analogs are outlined in the below section.

A. The Montreal Convention

The Montreal Convention was developed in an effort to guide international law dealing with terrorist attacks against airplanes (aerial terrorism). Cohen (2010) argues that these laws may apply to cyberterrorism attacks that interfere or endanger passengers of an aircraft by means of a cyberterrorism. While subject to varying interpretations, such laws may be an effective means by which to prosecute or detain cyberterrorist criminals.

B. The Convention for the Suppression of Terrorist Bombings

The Convention for the Suppression of Terrorist Bombings (1997) lead to international law that “prohibits bombing of targets that are certain to cause a large number of civilian casualties”66). This effort help strengthen international law enforcement in terms of combating international terrorism via the criminalization of certain types of weapons detonations, including biological, chemical, and radiological weaponry. Such law may apply well to acts of cyberterrorism. Discussed in great detail by Cohen, this is due to possibility of equal intent between a cyberterrorist and a physical terrorist, thus legal definitions may apply equally for both types of events. In short, Cohen argues that if a terrorist act involves the

---

disruption of the operation of a computer system that results in something equivalent to the detonation of a bomb (including release of deadly chemicals, or radiation, such as in a cyberattack against the critical infrastructure). In such cases, the Bombing Convention laws could be used to prosecute the cyberterrorist.

4. Conclusion

In terms of international cooperation, different types of efforts vary on governments and their related law enforcement agencies. These cooperative efforts are:
- Formal bilateral cooperation: Mutual legal assistance treaties (MLATs)
- Informal bilateral cooperation: Individual policy contacts (interagency cooperation, CERTs, etc.,
- Formal multilateral cooperation: Council of Europe
- Informal multilateral cooperation: G-8, OECD, APEC, CERT collectives

These types of cooperation have their own advantages and disadvantages. For example, there are a few disadvantages of MLATs. Firstly, the scope of MLATs is too narrow to have more participating countries, The U.S. State Department signed for MLATs only with 19 countries. Secondly, most of these treaties do not cover cybercrime specifically, but do so in general terms. Lastly, because of the bureaucratic process requiring much paper works, MLATs can be time-consuming. The last point is the biggest disadvantage. In contrast to traditional crimes which usually deal with physical evidence, evidence of cyberterrorism can be destroyed in few seconds or minutes. Time matters in investigating on cybercrime.

In addition to those discussed above, other opinions on advantages and im-

The importance of bilateral cooperation has been existed. Specifically, the importance of multilateralism has been highlighted because of big differences in legal provisions related to computer crime, criminal extradition, and legal assistance among countries. The most effective way to cope with cyberattack has been known as bilateral cooperation and the below cases support the effectiveness of bilateral cooperation.

**Table 6  Major Cases of Cyberterrorist Arrests**

<table>
<thead>
<tr>
<th>Date</th>
<th>Target</th>
<th>Damage</th>
<th>Outcomes of Bilateral Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998, February and March 1998</td>
<td>Civilian, governmental, and private sector computer systems in the U.S.</td>
<td>At least 200 unclassified U.S. military personnel and other government computer systems were penetrated.</td>
<td>The NIPC worked closely with the Israel’s law enforcement and identified two people in Cloverdale, CA and individuals Israel.</td>
</tr>
<tr>
<td>2000, February</td>
<td>CNN, Yahoo, Amazon.com, e-Bay, and other sites</td>
<td>DDoS took over the networks</td>
<td>The NIPC cooperated with the companies and worked with the Royal Canadian Mounted Police. They arrested a juvenile called “Mafiaboy”</td>
</tr>
<tr>
<td>2000, May</td>
<td>individuals and companies around the world</td>
<td>The computers around the world were attacked by the “Love Bug” or “I LOVE YOU” virus</td>
<td>The NIPC traced down the attack to the Philippines. The FBI worked closely with the Philippines’ National Bureau of Investigation and indentified the suspect, Onel De Guzman</td>
</tr>
</tbody>
</table>


The cases above are real cases proving cooperation between two countries works out. Given these good examples, it can be assumed that bilateral cooperation can bring good outcomes and is actually effective on investigating incidents.)

78
Moreover, the countries, which are vulnerable to cyberterrorism or potential attack, should put their effort to secure critical infrastructure and build partnerships and alliances with other countries. There are two ways of cooperation, informal and formal way, and its effectiveness and usefulness varies on issues. Generally, formal cooperation is considered to be desirable but it can be time-consuming. Time matters to legal enforcement and other governmental intelligence agencies during investigation and, more importantly, there is no time to be consumed to follow complex bureaucratic procedure. In terms of time efficiency, informal cooperation is better than formal cooperation but some countries do not authorize informal cooperation. Therefore, the effort to simplify bureaucratic procedure and formal and informal cooperation are necessary to improve the current respond to cyberterrorism and cybercrime. Bilateral cooperation can be an good alternative.\(^{(69)}\)

Among various organizations and agencies taking important role to facilitate cooperation at international and national level, organizations such as CERT and FIRST can serve instrumental act in formal and informal and bilateral and multi-lateral cooperation. In a field of cybercrime and cyberterrorism, informal activities between public and private sector lead to formal cooperation. Thus, establishing organizations or agencies such as coordination center for cooperation and coordination at every level should be established. Law enforcers should be aware that the purpose of this center is to facilitate cooperation and coordination not to monitor. For instance, programs such as the U.S.'s Secret Service Electronic Crime Task Force can build strong trust between private sector and law enforcement, support each other, and share information.


In sum, multilateral cooperation considered to be desirable whereas bilateral cooperation shows higher level of achievement than multilateral cooperation. In sum, multilateral cooperation considered to be desirable whereas bilateral cooperation shows higher level of achievement than multilateral cooperation. Only when countries practice cooperation and share information with others, real cooperation at international level can be achieved. Formal cooperation can guarantee some level of cooperation but has the biggest disadvantage, time-consuming, due to bureaucratic system and other obstacles.

Lastly, considering transnational characteristic of cyberterrorism, legal conflicts in relation to critical and sensitive issues on national sovereignty and jurisdiction can be occurred. Approach from other areas is a good option to solve this problem. For example, aviation is a field which has internationally accepted provision, Also, European Arrest Warrant can be a best practice to learn how international society overcomes the issues with jurisdiction.

III. Analysis of Cyberterrorism Response System of Major Countries

1. Cyberterrorism Response System of the United States of America

A. Overview

Response system against cyberviolation of the United States began developing rapidly after the crucial event of the 9-11 attacks of 2001. After 9-11, the United States began working on measures to safeguard the United States from terrorist threat and attacks, including both physical attacks and cyberattacks. For this pur-
pose, the Department of Homeland Security was newly established.

Recently, National Security Strategy(NSS), the first public report on current status of national security and future prospects since the inauguration of the Obama Administration in May 27th of 2010, emphasizes a new strategy, to focus on defining cybersecurity and implementation of new policies on cybersecurity. In other words, the U.S. clarified its will to recognize illegal acts, terrorism and hacking in cyberspace as national security issues and start managing digital infrastructure as important assets of the state. This is because there is constant concern about cyberterrorism, as most of critical infrastructure in the United States depend on computers.

To date, there was no case of a politically motivated cyberattack that caused major losses in life or property. However it should be noted that as terrorists hijacked airplanes to commit terrorism in the 911 attacks, cyberterrorism may aim for similar results as the 911 attacks through cyberspace. Cyberterrorism can target companies that design and develop hardware and software for airports and air traffic control systems in the United States. Regardless of whether it is military or civilian, the possibility that cyberterrorism can target civilian companies which produce airplanes or airplane parts is a cause for major concern. This concern was specified in a US government study conducted in 2010, which warned that the computer network of the Federal Aviation Administration is vulnerable to a cyberattack, and most air traffic control systems were not optimized for responding to cyberviolations. This means that even a computer equipped by Boeing 787 can be hacked to cause malfunctions, leading to a disaster. This evoked


concern that operation system of airports can be disrupted or even collapse by cyberterrorism.\(^{75}\) It was noted that this kind of fear can lead to decrease in economic activities related to travels and tourism.

As reviewed above, criminal acts of cyberterrorism can be prosecuted by extent criminal code and this code includes laws on traditional terrorism. In recent years, laws related to suppression and prosecution of cyberterrorism are specially enacted or amended. Here, applicable laws on cyberterrorism and the laws mentioned above is discussed in following parts,

### B. Cyberterrorism Policy

#### 1) Before the 911 attacks

(1) Law

Prior to the 911 attacks, one of US’s response to threats in cyberspace is The Computer Fraud and Abuse Act of 1986 (the Act hereafter). Before the legislation of this act, the Federal Wiretapping Statute was the only law stipulating crimes in cyberspace.\(^{76}\) First, the Act stipulates unauthorized access of a protected computer for acquiring information, acquisition of valuables using methods of deception or incurring losses on other person’s computer as illegal acts.\(^{77}\) Also, the Act stipulates distributing malware and incurring losses on other person’s computer as punishable acts.\(^{78}\)

The Act was amended several times since it was legislated, In 1994, it was amended to include regulations that punish the act of unauthorized access to com-

---

75) Ruwantissa Abeyrantne, cyberterrorism: The Next Great Threat to Aviation, 24 No. 1 Air $ Space Law. 5-6 (2011).
puters of the federal government, and the recently legislated the USA Patriot Act and the Cyber Security Enhancement Act of 2002 amended the Act to expand rules and increase level of punishment on acts related to cyberattacks. The Act was amended in 2002 through the legislation of the Homeland Security Act. A point of interest in the Homeland Security Act is that it stipulates actus reus of a cyberterrorist attack that results in losses in the real world.

Other relevant laws that US courts used to prohibit disruption of computer networks are the Electronic Communications Privacy Act of 1986 (ECPA), the Economic Espionage Act of 1996, and various state criminal statutes. The Economic Espionage Act imposes civil and criminal responsibility on acts relating to trade secrets belonging to others, which includes unauthorized access of a computer. The Economic Espionage Act does not specifically mention the act of computer hacking, but it rules are enough to govern the hack of hacking. ECWA prohibits the act interception an electronic communication for its acquisition or change, but ECPA is limited in dealing with state-of-the-art computer crimes due to a total lack of rules governing violations regarding stored communications.

Various state criminal statutes have rules on cyberattacks. Arizona and Florida were the first states to legislate laws regulating computer crime in 1978. Vermont was the last, which legislated computer crime law in 1999. The Computer Crime Prevention Law of Illinois has criminal codes against fraudulent use of computers or computer frauds. The Illinois Electronic Mail Act goes one

80) 6 U.S.C. § 225(g)(40 (codified in 18 U.S.C. § 1030(c)(5A-5B)).
83) Konop v. Hawaiian Airlines, 302 F.3d 868, 877 (9th Cir. 2002).
step further to impose civil responsibility on people who send spam e-mails. While these state statutes provide means to enhance cyber safety, they were not enough to deal with concerns that were brought up after the 911 attacks.

(2) Other Policies

To respond to concerns related to computer safety, the federal government made efforts other than legislations. A report published by the National Research Council, “Computers at Risk”, warns of the possibility of a cyberterrorist attack. In 1997, “Clinton’s Commission on Critical Infrastructure Protection” submitted a report that provided the basis of a presidential order. The presidential order instructs federal agents to develop protection plans of critical infrastructure and provides strategies to protect the US from cyberattacks.

2) After the 911 attacks

(1) National Strategy for Establishing Cyberspace Security

In February of 2003, the Department of Homeland Security of the United States adopted a policy report called National Strategy to Secure Cyberspace (the Report hereafter). The Report was made for the purpose of preventing cyberattacks against important critical infrastructures in the US, decrease national vulnerability against cyberattacks and minimize recovery time from a cyberattack. It is clear that the Report was made to deal with the novel threat of cyberterrorism after the 911 attacks.

In the Report, important and prioritized policies for cyberspace security are proposed. These propositions are establishment of a national cyberspace security

response system, establishment of a national cyberspace security threat and vulnerability reduction program, establishment of a national cyberspace security awareness and training program, securing governments’ cyberspace, and spending efforts on national security and international cyberspace security cooperation.\(^{90}\)

One of the policies proposed in the Report, which is the National Cyberspace Security Response System, consists of measures for the Department of Homeland Security to coordinate public institutions and private institutions against threats in cyberspace. The Cyberspace Security Response System performs analysis, issue warnings and coordinate response efforts on events important at the national-level, and enhance consistency between government systems and private facilities, and promote information sharing between institutions to enhance cyberspace safety.\(^{91}\)

(2) National Strategies against Threats to Cyberspace and its Vulnerabilities

a. Threats to Cyberspace and its Vulnerabilities

The Report states that American manufacturing, industrial facilities, banking and finance, informations and energy have adopted networked computer systems. While these networked computer systems decreased costs and enhanced productivity, collaterals of these developments were the security problems that often occurred. Attacks on infrastructure related to information processing have various forms, ranging from simple hacking violations and computer viruses to terrorist attacks on infrastructures for the purpose of large-scale harm.\(^{92}\)

The Report also points out that because methods of cyberattacks become more sophisticated day by day, more criminals can commit attacks on American infrastructure and cyberspace that can lead to serious national disasters, Terrorists on

their usual days take grasp of structures and systems of informations infrastructure in the United States, and when they get into action, they can threaten to attack critical facilities and cripple public trust on the informations system. Cyberattacks can disrupt informations systems to incur various kinds of property losses, violation of intellectual property and even loss of life.

The possibility that an attack in cyberspace may even out-scale ordinary terrorism is being reported. For instance, NIMDA(acronym of ADMIN), which is a computer virus that can bring about catastrophic disruption of critical infrastructure, is a good example of the potential of cyberattacks, NIMDA is a combination of a computer worm and a computer virus that can execute automated cyberattacks, NIMDA rapidly spreads itself among a wide range of computers through various means of infection until the targeted file is destroyed, NIMDA infected 86,000 computers all over the US in merely an hour. Two months before the advent of NIMDA, a cyberattack called Code Red managed to infect 150,000 computers.93)

The Report points out that characteristics of attacks in cyberspace are their wide range of targets and their ability to incur serious damage to them, and that such attacks can be committed from a far distance, Traditionally, the United States enjoyed the geographical advantage of being far apart from Europe and Asia, but this advantage is annuled by cyberterrorism, Vulnerability against cyberterrorism is not a problem a specific to the United States, but a global problem that exist anywhere so long as there are people with the capability of committing cyberattacks, and the report points out the necessity of declaring the dangers of cyberterrorism and devising measures to counter them.94)

b. National Policy and Principles on Cyberterrorism

According to the Report, the Department of Homeland Security provides six

principles for securing information systems of critical infrastructures, which are as follows. First, a national effort is needed. Second, effort to protect privacy and civil liberties is needed. Third, proper balance between regulation and market forces is needed. Fourth, effort to clarify accountability and responsibility is needed. Fifth, flexibility in approach is needed. Sixth, systematic multi-year planning is needed.\textsuperscript{95)}

The Report emphasizes government effort alone cannot deal with threats to cyberspace, and a united effort of all Americans is necessary. Also, considering that traditionally the federal government had jurisdiction within a limited bounds, it points out that role of the federal government in dealing with threats to cyberspace is limited. Roles that the federal government can fulfil through policy intervention are facilitating communications between NGOs, discovering potential impact of vulnerabilities in public goods can have on the nation and the economy as well as discovering relevant cases, and sharing information on threats to cyberspace and its vulnerabilities with NGOs.\textsuperscript{96)}

The Report states the federal government is responsible for the protection of privacy and civil liberties from potential violations by illegal acts in cyberspace. Cyberspace security and individual privacy are not conflicting objectives, and strengthening cyberspace security can be a means to strengthening protection of privacy. The government can encourage consumers, information networks or administrators of main online market sites to share private information properly and safely.\textsuperscript{97)}

Some federal regulatory agencies have the legal basis to intervene in matters regarding cyberspace security. However, the Report emphasizes self-initiative of the market itself to improve cyberspace security. It is also pointed out that if each agencies of the government do not coordinate their efforts, the situation can

\textsuperscript{97)} Homeland Security, The National Strategy to Secure Cyberspace, 2003,
backfire through inconsistencies, leading to possible reductions in security efficiency.\(^{98}\)

The Report also states that to establish a flexible and reliable information infrastructure, an administrative division or agency should be designated as a “Lead Agency” to coordinate cyberspace security policies of the federal government. After 2002, the Department of Homeland Security, established in accordance with the Homeland Security Act, became the “Lead Agency” for National Strategy to Secure Cyberspace. National Strategy to Secure Cyberspace includes strategies and agenda guidelines for the federal government, state governments, local governments and the private sector to secure cyberspace.\(^{99}\)

The Report emphasizes flexibility in responding to cyberattacks and addressing vulnerabilities, because of very rapid rate of change in threats to cyberspace. Each government agencies should constantly reexamine prioritization and allotment of resources to deal with cyberattacks.\(^{100}\)

According to the Report, securing cyberspace should be understood as an endless process due to continuous development of new technologies and vulnerabilities. The report recommends government divisions and agencies to establish multi-year plans for cyberspace security, and also recommends other public institutions and private organizations to do the same.\(^{101}\)

C. The Legal System

1) The USA Patriot Act

(1) Main Contents of the USA Patriot Act

The USA Patriot Act of 2001 (the Act hereafter) is an act intended to establish


national security and strengthen investigatory powers in order to respond to continuing through of terrorism after the 911 attacks, Main contents of the Act expands existent authority of law enforcement agencies to access phone records of suspects to electronic communications including the Internet and mobile phones, and adds authority to access IP addresses collected from programs such as DCS1000.\textsuperscript{102} The Act also dramatically increases severity of punishment for terrorist acts. Specifically, prior to the Act, first offence in cyberterrorism was punishable by maximum of five years imprisonment, and repeat offences were punishable by maximum of 10 years imprisonment, but the Act now stipulates maximum of 10 years imprisonment for first offence, and 20 years imprisonment for repeat offence. Furthermore, the Act stipulates that an offence of causing damages to computers related to national defence or national security are punishable without proof of damage.\textsuperscript{103} Also, the Act contains sanctions against money laundering.

\textsuperscript{102} Also known as the Carnivore program, it was developed in 1999 by the FBI to monitor e-mails to prevent cybercrime.

\textsuperscript{103} The Patriot Act amended the existent penal codes for fraudulent use of computers in 18 U.S.C. § 1030, under which a person who intentionally accesses a protected computer without authorization receives a maximum 5 years imprisonment or a fine if the act results in the following: 1. loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; 2. the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; 3. (III) physical injury to any person; 4. a threat to public health or safety; 5. damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or 6. damage affecting 10 or more protected computers during any 1-year period. If serious injury results from any act from the above the penalty increases to maximum imprisonment of 20 years, and if it results in death, the penalty increases to life imprisonment. In addition, the Act was amended so that the act of damaging a protected computer using a virus or other software technology is punishable by a maximum of ten years in imprisonment(if the person is guilty of another act of crime in hacking, the penalty is increased to a maximum imprisonment of 20 years).
through cyberspace related to terrorism.\textsuperscript{104} In order to tracking down terrorists easier, it abolished certain parts of the federal law that restricted electronic surveillance. The Federal Wiretapping Statute was prohibiting eavesdropping of communications using computers or other means of electronic communications.\textsuperscript{105} These prohibitions of eavesdropping targets not only interception of electronic communications but also prevents intrusion into a computer system.\textsuperscript{106} The Act legalized these kinds of surveillance activities.\textsuperscript{107}

Also, the Act allows interception of not only telephone communications, but also communications via the Internet, e-mails, web surfing and other means of electronic communications. In other words, federal agencies, by using a customizable packet sniffer, can acquire any email subjects transmitted or received by an email account, see any servers accessed by a suspect, track any users who access a particular web site, and track any web sites accessed by a particular suspect. This packet sniffer was first known as “Carnivore” program, but it was integrated into the DCS-1000 program, which is now the most commonly used program for electronic surveillance.\textsuperscript{108}

According to Article 2510 of the Act, warrants issued by the jurisdictional federal district court(or a state court of the same level) must provide ① confirmation of the applicant, ② detailed record of the alleged criminal charges, ③ facilities to be used, type of communication to be intercepted and detailed record of the surveil-

\textsuperscript{106} USA PATRIOT ACT § 217 (codified as amended at 18 U.S.C. § 2511(2)(i)(IV)).
\textsuperscript{107} USA PATRIOT ACT § 814 (codified as amended at 18 U.S.C. § 1030).
\textsuperscript{108} DCS-1000 is an Internet surveillance program developed by the FBI to perform court orders with cooperation between federal law informent agencies and internet service providers to seize certain information that stores e-mails and other forms of electronic communications sent or received by a certain user.(Electronic Privacy Information Center Web site on the Carnivore System, http://www.epic.org/privacy/carnivore).
General Issues of Cyberterrorism

lance target’s identity, \( \text{④} \) and less intrusive means to collect the information and the reason such means has failed or can fail.

Article 2518(7) of the Act includes ‘emergency’ provisions allowing electronic surveillance without a warrant in case of conspiracy, organized crime, or an impending threat of murder or severe bodily injury. According to these provisions in particular, with permission from the system owner ‘in case of a protected computer’, federal agencies can conduct surveillance and investigate contents of its communications without the restrictive legal oversight stipulated by Title III of the Act. For example, if the system owner of the system targeted by terrorist hacking gives permission, surveillance can be conducted without legal oversight, and any information acquired from such surveillance activity can be used as evidence in the court of law.

In addition, the Act, with regards to cyberterrorism, has numerous rules expanding authority of law enforcement and intelligence agencies to conduct surveillance and investigations. Particularly, the Act adds new rules allowing federal agencies to collect and monitor information on the Internet, and simplifies processes for federal agencies to share information with state intelligence agencies. For example, prior to the Act, the Cable TV Privacy Act and Title I II, Article 2703 of the United States Code stipulated ‘cable operator shall not provide any information of a particular individual of any contractors’. However, legislation of the Act amended this rule to ‘cable operator can provide ... such information to government agents’. Therefore, it became easier for government agencies to acquire information from internet services of a cable company. As such, there were no clear rules in the Act that required internet service providers to provide client information or communications in case of emergencies, but now it was amended so that in case of emergencies, the internet service providers are required to provide communications and related records(such as log records) to federal agencies.

Title VIII of the USA Patriot Act of 2001 contains elements that were developed
specific to cyberterrorism activities. The most prominent is Section 814, which was
developed in an attempt to deter and prevent cyberterrorist activity from occurring
(Maras, 2012). Section 814 also lays out penalties for those convicted for specific
acts of cyberterrorism. A person can be convicted in a US Court of Law if he or
she gains unauthorized access to a protected computer system and as a result,
causes physical injury to a person, loss of life, or in any way threatens public
safety or health. Section 814 also applies if the result is damage to a government
computing systems, a property loss of $5,000 or more, affects a person’s medical
examination, diagnosis or treatment. Extortion via a protected computer is also
covered under Section 814 of the Patriot Act.

An individual who is convicted under Section 814 of the Patriot Act faces a pris-
on sentence, the length of which depends on the severity of the act. A person
faces up to ten years in prison for attempting to damage a protected computer
through the use of computer malware (e.g., viruses, etc.). If a person is convicted
under Section 814 for a second time, the penalty is increased to a prison sentence
of up to twenty years.

(2) Problems of the Patriot Act

One of the most controversial legal system that deals with terrorism in the
United States is the Patriot Act. The Act brought large changes to the legal system,
intended for dealing with terrorism after the 911 attacks. Especially, there are
views that fundamental rights of citizens are under threat from the Act, The Act
includes many rules intended to prevent large-scale terrorist attacks in cyberspace,
such as new authority to intercept voice communications in hacking investigations,
strengthening authority to allow search warrants for voice communications stored
in a third party for investigation, expanding obtainable range of information
through a subpoena by an investigation agency necessary for ascertaining identity
of a suspect, such as the suspect’s IP address, credit card number and bank ac-
count number, new rules allowing law enforcement agencies to require in-
formation on contents and log records of an ISP, and expanding use of pen register or tarp and trace devices for tracking telephone calls.\(^{109}\)

With these new changes in mind, there are also others who see the Act as a prudent attempt to prevent terrorist attacks in cyberspace in the future, and there is also a view that evaluates the Act as 'one of the most important tools Congress has given the government to fight terrorism and prevent terrorist attacks'.\(^{110}\)

However, unlike these sympathetic views towards the Act, there are academics and civic groups who contend that the Act, which grants the federal government expansive powers such as clandestine investigations, collection of private information and phone tapping if it deems suspicion of terrorism is strong, is capable of limiting fundamental rights and therefore violates the Fourth Amendment. For instance, members of the city council of New York claimed 'The Patriot Act, despite its name, is in fact unpatriotic, and it violates our rights and liberties.'.

Meanwhile, city of Arcata, in the state of California, legislated an ordinance in March of 2003 that stipulated any act of a city worker cooperating with a federal agent on the basis of the Patriot Act would be a misdemeanor. According to this ordinance, any city worker who has received a request from a federal agent on the basis of the Patriot Act and contacted the federal agent and then has not immediately informed the mayor of this act are punishable by a 57 US dollar fine.\(^{111}\)

Especially, the Electronic Frontier Foundation (EFF) pointed out that the Patriot Act is full of problems. The EFF pointed out there is no constitutional check or any principle of balance against the expanded surveillance authority granted by the Patriot Act. The most serious problem of the Act is that it allows monitoring

\(^{109}\) Former President Geroge W. Bush repeatedly emphasized that these provisions of the Patriot Act are essential steps to protecting constitutional rights of the American people and eliminating terrorism.


any computer trespasser suspected by the government. In such case, the rights of the suspected computer trespasser can be violated, Examples given above shows how The Act renders fundamental rights guaranteed by the Fourth and the Fifth Amendments of the Constitution meaningless. Furthermore, the Act allows the CIA to conduct comprehensive surveillance on a US citizen. This has been criticized, that the CIA is capable of abusing information of a US citizen acquired for the purpose of securing cyberspace.\textsuperscript{112)} Also, a problem was pointed out if it is worth sacrificing rights of citizens for cyberspace safety and security.\textsuperscript{113)}

Also, the Patriot Act amended 6(e)(3)(c) of the Federal Rules of Criminal Procedure to expand information sharing in the grand jury, and stipulated that law enforcement has the authority to share information acquired by electronic, wireless or oral surveillance.\textsuperscript{114)} Here, by including voice mails among targets of interception warrants, targets of search and seizure were expanded from texts to include electronic communications. Not only did the Patriot Act expand range of targets for search and seizure, but it also drastically expanded range of information for sharing between intelligence agencies. For this, the Act is criticized for possibility of violating fundamental rights of an individual during an investigation by exceeding the necessary range of search and seizure, and it is also criticized that removing provisions that limited range of search and seizure of communications content is exceedingly expanding range of search and seizure of communications content. Furthermore, prior to the Act, range of warrants for electronic communication records were limited to names, addresses, bills for local and long-distance calls, telephone numbers, or the telephone number or identity of another user of the phone and user service duration.

\textsuperscript{112)} EFF Analysis of the Provisions of the USA Patriot Act, Electronic Frontier Found. (http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.)
\textsuperscript{114)} USA PATRIOT Act Article 203(a).
However, in article 210 of the Act, these provisions were amended for range of warrants for electronic communications to include name, address, local and long-distance phone records, records on duration of call, service time (including starting time and date) and types of services used, number of the phone or device including temporarily allotted network address and number or identity of other users, and payment method and financial source of the user (including credit card or bank account number). This expanded range of warrants amended by the Act is also criticized for possibly exceeding the necessary range of warrants needed for investigations.

2) The Cyber Security Enhancement Act as Incorporated into the Homeland Security Act

(1) Contents

The Congress has proposed the Public Safety and Cyber Security Enhancement Act of 2002 to resolve cyberspace security issues that have come into view by several hearings on cyberterrorism. Most issues were resolved by the Patriot Act, but there are some problems that still linger. To resolve these lingering problems, Lamar Smith, a senator from Texas, submitted the Public Safety and Cyber Security Enhancement Act of 2002, and it was eventually passed. Later, most contents of the Public Safety and Cyber Security Enhancement Act was incorporated into the Homeland Security Act.

The Homeland Security Act (the Act hereafter) is an act intended to protect national infrastructure of the United States from all forms of terrorism, including cyberterrorism. The Act consists of 17 titles, and with regards to cyberterrorism, rules stipulated by ‘Information Analysis and Infrastructure Protection’ of Title II and ‘Information Security’ of Title X are most relevant.

Title II, Section B of the Act is also called the Critical Infrastructure Information

Act of 2002. The Critical Infrastructure Information Act stipulates rules regarding information analysis and infrastructure protection, and has particularly detailed rules regarding protection of critical infrastructure. The Act stipulates the Critical Infrastructure Protection Program, through which critical infrastructures can be protected from not only physical attacks, but also attacks on information infrastructure and direct and indirect threats and attack on critical infrastructure or security systems. Critical Infrastructure Information is information regarding protection for protection systems outside the public sector, and elements of its meaning are as follows.\textsuperscript{116}

First, actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

Second, the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

Third, any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation,

As above, critical infrastructure information is designated by either the president or a director of the Department of Homeland Security, and receives special protection. Also, information voluntarily submitted to federal agencies for use in

\textsuperscript{116} Homeland Security Act Subtitle B, Section 212 (3)(A)-(C)
critical infrastructures such as security, analysis, warning, interdependent research, recovery, reconstruction and other information-related activities are exempted from the Freedom of Information Act’s requirement for public disclosure.\textsuperscript{117)\textsuperscript{118)} Also, if critical infrastructure information is submitted out of good will, the information cannot be used in civil lawsuits by other federal, state or local agencies or any 3rd party institutions without the written consent of the person who submitted the information.\textsuperscript{119)}

Title X of the Homeland Security Act is also referred to as the Federal Information Security Management Act of 2002 (FISMA). Under the Act, information security means protecting information and information systems from unauthorized access, use, disclosure, collapse, change or destruction in order to provide integrity, confidentiality, availability and authentication of the information.\textsuperscript{120)} Under FISMA, the Department of Homeland Security shall provide comprehensive programs to protect and control critical information resources that support the federal government, coordinate information security activities of both private and public sectors for protecting highly networked national infrastructures, and perform overall management and supervision of other divisions and agencies to effectively deal with a cyber emergency.

As such, the Homeland Security Act was legislated to protect national infrastructure of the United States from any form of terrorism, and Title II of the Act stipulates that functions of the National Infrastructure Protection Center of the FBI, the National Communication System of the Department of Defence, the Federal Computer Incident Response Capability (FedCIRC) of the General Services Administration, the Critical Infrastructure Assurance Office of the Department of Commerce, and the National Infrastructure Simulation and Analysis Center and en-

\begin{itemize}
  \item \textsuperscript{117)} 5 U.S.C. § 552, often referred to as the Freedom of Information Act
  \item \textsuperscript{118)} 2 U.S.C. § 212.
  \item \textsuperscript{119)} 2 U.S.C. § 214(a)(C).
  \item \textsuperscript{120)} 10 U.S.C. § 3532(a)(1).
\end{itemize}
ergy security and assurance program and activities of the Department of Energy be completely transferred to the Department of Homeland Security. Therefore, a legal basis is provided for the Department of Homeland Security to function as the executive institution against cyberattacks by receiving information from all relevant investigation and law enforcement agencies. In particular, Title II, Section 225 of the Act provides a much higher level of punishment for intentional or negligent acts or attempts of violations that results in serious physical harm or intentional or negligent acts or attempts by the perpetrator that causes loss of life.

As such, article 225 of the Homeland Security Act, which includes rules of the Cybersecurity Enhancement Act, in order to deal with increasing threat of cyberterrorism, amended criminal rules of the Computer Fraud and Abuse Act of 1986 (CFAA). Amendments to the CFAA mainly concern strengthening punishments of acts relating to cyberterrorism. According to the amended CFAA, cyberterrorist acts that intentionally or recklessly cause severe physical harm are punishable by a maximum 20 years of imprisonment, and if such acts cause loss of life, they are punishable by life imprisonment.121) Moreover, the U.S. Sentencing Commission has requested that CFAA should provide an appropriate standard of sentencing against the ever increasing threat of cybercrime.122)

Furthermore, CFAA, in accordance with the Stored Communications Act, expands exemption clauses for any company that voluntarily provides subscriber information to a government authority. In particular, a informations company, in emergency situations where death or serious physical injury to any person by a particular cause, is obligated to disclose or submit information related to the emergency situation. In addition, the attorney general is obligated to provide the information disclosed or submitted to the Department of Justice, number of subscriber accounts related to the disclosure or submission of information, and sum-

121) 6 U.S.C. § 225(g) (40 (18 U.S.C. § 1030(c)(5A-5B)).
maries of the disclosed information to the Committee of the Judiciary on an yearly basis.\textsuperscript{123)

(2) Problems of the Homeland Security Act

The Department of Homeland Security was established in March of 2003 on the basis of the Homeland Security Act to protect American territorial security after the 911 attacks. The Department of Homeland Security incorporated 22 counter-terrorist institutions dispersed throughout the executive government, and became the largest organization in the United States, having a workforce of about 170,000 people and a budget of about 38 billion dollars as of 2003. Through this incorporation, nearly all institutions in the United States regarding terror were entirely or partially integrated into the Department of Homeland security, except for counter-terrorist programs in the FBI and the CIA. Increase in efficiency by such integration of all counter-terrorist institutions cannot be denied, but there is there are negative views, such as the violation of fundamental rights of a citizen by such a large government entity and that there might have been too much reduction of counter-terrorist functions of other government agencies. Also, on a cautionary note, it should be pointed out that provisions of the Homeland Security Act allowing police surveillance on the Internet and increasing sentencing such as the life imprisonment sentencing for hacking computers may be abused, thereby violating fundamental rights of citizens.

As such, there is significant doubt on whether the USA Patriot Act and the Cyber Security Enhancement Act can effectively prevent cyberterrorism. In fact, applicable range of the Patriot Act is very broad, and it failed to focus on the terrorist problem with the necessary precision.\textsuperscript{124) Penal codes against terrorism have been enhanced significantly, but these are seen as having little contributions to

\textsuperscript{123) 6 U.S.C.(18 U.S.C. § 2702(b)(7)).}

\textsuperscript{124) EFF Analysis of the Provisions of the USA Patriot Act, Electronic Frontier Found. (http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.)}
actual prevention of terrorism. It is hard to consider that the Patriot Act brought about any actual improvements in the security field, and it only had a minor role of enhancing penal codes stipulated in The Computer Fraud and Abuse Act of 1986. The Cyber Security Enhancement also can be seen as failing to provide any institutional system to strengthening cyber security, except for strengthening statutory punishments against cyberterrorism. Such restrictive penal codes are more likely to be used to punish teenage hackers than preventing cyberterrorist activities.  

3) The Cyber Security Research and Development Act

(1) Contents of the Cyber Security Research and Development Act

The Science Committee of the House of Representatives stated that the 911 attacks brought attention to the issue of cyberterrorism, and in the hearing process, it found that the United States is very vulnerable to cyberterrorism. In June of 2001, under the US Senate Committee on Commerce, Science, and Transportation, the Subcommittee on Science, Technology, and Space held a hearing under the name of “Holes in the Net: Security Risk and the E-Consumer” to resolve security problems in cyberspace.

The Cyber Security Research and Development Act (the Act hereafter) stipulates that the Congress may spend almost 903 million US dollars over five years for research and development in the field of computer security. The National Science Foundation and the National Institute of Standards and Technology can cooperate to spend the allotted budget. The Act stipulates the allotted budget

be used for increasing number of students interested in computer and Internet security, and provide them with the opportunity to receive higher education. A very controversial part of the Act is that a foreigner who is connected to a state-sponsor of terrorism cannot benefit from support policies provided by the Act.

(2) Problems of the Cyber Security Research and Development Act

The Cyber Security Research and Development Act spent much effort in improving cyberspace security by providing funds for research and development, but it could not avoid some pitfalls. Any research and development area generally welcomes additional government funds, but there is concern that government support related to cyberspace security can hinder free development of electronic commerce and informations. There is still criticism against overspending taxpayers' money on a problem, cyberterrorism, that is yet to occur in the United States.

4) Other Efforts to Deal with Cyberterrorism

There are also other efforts by the Senate to secure cyberspace to deal with cyberterrorism. In 2003, by legislating the National Cyber Security Leadership Act of 2003, the Congress has shown its intent to capture vulnerabilities in cyberspace security. The National Cyber Security Leadership Act stipulates that funds be provided for the National Institute of Standards and Technology to develop checklists and related guidelines for the purpose of eliminating vulnerabilities and problems in cyberspace security. The Justice Enhancement and Domestic Security

131) 18 U.S.C. § 1030(e).
Act also includes numerous policies intended to enhance border security and computer security.\textsuperscript{135)}

Department of Homeland Security (DHS) - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Provides a control system security focus in collaboration with US-CERT (Computer Emergency Readiness Team) to respond to and analyze control systems related incidents, conduct vulnerability and malware analysis, provide onsite support for incident response and forensic analysis, provide situational awareness in the form of actionable intelligence, coordinate the responsible disclosure of vulnerabilities/malfunctions, and to share and coordinate vulnerability information and threat analysis through information products and alerts.

D. Organizations against Cyberterrorism

The Department of Homeland Security performs the mission of defending the US from attacks, reduce vulnerability of the US from the threat of terrorism, and minimization of recovery time and danger in case of a terrorist attack. Also, the President’s Critical Infrastructure Protection Board was established after the 911 attacks by presidential order to coordinate programs and propose policies for information systems and physical facilities supporting such information systems of critical infrastructures.

E. Law Enforcement and Prevention

1) Law Enforcement Response to the Cyberterrorism Threat

In many ways the law enforcement response to cyberterrorism must be drastically different from that of traditional crimes coming to the attention of police.

\textsuperscript{134) S. 187. 108th Cong.t § 5.}
\textsuperscript{135) S. 22, 108th Cong. (2003).}
departments. Law enforcement officers are accustomed to the investigation of crimes that transpire in the “real world”. Most criminal investigations center on a single crime scene and rely upon the accounts of eyewitnesses in order to identify the perpetrator of a crime. Further, linking the physical evidence at the crime scene to suspicious individuals serves a vital function in handling many conventional cases.

(1) Law Enforcement in the Cyber World

Crimes such as cyberterrorism that occur in the online environment lack these traditional elements. Beyond the absence of physical evidence and eyewitnesses, the concept of a crime scene is largely ambiguous for cyberterrorism events. Cyberterrorism creates a "fractured crime scene" in that the attacker may be physically located in one country, route his attack through a server in a different country, that ultimately produces harm in yet another country. For example, when the Air Force Rome Lab in New York was under cyberattack in 1994, investigation linked it to a local Internet service provider (ISP). Further examination showed the attack to have been routed to New York from a Washington State ISP, but ultimately to have originated in the United Kingdom. Such global considerations obviously overextend the resources and jurisdictions of local law enforcement.

Additionally, a cyberterrorism event is likely to be one of a series of similar occurrences separated in time or location—a scenario not often handled by law enforcement officers who overwhelmingly tend to handle cases as unrelated criminal incidents. It is clear from these distinctions that cyberterrorism requires a fresh response from law enforcement officers trained in both terrorist behavior and information technologies.

However, such training is not yet commonplace in the United States. A study of North Carolina law enforcement entities shows most departments to be under-prepared to respond to cyberterrorism should it occur within their jurisdictions.\footnote{Parker, A. M. S., Cyberterrorism: An examination of the preparedness of North Carolina local law enforcement. Security Journal, 23, 2010.} Importantly, these findings hold across all sizes of jurisdictions from small rural to large urban departments. Only one of the twelve interviewed police departments reported having a dedicated terrorism unit, although every department reported having at least one officer who had received some anti-terrorism training. As regards cyberterrorism specifically, only half of the North Carolina departments employed officers who had undergone cyberterrorism training. Further, merely one fourth of these departments had identified a procedure for handling cyberterrorism attacks within their jurisdiction. Finally, only a single department had made a specific hire for cyberterrorism prevention and response.

(2) Need for Federal Cooperation and Guidance

This lack of focus on cyberterrorism was undergirded by a pervasive sentiment that cyberterrorism should be handled at a higher level. The North Carolina departments largely agreed that due to their vaster resources, it was more appropriate for state and federal governments to handle cyberterrorism cases. The federal government has undertaken the responsibility of developing a set of procedures for a range of natural disasters and terrorist acts that are then disseminated to local and state jurisdictions. Likewise, the federal government should research and develop a protocol for responding to cyberterrorism events in order to assist the first responders to such acts.\footnote{Hua, J. & Bapna, S., How can we deter cyber terrorism? Information Security Journal: A Global Perspective 21, 2012.}

It has been suggested that the federal government can and should provide support to local departments in a number of ways.\footnote{Hua, J. & Bapna, S., How can we deter cyber terrorism? Information Security Journal: A Global Perspective 21, 2012.} The primary needs of most
departments are funding for cyberterrorism initiatives, specialized training programs and equipment. Supplying local law enforcement with the monetary support they need; developing training on effective counter-cyberterrorism procedure; and providing the technology (even old equipment that has been replaced in the federal agencies) to detect and investigate cyberattacks represent invaluable resources for a local department’s preparedness.

Also, the federal government can facilitate investigating cyberterrorism by encouraging alliances between local law enforcement and Internet service providers.\textsuperscript{141)\textsuperscript{141}} Allowing and encouraging ISP’s to use the latest technologies in order to record connection histories can provide vital information to law enforcement investigations of cyberterrorist incidents. Promoting ISPs to share this information with local departments following such an attack represents an important avenue available to the federal government in combating cyberterrorism. The Cyber Security Enhancement Act of 2002, a subsection of the Homeland Security Act, provides legal protection for ISPs that cooperate in this manner with investigations.

Additionally, federal law enforcement needs to collaborate with state and local law enforcement in the investigation of cyberterrorism and apprehension of cyberterrorists. As the Rome Labs case illustrates, a cyberterrorist attack that affects a local department is likely to have originated outside of the area, if not outside of the country entirely. The federal government is obviously going to be more effective at eliciting the help of allied nations in the investigation of such crimes. Ultimately, these attempts may be thwarted in countries that have yet to criminalize cyberterrorism (although the number of such countries is diminishing)\textsuperscript{142)} in

\textsuperscript{140) Brenner, S. W., At light speed: Attribution and response to cybercrime/terrorism/warfare. The Journal of Criminal Law and Criminology, 97(2), 2007.}
\textsuperscript{141) Hua, J. & Bapna, S., How can we deter cyber terrorism? Information Security Journal: A Global Perspective 21, 2012.}
\textsuperscript{142) Dick, R. L., Testimony before the House Committee on Governmental Reform, Government
nations that covertly sponsor such attacks. However, in many cases federal cooperation has the potential to assist local departments in cyberterrorism enforcement beyond its own borders.

(3) Global Cooperation in Law Enforcement

The United States federal law enforcement should strive for international alliances organized to combat cyberterrorism. One such organization is the United Nation’s International Multilateral Partnership Against Cyber Threats (IMPACT). While IMPACT is not aligned specifically to fight cyberterrorism, their 144-country membership creates a web of international agencies, corporations, academics and industry experts that serves (amongst other goals discussed below) to assist in the recognition of and reaction to cyber threats. Relying upon information garnered from various global resources can help to increase the identification of cyberterrorist events and provide a “best practices” response to such instances. Further, the FBI reports collaboration with various nation-states including Canada, the United Kingdom, Columbia and the Ukraine to provide international cooperation in the investigation of cyberattacks; a resource that could easily be utilized in the event of cyberterrorism.


2) Prevention Efforts from State/Local and Federal Law Enforcement Agencies

Response and investigation of cyberterrorist attacks is but one aspect of law enforcement’s role in combating cyberterrorism. Prevention of cyberterrorist attacks represents a proactive behavior that can greatly diminish the threat posed by cyberterrorists. Increasing the rate of successful identification of cyberterrorists via information sharing and publicizing increased punishment of cyberterrorist activity may provide some deterrent value.146 However, responses that focus instead on the prevention and early detection of cyberterrorism will potentially have a larger impact on cyberterrorism threats.147

(1) Prevention at the Federal Level

The main preventative role of the federal government is arguably that of increasing international communication on cyberterrorism. Ogun (2012) suggests exploring how the international organizations of Interpol and Europol can assist efforts to prevent cyberterrorism. IMPACT, the multinational organization discussed above, is an UN-sponsored organization comprised of national governments, private corporations and field experts designed to help these entities share information so that they can lead the development of strong cyber protection on a global scale. The US federal government representatives to this coalition can transfer the lessons learned from other countries to agencies and corporations within its borders. Likewise, threats encountered within the US can serve to educate our global IMPACT partners and promote greater global cybersecurity, ultimately impeding cyberterrorist agendas.

(2) Prevention at the State/Local Level

The greatest effect that smaller governments can have on reducing the cyberterrorism threat is through actively engaging the community to be aware of potential cyberterrorist activity on the Internet.\(^{148}\) Local and state law enforcement should educate their citizens to be alert to suspicious online activity and encourage them to report such behavior to a dedicated unit.\(^{149}\) Ideally, law enforcement would train an informal network of civilians on how to recognize potential cyberterrorist groups and on the procedure for documenting and reporting their discoveries to law enforcement.\(^{150}\) Such an endeavor would increase the reporting and web of knowledge concerning the presence of terrorist activities online.

3) Educating the Public and Corporate Entities on the Cyberterrorism Threat

Recognizing and reporting cyberterrorist threats represents one way that educating the public can diminish such risks. Another aspect of civilian education concerns providing general knowledge of cybersecurity.\(^{151}\) Civilians who practice unsecure Internet behaviors create weaknesses that can be exploited by cyberterrorists.\(^{152}\) Informing the public on the importance of securing home wireless networks through even the simplest means of employing strong password protection for Internet access can decrease the risk of cyberterrorist attacks. Further, the national government should mandate ISPs to require passwords for every wireless router they supply and encourage them to employ the most recent tech-

\(^{152}\) Holt, T. J., Exploring the intersections of technology, crime, and terror. Terrorism and Political Violence, 24, 2012.
nologies in cybersecurity; although many ISPs currently engage in these behaviors as standard practice.153)

Historically, government agencies have been met with resistance from the private sector when it comes to partnering on cyberterrorism initiatives.154) Corporations fear competitors obtaining delicate information, negative press associated with cyberattacks and the discovery of vulnerable infrastructure. Nevertheless, such collaboration represents a vital endeavor as private companies manage nearly the entire US critical infrastructure.

Corporate entities should be urged to adopt the newest authentication technologies in order to strengthen control over their own networks.155) Corporations need to be informed as to points of vulnerability within their network and ways to strengthen their online presence from threat of attack. InfraGard provides such a service to over 50,000 private and public entities within the United States.156) This FBI program provides private corporations and individuals with information on the techniques of cyberterrorist activity and advice on how to minimize their victimization risk. Through local chapters led by an FBI Special Agent Coordinator, interested individuals and companies can coordinate with fellow community members on how to proceed in the event of a cyberterrorist attack within their area. Such collaboration serves to decrease the threat of cyberterrorism, increases information sharing on cyberterrorist events and minimizes the harm caused by such acts.

Ideally, corporations should be proactive and build their network with security

being of paramount importance from the start.\textsuperscript{157)} It is safer to design a secure network from the beginning than it is to anticipate and correct the potential weaknesses in a system that is already in place. Corporations should also take ownership over training their employees on the threat of cyberterrorism and teach them to practice secure habits at their workspace. Finally, corporations should be encouraged to report cyberterrorism and to seek prosecution, which is speculated to otherwise be rare due to the fear of negative publicity.\textsuperscript{158)}

4) Law Enforcement Training Initiatives to Combat Cyberterrorism

Training for cyberterrorism appears to be largely nested within other cybercrime training programs that are designed to teach law enforcement officers how to detect and respond to digital evidence. These training initiatives are primarily located among the FBI’s 16 Regional Computer Forensic Laboratories (RCFLs) headed by the RCFL National Program Office (NPO). The NPO was established in 2002 to oversee creation of a nationwide RCFL program, whose responsibilities include the examination of digital evidence pertaining to investigations of terrorism, child pornography, financial crimes, as well as a number of other cybercrimes (Regional Computer Forensics Laboratory, 2012). According to the Department of Justice’s FY 2011 Annual Report for the RCFL program, over 32,000 individuals were trained by the RCFL between the FY 2004 and FY 2011 period, with the result that an estimated one in every three U.S. law enforcement agencies employs at least one officer who has attended a RCFL sponsored cyber training. Although these training sessions may not focus specifically on counter-cyberterrorism measures, it is often unknown whether a cybercrime has been committed by a terrorist.


group, an individual, or a nation-state, making it important to have local officials who are educated in seizing, collecting, and examining computer evidence regardless of the culprits or the motive.

Another agency created to help fight cyberterrorism is the National Cyber-Forensics & Training Alliance (NCFTA). The NCFTA was created in 1997 in order to combine the expertise, communication, and resources by enlisting the help of law enforcement agencies, private industry, and academia. Included in this agency are initiatives that enact international cooperation through internships designed to foster a greater knowledge base regarding cybercrime. For example, in 2010 investigators from the Ukraine, Lithuania, the Netherlands, Australia, Great Britain, and Germany convened for 90 days in an internship program designed to share knowledge and assist investigations. Training on an international platform is seen as necessary to combat the inherently global source of cyberterrorism, and the NCFTA has been hailed by Barak Obama’s administration as an “effective model” in national cyber security. It is important not to overlook the cooperation with private enterprises, which provide not only the best subject matter experts (SMEs) but also some of the most significant intelligence to the alliance.

5) Research on Law Enforcement and Cyber Terrorism

Empirically there is a lack of research examining the training of law enforcement to prepare for cyberterrorism. One notable exception is the study conducted by Parker (2010), who surveyed 12 police agencies in North Carolina to examine perceived cyberterrorism preparedness among the different departments. The survey asked the departments if any member had attended any type of anti-terrorism


training, and then if they had ever attended any cyberterrorism training. The results showed that 58 percent of agencies reported at least one member had received specialized cyberterrorism training and that the FBI or the U.S. Secret Service provided the majority of these training initiatives.¹⁶¹)

It must be noted, however, that problems with the definition of cyberterrorism obscure our understanding of training initiatives taken by law enforcement. It is important to differentiate between training designed to respond to real-world disasters caused by computer technology (e.g. water contamination) versus an attack based solely in cyberspace (e.g. denial of services attack) that cripples government agencies. Another issue is the degree of training, such that an officer who received even the slightest amount of cybercrime training may be seen as a cyberterrorism expert. Likewise, departments who take a broad definition of cyberterrorism may see traditional terrorist response training as equivalent to cyberterrorism training and report it as such. More research is needed, therefore, to understand the true extent of law enforcement preparedness in regard to cyberterrorist attacks.

2. Cyberterrorism Response System of the United Kingdoms

A. Overview

The UK punishes hackers and disseminators of viruses on the legal basis of Regulation of Investigatory Powers Act 2000, Computer Misuse Act 1990 and Anti-terrorism, Crime and Security Act 2001. The UK actively adopts basic information security and privacy protection policies of the EU, and also accepts information security policies primarily lead by other countries such as the United

States and the EU. In particular, the UK is an international leader in information security by realizing various guidelines of the EU into domestic laws.

**B. The Legal System**

The previous Prevention of Terrorist Act 1989 of the UK was a militaristic law with very strong provisions, and for this it was criticized for high possibility of human rights violations. To resolve these issues, the UK legislated the new Terrorism Act 2000 in the 20th of July, 2000, which was put into effect in the 19th of February, 2001. This law has bolstered investigatory powers on terrorism and recognized procedural exceptions in terrorist cases by allowing confiscation of terrorist funds and checking bank accounts for the purpose of investigation in terrorism.

Legislated after the 911 attacks in 14th of December, 2001, the Anti-terrorism, Crime and Security Act 2001 includes many counter-terrorist provisions necessary for responding to terrorism.

**C. Organizations against Cyberterrorism**

The Centre for the Protection of National Infrastructure (CPNI) is a new institution established in February of 2007, through incorporation of the Communications-Electronics Security Group, the National Infrastructure Security Co-ordination Centre and the National Security Advice Centre.\(^{162}\) CPNI provides security consultation service to public and private institutions related to national information infrastructure of the UK in order to prevent terrorist threat against national infrastructure. In this effort, multiple government departments and in-

---

\(^{162}\) NISCC was the representative counter-cyberterrorism and electronic violation response agency. NISCC was established 20\(^{th}\) of December, 1999 by the Home Secretary to protect government agencies, institutions and organizations in the private sector related to critical infrastructure from electronic attacks.
stitutions collectively participate, and performs comprehensive security advice activities for information, personnel and physical security of public and private organizations related to national infrastructure.\textsuperscript{163)}

The National Hi-Tech Crime Unit was established in April of 2001 under the British Police for the purpose of computer crime investigation. It is comprised of four sections, which are Investigations, Intelligence, Tactical and Technical Support and Digital Evidence Recovery. Investigations section was in charge of investigating organized or serious high-tech crime, and Intelligence section provided strategic and tactical intelligence to all law enforcement agencies and intelligence agencies of the UK. Digital Evidence Recovery section provided forensic technical support for high-tech crime investigation, and Tactical and Technical Support section provided technical support and consulting for UK courts and the government. In 2006, NHTCU was incorporated into the Serious Organized Crime Agency, newly established in accordance with the Serious Organized Crime and Police Act 2005. However, as SOCA only focused on national matters and failed to deal with problems related to public welfare such as cybercrime, the Police National E-Crime Unit was established under the Metropolitan Police Service in 2008 at the persistent request of private companies.\textsuperscript{164)}

3. Cyberterrorism Response System of the Federal Republic of Germany

A. Overview

In general, recognition for the need of improving safety and security of IT-dependent critical infrastructure and the will to adopt the necessary measures are

\textsuperscript{163)} http://www.cpni.gov.uk/About/whatWeDo.aspx.

\textsuperscript{164)} Lee, Dong Hee et al., Development of International Cybercrime Academy Model(Mid-term Report), National Police Agency, 2010.
gradually increasing in Germany. Especially after the 911 attacks on the United States, Germany began to focus on international cooperation out of desperation. Established in 1991 under the Federal Ministry of the Interior, Federal Office for Information Security oversees cyberspace security work in Germany. More specifically it provides support for legal tasks of the police and the prosecutors office, provides support for utilization and evaluation of intelligence collected by surveillance and intelligence activities on terrorist activities, and provides consultations for the private sector in case of an IT security problem.\textsuperscript{165}

**B. Legal System**

Germany was among the first countries in Europe to implement legal sanctions to punish terrorists. While extending range of punishable terrorist acts and increasing severity, special provisions were also made that severely limited the rights of terrorist suspects or defendants. The German government established strengthened counter-terrorist policies after the 911 attacks in 2001. Main elements of the counter-terrorist policies include procurement of budget for counter-terrorist policies, strengthening authority of efficient counter-terrorist institutions through legal amendments, improving the personal identification system, and bolstering security of critical infrastructure.

**C. Organization against Cyberterrorism**

With regards to cyberspace security, the Federal Office for Information Security is mainly responsible, and the Federal Criminal Police Office is charged with investigation and digital evidence analysis. Under the Federal Criminal Police Office is the Serious and Organized Crime Division, which is tasked with high-tech/computer crime. The high-tech/computer crime section consists of four teams.

The first team is charged with administrative management and international working group activities, the second team is charged with crime information and strategy analysis and coordination with the G8 24/7 Network, the third team is charged with Internet monitoring, and the fourth team is charged with investigations relating to cyberspace. The BKA separates operations of international cooperation activities and real-time international coordination, and also separately operates information analysis of cyberterrorism such as crime information and strategy analysis. The BKA operates various international cooperation activities with the National Central Bureau of INTERPOL, National Liaison Office of EUROPOL, G8 24/7 Network and United Nations Office on Drugs and Crime.

In order to implement the Convention on Cybercrime of the Council of Europe, Germany has made the 41st amendment of the criminal law in August of 2007 to deal with computer crime. Due to this amendment, Germany is recognized as the international standard of cybercrime regulations, and also as a leading nation in the field of cybercrime not only in international cooperation but also as an exemplary model in domestic legislations.166)

4. Cyberterrorism Response System of the French Republic

A. Overview

France recognizes cyberspace security as a national security issue, and has the General Secretariat for Defence and National Security (SGDSN), directly under the Prime Minister of France, in charge of cyberspace security. This is clearly stipulated Decree 96-67, declared in 29th of January, 1996, for the SGDN to directly take charge of information systems security. Also, Decree 2001-693, declared on

31st of July, 2001, stipulates the establishment of the Central Directorate for Information Systems Security (DCSSI) within the SGDSN, charging it with security of cyberspace and French information systems and foster trust in the coming information society. In 2009, DCSSI was replaced by the newly established French Network and Information Security Agency (ANSSI), under Decree 2009-834.

B. Legal Systems

France does not have a separate legal system regarding cyberattacks or cyberterrorism. However, cyberattacks are regulated by provisions on information crime (cybercrime) in the criminal law.¹⁶⁷)

Under article 323 of the criminal law, there are penal codes for ① unauthorized access of a computer system, ② obstruction of function of a computer system, ③ fraudulent introduction, deletion or modification of data in a computer system, ④ and participating in a group or conspiracy established for the commit of the above crimes as acts of violation of automated data processing systems.

While France does not have any specific laws regarding cyberterrorism, under current criminal law (§421), terrorist acts are stipulated as individual or collective acts that seriously disturb public order through intimidation or terror, and includes acts of violation of automated data processing systems as stipulated in article 323 as terrorist acts.

C. Organizations against Cyberterrorism

The Central Directorate for Information Systems Security was established under SDGN in May of 2001, which was replaced by French Network and Information Security Agency (ANSSI) in 2009. Main strategic objectives of ANSSI are securing

¹⁶⁷) For detailed information on criminal law sanctions on violation of automated data processing systems
information systems of critical infrastructures, securing cyberspace and securing confidential communications between government institutions.\(^{168}\)

SGDSN is in charge of international and domestic security matters, and under direct authority of the Prime Minister of France, it coordinates activities of government agencies regarding cyberspace security and critical infrastructure protection. Decree 96-67 stipulates that SGDSN is in charge of Information Systems Security. SGDSN focuses on information security of both the defence and private sectors, and also spends efforts on national defence policies and security policies as well as scientific and technological innovations. In this regard, SGDSN closely cooperates with DCSSI,\(^{169}\) and now its replacement, ANSSI.

5. Cyberterrorism Response System of Japan

A. Overview

Japan has yet to face any serious cyberterrorist threat, but cybercrime such as hacking is rapidly increasing. In response, the Ministry of International Trade and Industry is leading efforts to prevent cyberterrorism in advance, such as conducting analysis on current status of computer networks directly linked to public welfare, namely electric power and oil industries, and making guidelines for counter-cyberterrorism.

The Cabinet Secretariat, a Japanese government agency, lead the establishment of counter-cyberterrorist policies for social and industrial infrastructure. In August of 1997, with the government in lead, the Cabinet Office for Information Security

\(^{168}\) ANNSI, Information systems defence and security: France’s strategy, Feb. 2011.

was established, formed a committee for security measures for large-scale industrial facilities, pursued standardization of network protection technologies and operating systems, and proposed necessary measures for enhancing security. The Cabinet Office for Information Security was replaced by the National Information Security Center in 2005.

After the 911 attacks in the United States, Japan made strengthening counter-terrorist measures a priority and made some major progress in counter-terrorism capability through a special counter-terrorist action plan and other various follow-up action plans. In April of 2002, the National Incident Response Team (NIRT) was established to take charge of sharing information on cyberattacks against the e-Government and emergency response against cyberterrorism. A Cyber Force, consisting of specialists, was also established in the National Police Agency. In October of 2003, the Japanese government declared a comprehensive strategy for national information security and it was put into action. It strengthened the counter-terrorism response organization and its role in the Cabinet Secretariat, and it is pursuing establishment of information protection center, a private and public sector surveillance system.

As such, Japan, as advanced nation in information technology, is forming inter-institutional cooperation network, and is systematically preparing information security measures against cyberterrorism and cyberwarfare in the future.

B. Legal System

With regards to cyberterrorism, Japan has the Basic Act on the Formation of an Advanced Information and informations Network Society, also known as the ‘Basic IT Act’. This Act stipulates measures regarding safety and reliability of networks to secure safety of information and informations network, so that people may use networks without any fear or concern (article 21). Japan also has the "IT Strategic Headquarters" to make prioritized plans for safety and reliability of information
and information network. In this respect, the Act is in many aspects similar to South Korea’s Framework Act on National Informatization.\(^{170}\)

One particularity in Japan is that the Ministry of Justice, in the spirit of Convention on Cybercrime, declared plans in March of 2003 for a new legislation to add a new “Offence of Making Computer Virus,\(^{171}\)” of which actus reus is making and storing malware. In February of 2004, the Ministry of Justice submitted proposals for an amendment to the Penal Code including the new provisions regarding computer virus. In June of 2011, the Act for Partial Amendment of Laws such as the Penal Code to Deal with Advancement of Information Processing passed the Japanese Diet. The Penal Code was amended, adding provisions on the act of making electronic records that gives wrongful instructions to computers(Penal Code, Chapter 19, Article 168, Paragraph 2 and 3), and came into effect in July of 2011. Therefore, under these new provisions, the act of making, providing, acquiring or storing a computer virus for the purpose of executing on another person’s computer without authorization or justification violates Article 168 Paragraph 2(Making of electronic records giving wrongful instructions) and Article 168 Paragraph 3(Acquiring of electronic records giving wrongful instructions). Penalties for the violation of making and providing a computer virus is, in accordance with Article 168 Paragraph 2, under three years of maximum imprisonment or a fine under 500,000 yen, and penalties for the violation of acquiring or storing a computer vi-


\(^{171}\) Here, malware is a portmanteau for malicious software, which is a general term used for any computer code or software made with malicious intent for wrongful and harmful effects. Examples of a malware include virus, backdoor program, key logger, trojan horse, macro virus used in Microsoft Word or Excel, boot sector virus, script virus(e.g. BAT, Javascript), crineware, scareware, spyware, malicious adware. In Japan, this is referred to as “wrongful program with malicious intent” or “wrongful program”(トレンドマイクロ:セキュリティ用語集 参照). Therefore, the common term for such program in Japan and South Korea can be considered as malware.
rus is, in accordance with Article 168 Paragraph 3, under two years of maximum imprisonment or a fine under 300,000 yen.\(^{172}\)

As such Japan refers to the act of making malware such as a typical computer virus as “Offense of Making Computer Virus”. Japan amended the Penal Code to add new provisions that punish such offences, and these provisions are generally referred to as the Computer Surveillance Law.\(^{173}\)

C. Organizations against Cyberterrorism

Organizations in Japan that deal with cyberterrorism are the National Information Security Center, IT Strategic Headquarters, National Police Agency, Ministry of International Affairs and Communications, Ministry of Economy, Trade and Industry, Japan Computer Emergency Response Team Coordination Center (JIPERT/CC) and various private institutions. The National Information Security Center was established in 2005 in response to rapid development of IT and its increasing importance to infrastructure, public welfare and the economy. The National Information Security Center formulates strategies and coordinates information security efforts of government agencies, critical infrastructures, private businesses and individuals to protect central government computer systems, critical infrastructure and international cooperation and contribution concerning information security.\(^{174}\)

In April of 2001, the National Police Agency of Japan has created a special task force in the Cyber Terrorism Technology Office of the Info-Communications Bureau called the Cyber Force. Consisting of 60 specialists, the Cyber Force is tasked with preventing high-tech crimes and cyberterrorism and facilitate recovery

\(^{172}\) 情報処理の高度化等に対処するための刑法等の一部を改正する法律案新旧対照条文”. 法務省. www.moj.go.jp. 2011年6月20日 閲覧。


from any damages from high tech crime and cyberterrorism. The Cyber Force monitors any hacks against police networks through 57 offices including the Cyber Force Center, which is located in a civilian building in Tokyo. Along with its Cyber Force Center in Tokyo, it also has offices in eight local police agencies in Osaka, Nagoya, Hiroshima, Fukuoka, Sendai, Sapporo, Saitama and Takamatsu to facilitate police activities such as criminal investigations. The Cyber Force operates the Kenchi(検知) Network System, which monitors intrusion detection systems installed in police agencies throughout Japan 24 hours a day, and conducts collection and analysis of information from the intrusion detection systems.\(^{175}\)

In actuality, 'High-tech Crimes Comprehensive Countermeasures Center' of the Tokyo Metropolitan Police Department conducts investigations in cyberterrorism, while cybercrime in general is investigated by local police agencies. Under High-Tech Crime Technology Division of the Info-Communications Bureau of the National Police Agency of Japan are digital evidence analysis center and the Cyber Force Center. In particular, the Cyber Force Center was established in 1999 to become a national center of high-tech cybercrime countermeasures, to lead police agencies technologically in matters of cybercrime.\(^{176}\)

### 6. Cyberterrorism Response System of India

#### A. Overview

India wary that cyberterrorist attacks can cause collapse of information networks such as electronic government infrastructure by means such as combined usage


of virus attack and hacking. To deal with this threat, India has legislated various laws and established response systems.

B. Legal System

India, taking notice of threats to cyberspace such as DDoS attacks which can cause an overload of information systems of government and government agencies, resulting in serious financial and strategic losses. To prepare against such cyberterrorist attacks, India has legislated Information Technology Act 2000. In case of a DDoS attack, following provisions apply.

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, (a) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, (b) disrupts or cause disruption of any computer, computer system or computer network, (c) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means, the person shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Also, in case a combination of network damage and disruption is used in an attack, in other words attack involving a combination of computer intrusion, virus attack and hacking, the following provisions apply.

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, (a) accesses or secures access to such computer, computer system or computer network, (b) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, (c) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system
or computer network, (d) disrupts or causes disruption of any computer, computer system or computer network, (e) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.

Here, the expression “contaminant” means any set of computer instructions that are designed (a) to modify, destroy record, transmit data or program residing within a computer, computer system or computer network, (b) or by any means to usurp the normal operation of the computer, computer system or computer network. The expression “computer virus” means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource.

As such, any person tampering with computer source documents shall be punishable with imprisonment up to 3 years or with fine, which may extend up to 200,000 rupees or with both. Furthermore, if a person causes wrongful loss or damage to any person, by destroying deleting or altering any information residing in the owner’s computer resource or diminishes its value he commits hacking and thus, violates the privacy of the owner. The person hacking shall be punishable with imprisonment up to 3 years or with fine, which may extend up to 200,000 rupees, or with both. However, an innocent infringer will not be liable if he proves that he committed the act without any intention or knowledge. A network service provider will be liable for various violations and contraventions mentioned under the Act if he makes available any third party information or data to a person for the commission of an offence or contravention. However, an innocent infringer will not be liable if he proves that he committed the act without any intention or knowledge. A network service provider will be liable for various violations and contraventions mentioned under the Act if he makes available any third party information or data to a person for the commission of an offence or
General Issues of Cyberterrorism

contravention. However, a network service provider will not be liable if he proves that the offence or contravention was committed without his knowledge or he had exercised all due diligence to prevent such commission. Thus, these provisions can be safely invoked for meeting challenges posed by network damage and disruptions caused by cyberterrorists.177)

Also, the state government of Karnataka, with authority deriving from Information Technology Act 2000, made the Information Technology (Karnataka) Rules 2004. The Rules define “Cyber Cafe” as premises where the Cyber Cafe Owner/Network Service Provider provides computer services including Internet access to the public. Rule 3 (1) provides that the owner of the Cyber Cafe shall take sufficient precautions so that computers and computer systems in the Cyber Cafe are not used for any illegal or criminal activity, Rule 3 (2) mandates that the Cyber Cafe Owner / Network Service Provider shall not allow any User to use his Computer, Computer System and/or Computer Network without the identity of the User being established before him before use.

The Rule provides that the intending User may establish his Identity by producing any Photo Identity Card issued by any School or College or a Photo Credit Card of any Bank or Passport or Voters Identity Card or PAN Number Card issued by Income-Tax authorities or Photo Identity Card issued by the Employer or Driving License to the satisfaction of Cyber Cafe Owner. Rule 4 (1) provides that after the identity of the User is established, the owner of the Cyber Cafe or the manager or the attendant or on his behalf any authorized person managing the Cyber Cafe shall obtain and maintain the following information in the Log Register for each user: (i) Name of the User, (ii) Age and Sex of the User, (iii) Present residential address of the User, (iv) Log in time, and (v) Log out time. Rule 4 (2) provides that if a User cannot produce any Photo Identity Card to establish his

identity to the satisfaction of the Cyber Cafe Owner / Network Service Provider, he may be photographed by the Cyber Cafe Owner / Network Service Provider after obtaining his consent using a ‘Web Camera’ hooked onto one of the computers or computer systems in the Cyber Cafe and the User shall be explained that his photograph will be taken and stored in the hard disk of the computer, for verification by Law enforcement authorities, whenever required.

In addition to the entries made in the log register, the Rule further provides that in case the User does not agree for storing his photograph he shall not be allowed to use any computer, computer systems and / or computer network or access to the Internet in the Cyber Cafe, Rule 4 (3) provides that all time clocks in Cyber Cafes must be regularly checked and synchronized with Indian Standard Time (IST), Rule 4 (4) provides that maintaining proper account of the User as explained shall be the responsibility of the Cyber Cafe Owner / Network Service provider, Rule 5 (5) provides that the Log Register and the Photograph of the User shall be maintained by the Cyber Cafe Owner / Network Service Provider for a minimum period of one year and the same shall be provided to law enforcement agencies as and when required, Rule 4 (6) provides that the Cyber Police authorities may on complaint inspect Cyber Cafes at all reasonable time to ensure compliance of these rules, If any Cyber Cafe Owner / Network Service Provider fails to maintain Log Register and records he shall be liable for penalties as provided in the Act or any other Law, for the time being in force. These provisions are sufficient to take care of illegal use of Cyber Cafe for terrorist activities, Further, the government can also block web sites propagating cyberterrorism.

It must be noted that the Indian Computer Emergency Response Team (CERT-In) has been designated as the single authority for issuing of instructions in the context of blocking of web sites, CERT-In has to instruct the Department of Telecommunications to block the web sites after verifying the authenticity of the complaint and satisfying that action of blocking of web site is absolutely essential.\(^{178}\)
The 2008 Mumbai terrorist bombings was a turning point for India. After these attacks, the legislative and executive branches of India amended Information Technology Act 2000, modifying provisions on offences related to cybercrime and cyberterrorism, and explicitly distinguished the two acts. According to the amended Information Technology Act 2008, the concept of cyberterrorism is destruction of property, loss of life, disrupting critical infrastructure and essential supplies and services, and even without physical damage, causing terror among the public alone leads to the commitment of a terrorist act. The Act also stipulates acts of violation on secret information related to national security and diplomacy as acts of cyberterrorism. Under the Act, a cyberterrorist act is punishable by imprisonment, and which can be extended to life imprisonment.

C. Organizations against Cyberterrorism

The menace of cyberterrorism can be effectively curbed, if not completely eliminated, if the three sovereign organs of the Constitution work collectively and in harmony with each other. The legislature can provide its assistance to the objective of preventing cyberterrorism by enacting appropriate statues dealing with cyberterrorism. To this end, a new chapter specifically dealing with cyberterrorism was added to Information Technology Act 2008, which amended the existent criminal law to conform with current forms of terrorism.

The judiciary can play its role by adopting a stringent approach towards the menace of cyberterrorism. It must, however, first tackle the jurisdiction problem because before invoking its judicial powers the courts are required to satisfy themselves that they possess the requisite jurisdiction to deal with the situation. In this regard, the scholars point towards the following “theories” under which a country may claim prescriptive jurisdiction, which are (a) a country may claim jurisdiction

based on “objective territoriality” when an activity takes place within the country, (b) a “subjective territoriality” may attach when an activity takes place outside a nation’s borders but the “primary effect” of the action is within the nation’s borders, (c) a country may assert jurisdiction based on the nationality of either the actor or the victim, (d) in exceptional circumstances, providing the right to protect the nation’s sovereignty when faced with threats recognized as particularly serious in the international community. In addition to establishing a connecting nexus, traditional international doctrine also calls for a “reasonable” connection between the offender and the forum, and to this end Information Technology Act 2000 section 1 (2) and section 75 grants Indian courts with long arm jurisdiction to deal with cyberterrorism.\textsuperscript{179}

After the 2008 Mumbai terrorist bombings, amendments of Information Technology Act 2000 and legislation of National Investigation Agency Act 2008 were passed by the Parliament with almost no discussion, and with these laws, a new federal agency, the National Investigation Agency, was established. The new National Investigation Agency can investigate terrorist related crimes anywhere in India without special permissions from Indian states. Also, India is planning to establish National Counter Terrorism Centre, modeled after the National Counterterrorism Center of the United States.

7. Implications

According to the materials seen so far, the United States, Germany and France have a main organization that take full charge of cybersecurity, while Japan, UK and South Korea have multiple agencies with their own responsibilities. Currently

in South Korea, major organizations responsible for cyber emergencies are the National Cyber Security Center of the National Intelligence Service, the National Defence Cyberwarfare Response Center of the Ministry of National Defense, the Korea Internet Security Center of the Korea Communications Committee (under the Korea Internet and Security Agency), and those with more minor roles are Internet Crime Investigation Center of the Supreme Prosecutor’s Office, the Cyber Terror Response Center of the National Police Agency, the National Security Research Institute, the Information Sharing and Analysis Center (ISAC). There are many diverse government agencies dealing with cyberspace security, but there’s a lack of a legal system that could become grounds for coordinated activities of these government agencies, and there is no response system in place to respond to a cyberviolation with celerity and strong punishment. Therefore, emergency management system in case of a cyberterrorist attack needs to be bolstered. Also, research is important in developing effective responses to cyberterrorism. In the United States, after the 911 attacks, cyberspace security became a research priority in the federal government’s research and development programs, bolstering research in cyberspace security. South Korea should also legislate the necessary law to form an organization along with the budget to bolster research and development in cyberspace security.

Another characteristic of response against cyberterrorism is strengthening international cooperation and mutual assistance. Due to developments in transportation and information technology, traditional terrorist activity is increasingly becoming multi-national, and therefore to prevent terrorist attacks international sharing of relevant intelligence is of paramount importance. In the 21st century, with developments in science, transportation, communication, and along with globalization and the coming of information society, international terrorist organ-

izations are using these developments to their own advantage, establishing a global terrorist network and deploying terrorist cells throughout the globe. Due to these developments, establishment of a domestic and international counter-terrorist network is inevitable to deal with this new threat. This is even more so for cyberterrorism.

With regards to legal system of cyberterrorism response, the UN Security Council Resolution 1368 and Resolution 1373 after the 911 attacks called upon the nations to legislate strong counter-terrorist laws. Adopting these requirements from the UN, most countries are preparing various systems against terrorism, The United States has legislated and executed the Homeland Security Act, and the United Kingdoms drastically strengthened its Prevention of Terrorist Act, Germany also legislated the Anti-Terror Law for the purpose of amending various security-related laws to adapt to the new forms of threats from terrorism. Japan and France also have legislated laws for the purpose of counter-terrorism, South Korea should also establish a national counter-terrorist legal system, and for transparency of counter-terrorist activities and the need for international cooperation, a new counter-terrorist law is necessary. In particular, there is need for discussions on new provisions or a new law dealing with cyberterrorism to effectively deal with cyberterrorism.

In addition, as malwares spread quickly and have significant negative impact on public trust of the Internet and computer programs, which now have become important social infrastructures, it cannot be denied that malwares is a grave threat to society, In light of this, the Japanese precedent of legislating a new specific law dealing with malware has significant implications for South Korea. As the offense of making computer virus in the Japanese Penal Code is structurally similar to the crime of falsification or alternation of special media records in the Korean Criminal Act, 'intent to offer for use' can be used as the subjective element of actus reus, and considering that the offence can be considered as an offence of endangerment against public trust in computer programs, the act of executing
wrongful program can be punished as a violation of harming public trust in computer programs. With the above considerations in mind, a draft for amendment to the Korean Criminal Act can be proposed as follows.

The Criminal Act Article 232, Paragraph 3 [Crime of producing malwares and other related acts]

① any person who makes or provides a program(malware hereafter) that can damage, destroy, modify, fabricate or disrupt operation of information system, data or program for the purpose of using it on an information processing device such as a computer are punishable by maximum 3 years imprisonment or 5 million won fine.

② Any person who use a malware, as stipulated in clause 1, on someone else's information processing device such as a computer are the same as the previous clause.

③ Attempt of clause 2 is punished.

④ For purposes stipulated in clause 1, any person who acquires or stores malware, as stipulated in clause 1, is punishable by maximum 2 year imprisonment or 3 million won fine.

In the above draft amendment, the punished acts are making, providing, using, attempting to use, acquiring or storing malware. In this context, the crime of making, providing, acquiring and storing malware requires an intent to use the malware on an information processing device such as a computer belonging to a person, which is because the act of making malware is a crime against society by violating public trust in special media records. Therefore, the target of crime is an information system such as the computer of another 'person', but by stipulating the act itself of 'making' or 'providing' malware as elements of actus reus, it has the advantageous effect of preventing cybercrime.181)
8. Conclusion

This chapter reviewed the general issues of cyberterrorism. Review of conceptualization of cyberterrorism indicates that from the international legal perspective, the greatest advantage of establishing a specific concept of cyberterrorism is that it can put an end to the controversy surrounding the principle of legality, where a specific concept can prevent increase of punishment. Despite this advantage, the decision to use the broad conceptualization of cyberterrorism as the research scope of this research is the research purpose of examining and analyzing recent concept of the Terrorist use of the Internet, as defined by the UNODC. It was previously pointed out that there can be significant logical fallacies in dealing with cyberterrorism in general and use of the Internet by terrorist organizations as the same subject matter.

Nonetheless this field of research is rapidly emerging, and the current trend of

181) To this end, the EU’s Convention on Cybercrime Article 6 makes legislations against the act of programming malware compulsory on all member states. Programming malware is prohibited on the premise of violating the following provisions:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a. the production, sale, procurement for use, import, distribution or otherwise making available of:
      i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
      ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
   b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
the conceptualization of terrorism is becoming more inclusive and broader after the 911 attacks, and thus the same trends in the conceptualization of cyberterrorism is an issue that cannot be ignored. Broadening of the conceptualization of terrorism is inextricably linked to the broadening of the conceptualization of cyberterrorism. This is why terrorist use of the Internet was examined as a form of cyberterrorism.

Based on this conceptualization, what follows is chapter 3, which examines Trends in Terrorist Use of the Internet, and chapter 4, which examines strategies and objectives of use of the Internet by terrorist organizations and counterterrorist measures of law enforcement institutions,
Chapter 3

Terrorist Use of the Internet and Counterterrorism Measures
I. Introduction

Violent acts tend to be conditioned by space just like any other human conducts. Generally speaking, a person cannot locate two or more different places and cannot travel far and fast enough to attack any target he or she wishes. Initially, land and water are only two spaces and thus human's conducts are conditioned by the characteristics of given space. With the advent of the 20th century, air is entered as the 3rd space in violent acts of human beings. Air made human's travel farther and faster and changed dynamics of violent acts. But, still time consumption and distance are some conditional obstacles for human’s violent acts.

In the beginning of the 21st century, humans are now observing that the advent of another space in our violent and non-violent acts, It is called cyberspace. Due to the inclusion of this 4th space, now human’s violent acts are conditioned by four spaces and substantially transformed strategically in result. The strategic meaning of cyberspace is substantial in that it indeed removes the restriction of
time and distance which air insufficiently reduced. Through cyberspace, an attacker can reach any distant target in almost real-time. Logistical operations supporting attack becomes much easier, faster, and cheaper.

Today’s problem of terrorist use of the Internet is a direct outcome of the inclusion of cyberspace in the theater of human’s violent acts. Cyberspace allows a (potential) terrorist to overcome physical barrier of speed and location in the aspect of logistics for terrorist attack. Cyberspace created a huge holistic space which connects everyone logging in with everyone else logging in in real-time bases. Information is abundant and easily available. Communication is convenient, secure, and readily available with low cost. This quality of cyberspace provides a huge strategic and also tactical advantage for terrorists by substantially reducing the cost of logistics relating to an actual violent attack. In result, cyberspace opens a condition that more number of (potential) terrorists is capable of conducting terrorist attacks. Therefore, the world is facing to higher chance of terrorism.

Although This chapter only focuses on terrorists’ use of internet regarding the strategic meaning of cyberspace, it is not confined only to the matter of terrorism. The strategic and tactical implication of cyberspace as the 4 dimension impacts much wider and deeper. As other types of human’s violent acts, war and crime are also affected by the advent of cyberspace in the same context just like terrorism, Warfare is also composed of non-combat logistics and combat operation. Cyberspace provides a substantial strategic and tactical advantage for the former aspect. Crime also includes two parts, criminal preparation and tools and actus reus of crime itself. Cyberspace provides a huge advantage for the former as well. An impact of cyberspace on terrorist is part of this broad trend.

This chapter discusses the issue of terrorists’ use of internet within the perspective of strategic and tactical dimension. It treats the issue as a fundamental transformation of theater of terrorism much conditioned by the inclusion of the 4th space, cyberspace, into traditional spaces. Based on that assumption, it introduces the current threats of terrorists’ use of internet, argues its strategic and
tactical meaning, and suggests current and potential counterterrorism measures and possibilities.

For the writing of this article, participant’s observation, qualitative interview, and content analysis of written materials are used. The author has obtained some first-hand experience of database building activity, conference meetings, seminars, and trainings on relative matters. Also, he had interviewed with many experts and practitioners on the issue of terrorists’ use of internet in many different occasions. Adding to those first-hand references, various written reports, manuscripts, books, and institutional reports and manuals are used for content analysis.

II. Theoretical Discussions

1. Terrorist Use of the Internet and Cyberterrorism

This article discuss on terrorist use of the Internet, not cyberterrorism. Generally speaking, terrorist use of the Internet and cyberterrorism are two different concepts. One is mostly about how terrorists use internet to commit terrorist acts in the real world, while the other is about terrorists’ commission of terrorist acts in the cyberspace or against virtual targets such as websites, ISPs, IT(Information Technology) infrastructure, and computer facilities. The topic interested in here is the former and thus exclusively discuss about that issue only.

To clarify the concept, it seems useful to apply the military analogy. There are kinetic and non-kinetic operations in military. Kinetic operation is mostly about combat operation which indeed strikes an enemy target by use of firepower.

Non-kinetic operation is about all other logistics which support military strike itself. It’s examples are intelligence, communication, resource mobilization, supply, transportation, and etc.\(^{183}\) Similarly, terrorism is also divided into kinetic and non-kinetic activities. Here kinetic operation is terrorist attack itself. Terrorist attack includes IED (Improvised Explosive Device) attack, suicide bombing attack, hostage taking, assassination, sabotage, armed assault, hijacking, etc., These garden varieties of acts are violent acts themselves which kill or maim human beings, or destroy building, facilities, and infrastructure. Psychological spread of fear or terrorizing is also included in this concept of kinetic operation of terrorism, Non-kinetic operation is anything which is related to and supports for kinetic operation. Recruiting, fund raising, licit or illicit money making, money transfer, sending terrorists, surveillance and intelligence, training and education, obtaining weapons and tools, establishment of hide-outs, etc, are all included in this non-kinetic operation.

Shortly speaking, terrorists’ use of internet is by definition non-kinetic operation, while cyberterrorism is kinetic operation by definition. Cyberterrorism is a terrorist attack itself which occurs in cyberspace. Examples are DDOS (Distributed Denial of Service) attack, cracking, spread of virus, worm, or spyware, electronic infiltration, and electronic information theft etc., This type of attack aims at web sites, server, computer system, and IT infrastructure. Their destructive effects are by far minimal, unsubstantial, and only annoying. There is some development of destructive potential in cyberterrorism, STUXNET is considered as having such potential (Interview with a cyberterrorism expert from OSCE(Organization for Security and Co-operation in Europe). But, empirical evidence is inconsequential so far.\(^{184}\)

Some argue that cyberterrorism may cause devastating effect by hijacking control

system of electricity, water, airplane, or traffic control system. But, again, evidence is inconsequential at this point, although those concerns may prove sound in the future.185)

Terrorist use of the Internet is a different matter. It normally means not attack itself but supporting activities for kinetic attack. Cyberspace has been actively used for this purpose since the 9.11 incident. Al Qaeda is believed to manage its global network through cyberspace.186) Any non-kinetic operation through cyberspace or with use of cyberspace is considered terrorist use of the Internet. The issue which this article is mainly interested in is as such,

2. Physics and Strategic Advantage of Cyberspace

Terrorist attack is bounded by logic of physics, Clarke and Newman(2006) recognized this logic and proposed that terrorists are restricted by situational conditions in their rational thinking process of terrorist attack operation. They argued that terrorists need more resources and preparation to attack against far target, while they need less against near target. Thus, distance between terrorists and terrorist target among others affects terrorists’ thinking process. Here the logic of physics regarding the distance is further and deeper explored.

Here two logics of physics are proposed to explain a rule of terrorist attack. The one is the relationship between terrorists’ striking power, terrorist target’s sus-

tainability, counterterrorism defense capability, and the distance between terrorists’ home base and target location. Here the distance plays an important role in equation. If target’s sustainability increases, terrorists’ striking power should be equally increased. If counterterrorism capability increases, terrorists’ resources (preparation, covertness, and operation sophistication, etc.) for attack need to be increased. But, here the distance works against terrorists. The stronger target’s sustainability and counterterrorism defense becomes, the more resources and striking power should be mobilized. In this equation, the longer the distance becomes, the more efforts should be put to transport more resources and stronger striking power. Thus, only few terrorists can attack against a target far away. In other words, terrorists are conditioned by the distance in their calculation of terrorist attack given terrorists’ striking power, counterterrorism capability, and target’s sustainability.

The second logic of physics can be found with the respect of speed. There can be a rule of physics between terrorists’ attack speed, speed of counter-terrorism, the distance between terrorists’ home base and terror target, and covertness of terrorism operation. Because terrorists are inter-subjectively rationally calculating in their terrorist attack operation, the logic of physics tends to determine whether terrorist attack occurs or not. In this equation, the logic of physics acts as an important exogenous condition.

Here, $a$ represents for the sum of terrorist attack power, while $b$ for the sum of counterterrorism defense power. $a$ is derived from the following formula: $a = \frac{\text{attack speed (attack preparation speed + speed of maneuver)}}{\text{distance}}$. $b$ is from the following formula: $b = \frac{\text{defense speed (speed of intelligence + speed of counterterrorism response)}}{\text{covertness}}$. For $a$, attack speed mean the speed of terrorists’ attack against their target which is made of the speed of terrorist mission preparation and speed of transportation (of manpower, weapons, and other necessary tools) close to the target for an immediate strike. If the distance increases, it tends to negatively affect the speed of attack itself. Thus, $a$ is derived
from the attack speed divided by the distance per se. By contrast, $b$ is the defense speed composed of speed of intelligence and that of counterterrorism response. Here intelligence means knowing of terrorists’ attack operation before the occurrence of the attack in counterterrorism side. Counterterrorism response is any meaningful act to be able to stop an ongoing terrorist attack. It includes law enforcement, covert operation, military operation, or any kind of counterterrorism initiative stopping the incoming attack. The defense speed is negatively affected by the level of covertness of terrorists’ operation. Thus, here $b$ is derived from the defense speed divided by covertness.

If $a$ is equal to or greater than $b$, terrorists are more likely to decide to act for terrorist attack, since they can expect to complete their mission before counterterrorism obstacle is inactivated (when $a = b$, terrorist attack can still be successful by means of suicidal attack). If $a$ is smaller than $b$, terrorists are more likely to withdraw their consideration for terrorist attack, since they cannot expect to hit the target due to the presence of effective counterterrorism obstacle. Thus, $a$ and $b$ together tend to have a significant impact on terrorists’ consideration of act.

The first logic of physics tends to interplay with the second. If target is more sustainable, terrorists need greater striking power which requires more time of preparation and maneuver. Thus, $a$ becomes smaller. If the distance is also greater, $a$ gets even smaller. On the other hand, if counterterrorism capability increases, terrorists need greater covertness to counterbalance $b$. Thus, terrorists’ subjective decision of terrorist acts are the outcome of the balance between $a$ and $b$ derived from many factors of two logics of physics. Clarke and Newman (2006)’s explanation on “Near Enemy” and “Far Enemy” can be articulated by those logics of physics in terrorists’ rational calculation.

The balance between $a$ and $b$ and logics of physics can be substantially changed primarily due to the change of technological condition. This technological change can be an exogenous factor impacting on the balance of logics of physics. Although it is not terrorism case, there is a good example of this techno-
logical impact in war initiation. War is similar to terrorism, because war initiators are engaged in the same inter-subjective calculation bounded by two logics of physics. The invention of train and railway substantially affected on the inter-subjective calculation of war initiators for both Germany and Russia which are responsible for the beginning of the First World War.\(^{187}\) Train and railway provided the condition that the greater of attackers’ striking power can be more quickly and farther transported. Thus, under the condition that the defenders’ sustainability against attackers’ striking power and their defense capability are constant, train and railway allowed greater leverage for the sake of attackers. Meanwhile, train and railway provided greater speed for attacking forces, under the circumstance that the distance between attacking side and defending side is constant, this speed greatly disfavored the b by reducing both the speed of intelligence and the speed of counteract response under the condition that covertness of attacking side is constant.\(^{188}\) In this situation, any nation is conditioned and hurried to strike first against a potential enemy. This is what exactly happened in the beginning of the First World War. Both Germany and Russia are hurried to strike first against each other because both inter-subjectively reached the decision that a is greater than b, Taylor’s thesis (1969) of “War by Timetable” as a chief cause of WWI indeed explains the balance between a and b and two logics of physics discussed here.

What cyberspace today really means is that it tends to substantially affect those logics of physics as an exogenous factor much like train and railway in the past. Cyberspace substantially reduces the distance between terrorist attackers and their targets. Terrorists need less time and effort of preparation and more conveniently transport greater striking power with less cost and more speed. Their speed of maneuver is greatly increased through cyberspace, All these conditions works for


a and against b under the condition that all other factors regarding the defend-
ing(counterterrorism) side is constant. In short, the advent of cyberspace changes the logics of physics and the balance between a and b favoring for terrorist attackers.

3. Threats from Cyberspace and Existential Crisis of Nation-State

Threats from cyberspace are mismatched with the response of nation-state. This uncomfortable reality is mainly due to the difference of ways of operation, Cyberspace is run by the principle of holistic, borderless, networked operation, while the nation-state is by that of divisional, jurisdictional, and bureaucratic operation. Terrorism is made of three key factors, terrorist attackers, targets, and counterterrorism responders of nation-state. Through cyberspace, terrorist attackers can be anywhere to surf and strike targets in anywhere. Cyberspace is a huge single space where attackers and targets co-exist without wall of separation. Terrorist attackers can readily form network and operate with network-based.\(^{189}\)

By contrast, the nation-state is not readily adjusting to cyberspace. Its traditional principle of operation becomes a major hindrance against its effective operation in cyberspace.

Traditional principles of operation of the nation-state work against the nation-state in cyberspace, These principles are division of labor, jurisdiction, and bureaucracy. The nation-state operates based on the principle of division and assignment. When a problem is identified, the nation-state first judges for which

division within the governmental arm the problem belongs to and provides a rather exclusive assignment to the particular department. The nation-state has a specific jurisdiction based on the concept of sovereignty. Along this line, criminal justice and national security (or defense) is divided based on the concept of “division of labor”. Also, bureaucratic principle is the underpinning principle of the nation-state. Along chain of command within a particular division of governmental arm, structural integrity is firmly sustained and cooperation between different divisions is formed by division-to-division collective alliance.

Most security or criminal threats in cyberspace are not suitable for the nation-state to handle in the traditional ways of operation. Problems in cyberspace are often hard to judge in which division they should be assigned. Often they need to be addressed by multiple departments and agencies. The principle of exclusive jurisdiction and sovereignty does not fit well to most problems in cyberspace. They are often multi- or cross-jurisdictional. The traditional concept of sovereignty is often hindrance against effective countermeasures. Bureaucratic operation and cooperation is too slow for responding of problems in cyberspace. Most security challenges through cyberspace takes little time to accomplish, while the speed of bureaucratic response is no match with such speed (the 1st and 2nd meetings in UNODC Terrorism Prevention Branch).

In sum, in cyber-age, the nation-state is facing to an existential crisis. In cyberspace, the national-state cannot effectively deal with various security challenges including terrorist threats. This creates a situation that the protective role of the nation-state substantially diminishes and anarchic condition becomes worsened.

Thus the fundamental role of the nation-state as a chief security provider is questioned in cyberspace.191)

III. Terrorist Threats though Cyberspace: Terrorist Use of the Internet

1. Terrorist Use of the Internet

Terrorist threats from cyberspace have been recognized as an important issue. However, those threats are rather understood as technological challenges or problems of expert area such as IT (Information Technology). Cyberterrorism, cybercrime, cyberattack, or cyberwarfare etc., various terms are used to describe such threats and established a specialized division to exclusively deal with such emerging issues under the traditional wings of law enforcement, intelligence, and/or military. Then, cyber-threats are treated as an assigned problem of such specialized division. Certainly, this is the dominant view of cybersecurity challenges in Korea.

Yet, the true nature of problem is much deeper than the mere technological change. The advent of cyber-age substantially changed the space of human life. Not until the advent of cyber-age, human life is conditioned by three dimensions of space - land, water, and air. The conditions of space are very significant factors impacting on humans’ decisions and activities. They tend to shape how we live, produce, and also destroy. The change of space can substantially change our mode of economy, culture, and warfare (and crime and terrorism as well). Air space had been entered as the third dimension in the 21th century and its impact on human life was substantial. Today, what is undergoing is the fundamental

change of space. Cyberspace has been entered as the fourth dimension in our life. It greatly reshapes our life, economy, culture, and also warfare. Recently, Psy, a Korean pop singer, gained a great popularity around the world from his new released song, called “Gangnam Style”. In the traditional 3-dimensional space, this could never be possible within such a short-time frame. But, in the 4-dimensional space, we now observe such is indeed possible. An uncomfortable truth is that such phenomenon is also possible in area of violent destruction, either terrorism, warfare, or crime. Islamic extremism, racial hatred, right or left extremism can also gain such popularity quickly and widely. Violent attacks are also possible through the same cyberspace. So, the meaning of advent of cyberspace is more fundamental. The 4th dimension has been added in the human life and it transforms the existing rule of game regarding violent destruction constructed by land, water, and air.

Terrorists’ use of internet needs to be perceived as a phenomenon conditioned by the inclusion of the 4th dimension in the human life. In this context, its meaning and impact may be far more substantial than the mere cyberterrorism. By now, cyberterrorism has drawn much concerns and fears but its real damage in the real case has been minimal and only caused some annoyance and mediocre financial loss. However, terrorists’ use of internet may produce different and far more worrisome damages in the real world. Cyberspace serves as the gateway to actualize such violent attacks diverting traditional dimensions. Considering the fact that the nation-state has much trouble to provide effective security in this 4th dimension, terrorists’ use of internet is more worrisome.

2. Types of Terrorist Use of the Internet

Terrorists’ use of internet is classified into several types. Here cyberspace is used as tools, spaces, or routes supporting and facilitating terrorist acts. It tends to providing a substantial advantage for terrorists by reducing cost, increasing covertness, improving operational effectiveness etc. (the 1 and 2 meetings in UNODC Terrorism Prevention Branch). UNODC describes various types of terrorists’ use of internet observing in such fashion. They are five types which are often overlapping and interrelated with each other: propaganda (including recruitment, radicalization and incitement to terrorism), financing, training, planning (including through secret communication and open-source information), and execution.¹⁹³)

A. Propaganda

The dissemination of propaganda is one of the primary uses of the internet by terrorists. Propaganda takes the form of communications in cyberspace providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. Examples of this include virtual messages, presentations, magazines, written statements, audio or video files or online games. But, not all terrorist propaganda is illegal although some are certainly prohibited by law of many nations. Some may be considered as legitimate expression under the protection of freedom of expression. Nevertheless, those legitimate expressions may effectively serve for terrorists’ purpose of propaganda. The promotion of violence is a common theme in terrorism-related propaganda. The broad reach of content distributed via the Internet exponentially increases the audience that may be impacted. Further, the ability to directly distribute content via the Internet dimin-

ishes the reliance on traditional channels of communication, such as news services, which may take steps to independently evaluate the credibility of the information provided, or to edit or omit aspects deemed to be unduly provocative. The promotion of extremist rhetoric encouraging violent acts is also a common trend across the growing range of Internet-based platforms which host user-generated content (UGC). Content that may formerly have been distributed to a relatively limited audience, in person or via physical media such as compact discs (CDs) and digital video discs (DVDs), have increasingly migrated to the Internet. Such content may be distributed via a broad range of tools, such as dedicated websites, targeted virtual chatrooms and forums, on-line magazines, social networking platforms such as Twitter and Facebook, and popular video and filesharing websites such as YouTube and Rapidshare, respectively.194)

The fundamental threat posed by terrorist propaganda relates to the manner in which it is used, and the intent with which it is disseminated. Terrorist propaganda distributed via the Internet aimed at potential or actual supporters is generally focused on recruitment, radicalization and incitement to terrorism, through messages conveying pride, accomplishment and dedication to an extremist goal. These three goals of propaganda is a stream of process running from incitement through radicalization to recruitments. An potential terrorist wannabe or a terrorist sympathizer could be incited and further radicalized to be an active supporter, financial donator, or an accessory to terrorist operation. Through the further process of propaganda, one eventually decided to volunteer for terrorist attacker meaning being recruited. Other objectives of terrorist propaganda may include the use of psychological manipulation to undermine an individual’s belief in certain collective social values, or to propagate a sense of heightened anxiety, fear, or panic in a population or subset of the population. This may be achieved through

the dissemination of disinformation, rumours, threats of violence or images relating to provocative acts of violence.\textsuperscript{195)

B. Financing

Internet could be used to finance acts of terrorism. Terrorists can solicit and collect funds and resources through cyberspace. There are four ways to finance through internet: direct solicitation, e-commerce, and the exploitation of online payment tools and charitable organizations. Direct solicitation refers to the use of websites, chat groups, mass mailings or targeted communications to request donations from supporters. Websites may also be used as online stores, books, audio and video recordings and other items and souvenirs to supporters. Various online payments are used for electronic transfer of funds including Paypal or Skype. This activity can be an e-commerce of conventional business activities through cyberspace. Items are honestly sold and delivered and payments are collected through various online payment systems. However, online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud. An example of the use of illicit gains to finance acts of terrorism was seen in the U.K. case against Younis Tsouli. Profits from stolen credit cards were laundered by several means, including transfer through e-gold Ltd. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to fund terrorist activity. Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes. Some terrorist organizations have also been known to establish shell corporations, disguised as philanthropic undertakings, to solicit on-line donations. These organizations may claim

to support humanitarian goals while in fact donations are used to fund acts of terrorism. Examples of overtly charitable organizations used for terrorist ends include the innocuously named Benevolence International Foundation, Global Relief Foundation and the Holy Land Fund for Relief and Development, all of which used fraudulent means to finance terrorist organizations in the Middle East. Terrorists may also infiltrate branches of charitable organizations, which they use as a cover to promote ideologies of terrorist organizations or to provide material support to militant groups.196)

C. Training

Terrorists also use cyberspace as an alternative terrorist training ground. They provide practical guides in the form of on-line manuals, audio and video clips, written text of information and advice. These Internet guides provide detailed instructions on how to join terrorist organizations, manufacture explosives, firearms or other weapons or hazardous materials, plan and execute terrorist attacks. They also provide intelligence and counter intelligence skills including the security of illicit communications and online activity through the use of available encryption tools and anonymizing techniques. Literally terrorists use internet as a “virtual training camp”. For example, “Inspire Magazine” is an online publication allegedly produced by Al-Qaeda in the Arabian Peninsula with a stated objective to enable Muslims to train for jihad at home.197)


D. Planning

Terrorists’ use of internet also includes planning for a terrorist attack. According to many criminal justice practitioners, almost every case of terrorism prosecuted involved the use of Internet technology. Planning an act of terrorism typically involves remote communication among several parties. Preparatory steps must also be taken to identify a potential target of an attack and the most effective means of achieving the terrorist purpose. These preparatory steps may range from obtaining instructions on recommended methods of attack to collecting open-source and other information regarding a proposed target. The ability of the Internet to bridge distances and borders, and the vast amount of information publically available in cyberspace makes it a key tool in the planning of illicit terrorist acts. Typically, cyberspace is used either tool of secret communication among terrorists or of collecting information and intelligence for terrorist operation from publicly available information in cyberspace. For an example of the former, A simple on-line email account may be used by terrorists for electronic or virtual “dead dropping” of communications. This refers to the creation of a draft message, which remains unsent, and therefore leaves minimal electronic traces, but which may be accessed from any Internet terminal worldwide, by multiple individuals with the relevant password. Regarding the latter case, some critical information that may be used by terrorists for illicit purposes is made available through Internet search engines, which catalogue and retrieve inadequately protected information on millions of websites. Also, online access to detailed logistical information, such as real-time CCTV footage, and applications such as Google Earth, which is intended, and primarily used by individuals for legitimate ends, may also be mis-used by those intent on benefiting from the free access to high resolution satellite imagery, maps, terrain and buildings, for the reconnaissance of potential targets, from a remote computer terminal. Particularly in the age of popular social networking media, such as Facebook, Twitter, YouTube, Flickr and blogging plat-
forms, individuals also, voluntarily or inadvertently, publish an unprecedented amount of sensitive information on the Internet. While the intent of those distributing the information may be to provide news or other updates to their audience for informational or social purposes, some of this information may also be abused for terrorists’ use.¹⁹⁸)

E. Execution

Cyberspace provides a substantial strategic and tactical advantage for the execution of terrorist attack. For example, explicit threats of terrorist attack such as WMD(Weapons of Mass Destruction) may be disseminated via the Internet to induce anxiety, fear, or panic in a population or subset of the population.¹⁹⁹) Internet communications may also be used as a means to communicate with potential victims, or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the 9/11 attacks in the United States. The use of the Internet in furtherance of the execution of acts of terrorism may offer logistical advantages, reduce the likelihood of detection, or obscure the identity of responsible parties. Internet activity may also facilitate the acquisition of items (weapon and tools) necessary to the execution of the attack. Terrorists may purchase individual components or services necessary to perpetrate violent acts of terrorism by means of electronic commerce, Misappropriated credit cards or other forms of compromised electronic commerce.

¹⁹⁹) Interview with Terrogence CEO, May 30 – June 10, 2009
Terrogence is a private security corporation in Israel. The company runs web site and gather intelligence online about Islamic extremist terrorists and its supporters. It is operated by the support of Israeli government and provides its intelligence data and analysis with fee for Israeli government, private corporations, and individuals in need.
payment may also be used to finance such purchases. Internet also provides a huge advantage and convenience for terrorist to control, coordinate, and communicate with each other in the execution of terrorist attack. From the commanding center down to the field operators and accessories, chain of command and communication can be effectively sustained during the operation.\(^{200}\)

### F. Cyber–attacks

Strategically speaking, terrorists’ use of internet has far more worrisome impact working against the rule of law.\(^{201}\) Cyberspace functions as a huge channelling space bridging different terrorist groups and criminal groups which were traditionally geographically and culturally remotely separated.\(^{202}\) For example, likely minded terrorist groups and individual terrorists have formed strategic alliance across geographical and cultural borders through internet, Al Qaeda is now connected to home-grown terrorists in the western countries and other Islamic extremist groups regionally based such as Talibxan, Al Shabab, Boco Haram, and IMU(Islamic Movement of Uzbekistan). All these groups and individuals sharing similar beliefs form a global network much owing to the presence of cyberspace.\(^{203}\)

---


The strategic connection also bridges terrorists and criminals of various types. Crackers, swindlers, drug dealers, and organized criminals are now connected to terrorists through cyberspace for mutual benefits. Cybercrime, financial frauds, online gambling, money laundering, child pornography, and many other types of crime are exploited for terrorist or criminal purposes by this so-called “terrorist-criminal alliance.”

3. Terrorist Use of the Internet

Through cyberspace, terrorists and supporters around the world are connected regardless of geographical distance and national and cultural boundaries. An example of this can be global Islamic extremist network lead by Al Qaeda.

Recently, Al Qaeda has been structurally dispersed in the real space but re-emerged as a powerful and threatening entity of cultural and religious software in the virtual world. As a software, Al Qaeda conducts terrorism activities in global scale and functions as a hub of the large and interconnected network which coordinates and communicates various Islamic extremists. The core of Al Qaeda plays a role of command, control, and logistic support for the Islamic terrorist network and a concrete terrorist attack is carried by regional terrorist groups, home-grown terrorist groups, or self-motivated individuals. For example, in

---


Afghanistan, Haqqani network which is responsible for the recent armed assaults in Kabul and other areas maintains a close relationship with Al Qaeda.\(^{207}\)

In Nigeria, Boko Haram, a regional terrorist group, conducts serious level of terror attacks in February 2012. Recently, the influence of Islamic extremism has substantially increased. According to an intelligence report, Boko Haram has a close connection to and received a support from Al Qaeda.\(^{208}\) In France, a serious level of terror attack occurred, This incident was conducted by homegrown terrorists but Al Qaeda provided propaganda, training, support, and logistic supply.\(^{209}\)

In Iraq, a terrorist bombing recently occurred and 60 people got killed, This attack is also done by a terrorist group connected to Al Qaeda.\(^{210}\) According to the M16 of the U.K., Iran attempted to build a strategic alliance with Al Qaeda despite the traditionally hostile relationship with Al Qaeda.\(^{211}\) Cyberspace is the key used to construct Al Qaeda led Islamic extremists' network. This trend is not limited to Islamic extremists' groups, Various types and characteristics of terrorism

---


207) Interview with a DIA(Defense Intelligence Agency) analysts, April 19, 2012.

208) Зубов, Николай, У Всемирного Зла Новое Имя, Коммерсантъ ВЛАСТЬ, No 4958, 2012.


211) Joscelyn, Thomas, British Intel Concerned About Iran-Al Qaeda”, The Weekly Standard, 16 February, This article is a part of FDD(Foundation for the Defense of Democracies) Weekly Review Reports, 2012.
such as Right-wing, Left-wing, environmental protection, and animal liberation sharing similar beliefs and identities tend to form a strategic alliance through cyberspace. After all, terrorist threats through cyberspace connects various different types and characteristics of terrorism matters originated from different regions and countries around the world and elevates the threat of terrorism by summing up those separated regional issues. Accordingly, it is essential to take an integrated and networked perspective to approach at today's terrorism. Also, terrorists' use of internet needs to be handled as a more fundamental strategic issue.

IV. Transformation of Mode of Warfare: Marriage between Terrorism and Cyberspace

1. Overview

Terrorist use of the Internet has a feature of transformation of mode of warfare in the historical perspective of warfare. Traditionally terrorism had no such serious strategic meaning because its striking power is rather limited. But, the marriage between terrorism and cyberspace substantially elevated the seriousness of terrorism and tends to change the rule of game in the field of warfare. So, now global terrorism is approached as a new mode of warfare and cyberspace is the center of the argument.212)

Since 1990, there have been arguments suggesting that mode of warfare is undergoing of the fundamental change and a new mode of warfare is emerging in the contemporary world. Some call it "the 4th generational warfare",213) while oth-

ers “the 5th generational warfare”.214) Whether it’s the 4th or the 5th generational warfare, in the core of such arguments lays cyberspace. They recognized the importance of the inclusion of cyberspace into the theater of war which creates much different dynamics from the previous generational warfare only including land, water, and air.

Originally, the argument of the emergence of a new mode of warfare is centered on the warfare of information revolution argued by Arquilla and Ronfeldt (1996). Although they discussed on the issue of terrorism, their main focus of argument was about information revolution in the armed forces and national defense meaning the armed forces are networked and holistically integrated by information technology. This thesis was concretely actualized in the reformation of the U.S. armed forces which prioritized the Air Force, information warfare, and technology, while downplaying man-power on the ground.

However, throughout the period of “War on Terror” since 2001, the debate on the transformation of mode of warfare has moved to terrorism. For example, Reed (2008) argued that global war on terrorism is an emerging new mode of warfare. Through cyberspace, Al Qaeda is conducting the new generational warfare against the U.S. and its allies. This change of central focus of argument is due to the factual realities of two fronts (Iraq and Afghanistan) of “War on Terrorism”. Less man-powered and highly sophisticated IT-driven forces just could not effectively fought against terrorists and insurgents on the grounds. Both in Iraq and Afghanistan, much complex and non-conventional fights have continued.215) So, terrorism is brought into the center of debate on transformation of mode of warfare.


215) Interview with John P. Williams, May 30 – June 10, 2009. Mr. Williams had a first-hand experience of Iraq War. He participated in the War as an infantry colonel for the US Marines.
2. Marriage between Terrorism and Cyberspace

A very crucial and interesting observation on the impact of cyberspace on warfare is that cyberspace lowered the entry barrier of warfare business. Warfare is such an expensive business in the past and thus only the state actor with enough resources can enter this business. Thus, most small state actors, non-state actors, and individuals are driven out of the business due to the high entry cost. But due to the reason explained in the previous chapter of "Physics and Strategic Advantage of Cyberspace", cyberspace substantially lowered the entry cost of war business and thus the entry barrier. This allows more number of small players of desire to attack to be able to enter war business. Thanks to cyberspace, cost of maneuver, preparation, operation of attack has been substantially lowered. The distance between the attacker and target is revolutionarily overcome. Covertness of attackers is significantly improved. All these conditions work for the network of small state or non-state actors. In result, a new type of actors, such as terrorist network, appeared in the business of warfare, and this changed the nature of warfare as well.

The main characteristics of the emerging mode of warfare are “selective strike” and “system disruption” considering "War on Global Terrorism" as such new mode of warfare. Internet use tends to substantially help especially for terrorists or other weaker actors to conduct this strategic choice although it is theoretically possible to adopt such strategy without internet. Selective strike is to strike the

center of gravity (the most vulnerable point) of the enemy with optimal violent power to maximize strategic goals. For the democratic nation-state, this center of gravity can be ethics, public opinion, fear or anxiety among mass-civilian population, disruption of civil life etc, because the political power stems from the mass. For terrorist organization, its center of gravity could be the elimination of leadership, disruption of network, or restricting financial resources etc.

Recently “system disruption” becomes one of chief goals of the new mode of warfare. The “system disruption” is interrelated with “selective strike”. For the modern nation-state, the fundamental system is one of the most critical center of gravity. The system includes the criminal justice system and the infra-structure of electricity, water, energy supply, IT, social welfare, education etc. If these basic but critical systems are disrupted or malfunctioned, the state may lose its legitimacy and thus political power. Terrorists are now attacking to disrupt those systems. On the other hand, the state actor, especially the U.S. and NATO, is now redirecting its target to the system disruption of terrorists. Terrorists are formed and operated by network globally connected through both physical- and cyber-space. Thus this system itself could be the center of gravity working against terrorists. In sum, the appearance of fight could be dissimilar but the strategic logic for both sides, the state actor and terrorists’ network, is in deeper sense much similar.

3. Qualitative Changes on Mode of Warfare

In the new mode of warfare, kinetic and non-kinetic theaters are integrating through cyberspace. Also, the gravity which determines the outcome of war-

fare is sliding toward non-kinetic theater from kinetic one, the primary battle
ground for victory in the previous modes of warfare. Kinetic theater means the
stage where actual combats or violent attacks occur. In the conventional warfare,
this could be combat operation with weapon-strike. In the non-conventional fight,
such as terrorism, it could be selected surgical operation by intelligence or Special
Forces or arrest by intelligence or law enforcement. Non-kinetic theater mean all
other non-violent aspects of warfare including political power competition, eco-
nomic aspect, culture, knowledge and information, religious or ideological beliefs,
and social influence. In the non-kinetic theater, no visible violent acts are ob-
served but they are significantly related to the final outcome of warfare in more
covert and indirect ways. Traditionally, non-kinetic theaters played supporting
roles for kinetic theater and the final outcome of warfare is decided in the kinetic
theater. However, with the advent of cyberspace, this traditional balance between
kinetic and non-kinetic theaters is skewed toward non-kinetic areas. Now, we ob-
serve that gaining influence in the non-kinetic areas plays a more decisive role
to determine the victory of war, while the kinetic theater plays a supporting
role.221) The reason of this change is that cyberspace interconnects and networks
all kinetic and non-kinetic theaters and created one single holistic battle ground.
Due to the interconnectivity conditioned by cyberspace, a greater number of audi-
dences around the world watch the outcome of kinetic theater through the dis-
torted lens of internet. So, importantly, here happens symbolic distorted inter-
action between the actual outcome of kinetic battlefield and the subjected percep-
tion among viewers. Then, this subjected perception(or misperception) instantly

220) Reed, Donald J. Beyond the War on Terror: Into the Fifth Generational of War and
221) Reed, Donald J. Beyond the War on Terror: Into the Fifth Generational of War and
Minwoo. Insurgency warfare as an emerging new mode of warfare and the new enemy. The
affect all other non-kinetic theaters and further the chain-reaction quickly followed between kinetic and non-kinetic theaters all together. Because of this queer unexpected consequence, there appeared a great irony that even though one gains a substantial victory in kinetic theater, it still loses the warfare itself due to the loss of non-kinetic grounds. This could be evidenced in both “War in Iraq” and “War in Afghanistan” for the last decade. A recent case of Kabul attack well illustrated this changed balance between kinetic and non-kinetic theaters. Haqqani group, Taliban affiliated, was responsible for the attack and it stroke several targets with bombings and armed assaults around the city. The kinetic attack was minimal at best. In the case of the U.S. embassy assault, the bullets did not even reach the facility notwithstanding harming persons or buildings. So, in the kinetic theater, it was a mere failure. But, the attack was so successful to create an image around the world that Kabul is unsafe, terrorists gained its strength, and Afghanistan is still in severe chaos primarily due to the creation of image through cyberspace hitting non-kinetic areas.

4. The Fifth Generational Warfare

The advent of the fifth generational warfare is resulted from the advancement of information-communication technology. Cyberspace is emerged as an real entity and integrated to the existing space of warfare as another dimensional space. This 5th generational warfare has a qualitative difference unlike other previous generational warfare which historically existed. Overall, non-combat logistics is a

---

222) Interview with a DIA(Defense Intelligence Agency) agent, April 19, 2012. The author had an interview with a DIA agent. He is an analyst responsible for Afghanistan and Pakistan region.

Critical factor which tends to determine the detrimental victory of warfare. The logistics deals with matters of transportation, supply, intelligence, communication, and other non-combat operations.\textsuperscript{224}) The outcome of war is decided by the vital strike against the enemy's center of gravity.\textsuperscript{225}) The primary issue for the execution of this operation is how to deliver and support striking power. The striking power means combat force. But, the striking power which actually execute violent blow should be transported, equipped, and supported.

Overall, there exists a law of physics between the enemy's center of gravity and attacker's capability of non-combat logistics. When the enemy's center of gravity becomes more robust, the cost and effort of logistic operation increases. When the distance between the attacker's homebase and the location of the enemy's center of gravity becomes greater, the cost and effort of logistic operation also increases. After all, due to the limit of cost and effort for logistic operation, a large size operation of violent attack such as warfare was limited to the nation-state, because only state actors could afford the cost and effort of non-combat logistic operation. However, cyberspace and the advanced information communication technology radically changed the conventional law of physics in warfare, because it substantially reduced cost and effort of non-combat logistic operation. Through internet, surveillance and intelligence gathering on the target of attack becomes feasible and less costly. Financial transfer, recruitment of combatants, procurement of weapons, training, rapid deployment of striking forces are all possible with less cost and effort through cyberspace.\textsuperscript{226)(227)}

\textsuperscript{224}) Logistics includes all non-combat operations such as intelligence, transportation, supply, weapons, propaganda, communication, etc.

\textsuperscript{225}) Center of gravity means the opponent's critical point which can impact on the outcome of the warfare itself. Examples are capital city, commanding center, critical infrastructure, strategic hub, primary combat forces etc.

This substantial decrease of effort and cost of warfare qualitatively transformed the nature of warfare. The business of warfare becomes now available for less capable non-state actors such as terrorists groups or individuals. Those inferior forces now have an opportunity to strike against more superior state actors located far from the inferior attackers' homebase. The 9/11 attack in 2001, the 7/7 London attack in 2005, and the Norwegian terror attack in 2011 can be seen as examples of the 5th generational warfare which is driven by the low level of entry cost and effort for the warfare business.

Meanwhile, the decrease of warfare cost and effort by cyberspace resulted in the emergence of a single and holistic space of warfare which globally connected and integrated various local or regional stages of war which were traditionally segregated.\(^{228}\) By use of cyberspace, combat forces can be transferred, supplied, trained, recruited, and commanded with more speed and less cost. Thus, unlike the past, combat forces do not have to travel a long distance with the possession of weapon and hostile intention. The condition of opportunity allows an actor with hostile intention to attack a distant target of one's choice with the low risk of detection or interdiction before the strike. Thus, realistically, the changed condition produced the situation that one can be struck by any attacker remotely located with less time of detection, preparation, and counteraction. After all, the change of condition seems to create the single war-space globally-connected through cyberspace.\(^{229}\) The following figure 2. illustrates the concept of the fifth generational warfare.

---

227) The content was discussed in the EGM(Expert Group Meeting) of TPB(Terrorism Prevention Branch), UNODC(United Nations Office on Drugs and Crime), October 5-6, 2011, Vienna, Austria.


The fifth generational warfare can be illustrated as a three-dimensional cube made of six different war-stages. Each war-stage is its own competition ground. Cyberspace tends to substantially integrate these six separated war-stages into a holistic one. Inside of the cube illustrates the multi-dimensional war-stage which is extended from the surface of each separated war-stage and thus always has complex nature of warfare simultaneously including several dimensions of war-stage. Within this stage of warfare, a network warfare is conducted between the nation-state actors and the non-state actors. Today, the state actors are the U.S. led state actors and the non-state actors are the Al Qaeda led terror network. Two different sides are conducting network warfare meaning occupying a strategic
location within the battle space and gaining some influence within each war-stage. This type of game is similar to Baduk\textsuperscript{230} according to Yun.\textsuperscript{231} The essence of this game is the victory is decided by the occupation of hub of network and thus increase the influence over the space. But, unlike Baduk, in the fifth generational warfare, each war-stage is always connected to the other war-stages. Thus, each movement of action, meaning occupying the hub of space by deed, always has an immediate impact on other stages and thus multiple consequences often hard to calculate.

In the figure 1, the war-stage of violence means kinetic war-stage\textsuperscript{232} where the actual combat or violent strike is conducted. All other areas of politics, economics, religion/ideology, knowledge/technology, and society are considered non-kinetic war-stages where no actual combat occurs. In the fifth generational warfare, all stages are interconnected and integrated. Thus, the victory of one particular stage resulted in the defeat of the whole war-space because the very victory in the particular stage could negatively impact on the outcome of other war-stages and thus loose the influence over the entire war-space.

In the battle field of the three dimensional cubic space, the state actors tend to collide with the non-state actors today.\textsuperscript{233} In the figure 1, the white circle represents kinetic or non-kinetic acts of the state actors. By contrast, the black circle represents those of the non-state actors. The key point of this kind of war is that the victory of kinetic battle field is not necessarily related to that of non-kinetic

\textsuperscript{230} “Baduk” is a traditional game of Korea. It is called “Jo” in Japan.


\textsuperscript{232} Kinetic means an act which actually uses violence to kill or maim persons, destroy things or threatens to use such measure. Non-kinetic means an act is related to or support for the kinetic act but has non-violent nature.

\textsuperscript{233} Of course, this division is not absolute. In the case of North Korea, she is a nation-state actor but tends to ally with non-state actors in the matter of terrorism, drug trafficking, and weapon trafficking etc. Thus, North Korea could be grouped into non-state actors in the global fight of terrorism between two sides.
battle field. Traditionally, when each war-stage was disconnected with the others, this was the case. But, now the victory of kinetic field can be nullified by the loss of other non-kinetic fields. Kinetic methods can include military operation, covert operation by intelligence, and law enforcement measures. Those acts are violent measures of the state. In the past, these kinetic measures could produce its own outcome. However, today's fifth generational warfare shows that the kinetic acts are highly interrelated with its impacts on other non-kinetic areas. Sometimes a positive outcome of the kinetic field can produce negative outcome in non-kinetic areas and thus produce undesirable result in the whole stage of warfare. In other words, the victory of the kinetic war-stage can happen with the loss of the whole war-stage. This is because different war-stages are interrelated in the fifth generational warfare due to the connectivity of cyberspace. Without consideration of various stages of warfare as a holistic sum, a sectionalized approach of kinetic measures such as “search-and-destroy” or “identify-and-arrest” may backfire and result in the loss of the whole war-stage. Fights against terrorism in Iraq, Afghanistan, and Pakistan etc. since the 9 · 11 tend to show the irony of this kind of warfare.

V. Counterterrorism Measures:
   C&C(Communication & Cooperation) and Infiltration

1. Overview

Cyberspace and IT technology not only provide strategic and tactical advantage for terrorists but also for counterterrorism actors of the nation-state. As a matter

of fact, it is fair game but the current security problem is mostly derived from that CT(counterterrorism) actors has not fully capitalize cyberspace unlike terrorists. Terrorists’ use of internet is advantageous for terrorists but at the same time increase their vulnerabilities as well because internet use inevitably leave electronic traces all over the cyberspace.\textsuperscript{235} The real problem is that CT parties could not fully utilize the vulnerabilities.

Indeed, cyberspace provides proper opportunities for effective CT activities. Terrorists’ use of internet leaves electronic traces and leads in cyberspace and CT actors much utilize this potential asset by monitoring, collecting evidences, analyzing dots of such traces and leads.\textsuperscript{236} For example, CT actors may collect context of dialogue from the terrorists’ web forums for effective prevention.\textsuperscript{237} Bomb-making or terrorist-attack instructions available online can be a valuable resource for prevention measures. Also, just like terrorists, CT actors can utilize cyberspace for speedy and cheap communication tools for themselves. In short, it is important to understand that cyberspace is not an opportunistic condition only for terrorists but also for CT actors. CT actors need to focus on how to utilize cyberspace for their interest.

2. Counterterrorism Measures against Terrorist Use of the Internet

C&C(communication & cooperation) and infiltration are two crucial axes of CT measures which are so far focused, C&C means inter-agency communication and cooperation within a nation and also across nations. Agency here includes governmental, international, and non-governmental(both profit and non-profit) all together. Since the 9 \cdot 11 attack, many CT actors around the world well realized

\textsuperscript{235} Department of the Army. Open Source Intelligence. FMI 2-22.9. 2006.
\textsuperscript{237} Interview with Terrogence CEO, May 30 - June 10, 2009.
that traditional approach of divisional practices is not matching with terrorists with the use of internet, Intelligence sharing, mutual cooperation, and getting to know with each other is all important among various CT actors of law enforcement, intelligence, the military, private corporation, and academia around the world.\textsuperscript{238})

For example, in case of Germany, the representatives from approximately 30 agencies of both Federal and State including intelligence, prosecution, immigration, Armed Forces, police have a daily meeting in an office located in Berlin to share their current practices and intelligence in real-time basis. Also, Germany constructed the uniform database shared by both intelligence agency and the German Police.\textsuperscript{239)}

The new experiment of C&C is not the bureaucratic and formal integration of different agencies. It is more real-time based, networked, and individualized integration of different CT actors. No formal contract or treaty is necessary. CT actors can be connected through cyberspace in the form of web forum, email, ICQ, etc. A global network of CT actors could be formed for quick and need-based C&C. UNODC launched an interesting experiment to build a network based C&C online among governmental and private CT actors across the nations.\textsuperscript{240)}

Meanwhile, infiltration is another core CT strategy. Unlike the real space, cyber-

\textsuperscript{238) The author had his participant observations as a member of experts in the course of two Expert Group Meetings of United Nations Office on Drugs and Crime Terrorism Prevention Branch. Two meeting were held in Vienna, Austria, in Oct. 2011 and Feb. 2012. The topic of the meetings was about The Use of the Internet for Terrorist Purposes. In the meetings, representatives from 22 member nations and Council of Europe, Organization for Security and Co-operation in Europe, Eurojust, and private security companies, and UNODC TPB officials were attended.

239) Interview with Charles von Denkowski, March 22-23, 2012. Charles von Denkowski is an expert on Islamic terrorism in Germany. He served as a police officer and crime investigator in Berlin and Hamburg for the 20 years. Especially, he participated in the investigation of Hamburg Cell after the 9.11 attack. He had worked on Islamic extremism, pre-crime investigation, terrorism investigation and intelligence for the German police.

space is still relatively immune from the state control. Thus, increase of transparency in cyberspace is an important challenge for CT and infiltration is such an effort. Interestingly enough, globalization tends to blur geographical boundary between the nation-states, but at the same time there appear new type of boundaries of culture, language, or technology in cyberspace. The citadels made of a specific culture, language, or technology are formed and its members enjoy an immunity from the governmental surveillance or enforcement. A case of terrorists’ Arabic-speaking web forum well illustrates this situation. Due to a substantial linguistic and cultural barrier, the western government cannot effectively monitor what is going on and enforce the rule of law against it. Infiltration strategy is an pro-active effort responding to such dilemmas in cyberspace.²⁴¹)

Several CT experiments have been practiced as an infiltration strategy. The concept of pre-crime investigation has been suggested.²⁴²) In the case of terrorism in cyberspace, it is often practically impossible to distinguish between intelligence operation and crime investigation against terrorists’ operation. Many techniques of surveillance in cyberspace are to monitor or negatively influencing terrorism activities rather collecting criminal evidences. Incriminating evidence against certain terrorist individuals is unexpectedly discovered in the course of intelligence operation, This often cause problems in the stage of criminal trials since the criminal conviction requires more rigorous evidence strictly bounded by the rules of criminal evidence. Also, unlike ordinary crimes, terrorism investigation is often occurred before a particular terrorist attack not after the fact. Thus, technically crime is not occurred yet when investigation is practiced. But, the state cannot wait until the attack actually occurs because the after-facts cannot be tolerated.²⁴³) Upon

²⁴²) The author’s participant observations as a member of experts in the course of two Expert Group Meetings of United Nations Office on Drugs and Crime Terrorism Prevention Branch. Two meeting were held in Vienna, Austria, in Oct. 2011 and Feb. 2012; Interview with Charles von Denkowski, March 22-23, 2012.
these reasons, the concept of pre-crime investigation is suggested. Here, intelligence, investigation, and prosecution are integrated from the initial stage of CT surveillance and monitoring in cyberspace.\(^{244}\)

Also, various skills of surveillance in cyberspace have been introduced and practiced. In case of France, fake ID and passwords are provided to law enforcement agents from the ISP(Internet Service Provider). By using this fake ID and passwords for disguising the true identity of CT authority, intelligence is gathered and terrorists’ activities are monitored in cyberspace.\(^{245}\) Similar practices are conducted also in Israel. The CT actors actively participate in various web forums, web sites, chat rooms, Facebook, and Twitter of terrorist nature with the disguised identity.\(^{246}\) Sometimes, fake terrorists' web forums or web sites are constructed by the CT authority in cyberspace and lured active or potential terrorists. This practice is so called "honey-pot."\(^{247}\)

VI. OSINT(Open Source Intelligence) as a Counterterrorism Measure

1. Overview

OSINT(Open Source Intelligence) is a method of intelligence collection based on publicly available sources such as media reports and internet. It is equivalent to infiltration strategy into the less known space of internet. In the real space, terrorist act can be identified either by a report from victims or observers or by the discovery of a state agency. If an incident is not reported or discovered, it remains

---

243) Interview with Charles von Denkowski, March 22-23, 2012
244) The author’s participant observations as a member of experts.
245) The author’s participant observations as a member of experts.
246) Interview with Terrogence CEO, May 30 - June 10, 2009
247) The author’s participant observations as a member of experts.
The identification of terror incident follows the same logic in the cyberspace as well. It should be either reported or discovered. However, the real difficulty of terror identification in the cyberspace is that either way is not easily practiced. Unlike the police patrol in the real space, there is virtually no police patrol in the cyberspace. Also, victims of cyberterrorism or terrorists' use of internet rarely report the incident to the state authorities. Thus, virtually OSINT is a viable option to observe and identify terrorism incident. Since 2001, OSINT has been proposed by the U.S. and other Western countries.

2. The Concept of OSINT

OSINT is based on the advent of information age. Today's information age draws a different kind of problem unlike before. In the past, too scarce information was problematic. Finding a good information was usually a critical task. But, in today's information age, too much information is problematic. So, the question is how to handle too much information, not how to find it. Indeed, we live in the era that we cannot fully and effectively digest even daily media reports.

The real issue is how to handle abundant information which is usually available for the public. Too much information exists in somewhere, such as Internet, does not mean it can be easily, timely, and effectively used. So, the information just exists somewhere in internet is useless unless it is identified, managed, and analyzed. The state agencies such as law enforcement and intelligence body have faced similar situation. They also face to the challenge of handling and digesting too much information publicly available. OSINT is an answer to the challenge.248)

3. OSINT practices

Since the 9.11 terror attack, OSINT has drawn much attention and actively practiced as a counterterrorism measure against Islamic extremist terrorists in the U.S., NATO, and Israel. This trend is partly due to the active use of internet by various Islamic terrorists such as Al Qaeda, Taleban, Hizbullah, Hamas, and PKK. Also, a recognition on the intelligence value of publicly available information including internet, media report, book, journal article contributed to the OSINT practices. In the western allies, OSINT is considered another legitimate area of intelligence operation along with HUMINT (Human Intelligence) and TECHINT (Technical Intelligence). OSINT manuals published by the U.S. army and NATO can be good examples of such case.

Major activities of OSINT includes internet vetting, crime investigation, intelligence. Internet vetting is an newly emerging area. It investigates and

252) Department of the Army, Open Source Intelligence, FMI 2-22.9. 2006.
254) Appel, Edward J, Internet Searches for Vetting, Investigations, and Open-source
conduct background checks on a certain individual who usually applies for a job or already works for an employer. There is a necessity to check the background, reputation, and personality of those individual for the security reason of an employer. In the past, the vetting occurred in offline but now much information on an individual could be available online. Thus, online vetting becomes an essential tool to learn about a particular individual and his or her personalities. Today, most people tend to spend much time online and leave much information about themselves in cyberspace. Due to this change of cultural trend, the chance to know about an individual's personality, life history, and favor is much higher relatively in cyberspace, Internet vetting is a response to the changing cultural trend and a technique to collect information about an individual in cyberspace.255)

Criminal investigation is an activity of criminal evidence collection online. This activity may include digital forensic, but criminal investigation of OSINT is not exclusively about technical matters. Criminal investigation of OSINT includes evidence collection of written statement, message records, social activities and personal profile based on email records, SNS(Social Network Service) records, written texts, and web site information online.256) The area of intelligence is both data collection online and analysis of such collected data. It uses publicly available information online to collect and analyze information. Also intelligence of OSINT includes HUMINT in cyberspace. Such online HUMINT can be conducted by actively participating in criminals' or terrorists' web forums or online communities for intelligence purpose.257)

Analysis is an important process especially for OSINT. OSINT deals with a large data sources which is often seemingly insignificant on face value, and thus effective finding of meaning and associations latent in a large data is a key to successful operation of OSINT. If database is properly constructed, various advanced quantitative methods of analysis such as data mining, regression analysis, GIS (Geographical Information System) analysis, network analysis, time-series analysis can be properly used to discover an important latent associations and facts.258)

Data collection of OSINT is primarily conducted online, but also much aided by offline search. Various techniques and strategy for effective date collection and search is proposed. Regarding internet search, search techniques and tools, and procedures are developed and educated,259) Also, library research, cooperation with university, offline expert interview, hard-copy material search should not be ignored as an essential tool for successful OSINT online. Namely, OSINT should be conducted in holistic and integrated way including both online and offline. Regarding this matter,260) The OSINT manual of NATO and that of the U.S. Department of Army are available.261)262)

4. Things to Consider for the Use of OSINT

Regarding OSINT, it is important to understand “invisible web”. Invisible web means websites which cannot be searched by ordinary search engines such as

258) The author had participated as a leading researcher in the project of the ISVG (Institute for the Study of Violence Groups) which is based on Open Source Intelligence concept from January 2005 to July 2006.
262) Department of the Army, Open Source Intelligence, FMI 2-22.9. 2006.
Google, Yahoo!, and Naver. Also beside invisible web, the concept of deep web is also important to pay attention to. Deep web is websites which is searchable by ordinary websites but cannot be easily searched because it locates far behind in rank order of search. Shortly speaking, the fact that such invisible or deep web exists means a large portion information in cyberspace cannot be easily located. The portion of invisible web consists of approximately 80% of the entire cyberspace. Roughly 20% of websites are accessible by ordinary search methods using a single popular search engine such as Google.

The reason of invisible web or deep web is various. To be searchable, websites need to include information of text in the form of HTML or PDF. If a website includes only images or sound, it cannot be easily searchable. Also, the list of search results is rank-ordered based on the frequency of search hit, number of visitors, or amount of payment for advertisement. Thus, a particular searcher faces a difficulty to find his or her target web sites, OSINT deals with this kind of dilemma. It proposes some solutions for identification of invisible web or deep web and for effective search methods.263)

How to use of search engine is an important aspect of OSINT. Various different search engines has their own strengths and weaknesses. It is recommended that several different search engines(at least 5-6 different search engines) need to be used together. This is because that according to a specific topic proper search engines differ and different search engines can compensate for each other's weaknesses.

Indeed there are many search engines, Yahoo! and Google are popular search

engines widely used. Besides, Hotbot, Lycos, Bing, and Alltheweb etc. are examples of search engines. Also, there exists search engines served in local language. Naver and Daum are examples of search engines serviced in Korean, Yandex is the search engine of Russian language, Some search engines only deals with a specific topic, Findlaw is such search engine serving only for legal search, Meta-search engines serve use of several search engines all together, “ixquick” is an example of such, Meta-search engine uses major search engines such as Google, Yahoo!, and Hotbot all together in a single search. However, there is no deepness of search results comparing with the use of a single search engine.264)

Practical search techniques is also referred in OSINT. This is a matter of how to do in search, How to type key words in search, how to use Boolean techniques, how to use various symbols in key word search are included in this topic, Better and effective use of a search engine such as Google is also discussed, Google serves advanced search functions including translation, images, geographical and topic specification, Training of the proper use of advanced functions are also a part of OSINT techniques.265)

After the collection stage, OSINT deals with construction and management of database and the analysis of data. Examples of such operation can be the


ISVG (Institute for the Study of Violent Groups) and START program, Database of Terrogence in Israel is also such example. By use of the database, various quantitative and qualitative analysis could be implemented.

VII. Conclusion

SCP (Situational Crime Prevention) theory soundly suggests that human acts are conditioned by situational factors.\textsuperscript{266} A revolutionary change of technology similarly conditioned how we, humans, fight with each other. As the invention of airplane much changed the way of warfare, the advent of IT greatly changed the way we fight today. Terrorists’ use of internet is an outcome of such change of exogenous condition. Thus such phenomenon should be approached by the deep understanding.

This chapter aims at showing the fundamental characteristics of terrorists’ use of internet. It tries to show that cyberspace has reshaped the traditional rules of game between terrorists and the CT actors. For this reason, terrorists’ use of internet is not an isolated security threat but a symptom of our contemporary life. We download songs and movies online, buy commodities in e-commerce, and make friends in cyberspace. Terrorists do their work in the same fashion. So, the world surrounding human beings is changed and we now live in the 4-dimensional space. Our fights, either warfare or terrorism, will be in such space.

The real problem regarding terrorists’ use of internet is not such phenomenon itself. The real issue lies on the side of the CT, the CT actors are still behind to figure out how to fight in the 4-dimensional space. So, the balance is skewed to terrorists’ favor. Several experiments and policy measures have been practiced by many actors around the world. But, to effectively counterbalance against terrorists

in cyberspace, there is still more to go. This chapter hopes to address such a point.
Chapter 4

Terrorist Use of the Internet: an Analysis of Strategies, Objectives and Law Responses
I. Introduction

On June 10, 2009, James von Brunn shot and killed a security guard at the United States Holocaust Museum in Washington, D.C. Von Brunn was a white supremacist Holocaust denier and had previously been convicted of several ideologically motivated crimes. His prior ideological crimes included attacking a law enforcement official and plotting to kidnap federal bureaucrats. Von Brunn was a “lone wolf” because he was not affiliated with a terrorist organization at the time of the shooting. He did, however, subscribe to far-right beliefs and had previously been a member of racist far-right groups. Although he did not interact face to face in an organizational setting with like-minded individuals who validated his racist beliefs, he shared his views globally via the Internet. Von Brunn had a website called the “Holy Western Empire,” which featured his racist books, outlined his
beliefs, and provided his personal and extremist history. The website called “for the establishment of the white, Christian empire.” Von Brunn’s use of the Internet as a racist outlet was not sophisticated. But, it highlights the importance of understanding how terrorists, and their supporters, and political extremists attempt to harness this technological asset to further their ideological objectives.

The Internet has revolutionized how individuals, groups, corporations, and other entities produce, receive, and distribute information. It is hard to believe that less than a generation ago most people relied primarily on mass-mediated information that was delivered to them in their mailbox or through their television set. Access to information was constrained by the number of subscriptions one could afford, how many channels were part of a digital package, and the amount of time one had to collect information from libraries, museums, and other sources. This information is now available to anyone with a computer and access to the Internet. The information gathering process is more efficient and comprehensive. Cultural, social, and geographic boundaries have been overcome. The only limitations for retrieving information relate to abilities, time, patience, motivation, and some minimal costs.

Much of what is available on the Internet is not reviewed by an editor, publisher, or programming director. The Internet contains uncensored, often unedited images, illustrations, graphics, writings, audio recordings, and videos. The Internet has reshaped how, where, and when people interact. The Internet’s democratizing attributes help build and sustain communities. In fact, Simi and Futtrell state that “Communities that are linked through cyberspace expand the ways that individuals can connect to groups by overcoming constraints of time and place, al-


lowing for high volume information flows, and enhancing solidarity among users.269)"

The Internet, however, has also been described as a “double-edged” sword.270) The Internet has also been used in different ways by terrorists.271) According to Weimann, “Post-modern terrorists are taking advantage of the fruits of globalization and modern technology especially advanced online communication technologies that are used to plan, coordinate and execute their deadly campaigns, No longer geographically constrained within a particular territory, or politically or financially dependent on a particular state, they rely on technologically modern forms of communication-including the Internet.”272)

The terrorist attacks that occurred in the United States on September 11th, 2001 changed the world’s perceptions of terrorism and impacted relationships on individual and national levels. Terrorism was a fringe academic discipline prior to the attacks of September 11th. Over the last ten years, however, most nations have increased their funding for scientific research studies that investigate why individuals turn to terrorism, the mechanisms related to an individual joining a terrorist group, the types of counter-terrorism strategies used, and how governments collaborate to effectively prevent terrorism.

This increased funding and academic attention to fill knowledge gaps about terrorism has been unprecedented, Silke (2008) concludes that nearly 90% of all ter-


rorism research ever published has been produced in the last ten years. He estimates that a book on terrorism is produced every six hours. It is nearly impossible to keep up with the number of peer-reviewed publications that are produced annually.

Surprisingly, although there is anecdotal evidence that terrorists use the Internet to further their objectives, there has been little systematic research on this topic. Despite these research gaps, there are core works that identify critical issues. Most of these studies discuss what terrorist organizations use the Internet for. A few studies systematically look at what terrorist organizations present on the web, and how law enforcement organizations have responded to this terrorist threat. We use these sources to draw our conclusions.

This chapter reviews the literature on terrorists, political extremists, and their supporters, use of the Internet. This essay is divided into three sections. First, we discuss how terrorist organizations use the Internet and what is typically displayed on terrorist websites. Second, we discuss the objectives of their Internet usage. Specifically, we highlight their rationales for using the Internet as a resource. We provide examples of how terrorist organizations use this technology. Third, we examine how law enforcement organizations have responded to the terrorist threat on the Internet. Questions studied include whether terrorists use the Internet to aid their planning and execution of violent acts, or to recruit members. We also examine if the Internet has facilitated otherwise unconnected individuals to come together for terrorist collaboration. We pay special attention to the leading terrorist threats to public safety in the U.S. - far right, 273) far left such as animal and envi-

273) Far-right extremists are fiercely nationalistic, anti-global, suspicious of federal authority and reverent of individual liberties, especially their right to own guns and be free of taxes. They believe in conspiracy theories involving imminent threats to national sovereignty or personal liberty and beliefs that their personal or national ‘way of life’ is under attack. Sometimes such beliefs are vague, but for some the threat originates from specific racial or religious groups. They believe that they must be prepared to defend against this attack by participating in paramilitary training or survivalism (Source: Freilich, J.D., S.M.
II. The Strategies Used to Harness the Power of the Internet

Most terrorist organizations have an Internet presence. The growth in Internet usage by terrorist organizations corresponds to general public use. As the


274) Animal/environmental rights extremists support aspects of the following beliefs. They endorse biodiversity/biocentric equality (i.e., that humans’ have no legitimate claim to dominate earth). They believe that the earth and animals are in imminent danger and that the government and corporations are responsible for this danger that will ultimately result in the environment’s destruction. These extremists believe that the “system” is incapable of taking actions to protect the environment and biological diversity. Thus, there is a need to defend the environment and animals and that violent actions to achieve this are justified (Source: Freilich, J.D., S.M. Chermak, R. Belli, J. Gruenewald and W.S. Parkin., “Introducing the United States Extremist Crime Database (ECDB)”, Paper under second review, 2012).

275) Jihadi extremists adhere to aspects of the following beliefs. They believe that only acceptance of the Islam promotes human dignity. Islamic extremists reject the traditional Muslim respect for “People of the Book,” (i.e., Christians and Jews). They believe that “Jihad” (i.e., to struggle in the God’s path like the Prophet Muhammad), is a defining belief in Islam and includes the “lesser Jihad” that endorses violence against “corrupt” others. Islamic extremists believe that their faith is oppressed in nominally Muslim Middle-Eastern/Asian corrupt governments and in nations (e.g., Russia/Chechnya) that occupy Islamic populations. The U.S. is seen as supporting the humiliation of Islam, and exploiting the region’s resources. They believe that America’s hedonistic culture (e.g., gay-rights, feminism, etc.) negatively affects Muslim values. Islamic extremists believe that the American people are responsible for their government’s actions and that there is a religious obligation to combat this assault. They believe that Islamic law- Sharia provides the blueprint for a modern Muslim society and should be forcibly implemented (Source: Freilich, J.D., S.M. Chermak, R. Belli, J. Gruenewald and W.S. Parkin., “Introducing the United States Extremist Crime Database (ECDB)”, Paper under second review, 2012)
Internet’s popularity increased in the 1990s, the number of people using the Web, the amount of available information and number of online transactions grew exponentially. Similarly, while initially only a handful of terrorist groups used the Internet, this has steadily increased and currently terrorist groups of all ideologies use the web for various purposes. Weimann explains that “Islamists and Marxists, nationalists and separatists, racists and anarchists: all find the Internet alluring.”

Weimann, is one of the leading authorities on terrorist Internet usage and he has tracked the connectivity of terrorist groups. Weimann concludes, “When this research was started in the late 1990s, there were merely a dozen terrorist websites; by 2000, virtually all terrorist groups had established their presence on the Internet and in 2003 there were over 2,600 terrorist websites. The number rose dramatically and by January 2010 the archive contains over 7,600 websites serving terrorists and their supporters.” He also finds that all organizations designated as Foreign Terrorist Organizations by the United States State Department have a website. Similarly, research by Chermak, Freilich and Suttmoeller (2011) compares the organizational characteristics of violent and nonviolent hate groups in the United States. Their data were unique because they sampled from all hate groups- both non-violent and violent- in the United States. They found that the vast majority of hate groups involved in ideologically-motivated violence had an Internet presence. Nearly half of the organizations attempted to recruit individuals to their organization using the Internet.

The far right, for example, has long attempted to communicate with followers,


recruit individuals, and spread rhetoric using the Internet and other technologies. In the 1980s, the Aryan Nations and White Aryan Resistance established computer bulletin boards to connect individuals and disseminate ideological documents. In the early 1990s, public officials, watch-group organizations, and scholars noted that technologies were critical to the growth of the far-right militia movement.\(^{279}\)

While the number of militia groups declined in the late 1990s, there was a resurgence of this movement in the last decade. Online discussion forums and email distribution lists are critical to this reemergence.\(^{280}\)

In the mid-1990s, the racist and extremist far-right group Stormfront.org established a presence on the Internet.\(^{281}\) This is regarded as the first “hate site” on the World Wide Web.\(^{282}\) Stormfront.org emerged as a model for the large number of groups creating “virtual communities of hate” (Bowman-Grieve, 2009). Social network analysis indicates that it became a central link in the White Supremacist network. Stormfront’s incoming and outgoing links were widely distributed across the network and… [it] served as a crucial intermediary between otherwise unlinked sites.\(^{283}\) An analysis of the Stormfront.org website found that articles and discussions on its site target Jews and nonwhite populations.\(^{284}\)

---


These researchers conclude “Stormfront provides a “cyber transition” between traditional hate speech and “reasonable racism,” a tempered discourse that emphasizes pseudo-rational discussions of race, and subsequently may cast a wider net in attracting audiences.”

White supremacists use the Internet to disseminate their message. Scholars have concluded that the Internet is being used to build a community where hate and violence are reasonable. The amount and type of information provided by different types of extremist and terrorist groups on the Internet varies. This is not surprising because there is variation in the technological expertise of groups, the access an organization has to monetary resources to create and maintain a web presence, and the amount of time a group has for updating and improving the website. For example, it is estimated that al Qaeda has an annual operating budget of nearly thirty million dollars per year. It is thus not surprising that al Qaeda has used the Internet extensively to accomplish various objectives, compared to other terrorist groups that have fewer resources. Al Qaeda used the Internet extensively to plan and execute the September 11th attacks. The investigation following the attacks revealed that al Qaeda shared intelligence about potential targets using encrypted messages, Internet-based telephones, and exchange-

ing e-mail via Yahoo!, Al Qaeda also conducted research on-line about using crop-dusting airplanes to distribute chemical agents, and used the Internet to make airline reservations at AmericanAirlines.com.\(^{288}\)

Al Qaeda use of the Internet has expanded since the September 11\(^{th}\) attacks. It has recognized the power of communication and its “goal has always been to build an army of believers.”\(^{289}\) Some officials argue that al Qaeda does 99% of its work on the Internet.\(^{290}\) Al Qaeda, and its supporters, may have thousands of Arabic, English and other language websites. These sites direct potential recruits to more secure websites, provide information about the operations and ideology of the organization, and share information on how to commit cyber-attacks and violent crimes like bombings, or suicide attacks.\(^{291}\) All the evidence related to Internet use by Al Qaeda points to these conclusions: “Al Qaeda [is] a computer-savvy terrorist conglomerate”\(^{292}\) and “Internet communications

---


\(^{292}\) Levin, Brian., “Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer
have become the main communications system among al Qaeda around the world because it’s safer, easier, and more anonymous.” 293)

Although many terrorist organizations have used the Internet to achieve their political objectives, examinations of various websites find different levels of sophistication. Most terrorist organizations share information about themselves on a website, or their supporters/members will distribute such information, targeting various audiences. The types of information disseminated varies by website but might include information about a group’s leaders, their public appearances, the organization’s goals, communiqués, discussions about tactics, maps, support for the use of violence, listings of specific attacks they committed, and instructions or calls to commit future crimes. 294)

These calls vary from justifying future violence, calling for attacks against general categories of enemies (e.g., the New World Order, the hedonistic West, the Zionist Occupied Government, the Jews, etc) to encouraging strikes against specific targets or individuals. 295) Websites affiliated with the Earth Liberation Front

293) Weimann, Gabriel., “Cyber-Fat was and Terrorism”, Studies in Conflict & Terrorism, 34 (10), 2011, p. 769.
(ELF) or Animal Liberation Front (ALF), for example, have “do it yourself booklets” that provide instructions on to make basic incendiary devices and the types of material needed to do so.\(^{296}\) The Earth Liberation Front’s website has regularly listed bombings and arson attacks that its supporters have committed.\(^{297}\) The Earth Liberation Front’s website, like some far-right websites, has also encouraged its supporters to embrace lone wolf and leaderless resistance tactics and to commit violence to further their ideology.\(^{298}\)

Most groups’ websites seek to further their movement generally. There are several websites, for example, where Islamists post “cyber fatwas,” Websites, such as FatwasIslam.com and Fatwaonline.com, are used as vehicles for “spreading terrorist fatwas”,\(^{299}\) and relate “to key issues in promoting terrorism: justifying the use of suicide terrorism, the killing of innocents, the killing of children and women, the killing of Muslims or the use of various weapons (including weapons of mass destruction [WMD] and cyberterrorism”).\(^{300}\) Again, sometimes these rulings list specific individuals (for e.g., Salmon Rushdie) or targets that should be attacked, Similarly, far-right anti-abortion activists have publicized “hit lists” online that contain names and addresses of specific physicians who have performed abortions, Eco and animal rights extremists have also publicized (online) specific potential


targets.

Organizations harness other powers of the Internet. Terrorist groups use forums, e-groups, message boards and chat rooms. Weimann (2010) argues that terrorist chat rooms, such as PalTalk, are popular and used to generate support and share operations information.\(^{301}\) Groups will use services like “Yahoo! Groups ... whereby members of the group can discuss the topic, post relevant articles and multimedia files, and share a meeting place for those with similar interests, Creating a Yahoo! Group is free, quick and extremely easy, and several terrorist groups have used Yahoo! Groups to communicate with their supporters, to post the latest links to other terrorist websites and to post communiqués to the public\(^ {302}\). These forums are also monitored by terrorist groups to identify potential recruits.\(^ {303}\)

Terrorist organizations attempt to protect the information shared through encryption. According to Hummel, “Encryption plays a significant role in the terrorist’s use of the Internet for communication, U.S. officials estimate that terrorists began using encryption in 2001. Encrypted messages can only be unlocked using a private key selected by the recipient. Officials concede it is difficult to intercept, let alone find, encrypted messages and images on the Internet’s estimated 28 billion images and 2 billion websites\(^ {304}\)”

Terrorist groups sometimes use social media sources such as Twitter and Facebook to achieve objectives. These social media platforms might allow them to gather information about their enemies. Information about soldiers and their families can be gleaned from Facebook. The immediacy of communication of sources like Twitter provides an opportunity to provide real time tactical information about the geographic locations and movements of troops or law enforcement organizations. Conversely, such social networking tools will be monitored by terrorist organizations for information from soldiers and others that might point to strategies or locations.305) Information about counterterrorism strategies are shared using these sources as well so that members can adapt and pursue attacks using other means or variations of terrorist tactics. Terrorist organizations might circulate propaganda or "call-to-action messages" using these platforms.306) Video sharing websites, such as YouTube, are used to disseminate propaganda and training materials widely.307) The satellite imagery provide by Google Earth can be used to better identify the characteristics of a target. Sensitive operations information might be shared using "Dead Drops." According to Hummel, "Dead drops are a method in which terrorists reveal some of their most sensitive information. An online dead drop works by having a person open an account on a free, public e-mail service. The individual then writes a message and saves it in draft form. The account information is then spread, allowing the recipients to read the message. Tactically, dead drops are beneficial because the two parties are never seen together, nor do they need to personally meet the other operatives. This is a good security measure that helps prevent one person from

305) Brown, Ian and Douwe Korff, “Terrorism and the Proportionality of Internet Surveillance.”, European Journal of Criminology, 6 (2), 2009, pp. 119-134.
III. Understanding the Rationale for Using the Internet

In this section, we explore more specifically what terrorist organizations hope to accomplish by opening themselves to scrutiny by publicly communicating via the World Wide Web. Their rationale for using the Internet can be categorized into three core areas: propaganda, recruitment and radicalization, and strategic tactics.

1. Propaganda

Some organizations use terrorism tactics to challenge issues they object to. A fundamental difference between most definitions of “regular” crime compared to “terrorism” is the political nature of the latter act. Most criminal behavior is episodic—a criminal attempts to accomplish a specific objective by committing a specific act. Terrorism may be more strategic where acts, both legal and illegal, occur at specific points in time and are part of a larger campaign to make a political statement. In short, the organization finds current political conditions objectionable. Such conditions bring together like-minded individuals to protest and develop a strategic plan for change. Legal and illegal tactics can be used to

achieve this change, but of particular concern are organizations that turn to mass causality terror. Successful terrorist organization must have a communication strategy to achieve their goals, Groups must highlight “political victories,” discuss the rationale for committing certain acts, and share their political platform, The Internet has become an important tool to share uncensored propaganda about terrorist organizations and also extremist movements that may support them.\(^\text{310}\)

Terrorist organizations rely on many communication strategies that are time-consuming and require manpower. Strategies include organizing protests and rallies, making public speeches, disseminating leaflets and pamphlets, and producing newsletters and radical literature. These strategies directly communicate with potential sympathizers, “enemies,” and the general public. Many strategies are designed to generate news media coverage. In general, however, if an event is not large, if a charismatic leader is not present, or if no violence occurs, it will receive

only small news coverage or be ignored. Importantly, even if an event receives news coverage, the content and tone of the publication is influenced by news routines and news ideology. The Internet could be used to overcome these obstacles. It is cheap and accessible, and messages could be broadcast to a global audience. Information can be distributed without censorship or outside editing. In short, terrorist organizations have almost complete control over the information that is disseminated.

Much of the propaganda distributed over the Internet by terrorist organizations replicates what could be distributed using more traditional strategies. General information, activities and meetings, biographies about leaders and members, and specific ideological statements are presented on their websites. Any information through traditional communication strategies can be easily adapted for presentation on the Internet. According to Wright, “global jihadist messages are aimed directly at the individual, claiming that the Islamic community faces assault from aggressive infidels and their apostate allies;\(^{311}\) it is threatened by military attack, cultural corruption, social disintegration, and substandard zeal.\(^{312}\)”

But the Internet’s structure allows terrorist organizations to use their creative skills to spread their propaganda to wider and more diverse audiences. Organization can upload videos and films that contain dramatic images. For example, Hezbollah, Hamas and the Communist Party of Peru (i.e., the Shining Path) post videos on YouTube to disseminate propaganda.\(^{313}\) Terrorist organizations

---

upload literature, manuals, newsletters, and magazines and other files to free document sharing websites. One example is the publication *Inspire*, an online magazine that is used by al Qaeda to promote violent jihad. According to Jenkins, "[Inspire] reinforces al Qaeda’s narrative, profiles jihadists, and offers suggestions for simple attacks and practical instructions for building improvised weapons and bombs. The producers of Inspire probably also see the publication as part of the continuing campaign of terror, hoping that by describing methods of attack, they can spread fear and rattle the nerves of those charged with security, who must now answer questions about how they plan to prevent such attacks," Terrorist organizations also sell music, t-shirts, and other goods using the Internet, and some produce video games or distribute other types of games to attract young recruits.

Terrorist organizations are distinct in the tactics they use and in their ideological belief systems. Often there is competition between groups and sometimes there are fierce ideological disagreements. Most terrorist organizations do not last

long and many are undermined by internal disputes that lead to their demise or splintering into different cells. Competition across organizations and infighting sometimes result in public wars of words. The Internet has become an important location where ideological, personal, and organizations issues are debated.\textsuperscript{317) Weimann (2006) discusses how groups like al Qaeda are not ideologically monolithic and that the different factions publish on the Internet to debate core issues and tactics. Similarly, competing organizations, such as Hamas and al Qaeda, rely on the Internet to air grievances and debate issues. Thus, the propaganda that is presented by a terrorist organization must compete with counterpropaganda that includes messages from news organizations, political organizations and bureaucrats, and other terrorist organizations.}

2. Recruitment and Radicalization

There are many reasons why an individual may be radicalized to terrorism, Sageman (2004) and Bakker (2006) studied the radicalization process of al Qaeda influenced terrorists, Sageman used network analysis to study 172 persons who joined the global Salafi jihad, and Bakker replicated this study with 250 jihadists in Europe. They found that individuals became radicalized in clusters and that peers played an important role, Post, Sprinzak, and Denny (2003) interviewed 35 incarcerated Hamas, Hezbullah, and Fatah terrorists and examined "the social context, mindset, motivations, and recruitment of these individuals,"\textsuperscript{318) They found

\begin{itemize}
\item National Institute of Justice in fulfillment of requirements for Award Number 2006-IJ-CX-0038, 2011 on jihadi groups conflict and competition)
\item 318) Post, J.M., Sprinzak, E., and Denny, L.M., “The terrorists in their own words: Interviews
that the belief that one’s group/people had been humiliated played a large role in inspiring terrorist actions. Berko and Erez (2005, 2007) interviewed Palestinians imprisoned in Israel for security offenses, including seven arrested for attempted suicide bombings. One study examined the role gender played in female Palestinian participation in terrorism,\textsuperscript{319} while the other focused on dispositional issues related to becoming a suicide attacker (Berko and Erez, 2005), Jurgensmeyer’s (2003) and Stern’s (2003) interviews of Buddhist, Christian, Islamic, Jewish, and Sikh religious terrorist leaders stressed the importance of humiliation, sacredness, and the past. Meanwhile, Horgan (2009) found that “opportunity” factors played a key role in why certain individuals became terrorists.

In sum, individuals do not become terrorists overnight. The movement to terrorism is a process with variation across individual terrorists. Factors that influence the decision to turn to violence, include the influence of charismatic leaders, the restructuring of a group, a critical event, backlash from a government action, or a culmination of grievances. Importantly though, most radicalized individuals never commit violent acts. An individual may be angry and spew ideological rhetoric, but is usually unwilling to cross the line to commit criminal action in support of that ideology.

The Internet is also used by terrorist groups to recruit and radicalize individuals.\textsuperscript{320} Without new and committed members, terrorist organizations will

---


not survive. Although personal contacts remain important, the influence connecting to a wider audience using the Internet should not be underestimated. It is not surprising that groups target youths in this way—youths are impressionistic, have fewer bonds to legitimate social and political institutions, and spend a large amount of time using the Internet. Message boards, on-line forums, and bulletin boards can be used to find recruits. Some terrorist groups capture information about who visits their website and may attempt to contact frequent visitors as recruits. \(^{321}\) Keene (2011) writes that “The internet provides a truly global reach in that a terrorist recruiter is able to communicate with potential recruits irrespective of location. In addition, this global reach is further strengthened by technology in that the challenge of languages can also be overcome through web browsers, including Netscape and Internet Explorer, … This allows recruiting to be audience and language specific, enabling the web to serve as a recruiter of talent for a terrorist cause.\(^{322}\)” Similarly, Kunkle (2012) argues that social media are used to doctor news stories to fuel anger and dissent, “making grassroots radicalization more feasible.\(^{323}\)”

---

Footnotes:


Jenkins (2011) analysis of 176 American “Homegrown” Jihadists concludes that Al Qaeda is using the Internet for recruitment and radicalization. He suggests that al Qaeda is less likely to commit a large-scale attack because of post September 11th improvements in intelligence work. He notes though that it has shifted strategies to recruit Americans and then encourage them to implement an individual, do-it-yourself terrorist campaign. Many American Jihadists “began their journey toward radicalization on the Internet, where they found resonance and reinforcement for their frustration and anger”. Similarly, Silber’s (2012) recent analysis of 16 case studies of al Qaeda influenced plots found that the Internet was used to radicalize many of the participants.

Jenkins notes that al Qaeda has fully committed to exploit the Internet because of the limitations of traditional means of communications. This important analysis wonders if al Qaeda’s attempt to gain strength in numbers by using the Internet could backfire. The number of American Jihadists is small and most plots uncovered never move beyond the discussion stage. The few terrorist plots that progressed to an operational plan were, in fact, closely monitored by the Federal Bureau of Investigation. Jenkins hypothesizes that the Internet may have become a substitute for real action—that al Qaeda may only succeed in creating a virtual army. While communicating on the Internet, in other words, provides the opportunity to make a political statement about an issue, such statements might not be accompanied by any actions: What people say differs from what they actually do.

Similarly, Kenney (2010) questions the value of the Internet as a source of training for terrorism. He wonders if the Internet has replaced the effectiveness of


face-to-face strategies, Kenney concludes that “in the 1970s and 1980s, before the Internet became widely used, ethnic-based terrorist groups in the United States were comparatively better organized, and collectively they were able to recruit numbers equal to—certainly not significantly smaller than—today’s jihadist collective. They also were able to sustain their terrorist campaigns over a period of years, something America’s jihadist terrorists thus far have been unable to do.325)” He argues that video instruction training is simply insufficient compared to hands-on training.

3. Strategic Tactics

Violent terrorist actions require planning, financing, coordinating, and training. Investigations into foiled plots and completed terrorist actions by terrorist organizations reveal that the time to crime—from committing to an action to carrying it out—sometimes is significant. Many elements must fall into just the right order for a planned terrorist action to evolve into a “successful” terrorist act. The Internet is a tool that has been used in different ways to aid terrorist organizations to achieve their violent objectives.

Planning and coordination are critical and details need to be shared to succeed.326) First, terrorist organizations use Internet technologies to protect com-

communications and increase the speed of delivery with encryption and secure message systems.\textsuperscript{327)} Second, because of the availability of information on the Internet, terrorists can open-source search documents for information about potential targets. Google Earth, for example, is a useful tool for choosing and planning how to attack a target.\textsuperscript{328)} Third, online conversations review the successes and failures of particular strategies and may allow terrorist organizations to learn and make strategic adjustments. Fourth, the Internet can be used to network across organizations that result in distributing resources or information in support of carrying out an attack, Simi and Futtrell’s (2006) analysis of the White Supremacist Movement documents how cyberspace intersects with real world activities, The Internet provides opportunities for conversations to occur and bridges to be built.\textsuperscript{329)} They conclude that the “Internet, as it is not confined by time or space, opens up opportunities for communication and collaboration,” and that cyberspace provide coordination opportunities because they “supply online links to an array of members and groups, provide information about movement ideals and activities, are repositories for the movement’s cultural items, and facilitate awareness about and

\begin{quote}


entree into real world spaces that might otherwise be unknown to many members.”330) How a person’s on-line life impacts real world behaviors has also been highlighted in research examining prostitution and other computer crimes. For example, Holt and Blevins (2007) find that men who solicit sex use on-line forums to identify prostitutes and make decisions about managing risk.

Financing operations is also critical to success.331) While it may not be expensive to fund a specific terrorist act, financing an operational capacity requires significant resources. Organizations receive funding from legal and illegal sources. Terrorist organizations, for example, receive donations from charities and other non-governmental organizations through the Internet. Funds are solicited in chat rooms and online forums and payments are made via online systems. Potential donors are often deceived to provide funds because terrorist organizations sometimes design a website to appear as if it is in support of a humanitarian cause. Terrorist organizations might even partner with a “front group” to solicit funds for the organization. Various types of criminal activity, such as online credit card fraud, identity theft, hacking, and money laundering, are also used to finance or support terrorist plots and operations.332)

The Internet can be used to coordinate attacks and disseminate information about tactical operations. Manuals and videos are posted online that explain how to make explosive devices, construct suicide belts, extract toxins, or mix chemical weapons. Kunkle (2012) discusses how the Global Islamic Media Front, al Qaeda’s media arm, released a bomb-making manual on various social media platforms. The manual included instructions on “kitchen laboratory operations, general chemistry; in-depth instructions for synthesizing primary, secondary, and improvised explosives from commonplace ingredients; and directions for making detonators and IEDs.”

Keene (2011) discusses websites used by terrorist organizations that provide radio frequencies used by United States law enforcement agencies, but also provide specific instruction how to commit cyber-attacks. Cyberterrorism refers to unlawful strikes through cyberspace against government computers and their information that result in fatalities or property violence or generate great fear, to achieve poli-


Cyberterrorism: Trends and Responses

cal objectives.\textsuperscript{336}) Similarly, Wright (2008) argues that the Internet can be used to enhance communication between groups and provide a mechanism to coordinate cyberattacks.\textsuperscript{337})

In addition to cyberterrorism, some terrorist organizations, and more likely their supporters, could use the Internet to conduct hacker crimes. Weimann\textsuperscript{338}) explains that there are four types of hacker crimes. First, hacker crimes include virtual sit-ins, such as planned large scale visiting of specific sites to crash them. For example, supporters of Palestinian movements have successfully crashed Israeli government websites. Second, there are campaigns to overwhelm an email address through sending it thousands of messages. Third, hacking crimes encompass breaking into computers to steal information, and creating or using viruses and worms to disable and infect computers. Fourth, terrorist organizations may use other virtual systems for hacking.\textsuperscript{339}) Terrorists and their supporters have engaged in all of these activities at times.\textsuperscript{340}) For example, in 2007, Younes Tsouli, known better as Irhabi 007, was convicted and sentenced to over fifteen years in prison for committing acts in support of terrorism. He committed multiple financial crimes, such as credit card fraud, and used the financing to establish a significant web presence for the dissemination of materials that supported al Qaeda and their


IV. Law Enforcement Response to Terrorism on the Internet

The utilization of the Internet to achieve various organizational goals is not only of strategic use to terrorist organizations. Although terrorist organizations may perceive it to be a necessary tool, their use of this technology also exposes them to scrutiny by outsiders, including law enforcement intelligence officials. Since terrorist organizations may provide useful knowledge on the Internet, frequent chat rooms looking for potential recruits, and distribute information about targets and tactics, law enforcement agencies have an opportunity for intelligence gathering. It is easy to remain anonymous and pretend to be somebody you are not on the Internet. Law enforcement officers can enter these chat rooms and online forums posing as potential recruits. If and when an overture from a terrorist organization is made, an investigation might follow providing the law enforcement agent an opportunity to infiltrate the organization. Law enforcement agencies have historically studied the tactics of criminal organizations to understand their strategies and use this information to craft responses. Similarly, law enforcement agencies have significantly adapted their tactics to conduct computer crime investigations341) and consider the commission of computer crimes to be a serious threat.342) It follows that law enforcement currently studies how terrorist organizations are using the Internet and are devising strategies to better respond to the terrorist threat.

The intelligence apparatus of the law enforcement community has changed in the last ten years. Intelligence gathering and information sharing has long been


a priority of federal law enforcement organizations, like the Federal Bureau of Investigation, the Secret Service, and Drug Enforcement Administration, but much of what occurred was done in a vacuum. Many federal agencies collected intelligence information, but there were problems in the sharing and fusing of intelligence across agencies. Indeed, one of the primary reasons why the September 11th attacks were not prevented was the lack of information sharing. The gaps across organization may be problematic for computer crime investigations because of the anonymity that law enforcement officers use when they conduct online investigations. For example, an FBI agent involved conducting an online investigation in a carding forum could be interacting with Secret Service agents without realizing it until an attempt is made to deconflict across investigations.

Expectations about the nature of law enforcement intelligence practices changed dramatically in the past ten years, but two changes stand out. First, there is now an expectation that all law enforcement agencies—federal, state, local and tribal agencies—build an intelligence capacity within their agency. The rationale for this change was that terrorists have frequent contacts with all types of different law enforcement agencies—most often for relatively minor criminal activities such as traffic violations or theft. All law enforcement agencies have an important role to play in preventing terrorism, and there are benefits to systematically collecting and sharing different types of intelligence. Second, it is also expected that all agencies contribute directly to the prevention of future terrorist acts by sharing information widely. The United States has created an information-sharing network where local agencies feed intelligence into state fusion centers that share this information with national information sharing processing units.

What is critical to this new system is the sharing of raw intelligence for processing. One early fear was that there might not be enough information to

Terrorist Use of the Internet: an Analysis of Strategies, Objectives and Law Responses

share. But, the opposite has occurred—law enforcement intelligence agencies are overwhelmed with the amount of knowledge, information, and data being shared across agencies. It is difficult—if not impossible—for agencies to manage such a large amount of information. The Internet has been critical to the identification and use of actionable intelligence. Freilich, Chermak and Simone’s (2009) survey of state police agencies asked respondents to rank the usefulness of a variety of sources for providing information about terrorism. Open source information was highly valued by state police officials, and, in fact, their top source of information was the Internet.

Highly trained analysts have surfed the web for intelligence and to develop a better understanding of terrorist organizations—from the types of strategies used, to why they choose targets, to why individual join terrorist groups. Importantly, analysts have attempted to understand the nature of terrorist organization presence on the Internet and develop strategies to intervene and investigate their activities from what they learn. Although there is great potential for using the Internet as an investigative tool, there are limitations to these efforts to date.

There are several ways that the Internet has been used by law enforcement and other government agencies to respond to terrorists’ use of the Internet. One strategy has been the implementation of new policies and development of task forces and interagency cooperative agreements. Some of the post 9/11 policy changes addressed computer and Internet enforcement.344) Specifically, the Patriot Act of 2001 provides enhancements that allow law enforcement to more closely monitor Internet and e-mail messages, requires that Internet Service Providers share and store information about its users activities when there is the potential for violence, and provides sentencing and/or sentencing enhancements if suspects deface the Web.345)

345) Levin, Brian., “Cyberhate: A Legal and Historical Analysis of Extremists’ Use of Computer
There also have been efforts to develop relationships across government agencies through task forces, interagency agreements, and information sharing. Weimann and Von Knop note that agencies, like the National Security Agency, the CIA, the FBI, Department of Defense, international agencies and private organizations have collaborated to develop counter-terrorism strategies and specific responses to concerns about the Internet.346) Another collaborative group has been formed to initiate counter-propaganda strategies.347) The United States State Department has established a counterterrorism communications center—a collaboration that includes the Departments of State, Defense, and the U.S. Agency for International Development. This collaborative group focuses on delivering proactive messages that might lead to the deradicalization of individuals and developing strategies in response to specific terrorist messages.348)

Law enforcement has attempted to partner with private organizations, like Internet Service Providers, asking them to shut down some terrorist websites.349)

Proponents of situational crime prevention have long called for collaborations between government and private entities to implement strategies that could prevent crime, and in recent years to also prevent terrorist strikes. Indeed, past successes have included obtaining civil abatements to shut crime prone establishments. At times though it is difficult to get private industries to agree they are responsible, or partially responsible, for implementing the situational strategy that could reduce crime. This is particularly important because although terrorists use systems owned by private companies when they conduct cyberterrorism, it is law enforcement agencies that are responsible for enforcing and managing illegal uses of these systems. Other situational crime prevention techniques that could combat terrorists’ use of the Internet include policies that authenticate individual identities and make it more difficult to remain anonymous by increasing surveillance by the police but more importantly others to monitor online activity.

Efforts have been made to better understand the messages presented on terrorist group websites. Narrative and content analyses have been completed on the content of these websites, and, in turn, influence the types of tactics used in response to particular groups (Erez, Weimann and Weisburd 2011; Weimann and Von Knop, 2006). Finally, “after completing a 60-day comprehensive policy review, the Obama administration also took a broader step to address the cyber-threat, creating a “Cyber-czar” at the White House to coordinate the government’s efforts”.


Although these policies and strategic partnerships influence the nature of the response to Internet usage, the burden of combating terrorism on the Internet falls directly on law enforcement agencies. Law enforcement has used various investigative techniques that include sophisticated electronic surveillance tools. Law enforcement agencies monitor billions of Internet records and email communications, use hard to detect monitoring devices, and “remotely and secretly monitor a suspect’s online activities, passwords and email, and even the computer’s camera and microphone.”

For example, the FBI has used a monitoring device called “Magic Lantern” which is delivered via email. This software records keystrokes and passwords, allowing for encrypted messages being intercepted. Law enforcement agencies also collect information about the data trail of individuals, referred to as “dataveillance.”

Law enforcement agencies may attempt to destroy the trust of leaders of specific organizations by using “black propaganda.” If law enforcement “agencies can identify and ‘take out’ purveyors of good technical information, they can flood channels with misinformation and leave the less informed to propagate bad information. At the same time they gather intelligence on participants, organizations and their modus operandi.” Law enforcement has also targeted money remitters that do not have adequate money compliance systems in place, and pursued those that target U.S. citizens but are not registered in the United States.

Prosecutors are concerned about the role of Internet support in furthering the goals of terrorist organizations. The United States has sought to prosecute suspected terrorists and individuals that provide Internet and other computer assistance to terrorist organizations. Wesam El-Hanafi and Sabirhan Hasanoff were indicted and Hasanoff recently pled guilty to conspiring to provide support to al Qaeda in the form of computer assistance. These two individuals provided technological computer assistance to al Qaeda for at least three years.\footnote{Moynihan, Colin., “A Guilty Plea to Giving Aid to Al Qaeda Since 2007”, \textit{New York Times}, 2012.01.04.} Although these individuals were clearly indoctrinated and ideologically committed to al Qaeda, law enforcement recognizes that often ideological motivated terrorist groups’ partner with specific individuals, who are not extremists, but who provide needed expertise.\footnote{Freilich, J.D., S.M. Chermak, R. Belli, J. Gruenewaldand W.S. Parkin., “Introducing the United States Extremist Crime Database (ECDB)”, Paper under second review, 2012.} These non-extremist service-providing individuals are targeted for prosecution, and may become invaluable sources of information on the structure and operations of various terrorist organizations.

There are limitations in the current efforts to respond to Internet use by terrorists. First, although law enforcement intelligence analysts are aware of the potential threat of terrorists using the Internet, current structures and practices still have gaps. Kohlmann notes that law enforcement organizations lag behind terrorist organizations in technological savvy, and that senior officials have not made it a priority to respond more effectively.\footnote{Kohlmann, Evan., “The Real Terrorist Threat”, Foreign Affairs, 85, 2006, p. 116.} Second, although there have been improvements in the creation of new information sharing systems gaps remain.\footnote{Weimann, Gabriel and Katharina Von Knop., “Applying the Notion of Noise to Countering Online Terrorism”, \textit{Studies in Conflict & Terrorism}, 31(10), 2008; Carter, David, Steven Chermak, Edmund McGarrell, Jeremy Carter, and Jack Drew., Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies, Washington}
Third, although some terrorist investigations are global, there are no standard operating practices for the investigation of Internet criminal activities. Similarly, cooperative agreements should be put in place to facilitate investigations between line-level officers and technical experts. Fourth, concerns have been raised about privacy and First Amendment rights of individuals. Finally, as noted by Weimann and Von Knop “counterterrorism on the Net suffers from the lack of strategic thinking. Various measures have been suggested, applied, replaced, changed, and debated. Yet, there was never an attempt to propose a general model of online counterterror strategy. Countering terrorist use of the Internet to further ideological agendas will require a strategic, government-wide (interagency) approach to designing and implementing policies to win the war of ideas.”

V. Conclusion

This essay has explored how terrorists use the Internet to accomplish strategic objectives. Although the amount of research examining various terrorism topics has grown dramatically in the last ten years, research gaps remain. Most research is anecdotal in nature. Scholars and policy makers have written research essays that provide some understanding of the use of the Internet but more systematic empirical work is needed. We conclude with a brief overview of the lessons learned and outline the important work that still needs to be done.

Terrorist organizations have attempted to exploit the Internet. Terrorist organizations adapt to their external environment—operations and strategies change be-

cause of political, social, legal, and cultural pressures. Terrorist organizations seek to capitalize on successes and learn from the failures of other organizations. Such imitation helps terrorist organizations increase efficiency and effectiveness.

Internet use has grown dramatically because there are few needed technical skills, costs are minimal, and access in many places is uninhibited. Some organizations use the Internet to increase profit margins, enter new markets and seek out new partnerships. Individuals use the Internet for many of the same reasons, but also for entertainment, friendship, and personal development.

It is not surprising that terrorist groups representing different types of ideology have all used the Internet, but some are more sophisticated than others. It is easy to post basic ideological information and propaganda on the Internet, and monitor chat rooms for potential recruits. It is more difficult to create a secure system to transfer instructions about targets, make money drops, and gather useful intelligence. Groups that have the longest history appear more able to gather resources to create a sophisticated Internet presence. Worldwide threats, such as Al Qaeda, Hizbollah, and Hamas, have successfully used the Internet to further their objectives. White supremacist organizations in the United States have a significant presence on the Internet, but most of what they post is rhetoric and information gathering. As the Internet continues expands and new sources become popular that redefine how information is circulated and individuals interact, it is possible that terrorist organizations will also adapt to tailor these sources to their objectives.

Terrorist organizations use the Internet for different purposes. The Internet’s uncensored accessible information is a tool to spread propaganda. Websites, chat rooms, and online discussions are places where information can be used to reach potential recruits. This propaganda can be tailored to reach particular targets. Terrorist groups hope that individuals might join specific movements, but they also seek to accomplish their agenda through violent means. Recruitment can occur to a specific group or to the movement in general. If an individual takes action,
then the group may be isolated from prosecution and it brings added publicity to their cause. Individuals may be interested in the ideas of the movement, and thus by reading the materials and being engaged via various forums, the Internet can radicalize a person towards violence.

The Internet can also be a valuable tool in the completion of specific operations. Information about how to use various tactics, how to pick and collect intelligence on a target, and instructions for avoiding apprehension can be gleaned from sites on the Internet. The collection of the material necessary, transportation needs, and documents needed to carry out specific actions can also be collected anonymously on the Internet.

Law enforcement has recognized the threat posed by terrorists’ use of the Internet. Most police responses are strategic and focus on building an infrastructure and policy response mechanisms. Legislation has been passed that expands the opportunities to monitor groups on the Internet. Police organizations have also invested in collaborative task forces and working groups to think more strategically about how the Internet can be used to respond to terrorism. Law enforcement has benefited from these changes as new resources have been provided. Further, changes within the intelligence community have highlighted the need to understand the relationship between technology and terrorism. Law enforcement agencies are developing investigative techniques and using technological tools to collect intelligence about organizations, identify potential terrorists, and disrupt the planning of terrorist organizations.

The research community has contributed by providing information to better understand this important topic. Research has studied what types of information are presented on terrorist websites and why the Internet is so appealing to terrorist groups. But there is a need to know more about how the Internet actually impacts terrorist organizations. For example, has the dissemination of information on various extremist websites led to increases in participation in terrorist organizations? In other words, is the use of the Internet for terrorist recruitment and radical-
ization effective? It would be valuable for researchers to examine different strategies used and identify more closely how an individual came to be involved in an organization. It is possible in fact that empirical research will soon be funded to investigate this. The National Institute of Justice’s recent Request for Proposals (RFP) on domestic radicalization in the United States noted that a specific area of concern was the use of the Internet to radicalize and recruit individuals to terrorism.

Another question is whether the Internet has had the opposite effect on what many terrorist organizations intend: that participants in online activities are less likely to commit violent or illegal actions. This is a difficult question to study, but examining the motivations of extremists and those that turn to terrorism compared to those that do not are important first steps. Finally, more information on the effectiveness of counter-terrorism strategies is necessary. Terrorist organizations use the Internet has expanded into new areas. As social networking platforms increase in popularity terrorist organization have attempted to use sources like Facebook and Twitter in various ways. These sources are, however, also changing how individuals are recruited into terrorism. An individual does not have to travel abroad to be indoctrinated and learn the skills of a terrorist—this information is available with a click of a mouse. It is thus important for law enforcement agencies to adapt and develop new strategies to combat novel terrorist radicalization strategies. Prior research has provided little guidance about what works in responding to terrorism. There are no empirical studies that have evaluated Internet strategies attempted to date. This is a critical gap to overcome so that more intelligence-led responses can be implemented in understanding and responding to terrorist use of the Internet,
Chapter 5

Current Status and Legal System of Cyberterrorism in the Republic of Korea
I. An Overview of the Republic of Korea’s Penal Measure and Cases pertaining to Cyberterrorism

1. Overview

This section will mainly examine penal measure on cyberterrorism according to its behavior pattern and statutory punishment by treating penal measure in criminal law and special law distinctively. In dealing with penal measures within the criminal law, not only an overview on its relationship with cyberterrorism, but also every possible contrived overview will be introduced. Further analyses on cases which may occur with potential punitive measures in the future are also examined for preparation.
2. Case Study of Cyberterrorism in Korea

A. Major Cases

1) The 2003 January 25th Crisis

The January 25th Crisis is a Slammer Worm inflow attacking the Microsoft database (SQL Server) that paralyzed 8,800 Korean and 75,000 computers worldwide. In case of the Republic of Korea (ROK), the international circuit and major DNS server of Internet Service Provider (ISP), and Internet Database Center (IDC) internal network suffered an overload. International mutual investigation with the FBI could never identify the event as cybercrime, cyberterror, nor cyber-warfare. The case became the first evident case that a virus worm is capable of paralyzing the internet system.

2) 2004 Government Institute Hacking Case

This is a case where the Korean Parliament, the Korean Institute for Defense Analyses (KIDA), the Korea Atomic Energy Research Institute (KAERI), and seven other governmental institutes' 222 computer system were attacked by an organization of hackers from China. The case was recorded as a case with one of the biggest victimizations in the history of cyberterrorism against national security. For approximately 6 months, the intrusion allowed for a leak major national secrets related to national security. At the time being, the National Police pointed at a particular Chinese hacker as a suspect to further investigate, however, the Chinese government rejected cooperation for investigation. This case greatly contributed to the establishment and management of the National Cyber Security Center in the National Intelligence Service (NIS).
3) **2009 North Korean July 7th DDoS Attack**

The July 7th DDoS attack from North Korea invaded 21 governmental websites including the Blue House, Department of Defense, NIS, and other central agencies such as banks and major press companies to interfere with the operating system. It was the notorious case of first North Korean attack disclosed externally. Attackers installed malicious code while using sophisticated techniques so that these code are either self-destructive or disguised as picture file. The law enforcement agencies failed to trace the infected zombie PC’s hard disk which was already destroyed and this drew a lot of trouble at the time of the investigation. The incident vividly demonstrated a global form of attack mobilizing 435 servers from 61 countries to perform DDoS attacks. Agencies such as the NIS and the Korea Communications Commission (KCC) were neither able to detect these attacks nor prepare a responsive measure between the agencies. This case became another notorious DDoS attack of history serving as the crucial instrument in establishing government’s national comprehensive cyber-crisis measure.

4) **2011 North Korean March 4th DDoS Attack**

North Korea mobilized 100,000 Zombie PCs to launch a DDoS attack against the 20 government websites, such as the National Assembly, the Ministry of Public Administration and Security, the Ministry of Unification, and plus 20 other websites such as banks, brokers, and portals. They build the 746 attack command server in 70 countries overseas to paralyze government agencies private homepage while controlling the Zombie PCs real time.

Whether North Korea was responsible for the DDoS attack since it occurred shortly after the July 7th attack became the issue under the discussion. The National Police Agency (NPA) reported that by looking at the fact that the malware was distributed through file sharing sites, the similarities between the attack system, and the malicious code-summary match, it is reasonable to believe that
the attack was identical in its principal agent with the July 7th attack.

5) 2011 National Agricultural Cooperative Federation (NACF) Hacking

April 12, 2011, the NACF computer network was hacked and data was destroyed, resulting in days of service paralysis. The investigation by the Seoul Central District Prosecutors' Office concluded that the NACF a laptop of an employee from the computational server maintenance has been hacked, been exposed for seven months, and remotely attacked via Internet. The programming approach, distribution, and method were highly similar to the July 7 and March 4 DDoS attacks and were therefore subjected to be reported as North Korea was responsible.

6) Central Election Management Committee Cyberterrorism Case

The websites of Park, Won-soon, a candidate of Seoul Mayor election, and the Central Election Management Committee were attacked by DDoS on 2011 October 26th. The election was interfered by paralyzing the search function. The case is evaluated as the first DDoS attack that comprised political purposes to affect the election. The National Police arrested five suspects including an executive assistant from the opposing party, the Grand National Party (now Saenuri Party), however, due to insufficient allegations raised by the media and the politics, the independent counsel was later involved.

B. Implications

Analyzing the cyberterrorism attacks occurred in South Korea, few implication points can be found.

First, the North Korean cyberterrorist attack is an inevitable reality. If past attacks were covertly conducted, the attacks since 2009 such as the National
Agricultural Cooperative Federation computer network attack would be portrayed as more visible and bold in its character. It is a likely theory that in the near future there exists a possibility of expanded dimension of cyberattack by North Korea to SCADA networks such as nuclear power plant, aerospace, transportation, etc.

Second, the governmental agencies cannot detect cyberterrorism. Most of cyberterrorist activities are detected right after the occurrence of incident in which the nation's threat in not systematically measured. This is not just a complication for South Korea, but a problematic issue for the rest of the global community. Pre-detection may be difficult since it uses server located in the overseas often using the new malicious code. However, considering the extent of damage and the rate of dispersion, pre-detection is an important asset of evaluation to national security. Therefore, we need to reinforce the early warning system that can respond to such intrusion and attack.

Third, the law enforcement agencies play a significant role pertaining to the attribution of attack. In the early stages of a cyberterrorist incident, the NIS, KCC, NPA, and Supreme Prosecutor's Office (SPO) were all part of participatory agencies, but the was later attributed to the investigative agencies, the police and prosecutors, who identified the main group behind the attack as North Korea and China. A legal system that applies to the initial response that systemizes the attribution of roles and responsibilities is mandated.

Fourth, most attacks were conducted through overseas servers. 2009 DDoS attack involved servers from 61 countries and 2011 involved servers from 70 countries. This reveals the fact that a cyberterrorist activities are implausible to be properly investigated without the international cooperation. The core competency of response measures against cyberterrorism lie within the efficient system of mutual assistance and enabling the longevity of cooperation,
3. Analysis on Cyberterrorism Penal Measures in Criminal Law

Requisite conducts to be considered as obstruction, destruction, or cyber warfare of information communication network can be divided into:
- Limiting proper utilization through damage, concealment, and etc.;
- Causing disturbance through destruction, disruption, etc.;
- Derailing, burying, declining, and etc.;
- Disabling data processing through destroying, inputting a false information, inputting an improper order, etc.;
- Inputting a false information, inputting an improper order inputting the date without authority, altering the data into the date processor;

These types of requisite conducts may occur within the cyberspace and hence cause massive victimization through:
- Creating a violence for the purpose of usurping the national territory or subverting the Constitution (Korean Criminal Law, Art. 87)
- Destroying or providing for the benefit of an enemy country troops, fortresses, camps, or vessels, airplanes, arms, ammunition, or such goods such other places, equipment or structures to be used for military purpose (Korean Criminal Law, Art. 96)
- Damaging or concealing documents or other goods, or special media records, such as electromagnetic records, etc., used by a public office or spoils its utility by other methods (Korean Criminal Law, Art. 141 Sec.1)
- Damaging, destroying or blocking a road, water-way, or bridge, or obstructing traffic by other means (Korean Criminal Law, Art. 185)
- Damaging or destroying a railroad, light-house or its signal or by any other means, obstructing traffic of a train, electric car, automobile, vessel or aircraft (Korean Criminal Law, Art. 186)
- Overturning, burying, crashing or destroying a train, electric car, automobile, vessel, or aircraft in which persons are actually present
- Committing the crime as prescribed to in Articles 185 through 187 to injure another person (Korean Criminal Law, Art. 188)
- Interfering with another person’s business by damaging or destroying any data processor, such as computer, or special media records, such as electromagnetic records, or inputting false information or improper order into the data processor, or making any impediment in processing any data by other way (Korean Criminal Law, Art. 314 Sec. 2)
- Carrying away, concealing, destroying or damaging his own property, or special media records, such as electromagnetic records, etc., which is possessed by another or is subject to another’s right, thereby obstructing the latter from exercising ones right (Korean Criminal Law Art. 323)
- Acquiring any benefits to property or has a third person acquire them, by making any data processed after inputting a false information or improper order, or inputting or altering the data without any authority into the data processor, such as computer, etc. (Korean Criminal Law Art. 347-2)
- By destroying, damaging, or concealing another’s property document or special media records, such as electromagnetic records, etc., or by any other means, reduces their utility (Korean Criminal Law, Art. 366)

The above types of behaviors involve various types of violation against benefit and protection of law: Article 87 and 96 pertains to invasion of national benefit and protection of law, Article 141, 185, 186, 187, 188 pertains to invasion of social benefit and protection of law, and Article 314, 323, 347, 366 pertains to invasion of individual benefit and protection of law. In case of violating Article 188 and 366 involves both social and individual benefit and protection of law. Although these requisites regulate the information communication network, whether or not these may be applied to cases occurring within the cyberspace is obscure. Out
of all the above mentioned laws, Article 141, 314, 323 347, and 366 are applicable to such case. Furthermore, Article 314, 323, and 347 merely involve violations on individual benefit and protection of law, and therefore, the only regulation effective to control information communication network in the criminal law of Republic of Korea are Article 141 sections 1 and Article 366.

Any act of hostility within the cyberspace regardless of the national decision on the matter and if such hostility is forced or organized in its character, Article 111 (Private War against Foreign Country) and Article 114 (Organization of Criminal Group) may be applied. If we were to regard these terror or hostility in cyberspace as violation, these may be categorized into national or organizational.

Based on the background information on criminal law in the Republic of Korea, statutory punishment for cybercrime are as indicated as in the following table.

<table>
<thead>
<tr>
<th>Statutory Punishment</th>
<th>Conduct</th>
<th>Applied Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Death/Life sentence</td>
<td>Inducement of Foreign Aggression</td>
<td>Criminal Law (CR) Art. 92</td>
</tr>
<tr>
<td></td>
<td>Benefiting Enemy by Destroying</td>
<td>CR Art. 96</td>
</tr>
<tr>
<td></td>
<td>Equipment</td>
<td></td>
</tr>
<tr>
<td>Death/Life sentence for not less</td>
<td>Spy</td>
<td>CR Art. 98</td>
</tr>
<tr>
<td>than 7 years</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life sentence for not less than</td>
<td>Derailling Train, etc. (murder)</td>
<td>CR Art. 187</td>
</tr>
<tr>
<td>5 years</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life sentence for not less than</td>
<td>Benefiting Enemy by Other Methods</td>
<td>CR Art. 99</td>
</tr>
<tr>
<td>3 years</td>
<td>Derailling/Overtur/ Crash/Destroy</td>
<td>CR Art. 187</td>
</tr>
<tr>
<td></td>
<td>Train, etc. (murder)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Derailling Train, etc. (bodily injury)</td>
<td>CR Art. 187</td>
</tr>
<tr>
<td>Imprisonment for not less than 1</td>
<td>Obstruction of Train and Vessel</td>
<td>CR Art. 186</td>
</tr>
<tr>
<td>year</td>
<td>Traffic</td>
<td></td>
</tr>
<tr>
<td>Limited imprisonment without</td>
<td>Private War against Foreign Country</td>
<td>CR Art. 111</td>
</tr>
<tr>
<td>prison labor for not less than 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>year</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imprisonment or imprisonment without prison labor for not more than 3 years</td>
<td>False Preparation or Alteration of Public Electromagnetic Records</td>
<td>CR Art. 227–2</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Imprisonment or imprisonment without prison labor for not more than 7 years</td>
<td>Uttering of Falsified Private Document, etc.</td>
<td>CR Art. 234</td>
</tr>
<tr>
<td>Imprisonment for not less than one year or more than 10 years or by a fine not exceeding 15 million KRW</td>
<td>General Obstruction of Traffic</td>
<td>CR Art. 185</td>
</tr>
<tr>
<td>Imprisonment for not more than 7 years or by a fine not exceeding 10 million KRW</td>
<td>Assaults, etc. against Foreign Sovereign</td>
<td>CR Art. 107</td>
</tr>
<tr>
<td>Imprisonment for not more than 5 years or by a fine not exceeding 15 million KRW</td>
<td>Invalidity of Public Documents, etc. and Destruction of Public Goods</td>
<td>CR Art. 141 Sec. 1</td>
</tr>
<tr>
<td>Imprisonment for not more than 5 years or by a fine not exceeding 10 million KRW</td>
<td>Interference with Business</td>
<td>CR Art. 314 Sec. 1</td>
</tr>
<tr>
<td>Imprisonment for not more than 5 years or by a fine not exceeding 10 million KRW</td>
<td>Interference with Business (electromagnetic records)</td>
<td>CR Art. 314 Sec. 2</td>
</tr>
<tr>
<td>Imprisonment for not more than 5 years or by a fine not exceeding 7 million KRW</td>
<td>Divulgence of Diplomatic Secrets</td>
<td>CR Art. 113</td>
</tr>
<tr>
<td>Imprisonment for not more than 5 years or by a fine not exceeding 7 million KRW</td>
<td>Drafting of Private Document by Assuming False Capacity</td>
<td>CR Art. 232–2</td>
</tr>
<tr>
<td>Imprisonment for not more than 3 years or by a fine not exceeding 7 million KRW</td>
<td>Rendering Void or Null Symbol of Official Secrecy (electromagnetic records)</td>
<td>CR Art. 140 Sec. 3</td>
</tr>
<tr>
<td>Imprisonment for not more than 3 years or by a fine not exceeding 7 million KRW</td>
<td>Obstructing Another from Exercising ones Right</td>
<td>CR Art. 323</td>
</tr>
<tr>
<td>Imprisonment without prison labor for not more than three years or by a fine not exceeding 5 million KRW: Provided, that when he denounces himself before the commission of such intended crimes, the punishment shall be mitigated or remitted</td>
<td>Assults, etc. against Foreign Envoy</td>
<td>CR Art. 108</td>
</tr>
<tr>
<td>Imprisonment for not more than 3 years or by a fine not exceeding 5 million KRW</td>
<td>Destruction and Damage, etc. of Property</td>
<td>CR Art. 366</td>
</tr>
<tr>
<td>Imprisonment for not more than 3 years or by a fine not exceeding 5 million KRW</td>
<td>Private War against Foreign Country</td>
<td>CR Art. 111</td>
</tr>
<tr>
<td>Imprisonment without prison labor for not more than three years or by a fine not exceeding 5 million KRW</td>
<td>Organization of Criminal Group</td>
<td>CR Art. 114</td>
</tr>
</tbody>
</table>
4. Analysis on Cyberterrorism Penal Measures in Special Law

A. Act on the Protection of Information and Communications Infrastructure

1) Background

The purpose of the Protection of Information and Communications Infrastructure (hereinafter the “Protection Act”) is to operate main information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in preparation for intrusion by electronic means, thereby contributing to the safety of the nation and the stability of the life of people (refer to Protection Act, Article 1).

The term, information and communications infrastructure, means electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation and energy, and information and communications network under the Article 2 (1) 1 of the ‘Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.’ The term electronic intrusions means acts of attacking information and communications infrastructure by hacking, computer viruses, logic or email bombs, denial of service or high power electromagnetic waves, etc. The term intrusion incident means a situation where any intrusion takes place by electronic means (refer to Protection Act, Article 2). The Committee for Protection of Information and Communications Infrastructure (hereinafter the “Committee”) shall be established under the control of the Prime Minister (refer to Protection Act, Article 3), so as to premeditate on matters concerning the protection of main in-
formation and communications infrastructure.

2) Behavior Pattern and Statutory Punishment

In terms of the prohibited conducts against intrusion of main information and communications infrastructure: (1) accessing main information and communications infrastructure by any person who has no access authority, or manipulating, destroying, concealing or leaking stored data by any person who exceeds his/her access authority; (2) destroying the data of main information and communications infrastructure, or using programs, such as computer viruses and logic bombs, with the purpose of obstructing the operation of main information and communications infrastructure; (3) abruptly sending large amounts of signals with the purpose of obstructing the operation of main information and communications infrastructure, or causing a fallacy in information processing by inducing the processing of a wrong order, etc. (refer to Protection Act, Article 12). Anyone who disturbs, paralyzes or destroys main information and communications infrastructure, in violation of the Article 12, shall be punished by imprisonment and any person who is attempted a crime under such circumstance shall be subject to punishment (refer to Protection Act, Article 28 Section 2).

3) Examination

As mentioned, the term electronic intrusions in the Protection Act is defined as acts of attacking information and communications infrastructure by hacking, computer viruses, logic or email bombs, denial of service or high power electromagnetic waves, etc.; however, in case of the (1), the subjects of application are divided into persons with or without access authority. The type of intrusion differs by any persons without access authority (outsider) who usually commit hacking and any persons with access authority (insider) who usually commit manipulation, destruction, concealment or leakage of stored data. Anyone who attempts to in-
trude upon main information and communications infrastructure are considered as a premeditive offender. In case of the (2), the act of destroying data or using programs with the purpose of obstructing operation of main information and communications infrastructure is considered as crime inquiring a subjective purpose. In case of (3), the act of sending large amounts of signals with the purpose of obstructing the operation of main information and communications infrastructure, or causing a fallacy in information processing would also be considered as crime inquiring a subjective purpose.

In sum, hacking is categorized under case (1), computer viruses and logic bombs are categorized under case (2), and denial of service and sending large amounts of signals categorized under the case (3). Although the statutory punishment regulates all above cases under congruent criteria, the act of hacking mandates ‘deliberation’ and the rest of the cyber-attack mandates ‘purpose.’

B. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

1) Background

The purpose of this Act on Promotion of Information and Communications Network Utilization and Information Protection (hereinafter the “Promotion Act”) is to contribute to the improvement of citizens’ lives and the enhancement of public welfare by facilitating utilization of information and communications networks, protecting persona information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a sounder and safer way (refer to Promotion Act, Article 1).

The term information and communications network in the Promotion Act means an information and communications system for collecting processing, storing, searching, transmitting or receiving information by means of telecommunications
facilities and equipment under subparagraph of Article 2 of the Telecommunications Business Act\textsuperscript{364}) or by utilizing computers and applied computer technology along with such telecommunications facilities and equipment. The term personal information means the information pertaining to an individual alive, which contains information identifying a specific person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables to identify such person easily if combined with an other information). The term intrusion means an event that occurs due to an attack to information and communications network or an information system related to such an network by means of hacking, computer viruses, logic bombs, mail bombs, denial of service, high-power electro magnetic wave, etc,(refer to Promotion Act, Article 2).

2) Behavioral Pattern and Statutory Punishment

Through examining the Protection Act and to draw a behavioral pattern: (1) committing defamation of another person by disclosing a fact to the public through an information and communications network purposely to disparage his/her reputation shall be punished by imprisonment, with or without prison labor, for not more than three years, or by a fine not exceeding 20 million KRW and defamation of another person by disclosing a false fact to the public through an information (refer to Promotion Act, Article 70 Section 1) and communications network purposely to disparage his/her reputation shall be punished by imprisonment with prison labor for not more than seven years, by suspension of qualification for not more than ten years, or by fine not exceeding 50 million KRW.

\footnote{364) Telecommunication Business Act Article 2 Section 2. The term \textit{telecommunications equipment and facilities} means equipment and facilities necessary for telecommunications, such as machinery, appliances, lines, etc;}
(2) collecting personal information with consent of the relevant user (refer to Promotion Act, Article 71 Section 1), collecting personal information that is likely to seriously undermine rights, interests (refer to Promotion Act, Article 71 Section 1), or privacy of a person without consent of the relevant user (refer to Promotion Act, Article 71 Section 2), using or furnishing a third party with personal information (refer to Promotion Act, Article 71 Section 3), or knowingly receiving such personal information for profit or for any other wrongful purpose (refer to Promotion Act, Article 71 Section 4), entrusting someone with handling of personal information with consent of the relevant user (refer to Promotion Act, Article 71 Section 1), mutilating, infringing, or leaking personal information (refer to Promotion Act, Article 71 Section 5), knowingly receiving any leaks personal information for profit or for any other wrongful purpose (refer to Promotion Act, Article 71 Section 6), furnishing someone with or uses personal information without taking necessary measures (refer to Promotion Act, Article 71 Section 7), collecting personal information of a child of less than 14 years old without consent of his/her legal representative (refer to Promotion Act, Article 71 Section 8), conveying or circulating a malicious program (refer to Promotion Act, Article 71 Section 9), causing a trouble to an information and communications network (refer to Promotion Act, Article 71 Section 10), and mutilating another person’s information or who infringes, misappropriates, or divulges another person’s secret (refer to Article 71 Section 11, Promotion Act) shall be punished by imprisonment with prison labor for not more than five years or by fine not exceeding 50 million KRW.

(3) either an attempt or intruding on an information and communications network (refer to Promotion Act, Article 72 Section 1), collecting another person’s personal information (refer to Promotion Act, Article 72 Section 2), and divulging to another person any secret known to him/her while performing his/her duties or uses such secret for any purpose other than his/her duties (refer to Promotion
Act, Article 72 Section 5) shall be punished by imprisonment with prison labor
for not more than three years or by a fine not exceeding 30 million KRW.

(i) having a user’s personal information that he/she learned in the course of
performing his/her duty lost, stolen, divulged, altered, or mutilated because
he/she has not taken technical and administrative measures and knowingly receive
any divulged personal information for profit or any unlawful purpose (refer to
Promotion Act, Article 73 Section 1), providing an unwholesome medium for juve-
nile for profit without labeling it as an unwholesome medium (refer to Promotion
Act Article 73 Section 2), transmitting to a juvenile any information containing ad-
vertisement of an unwholesome medium for juvenile or displaying such in-
formation openly without taking any measures to restrict access by juvenile (refer
to Promotion Act Article 73 Section 3), failing to perform an order of the Korea
Communications Commission (refer to Article 73 Section 5, Promotion Act), entic-
ing another person to furnish him/her with personal information (refer to
Promotion Act, Article 73 Section 7) shall be punished by imprisonment with pris-
on labor for not more than two years or a fine not exceeding ten million KRW.

(5) distributing, selling, lending, or openly displaying any obscene codes, let-
ters, sound, images, or motion pictures (refer to Promotion Act Article 74 Section
2), making any codes, letters, sound, images, or motion pictures arousing fear or
apprehensions reach another person repeatedly against the victim’s will explicitly
manifested (refer to Promotion Act, Article 74 Section 3), collecting, selling, circu-
lating any electronic mail address, or using any electronic mail address in trans-
mitting information (refer to Promotion Act, Article 74 Section 5), transmitting any
advertising information (refer to Promotion Act, Article 74 Section 6) shall be pun-
ished by imprisonment with prison labor for not more than one year or by a fine
not exceeding 10 million won,
3) Examination

The Promotion Act protects personal information and information communications network. It regulates a person who collects another person’s personal information with consent of the relevant user, that is likely to seriously undermine rights, interests, or privacy of a person without consent of the relevant user, or of a child of less than 14 years old without consent of his/her legal representative (refer to Article 72 Section 1, 2, 8, Article 72, Section 1-2). It regulates a person who uses or furnishes a third party with personal information, or who knowingly received such personal information for profit or for any other wrongful purpose and personal information for profit or for any other wrongful purpose, It regulates a person who furnishes someone with or uses personal information without taking necessary measures and provides an unwholesome medium for juvenile for profit without labeling it as an unwholesome medium. It regulates a person who entices another person to furnish him/her with personal information, a person who mutilates infringes, or leaks personal information, a person who mutilates another person’s information or who infringes, misappropriates, or divulges another person’s secret (refer to Article 71 Section 5, 11) a person who divulges to another person any secret known to him/her while performing his/her duties or sues such secret for any purpose other than his/her duties (refer to Article 72 Section 1, 5). Also, a person who has a user’s personal information lost, stolen, divulged, altered, or mutilated because he/she has not taken technical and administrative measures, a person who transmits to a juvenile any information containing advertisement of an unwholesome medium for juvenile or displays such information openly without taking any measures to restrict access by juvenile, and a person who distributes, sells lends, or openly displays any obscene codes, letters, sound, images, or motion pictures, a person who collects, sells, circulates any electronic mail address, or who uses any electronic mail address in transmitting information, and a person who transmits any advertising information are also regulated (refer to Article
The term *intrusion* means an event that occurs due to an attack to information and communications network or an information system related to such a network by means of hacking, computer viruses, logic bombs, mail bombs, denial of service, high-power electromagnetic wave, etc. (refer to Article 2, Section 1-7). The relative penal measures with above section are: (1) a person who conveys or circulates a malicious program (refer to Article 71 Section 9); (2) a person who causes a trouble to an information and communications network (refer to Article 71 Section 10); (3) a person who intrudes on an information and communications network and attempting to do so (refer to Article 72 Section 1-1, 2).

Therefore, examining the above the Promotion Act through its justification of intrusion, hacking can be directly compared with the criminal behavior mentioned in case (3) when committed or attempted with a deliberation. Behaviors such as attacking through computer viruses, logic bombs and mail bombs would be symmetrically compared to the case (1), whereas denial of service or high-power electromagnetic waves would be compared to the case (2). However, the statutory punishment is not regulated under same criteria. Hence, although hacking is regulated at the stage of attempt, however, the statutory punishment is relatively lenient. On the other hand, conveying or circulating a malicious program or causing a trouble to an information and communications network is relatively punitive in its measure.

### C. Special Law relative to Regulations on Cyberterrorism

Penal measures within the Special Law in the Republic of Korea are categorized into regulation relative to the protection of information and communications network, personal information, and protection of both categories. The Protection Act is one of the major laws that pertain to information and communications network and the Promotion Act is one of the major laws that pertain to personal
Among these types of criminal behaviors that falls under the category of destruction and manipulation of information and communications network are: accessing main information and communications infrastructure by any person who has no access authority, or manipulating, destroying, concealing or leaking stored data by any person who exceeds his/her access authority (hacking); destroying the data of main information and communications infrastructure, or using programs such as computer viruses and logic bombs, with the purpose of obstructing the operation of main information communications infrastructure; abruptly sending large amounts of signals with the purpose of obstructing the operation of main information and communications infrastructure, or causing a fallacy in information processing by inducing the processing of a wrong order (denial of service, high-power electromagnetic waves), etc.; accessing the unauthorized information and communications network (hacking); altering, deleting, searching, copying personal information from the credit information data system without authorization and etc.

In the perspective of requisites of in a subjective aspect, in order for a case to build up as hacking would require premeditation and computer virus/logic bombs would require purpose in current structure of legal system in the Republic of Korea. The cases requiring the purpose would be: the purpose of destroying the data or disrupting management of information and communications infrastructure; for the purpose of disrupting management of information and communications infrastructure; the purpose of utilizing in foreign country; the purpose of disrupting administration of process; the purpose of changing or altering private information to disrupt the operations of private management of a public institution; and the purpose of disrupting safe management of information and communications infrastructure.

The information and communications network in relation to individual concepts stated in the special laws, the term information and communications infrastructure
includes electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation and energy, and information and communications network under Article 2 Section 1-1 of the Promotion Act, etc., and *electronic intrusions* include acts of attacking information and communications infrastructure by hacking, computer viruses, logic or email bombs, denial of service or high power electromagnetic waves, etc. Here, the term intrusion incident means a situation where any intrusion takes place by electronic means (refer to Protection Act, Article 2). *Information and communications network* includes utilizing telecommunications facilities and equipment stated in the Article 2 Section 2 of the *Framework Act on Telecommunications* to collect, process, store, search, transmit, or receive information by means of telecommunications facilities and equipment such as computers and applied computer technology along with such telecommunications facilities and equipment, and information system means the organized system of utilization relating to collect, process, store, search, transmit, or receive information (refer to Framework Act on Telecommunications, Article 2).

Based on such knowledge, the table below is an arrangement of special law in relation to its criminal conduct and statutory punishment.

### Table 8 Statutory Punishment on Cybercrime in Special Law based on Behavioral Types

<table>
<thead>
<tr>
<th>Statutory Punishment</th>
<th>Criminal Conduct</th>
<th>Applied Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imprisonment for not less than 10 years</td>
<td>Changing or altering private information for the purpose of disrupting the operations of private management of a public institution</td>
<td>Act on the Protection of Personal Information Maintained by Public Institutions Article 23</td>
</tr>
<tr>
<td>Altering or deleting administrative information for the purpose of disrupting the operations</td>
<td>Electronic Government Act Article 76 Section 1</td>
<td></td>
</tr>
<tr>
<td>Imprisonment for not less than 10 years or more than 10 years or by a fine not ex--</td>
<td>Disturbing, paralyzing or destroying main information and communications infrastructure</td>
<td>Protection Act Article 28 Section 1</td>
</tr>
<tr>
<td>Imprisonment for not less than 5 years or by a fine not exceeding 50 million KRW</td>
<td>Collecting, furnishing, leaking, mutilating, infringing personal information</td>
<td>Promotion Act Article 71 Section 1~8</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Conveying, circulating malicious program to disrupt information and communications system/data/program</td>
<td>Promotion Act Article 71 Section 9</td>
</tr>
<tr>
<td></td>
<td>Causing trouble to an information and communications network</td>
<td>Promotion Act Article 71 Section 10</td>
</tr>
<tr>
<td></td>
<td>Mutilating another person’s information or who infringes, misappropriates, or divulges another person’s secret</td>
<td>Promotion Act Article 71 Section 11</td>
</tr>
<tr>
<td></td>
<td>Damaging any electronic document recorded in the computer files of an electronic trade infrastructure business operator/divulging or abusing any confidential information pertaining to electronic trade documents or trade information</td>
<td>Electronic Trade Facilitation Act Article 31 Section 2</td>
</tr>
<tr>
<td>Imprisonment for not less than 3 years or by a fine not exceeding 50 million KRW</td>
<td>Disclosing or disseminating, to the public, any method or program, by which administrative information can be altered or deleted</td>
<td>Electronic Government Act Article 76 Section 2</td>
</tr>
<tr>
<td></td>
<td>Impairing the logistics information processed, stored or transmitted by the composite logistics information network or the consolidated national logistics database, or infringing, used by stealth or revealed such confidential information</td>
<td>Framework Act on Logistics Policies Article 71 Section 3</td>
</tr>
<tr>
<td></td>
<td>Intruding on an information and communications network</td>
<td>Promotion Act Article 72 Section 1-1</td>
</tr>
<tr>
<td></td>
<td>Collecting, lending another person’s personal information</td>
<td>Promotion Act Article 72 Section 1-2</td>
</tr>
<tr>
<td>Imprisonment for not less than 3 years or by a fine not exceeding 30 million KRW</td>
<td>Collecting, investigating, processing information pertaining to national security and classified information, company’s trade secret or initiative research and development information, political belief, religious faith, or other personal information irrelevant to credit information, personal credit information not ascertained, individual’s disease or provide it to a third party</td>
<td>Use and Protection of Credit Information Act Article 16 Section 1 and 2</td>
</tr>
</tbody>
</table>

*Note
~Attempt: Disturbing, paralyzing, or destroying main information and communications infrastructure (Protection Act, Art. 28 Sec.1), Forging or modifying any electronic trade document recorded in the computer files of an electronic trade infrastructure business operator, a service
business operator specializing in electronic trade, a trader or a trade–related agency, or any trade information entered in their database, or uses any forged or modified electronic trade document or trade information (Electronic Trade Facilitation Act, Art. 30 Sec. 1–1), making a certificate to be issued by means of information processing, etc. after entering false information or illegal orders in a computer or any other information processing device of an electronic trade infrastructure business operator (Electronic Trade Facilitation Act, Art. 30 Sec. 1–2), Forging or falsifying electronic documents or uttering the forged or falsified electronic documents knowingly (Framework Act on Logistics Policies Art. 71 Sec. 1)

D. Conclusion

The Republic of Korea has been making amendments to necessary legislative measures in response to emerging forms of cybercrime.365) This method is applied merely to simply respond to evolving forms of social reality through punitive measure oriented suppression without a warranted theory on criminal law or criminal justice.366) The government’s legal counteraction have so far caused an imbalance in legality and penalty, problems with the legal system, repetitive regulatory measures, and so forth.367)

In a more practical sense, hacking, DDoS, phishing, distribution of malicious programs are prohibited by the Protection Act and Promotion Act. Thus, when making amendments to the special laws regulating cyberterror, the balance between the offline crime systems, inserting procedural law suitable for its high-technological characteristics, inserting obligation for online service provider (ISP), mandating the ISP to cope with the technology of the information and communications network, and instituting probation/community service/lecture order system must be contemplated.368) On the other hand, making the amendments without

evading from the existing terms and definition of regulation in the benefit and protection of law should be emphasized.\(^{369}\)

II. Response System and Conditions on Cyberterrorism in the Republic of Korea

1. Cyberterrorism Cases

A. Overview

The first cyberterrorist attack occurred on Jan. 25, 2003 in the Republic of Korea (ROK). The opinions aroused calling the incident as the Internet crisis, but this case is close to a domestic accident caused by untimely installation of security patches by the Internet service provider (ISP, Internet Service Provider) rather than an attack to paralyze the domestic internet domain services.

Therefore, it is more legitimate to consider the "Hacking against National Governmental Institutions" of 2004 as the first cyberterrorist incident that occurred in Korea. The case was reported by a researcher working on defense-related research institutions, who received a suspicious email from a one of a so-called defense contractor employees. The attached Word file was programed to install a malicious program when opening and viewing the file. The installed malicious program is able to leak confidential documents of the victimized PC just by disguising the name of the email sender. In result, the incident ended up in information leakage from 222 computers from the Korea Atomic Energy Research Institute, the National Assembly, and 10 other public agencies by using and the private system.

---

has been hacked, plus 79 private computers.

There were numerous DDoS attacks and hacking incidents from the year 2005 to 2008, but they were often financially motivated for extortion against the management, not terror related. Ever since 2009, one or two cases of cyberterror-type had been apparent in Korea annually. The 'July 7th DDoS attack' (2009), 'March 4th DDoS attack' (2011), 'National Agricultural Cooperative Foundation hacking attack' (2011), 'The Joong-ang Newspaper Co. hacking attack' (2012), are the one of the known cases in Korea. Although these attacks are different in its feature compared to the attack against the national governmental institutions in 2004.

The attack against the national governmental institution specifically targeted the operating system from the government and the military, where the 'July 7th DDoS attack,' targeted the operating system of financial institutions, IT companies including private companies, and private PCs as well. If the mobilized network to attack the governmental agencies was limited to hack Korea, China, and the US, globally operated servers and PCs were exploited during the 'July 7th DDoS attack' (July 7th case - 61 countries, March 4th case - 70 countries).

<table>
<thead>
<tr>
<th>Case</th>
<th>Method of crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>National governmental institutions Hacking</td>
<td>Sending malicious code attached e-mails to leak confidential affairs</td>
</tr>
<tr>
<td>July 7th DDoS case</td>
<td>Spreading malicious code by web hard-disk updating server to DDoS attack and leak personal information</td>
</tr>
<tr>
<td>March 4th DDoS case</td>
<td>Spreading malicious code by web hard-disk updating server to DDoS attack</td>
</tr>
<tr>
<td>National Agricultural Cooperative Federation hacking case</td>
<td>Installing malicious code on the maintenance staffs' laptop to leak information and destroy Server</td>
</tr>
<tr>
<td>Joong-ang Newspaper Co. hacking case</td>
<td>Destroying server using malicious code</td>
</tr>
</tbody>
</table>

The case of the 'national governmental institutions,' was designed to secretly, privately, and non-destructively obtain confidential information in a disguised
state. On the other hand, starting with the 'July 7th DDoS attack,' the routing system or zombie PCs were destructed upon termination through a method called defacing to make the tracing and investigation difficult. Thus, the damage was increased from information leakage, to further service failure and hard-disk damage.

B. Case Analysis on July 7th DDoS Attack

1) Outline of the Organization of July 7th Attack

On July 7, 2009 approximately 18:00, 35 websites of domestic government agencies, political parties, portal websites, the media, Internet shopping malls, financial institutions, vaccine manufacturers, and websites operated by the US government were attacked by DDoS simultaneously. The attack stopped with destroying the exploited zombie PCs by midnight on the 10th of July after 3 stages of attacks on the 7th, 8th, and 9th. Although the July 7th DDoS attack was similar in structure with other DDoS attacks, they were of different dimension in its sophistication and mobilized multiple number of servers.

In general, the basic structure of the DDoS attacks are: (1) the C&C server; (2) the DDoS attack server distributing program; (3) the use of the zombie PCs. The C&C server is the commanding server. The attacker may manufacture malicious program separately or use another method such as IRC channel. The attack program distributing program server is the server that the DDoS attacking program will be stored to be installed in a zombie PC and the zombie PC is a device executing the homepages with the C&C server which commands the attack.

370) C&C Server (Command and Control Server): The server that is responsible for order command of attack or termination to the zombie PC

371) IRC (Internet Relay Chat): A chatting program designed to enable communicate with people worldwide. The victimized zombie PCs infected with malicious program access a specific channel in IRC to receive commands.
In case of using the C&C server, only one to two computers usually owned or secured by the attacker were used. In case of the July 7th DDoS attack, 435 single servers from 61 were countries hacked and built a network-type C&C server. The network-type C&C can be categorized into 4 different servers: (1) management server; (2) information disclosure server; (3) attack performed server; (4) destroying zombie PC server. The reason for preparing the four different servers are to extract information from the zombie PC and to make possible the efficient division of labor, such as additional attack (destruction).

The management server manages: (1) the list of the zombie PC; (2) collection of system information such as attacking time, user name, name registered in the system, and IP address; (3) the history of the information leakage to the zombie PC.

The information leakage server manages: (1) storing the list of the out flow, such as MS Office recent documents, My Documents, Desktop, and recent documents of the Windows Operating System from the zombie PC; (2) to retransmit the data stored in the information leakage server to refrain from manually transferring the data from 59 countries and 416 computers; (3) the role of passing on the location of the server that is performing the attack to the zombie PC.

The information leakage server is the main server that functions as in which the malicious code, disguised in a jpg file, includes the information regarding the attack time and target that will be transmitted to the zombie PC.

A zombie PC destruction server which is responsible for the transmission of the destroying function of the malicious code, disguised as gif file, to the zombie PC. The malicious code called MBR (Memory of the Independence Day) that was distributed on July 10th 2009 at 00:00 that deletes partition information in order to ultimately disables the PC to boot,
2) Characteristics of July 7th DDoS Attack

(1) Constructing Automatic Attack System

What is unique about the July 7th attack was that the process of the attack has become more automatic, rather than manual. The following two aspects may address the reason.

First, the attack through the C&C server in the past was executed manually through the attacker accessing the C&C server periodically to be directed by the C&C program to start and stop the process. Therefore, it was possible for the investigative agencies to track the C&C server in order to possibly defend against the attack by blocking the IP or URL of the server, even if the attack was subjected to change its IP or URL. With the July 7th DDoS case, however, the principal attack was impossible to cope with since the stored information such as timing and target website in the command files were distributed to the zombie PCs which the process ran like a ticking time bomb.

The prior DDoS attack program disseminated in a manner that was uploading the program while disguising as a MP3 or real-time TV downloader, on websites such as Internet cafe clubs, then waiting to ensure that they were downloaded. The number of zombie PCs were merely 1,000 units. However, in July 7th DDoS attack, the whole process was automatically executed though PC web-hard-disk programs that periodically remotely updated itself. Using these web-hard-disks were prevalent throughout Korea in the year 2009 and the remote update server was hacked in order to distribute malicious codes that eventually turned these updated PCs into zombie PCs.

(2) Using Network-type C&C Server

As mentioned earlier, the existing DDoS attacks using the C&C server merely involved 1 or two servers that the attacker obtained, but the July 7th attack was able to not only obtain multiple servers for multiple attacks, but the division of
each functions enabled the establishment of a network-type C&C server. The network-type C&C comprised 435 single server configuration and 61 countries worldwide with four sub-division of functions: (1) zombie PC management functions; (2) storing function of leaked information; (3) distribution function of the attack command; and (4) PC destruction capabilities.

(3) Zeroday-type DDoS Attack\(^{372}\)

Of the prior DDoS attacks, the process of obtaining zombie PC to spread malicious programs took more than several weeks. This was a big risk the attackers because these codes were caught by the vaccine manufacturers during the time period. The July 7th DDoS attack was able to instantly obtain thousands of zombie PCs at once, which implicated the fact that prevention and response was a difficulty.

2. Overview of Response System on Cyberterrorism

Cyber-infringement and its related prevention and post-recovery work are currently administrated by the agencies such as the National Intelligence Service (NIS), Korea Communications Commission (KCC), the Ministry of Public Administration and Security, and the investigative agencies from the Supreme Public Prosecutor's Office (SPO) and the National Police Agency (NPA).\(^{373}\)

---

372) Zeroday Attack: A security attacks conducted while information on the malicious code has not yet disseminated and exploit the vulnerability of security during the period. It is defined as the immediacy of attack. Generally, when computer detects a vulnerability, the manufacturer or producer distributes vaccines and users download these programs; however, it is difficult to respond to zeroday attack since there's lack of time for such procedure.

373) Cyberterror Expert Workshop predominantly discussed the cyberterrorist response system of the NPA; hence I delivered the pertaining information here.
A. Legal Foundation on Cyberterrorism

In response to the emerging cyberterrorist attacks on information and communications infrastructure\(^{374}\) in Korea, the Act on the Protection of Information and Communications Infrastructure was first enacted in 2001. Following the enactment, the Korea Internet Security Center (KrCERT) under the Korea Information Security Agency (KISA), National Cyber Security Center (NCSC) from the National Intelligence Service (NIS), and Information Warfare Response Center (IWRC) under the Defense Security Command (DSC) were established and managed these institutes under the National Security Council (NSC).\(^{375}\)

Since 2004, after the attack against the national government institutions, National Security Management Act was enacted as a Presidential Decree in 2005 and became a regulation for the first time. In 2006, a provision on the Prevention and Response against Cyber Crisis had been called to attention, but was not passed by the Parliament due to the reasons such as granting excessive privileges for certain institutions, opposition from civil organizations, and the inter-agency disagreement. Whereas, for the case of the 2009 North Korean DDoS attack to the military forces, the National Assembly in January 2010 enacted the Act on Establishment of Infrastructure for Informatization of National Defense and Management of Informational Resources for National Defense and established the Cyber Headquarters for People's Defense (CHPD) under the Korean Defense Intelligence Agency (KDIA) in the Unit 777.\(^{376}\)

\(^{374}\) According to the Act on the Protection of Information and Communications Infrastructure, Article 2, Section 1, [the] term “information and communications infrastructure” means electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation and energy, and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and communications Network Utilization and Information Protection, etc.


B. Response System of Cyberterrorism

Various governmental agencies are responsible for cyberterrorist attacks occurring in South Korea. Korea Internet Security Agency's (KISA) KrCERT is responsible for the private sector, the NCSC from the NIS is responsible for the public sector, and the CHPD from the KDIA is responsible for the entire system. The NPA and the SPO are responsible for the cyberterrorism related investigation.

The previous cyber investigation organization has expanded in its size and currently operating as the Cyber Terror Response Center (CTRC) under the Criminal Investigation Bureau. In 2000, the Regional Public Procurement Service (RPPS) incorporated cybercrime investigation sub-divisions nation wide. In 2007, the police stations implemented a team of cybercrime investigation around the country to build a national investigation systems. Currently, the government is aiming at increasing the cybercrime workforce to approximately 1,000 in its number. The NPA operates a separate investigative organization as a middleman who often assist on the response measures and international mutual legal assistance. The RPPS mainly deal with personal information leakage, and obscenity and gambling websites. The police stations are responsible for internet fraud, cyber defamation, digital content copyright infringement, and distribution of obscene materials.

C. Master Plan for National Cyber Security

In 2011 March 4th, the North Korea DDoS attacked the governmental and private websites and the computer network of the National Agricultural Cooperative

---

Federation was paralyzed. In response, the NIS established the Master plan for National Cyber Security.

While the Master plan expands the cooperation and participation from the private sectors for coordination and inter-agency cooperation, it also minimizes the confusion of roles between agencies and help the NIS play the head role. The Master plan declared cyberspace as a territorial, aerial, marine jurisdiction to be protected under the nation and selected the plan for its five major areas (prevention, detection, response, system, and foundation).

D. Reestablishment of its Function and Role

The regulation by the Act on the Promotion of Information and Communications Network Utilization an Information Protection, etc., the Act on Protection of Information and Communications Infrastructure, the Electronic Government Act, and the National Cyber Security Management Act (Presidential Decree) may often run into over lapping of the inter-agency mission. Although various agencies are extant, when an actual cyber crisis occur, the uncertain roles and responsibilities of each agency may be problematic. In particular, when investigating cyber terror, the motivation, political or social or financial, and origin of the attack must be identified in order for a proper investigation. However, previous to identifying these elements, the investigation and intervention of the police department is legitimized.

Therefore, the police must actively be involved in identifying the factors and relationships involved in the case in order for a proper attribution process to oc-


current cooperation between agencies.

3. Problems Confronted by Response System on Cyberterrorism

A. Initial Response and Variety of Legislation Causing Confusion

1) Lack of Systemized Legislation

Identifying whether an occurred cyberterrorism case is against personal, organizational, or national is difficult. Therefore, it is also difficult to decide which department, military or information agency, is responsible for the attack. This point of view confronts a contradictory claim that even if the March 4th and July 7th DDoS attacks were all executed by North Korea, the investigation agencies were supposed to administrate the investigation rather than the military. At the time of the attack, the military forces were massively criticized for its irresponsibility.

In addition, to a number of problems of the initial response to cyberterrorism are merely limited to the Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc., the Act on Protection of Information and Communications Infrastructure, and the National Security Management Act (Presidential Decree). The Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc, deals with the private sector, the Act on Protection of Information and Communications Infrastructure and the National Security Management Act (Presidential Decree) deals with central administrative agencies, local governments, and public agencies. But, it is stated in the Act on the Protection of Protection of Information and Communications Infrastructure Article 8, Information and Communications Infrastructure designated in this section are excluded from legal application,
2) Limitations in System of Initial Threat Estimation

The threat of cyberspace is cannot be measured visually nor for government to have access to the private systems. Also, the law requires to report any activities of cyberattack to the NIS or KCC, but reporting is often just ignored and therefore not calculated properly. These intrusion and cyberattack registration centers are only focused on prevention measures, but not the elimination of the threat itself.

<table>
<thead>
<tr>
<th>Law</th>
<th>Article</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal procedure act</td>
<td>Article 234 clause 2</td>
<td>When a public official in the course of his duty believes that an offense has been committed, he shall lodge an accusation.</td>
</tr>
<tr>
<td>Instructions on cyber safety management</td>
<td>Article 12 Clause 1</td>
<td>The head of a management organization shall take necessary measures to restore and minimize damages, when intrusion incidents against main information and communications infrastructure under its jurisdiction occur, and shall notify the head of National Intelligence Service in a swift manner</td>
</tr>
<tr>
<td></td>
<td>Article 13 Clause 2</td>
<td>The head of National Intelligence Service can notify investigative agency when suspicion of an offense is found after consultation with relevant organization</td>
</tr>
<tr>
<td>Act on promotions of information and communications network</td>
<td>Article 48 – 3 clause 1</td>
<td>A person falling under any of the following subparagraphs shall, if it discovers an occurrence of intrusion, immediately report it to the Korea Communications Commission or the Korea Internet and Security Agency. 1. A provider of information and communications services 2. A business operator of clustered information and communications facilities.</td>
</tr>
<tr>
<td>Act on the protection of information and communications infrastructure</td>
<td>Article 13 clause 1</td>
<td>The head of a management organization shall take necessary measures to restore and protect the relevant information and communications infrastructure in a swift manner, when intrusion incidents against main information and communications infrastructure under its jurisdiction occur</td>
</tr>
</tbody>
</table>

3) Limitation in Initial Attribution of the Attack

It is difficult to confirm the origin of the cyberattacks within the cyberspace, and therefore identifying a specific attack to an act of infringement is also
difficult. In other words, in the beginning stage of the cyberterrorist incident, it is difficult to confirm that the subject is a person, an organization, or a nation. Thus, in situations where the subject of a specific cyberterrorism has not been identified, it serves as a burden for the military or intelligence agencies be involved. However, the investigative agencies, on the other hand, regardless of the character of a subject may be involved. We can observe this with the 2009 July 7th and the March 4th DDoS attacks executed by the North Korea; the investigative agencies were responsible for both the investigation and reporting.

The response measures for cyberterrorism do not address the roles of the investigative agencies, but only state the role of the NIS and KCC as central actors. Whereas the US's National Strategy to Secure Cyberspace released in 2003 states it emphasizes the proper cooperation between the law enforcement agencies and national defence agencies play a significant role in prevention of attack from the cyberspace. It also claims that the law enforcement are executing criminal justice authorities to play a central role in attribution.

According to law enforcement and national security communities to play an important role in the prevention of cyberspace attacks, law enforcement agencies and the importance of the role of law enforcement agencies to play a central role in the attribution of the attack by the enforcement of the criminal justice authority.

---


383) The reason for the difficulty of attribution in technical aspect could be such as following the evidence trail of the attacker, the easy disguise and getaway, lack of credibility to Internet information. In legal aspect, difficulties of tracing off-territory information and tracing and lack of voluntary cooperation. Refer to Gi Bum Kim, Yoonshik Jang, “Theory of Criminal Investigation,” Korean National Police University, 2012, p. 89.


B. Limitation on Cooperation with the Information Institutes and Law Enforcement Agencies

Cyberterrorism is directly related to our cyber security. But in the case of Korea, the intelligence agencies mainly involved in the enforcement of the cyberterrorist policies. The fact will ultimately cause: (1) the departments and policy competition; (2) limitations in information sharing of the intelligence agencies; (3) lack of legal evidences of information agency activities; and (4) limitations in international cooperation. Unless these problems, especially the cooperation between the agencies, are solved, the efforts will be criticized.

In addition, the law enforcement agencies are main actors of the foreign national cyber crime response policy and cyber security policy. However, with the cyber security Master plan, the role of the police is not mentioned anywhere. This is not an indication that we are performing a multi-dimensional approach to the fact, because the investigation and prosecution part is eliminated.

C. Limitation on Expedited Responses due to Division of Functions amongst Public, Private, and National Defense

The attackers will attack regardless of the status of the target being the government, public, private, or national defense. Also, cyberterrorism occurs regardless of the area corresponding jurisdiction, but rapid response is difficult since there are divisions of work function. A Control Tower issue was brought up and Secretary of the Executive Office of the President was built for policy coordination, but there are still limitations. Considering the establishment of the Cyber Protection and Cyber Security Department seems necessary.

While the government is playing the leading role in these policy promotion, the private sectors became a passive participant to the issue. The lack of self-initiative to prevent cyberterrorism and cyber security could be from the lack of social power movement. Offline crimes are prevented primarily by the law enforcement, On
the other hand, the recent Kakao messenger system, POS terminals, and messenger-phishing can be prevented and enforced by the private companies of manufacture. In other words, cyberterrorism occurs in the Internet network and therefore a large portion of prevention of cyberterrorism may be facilitated by these private companies.

III. Countermeasures for Cyberterrorism

1. Intelligence

Cyberterrorism must be detected and prevented rather than responding afterwards. The March 4th DDoS attack and the Joong-Ang Newspaper Co. hacking failed to be detected both at state and private level. If the efforts against cyberterrorism were focused on technological aspect of criminal information, we now need an integration of analysis system that combines the Hugh Mint and Tech Mint. It would require a profiling system and a long-term plan, rather than a short-term plan, to counteract to cyberterrorism.

We shall develop a methodology for measuring the cyberterrorist threat at a national level, and find means to collect and analyze the government departments and private information systematically. The limitation of technological information should be expanded further to be supported by a variety of information rather than mere methodological research, including personal information, crime information analysis, cyberterrorism profiling, data mining, expert systems, and technical information should be supported. Cyberterrorist threat should be accurately measured for an efficient utilization of resources and budget, and to be able to achieve the desired results on the Cyber Terror Response.
2. Expert System and Founding National Digital Evidence Research Institute

Current response measures against cybercrime is focused on post investigation and therefore there is a limitation in its effective prevention. Existing investigation strategy also lacks proper methodology, but merely based on the investigators personal experience, information sharing, and decision-makings by the designated agency. This investigation agency owns a large amount of data, but does not utilize these information because the proficiency to analyze these data is limited. Therefore, an "Expert System" which enables analysis of a large amount of data to utilize in prevention and investigation must be developed.

In order to develop such system, the existing psychologists, criminologists, and legal scholars and investigative practitioners, must cooperate in interdisciplinary collaborative research and utilize existing academic sources on profiling, data mining, scientific investigative techniques, as well as the personal experience of the investigators to encourage the development of an integrated expert system.

National Forensic Service (NFS) have a collection of data in physics and biology, but lack in research on digital evidences. There are no research institute that mainly focus on research on counter-cyberterrorist response technology in Korea. A specific organization must be established in analyzing digital evidence and malicious codes.

3. Improvement on Cyberterrorism Legislation

A. Necessity of Enacting Legislations on Cyberterrorism

Policies on cyberterrorist response and crisis management that are scattered in different legislation must be consolidated for a prevention of cyber-crisis and a consolidated system.\(^{386}\) In other words, an Act on cyberterrorist legislation frame-
work that integrates the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., Act on the Protection of Information and Communications Infrastructure, and National Security management Act must be enacted. This framework Act must include the response system at the national level, including the definite roles and responsibilities clearly defined in order to eliminate unnecessary inter-agency conflicts. For example, the role division must be separated between prevention & response agency and investigation agency, between investigation agency and the military, and between prevention & response agency and the military. A clear definition of cyberterrorism must also be considered. Intrusion of civil privacy and criticism on treating cyberterrorism like other petty crime may occur without a clarification on definition of cyberterrorism.

B. Necessity for Act on Zombie PCs

In the case of cyberterrorism, the most effective response measure is to detect and prevent cyberterrorism prior to an attack and monitor in real-time basis since the scale of victimization may increase every minute. Identifying the ISP before detecting the victimized PC would be a desirable measure under the current system.

This is mainly due to the possibility of PC users not agreeing to be searched without a warrant. Currently, the investigation forces are using a warning tactic to let the user know that he could later be charged as a perpetrator. Hence, a proper law would greatly aid the investigation of cyberterrorism.

In this regard, an Act pertaining to the investigation of the zombie PC is a necessity. However, the measure may clash with the violations of human privacy and fundamental rights stated in the Constitution. Therefore, a discussion of integrating such measure in the Personal Information Protection Act is currently being debated. Although, the aim is to ultimately protect the mankind from cyberterrorist attacks, not personal PC. In this sense, a contemplation on regulating the Act on the Protection of Information and Communications Infrastructure seems to be valid.

C. Restricting the Remote Update Function

Many programs, such as vaccines and web hard-disks are using the remote updating feature. This is mainly due to the commercial purposes to profit the small business enterprises who manufacture a program without proper security measures. As we can see in case of July 7th and March 4th DDoS attacks, the remote update server is dominated by the attacker, multiple number of computers are victimized. The usage of such functions must be regulated and security management on update server should be implemented,
D. Recommending Diversification in Operating Systems and Installation of Firewall Programs

All of the cyberterrorist attacks involved the Microsoft Windows and operating system for the PC. Windows are accounted for the majority of Korean computer users and a diversified operating system is to be taken into consideration. Also, detecting a reverse connection\(^{387}\) and personal firewall program for logging should be encouraged to be used for post-measures of being infected by malicious programs.

E. Fostering Professional Investigators

UN, OECD, ITU, Interpol, and other international organizations are hotly debating on the topic of cybercrime and cyberterrorism. Investigating cyberterrorism requires the premise of international cooperation including technological expertise and sufficient foreign language skills. We must train professional investigators and, if necessary, consigning overseas education through a long-term professional training. We must also implement comprehensive and systematic education of professional level, such as masters degree in domestic Universities, to disseminate and follow up with the training is highly recommended. Also, it is also important for cybercrime experts to be able to participate in decision-makings with the NPA.

---

\(^{387}\) Reverse Connection: An abnormal access to the server where the designated server becomes a client and connects to an outer server or the client becomes a server allowing the access from outside.
4. Examination on Cybercrime Investigation Cooperation System

A. Private–Private Cooperation

1) Necessity

Internet network, digital devices, and Internet services are public information, they are free to analysis the information that they come across. Similarly, private users and companies will be the first ones to be victimized and recognize the victimization. The competitive market structure will increase the IT technology, equipment, and services every day while also increasing the possibilities for newly emerging security holes. In other words, in order to be successful in the market, the corporations will prioritize profit rather than security checks. When applying for patent, even if the security measures are unfulfilled, they would haste the filing first and repairing for the mistakes later on. Nevertheless, there are little of sharing these fallacy between the private sectors or personal users.

2) Countermeasure

Information sharing system at a private level needs to be established. The companies and personal users are becoming increasingly sensitive to the privacy of individuals making national intervention more and more difficult. The companies are also unwilling to share corporate secrets. A system that similar companies and personal users share the information of victimization is necessary. Extorting personal information in portal websites in order to get access to banking information often occurs. If these private portal website companies would share the seized information of the offender with the financial institutes, we may be able to prevent these crimes ahead. These kind of voluntary initiatives mutually benefit and protect these private companies from cyberattacks and enhance national response measure for cyberterrorism.
B. Law Enforcement–Private Cooperation

1) Necessity

The criminal incidents occurring offline can be visually and systematically detected. However, estimation of cyberterrorist attack is impossible without reports from personal computer users and companies. These program manufacturers must decide whether to keep their problems confidential or to report to the law enforcement to be able to arrest and prosecute these cybercrime offenders for the greater good of the country and customers. Through proper practice of such reporting may prevent us from bigger victimization in the future and determine the possible damage to other companies as well.

Also we need to admit the country's lack of professionalism. The private corporation are responsible for manufacture of the systems, digital devices and services which contributes to the lack of technological background by the state. Technology development will be faster in process than country's intervention to train professionals. Our IT experts are being transferring to the public sectors for better security of life, but in the US, the IT professionals are continuously transferring to private sectors.

2) Countermeasure

A conscious of reporting criminal activities are needed. Essentially cyberattacks, cyberterrorism, and cyber infringement all fall in to criminal activity and strictly prohibited by law. Reporting offline crimes are well-implemented relative to the low reporting rate of crimes with in the cyberspace. In addition, law enforcement agencies should strive constantly to cooperate with the private sector in order to enable the sharing of private information between the government. Organizing conferences and training should be done through government efforts.

Further investigation process must involve private sector experts. The US, when
investigating the DNS Changer Botnet, cooperated with the police force around the world, vaccine manufacturers, security companies, and financial institutions. Excluding the private sector experts for the investigative security is unwarranted and will ultimately make the investigation more difficult.

The information of vulnerabilities of programs obtained during the investigation must be quickly shared with the private sector. We must deviate from the conventional investigation method and provide these information to the public. Therefore, the PC users and companies may better protect their information assets themselves. For this to happen, reporting of suspicious activities and cyberterrorism should be mandated.\(^{388}\)

C. National LE—National LE Cooperation

1) Necessity

Cyberterrorist attacks are often a global scale. For the DDoS investigation in 2009 involved a total of 46 countries and a total of 70 countries participated in DDoS attack in 2011, Dutch KPN case was also jointly operated between South Korea and the Netherlands police and was successful in arresting two hackers who attacked 300 computers in nine different countries. Likewise, cyberterrorism does not only need international Mutual Legal Assistance Treaty (MLAT). However, we cannot entirely eliminate the official procedures as well. Currently, each police force in designated countries are following their own protocols in international cooperation. Even so, we cannot achieve any outcome without international cooperation in investigating cyberterrorism.

Europe is currently planning on establishing cybercrime response center under the Europol, and the Interpol is promoting the creation of Digital Crime Center

in Singapore, and the US has been considering on dispatching cybercrime resident officer in 12 countries. Thus, this implicates that these international organizations are committed to the expansion of international cooperation capabilities.

2) Countermeasure

Observing the facts, most cyberterrorism occur in a foreign setting or detouring through international routes; we must commit to diversified efforts in international cooperation. In case of Korea, the KCC is operating under the UN Asia Pacific Centre for Information and Communication Technology for Development. But since 1964, after becoming a member of the Interpol, Korean police force has never granted financial contribution to any projects. In the last decade, some expansion of network through the KOICA program has been obtained. Active involvement in international activities and concluding treaties must be conducted. We should first accede to the Council of Europe Cyber Crime Prevention. We may learn and solve problems between countries of conflicting cybercrime related substantive laws and procedural laws through subsequent legislation. Second, international cooperation centering on the works of the Interpol shall extend the investigation capabilities. Recently, the Interpol is planning on founding the Digital Crime Centre and Korea should support the establishment. Third, through professional training of counter-cyberterrorism experts, Korea should actively participate in the UN, Council of Europe, NATO, and Interpol. Considering the geographical structure of South Korea, being adjacent to North Korea, and the advancement of information and communications infrastructure, we must be part of the force deterring cyberterrorist activities around the world,
Chapter 6

Conclusion
As discussed previously, terrorism has evolved after the 911 attacks on the 11th of September, 2001. It is hard to simply ignore cyberterrorism and threats to cyberspace, which is already deeply ingrained into our everyday life. Cyberterrorism threatens our lives in variety of ways. For example, recent DDoS attacks and hacking of national government agencies initiated from China prove these threats to be real. Examples of direct forms of cyberterrorism are DDoS attacks, the Stuxnet worm, hacking and use of botnets. Other forms of cyberterrorism are utilization of the Internet for logistics of traditional terrorist activity, recruitment, propaganda, training, education, financing, command & control, and procurement of supplies. UNODC defined this type of activity as “the use of the Internet for terrorist purposes” and classified this as an issue with special concerns. Cyberterrorism is globally recognized as fundamental threats to national security as well, Therefore, there is a need to look into the topic with a more strategic approach, and consider more systematic and inclusive policies and responses.

In this regard, this research aims to introduce cyberterrorism as a new form of threat to our society, which reflects the distinctive characteristics of information society of the 21th century. By promoting public awareness of this threat, mass confusion can be prevented in case of a real cyberterrorist attack. Also, through anal-
ysis of new trends of cyberterrorism, this research intends to propose effective and systematic responses to cyberterrorism.

This research is an international joint research conducted as a part of UN Cooperation Project. Thus, the study is conducted cooperatively with foreign counter-cyberterrorist agencies and professionals whose empirical methodologies use qualitative data such as interviews with specialists and professionals in the field and press release. Also, the most important theme dealt by UN agencies and international society, use of the Internet for terrorist purposes, is included in the study. As terrorists use the Internet as a means to committing terrorist acts, there is necessity to conduct research on this emerging issue. Thus, this study aims to analyze trends of cyberterrorism and propose countermeasures.

Therefore, in this chapter, research materials are discussed and organized into three general frameworks, and on this basis implications are drawn, Policy recommendations that suit the present reality of South Korea are made, and the necessity of further research is proposed, First, discussion and organization of research materials thus far and their implications are as follows,

First, there is a general theoretical discussion on current terrorism trends of increasing sophistication against the backdrop of convergence of national security, public security, crime and warfare. Hence, the reality of the threats that we are experiencing in relation to some of the attempted countermeasures of the major international organizations are examined.

With regards to conceptualization of cyberterrorism, a number of national and international professionals agree upon a common element of cyberterrorism definition, which is "attacks against infrastructure of society using computer network."

Here, 'social infrastructure' refers to infrastructure in the real world such as ports, airports, medical facilities and powerplants, but they can also mean the system itself consisting of operating software running on computer networks of large scale online markets, governments and public or private institutions.
Nevertheless, the general concept of cyberterrorism is still yet to be defined. As we have observed earlier, since the concept of cyberterrorism brought us a significant controversy, a detailed course of its criminal action and victimization must be prescribed and defined. However, we cannot deviate from these controversies since we are already aware of the concept and in use of the word cyberterrorism; the debate whether to distinguish cyberterrorism from cybercrime still remains fervent. In order to effectively respond to transnational crimes such as cyberterrorism, it is important to operate under an equivalent justification of the debated crime and to cope with crimes in consideration of its characteristics. This way, international cooperation is enabled and investigation procedures are simplified.

Results indicate that the definition of cyberterrorism cannot be fully justified due to the reason that the nature of the cyberterrorist crime being too comprehensive. New methods and technology are constantly emerging through the characteristic of cyberspace. Some do not recommend that we define cyberterrorism in order to impose punitive measures made possible by ambivalent legal interpretation of its definition and concept. Nevertheless, with technology in constant advancement, any law to regulate cyberterrorism will prove to be difficult due to anomalous intents of cyberterrorists. Thus, it is also difficult and meaningless to clarify a particular form of cyberterrorism in legislation. Therefore, the derived conclusion is to necessitate a legal measure that accommodates variant forms of cyberterrorism, which is broad and mutating in its nature.

With regards to international cooperation, the necessity of multilateral cooperation is emphasized in consideration to extradition and legal aid. In the light of currently identified variables, the effectiveness of bilateral cooperation to counteract cyberterrorist attacks has been warranted through examined cases. In order for the governmental agencies to arrive at a successful result in the enforcement of existing legal measures, ways for efficient cooperation must be sought out. Particular attention should be paid to the countries with vulnerabilities to cyberterrorism in order to secure their critical infrastructure and support establish-
ment of alliances between those countries. Therefore, minimization of administrative procedures and cooperation, both official and unofficial, needs to be mandated. In this sense, bilateral cooperation can be one of the solutions.

Among various organizations and agencies taking important role in facilitating cooperation at international and national levels, organizations such as CERT and FIRST can serve instrumentally in formal, informal, bilateral and multilateral cooperation. In the field of cybercrime and cyberterrorism, informal activities between the public and private sectors lead to formal cooperation. Thus, establishing organizations or agencies such as a coordination center for cooperation and coordination at every level should be established. Law enforcers should be aware that the purpose of such a center is to facilitate cooperation and coordination, not for surveillance. For instance, programs such as the U.S.'s Secret Service Electronic Crime Task Force can build strong trust between private sector and law enforcement, support each other, and share information. Those examples may have meaningful implications.

With regards to legislation on cyberterrorism, the UN Security Council Resolution 1368 and 1373 after the 911 attacks urged the Member States to enact counter-terrorism laws. To meet the demands of the UN, most of the states modified their policies including South Korea. South Korea established a legal system of counter-terrorist activities, secured transparency in counter-terrorist activities, and reinforced cooperation with the international community. The necessity of counter-terrorist legislation must be accepted and a new provision on cyberterrorism must be discussed. Based on such theory, as cyberterrorism must be detected and prevented beforehand, a profiling system needs to be taken into consideration, and, case administration must shift from a short-term to a long-term process. Also, there is a need to develop a methodology that can be applied to analyzing cyberterrorist threat, following a policy that enables a systematic collection of private and public data. Cyberterrorist threat must be properly calculated in order to efficiently use the existing resources and accomplish our agenda on
the combat against cyberterrorism,

Most importantly, amending and consolidating the existing legislation pertaining to cyberterrorism is an international priority. Comprehensive and integrated cyberterrorist response and crisis management system should be established. This is to eliminate unnecessary conflicts that emerges from undistinguished roles and functions between government agencies. Like in the cases of July 7th and March 3rd DDoS attacks, we must refrain from countless victimizations by remote update servers; the usage and security must be regulated by a tool that may restrict public usage. Most PCs in South Korea use the Microsoft Windows operating system, and diversification of operating system should be considered. Whether or not detecting reverse connection and personal firewall program for logging will be recommended for public usage is also an area requires further research.

Cyberterrorism prevention and response depend on private and mutual voluntary inspection system and therefore it needs modification; for this, the private sector must play a role in investigation procedures. In the United States, when investigating the botnet involved in the DNSChanger case, police agencies, anti-virus program companies, security companies and financial institutions from all around the world took part in exchanging expertise. Therefore, when a cyberterrorist attack occurs against government agencies, reporting must be mandated,

Second, an examination on how terrorists, political radicals, and their advocates use the Internet was conducted in relation to three issues: (1) how the terrorist organizations use the Internet is discussed with the materials published in their website; (2) the purpose and reason behind the abuse of the Internet by the terrorist organizations; (3) how the law enforcement agencies cope with the terrorist threats from the Internet.

According to results, terrorist organizations were using the Internet for various purposes, Accessibility to uncensored information on the Internet has made it more cost-effective and enabled aggregation of dormant members through web-
sites, chat rooms and online discussion sites. In addition, the Internet served as a valuable tool for collecting information on tactics, information about the target victim, and ways to avoid getting arrested. Law enforcement agencies are aware of the terrorist abuse of Internet and many police responses has been establishing infrastructure and legal mechanisms. Furthermore, these agencies have been developing investigative strategies to collect information on terrorist organizations, identify dormant terrorists, and disrupt terrorist agenda. They also internationally cooperate in surveillance of terrorist Internet usage. Improving relationship between the agencies in different countries requires considerable time and effort.

Pertaining to recent abuse of the Internet by terrorists, South Korea was urged to introduce the practices of international organizations of Western countries for better understanding. As a result, an integrated counter-terrorist method that combines intelligence agencies, military, police, prosecutor, fire protection, and private security was suggested.

Also, accurate identification and comprehension of the emerging threat of cyberterrorism must be acquired to present a suitable response measure. More attention to the understanding of newly emerging security threats and concept of networked counter-terrorist response system is what the society needs. Many research lack systematic and empirical evidence and, hence, this research focused on empirical evidences from the most current research. In conclusion, terrorist organizations have been abusing the Internet and has been adapting to the external environment. Politically, socially, legally and culturally oppressive management and strategy augmented the efficacy of terrorist organizations. Their abuse of the Internet does not require expertise and expense, can easily proliferate for more network, and self-development. They advertise their basic ideologies online to recruit new members, monitor chat rooms, transfer orders to attack a target victim, accrue financial resources, and collect confidential information through the Internet. The Internet serves as a valuable tool for the terrorist organizations, which abuse the Internet for various purposes to accomplish their goals.
Law enforcement agencies, with regards to perception of threats posed by terrorists using the Internet, police response is mostly strategic, focusing on establishing necessary infrastructure and policies, and invest in cooperative task forces and practitioner groups to strategically assess how counter-terrorist responses and related laws can be utilized. Through this strategy, there is a need to understand the relationship between technology and terrorism, and law enforcement agencies need to develop investigation techniques, collect information on terrorist organizations, identify potential terrorists, and use technical tools to disrupt terrorist plans. To this end, further research is needed in the academia on how the Internet can affect terrorist organization. For instance, it would be valuable intelligence to know effectiveness of terrorist recruitment strategies and promotion of extremism on the Internet, the process in which an individual becomes involved in an organization, and other related strategies. In fact, National Institute of Justice funded research on extremism came with results that there is significant concern for the involvement of the Internet in the process of an individual becoming an extremist and his recruitment into a terrorist organization. This concern has significant implications for South Korea. Use of the Internet by terrorist organizations is a new phenomenon of the information age, and as social networking becomes popular, terrorist organizations are attempting to tap the potential of social networking services such as Facebook and Twitter. Moreover, social networking is also affecting the process of terrorist recruitment.

Research thus far has not been able to provide any practical results on what responses work against terrorism, and the fact is that there is no empirical evaluations of counter-terrorist strategies on the Internet used thus far. This study indicates only a state-lead response can understand the terrorist use of the Internet and execute countermeasures. Therefore, there should be further research on the terrorist use of the Internet and its future trends, along with further research on related subjects.

Third, in case of the United States, there is no determinant proof yet that a cy-
berterrorist attack took place against an American citizen. However, there were cyberattacks without political motives, and this means without a doubt that the threat of a cyberterrorist attack is real. Therefore all levels of law enforcement need to prepare countermeasures against a possible cyberattack, and in order to prevent cyberterrorism, the law enforcement needs to minimize the threat of cyberterrorism by providing education programs on cyberspace security and cyberterrorism to the general public and the private sector.

Law enforcement response to the cyberterrorist threat should take an entirely different approach than other traditional forms of crime. A cyberterrorist attack can proceed and occur as serial incidents with some similarity through a wide range of space and time, but the police, who are used to dealing with discriminate incidents, will not prepared for this type of attack. This unique characteristic of cyberterrorism requires police officers trained in both terrorism and information technology to effectively respond against cyberterrorism.

Such training is not very common even in the United States. For instance, a research on police departments in North Carolina found that most departments did not have adequate countermeasures against potential cyberterrorist attacks in their jurisdictions. With this finding in mind, the federal government, through research, developed an action plan to support first responders to a cyberterrorist attack, and encouraged cooperation between local law enforcement agencies and internet service providers to facilitate investigations in cyberterrorism. Such measures have significant implications for South Korea. Also, the United States is actively using the community as the most effective means to detect potential cyberterrorist acts on the Internet, and law enforcement agencies are providing training to informal networks on reporting procedures on the event a potential cyberterrorist organization is found. Such efforts can promote public awareness of terrorist activities on the Internet and encourage citizens to report any suspicious activities.

Cooperation efforts between the government and the private sector are very important because the private sector manages almost all of America’s critical
infrastructure. To contribute to this effort, private companies should implement state-of-the-art verification technologies to strengthen company network control. Private companies should also need to seek ways to find vulnerabilities in their networks and ways to bolster their defenses against potential attacks. InfraGard provides such services to more than 50,000 private companies and public institutions in the United States, and the FBI provides consultation to private companies and individuals on cyberterrorist attack methods and ways to minimize impact of such attacks. Such cooperation decreases the terrorist threat, increases information sharing on cyberterrorist attacks, and minimize impact of such attacks, which has significant implications for South Korea.

There is also training on cyberterrorism, provided by the RCFL National Program Office (NPO) and the National Cyber-Forensics & Training Alliance (NCFTA), which are said to be the “effective model” in national security. These models could be benchmarked for its application in South Korea.

As terrorist organizations evolve continuously through constant acquisitions of new technological methods, cyberterrorism is unavoidable and inevitable. The best response to this type of threat is security provisions that continue to change and improve to minimize the cyberterrorist threat. Due to lack of research on this topic, researchers should start from cyberterrorist attitudes, acts, methods and targets and apply innovative research methods to produce new knowledge on cyberterrorism. At the same time, a major finding in this research is that in order to prevent cyberterrorist attacks and bolster cyberspace security, there needs to be innovative and meaningful interaction between the government, the private sector, and the citizens. Therefore, this is where the discussion should start on finding the most optimal approach to respond to cyberterrorism and minimize its impact.

In conclusion, the most pressing matter for South Korea is establishment of safety measures for cyberterrorism and further research on the topic. Furthermore, individuals and private companies should prepare security measures and reporting protocols. Also, with regards to investigations in cyberspace, a cooperative system
should be created to promote information exchange between law enforcement agencies and cyberviolation response institutions. Considering the current trend of terrorist using the Internet as a means, it is imperative to establish a cooperation system between law enforcement agencies and internet service providers, and also between public and private sectors, government agencies, and furthermore, an international cooperation system between nations. These cooperation systems should be given priority to prepare a prudent and effective response system against the threat of cyberterrorism.

Furthermore, considering the real threat of cyberterrorism, future-oriented research should continue to prepare for this threat. Joint researcher Morris, in the following research, points to the important of research on cyberterrorism and continued research on cyberterrorism. This research shall be concluded with Morris’s proposal for further research on cyberterrorism.

With regards to recent trends in scholarly research on cyberterrorism in the United States, joint researcher Robert G. Morris proposes the following.

i) With regards to empirical findings on cyberterrorism, Research on cyberterrorism is still in its infancy. Given that there is no verified instance of cyberterrorism in the US, little empirical analysis exists concerning such crime. Since cyberterrorism unites two of the most predominant public fears—that of technology and terrorism—it is not surprising that the threat of such acts are dramatically overstated, Scholars tend to focus on determining the true threat posed by cyberterrorism and analyzing the benefits of these acts for terrorist agendas in order to ascertain the realistic likelihood of such events transpiring. The available evidence on Islamic extremists does not provide support for the contention that their terrorist organizations have strong cyberterrorism capabilities. Relying upon the available information on known terrorists, these researchers showed that only a small percentage (less than three percent) of their overall sample had advanced training in computer-related engineering. While men with advanced degrees were over-represented within these terrorist organizations, very few held degrees in com-
puter science and/or engineering. Lacking the requisite knowledge base, the ability of these groups to coordinate an effective cyberterrorist attack is questionable.

Many scholars contend that the true threat of cyberterrorism is overestimated. Lewis (2002) points out that critical infrastructures experience failure quite often that results in little to no disruptions in civilian life and certainly is not detrimental to national security. Further, he compares the expectations for damage induced by cyberterrorism to the early literature on the expectations for strategic bombings of Germany in World War II. These bombings were anticipated to cripple the German infrastructure, but the country was found to be remarkably resilient to such attacks, Lewis speculates that the same would hold true for US civilians in the face of a cyberterrorism event.

Reasoned discussion on cyberterrorism indicates that the benefits of cyberterrorist acts may be substantially lower than it initially appears. Lewis (2002) reports that having a marked effect on the US water supply, for example, which is spread over thousands of systems would require a continuous and simultaneous interruption in hundreds of these water systems in order to effectively attain the intended terroristic impact. The electrical system, another commonly cited primary target of cyberterrorism, is also a vastly integrated system with built-in redundancy to minimize the risk of failures. Similar to the water supply, it would require a large-scale attack spanning multiple points in the electrical grid over a sustained period of time. Ultimately, these systems are accustomed to failures and the effects of cyberterrorist actions against them are likely to be short-lived and of little prolonged consequence—more “weapons of mass annoyance” than mass destruction.

Further, cyberterrorist attacks will not tend to cause the widespread panic and loss of human life that terrorist organizations prefer in order to disseminate their messages. A cyberterrorism act that is capable of conforming to these standards is likely to come at large financial and temporal costs from the terrorist group for comparatively little payoff. Giacomello provides preliminary estimates that an act
of cyberterrorism has the potential to produce 25 billion dollars in damage via economic disruption, network failures and physical injuries or death. Meanwhile, a series of simple bombings is capable of 10 billion dollars in damages—ultimately a higher payoff for the time and costs involved with such an act. When compared to the relative ease and results of traditional terrorist activity such as car bombings it is speculated that terrorist organizations are not likely to adopt cyberterrorism into their repertoire.

It appears that cyberterrorism alone is not likely to have a dramatic impact on the lives of civilians. It has its strongest potential for harm when coupled with real-world, traditional terrorist activities. Cyberterrorism could serve as an effective “force multiplier” that increases the damage caused by a physical attack. For example, terrorist organizations could conduct a series of building bombings and simultaneously disengage the area’s water supply, which would impede the fire department’s ability to extinguish the fires that result from these explosions. Additionally, as a force multiplier, cyberterrorism portrays an image that the terrorist group is stronger than they really are.

ii) with regards to limitations of cyberterrorism academic literature, the greatest limitation of the cyberterrorism literature is the lack of research on the topic. Much of the available research on cyberterrorism, as exemplified above, is hypothetical and speculative. Even samples of known terrorists, such as that employed by Gambetta and Hertog (2007), suffer from the obvious bias that the individuals who constitute “known terrorists” are those who were caught and were probably more highly involved in the group’s activities. The ability to generalize knowledge on these individuals to the full population of terrorists both known and unknown is a weak assumption in need of future research.

In the interest of increasing available data on cyberterrorism, Holt (2012) suggests gathering data from Internet sources to track terrorist groups’ communication over the Internet as a means for assessing changes in their techniques and targets. Further, culling data online can be informative as to the rate at which terrorist
groups are adopting new technologies, ultimately bolstering prevention efforts and staving off cyberterrorist attacks.

Finally, Holt (2012) suggests that looking beyond cyberterrorists to the greater realm of cyberattackers in general will prove vital to our understanding of cyberterrorism. As there is no documented evidence of cyberterrorism in the US, scholars have no way to assess the tactics and motivations of cyberterrorists. However, we can develop an understanding of these behaviors in politically motivated cyberattackers that are not aligned with a terrorist organization. This information will aid our understanding of extremist behavior and viewpoints, which will ultimately assist our understanding of cyberterrorists.

iii) With regards to the future of cyberterrorism, Cyberterrorism will inevitably occur as terrorist groups gain technological savvy. Combating this threat will require ever-changing and ever-improving security protocol to minimize the threat of cyberterrorism. Given the lack of data on the topic, researchers will need to be creative in how they proceed in developing a knowledge base on cyberterrorist attitudes, behaviors, techniques and targets. In tandem, the prevention of cyberterrorist attacks requires innovative and meaningful interaction between governments, the private sector and the citizenry in an effort to enhance cybersecurity. Increasing the pro-collaborative attitudes amongst stakeholders represents a meaningful endeavor for future research. Ultimately, the threat of cyberterrorism is real and research and policy initiatives need to begin with a reasoned discourse on the likelihood of such events, the profiles of its perpetrators and the best approach for minimizing and responding to these acts. Therefore, further research should be performed not only for these issues, but also to introduce scholarly theories that can be applied to cyberterrorism risk analysis method and cyberterrorism research.


Affidavit in Support of Criminal Complaint at 2-5, United v. Martinez No, 10-4761-JKB (D. Md, Dec, 8, 2010).


Ballard, D. J., Hornik, J. G., & McKenzie, D., Technological Facilitation of
Bortner, Mark, Cyberlaundering: Anonymous Digital Case and Money Laundering. Presented as final paper requirement for Law & the Internet (LAW 745). A seminar at the University of Miami School of Law. 1996.
Brown, Ian and Douwe Korff., “Terrorism and the Proportionality of Internet
Surveillance,”, European Journal of Criminology, 6 (2), 2009.


Cassara, J., and Jorisch, A, The Afghan transit trade: How AF/Pak drug lords and terrorists are moving money and transferring value, Foundation for Defense of Democracies, Redcell Intelligence Group, 2009


Conway, Maura., Against cyberterrorism, Communications of the ACM, 54,


Cyber Terroror Response Center: www.netan.go.kr


Department of the Army. Open Source Intelligence. FMI 2-22.9. 2006.


EFF Analysis of the Provisions of the USA Patriot Act, Electronic Frontier Found, (http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.)


Holt, Thomas J. and Kristie Blevins, "Examining sex work from the client's per-
Jarret Brachman, Watching the Watcher, Foreign Policy, 2010, 11, 10.
Joselyn, Thomas, British Intel Concerned About Iran-Al Qaeda”, The Weekly Standard, 16 February, This article is a part of FDD(Foundation for the Defense of Democracies) Weekly Review Reports, 2012.
Keene, Shima D., “Terrorism and the Internet: A Double-Edged Sword”, Journal
of Money Laundering Control, 14 (4), 2011.
Institute of Wonkwang University, 2008.


Lee, Hwang woo., Han, Sang Am, Policies on Counter-terrorism, Jin Mung, 1996.


Maras, M. H., Computer forensics: Cybercriminals, laws, and evidence, Sudbury, MA: Jones and Bartlett Learning., 2012.


National Information Security Center(NISC), Japanese Government’s Efforts to
Nakashima, Ellen. FBI director warns of ‘rapidly expanding’ cyberterrorism threat. Washington Post. 2010, Mar. 4


Open Source Center, Advanced Googling for Senior Executives, Open Source Academy Internet Science Faculty, 2009.


Reed, Donald J. Beyond the War on Terror: Into the Fifth Generational of War and Conflict, Studies in Conflict & Terrorism, vol. 31, no. 8. 2008, Aug.


Riley, Duncan, Holocaust Memorial Shooter Called for a "Holy Western Empire. The Inquisitr, 2009. (http://www.inquisitr.com/25747/holocaust-memorial-shooter-called-for-a-holy-western-empire/)


Ruwantissa Abeyrantne, Cyberterrorism: The Next Great Threat to Aviation, Vol. 24 No. 1 Air $ Space Law, 4, 2011.

Ryu, Seok-Jun, Foreign Countries' Lawmaking Examples against Cyber Crime, Vol. 5 Issue 1, Young-San University, 2008.


2011,


Steven R. Morrison, Terrorism Online: Is Speech the Same As It Ever Was?, 44 Creighton L. Rev. 963 2011.

Stohl, M., Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games, Journal of Crime, Law, and Social Change, 46, 2007.


U.S. Department of Justice, FBI Annual Report, Regional Computer Forensic


Weimann, Gabriel., “Cyber-Fat was and Terrorism”, Studies in Conflict & Terrorism, 34 (10), 2011.


William Jackson, In Cyberspace, a Good Offense is Not Always the Best

WordNet: A Lexical Database for English; http://wordnetweb.princeton.edu/perl/webwn


Зубов, Николай, У Всемирного Зла Новое Имя. Коммерсантъ ВЛАСТЬ, No 4, 958: 27.2012, ЯНваря 30

Крючков, Игорь, Север Мали может стать новым тренировочным аггер ем Аль-Каиды, Московские Новости, Газета, No 221, 6 април я,2012. (http://mn.ru/world_africa/20120406/315048477.html),

With rapid advances in information technology, terrorism has evolved to a new form of terrorism - cyberterrorism. This research aims to examine important issues of cyberterrorism, including types of cyberterrorist cases and characteristics, conceptualization of cyberterrorism, international cooperation against the cyberterrorist threat, use of the Internet for terrorist purposes, and legal, governmental response and crisis management systems regarding cyberterrorism in major countries with particular focus on South Korea and the United States.

This is a joint research conducted as part of the UN Cooperation. This research uses qualitative data derived from previous research, interviews and workshops with professionals and academics, and documentary evidence such

* Associate Research Fellow, Korean Institute of Criminology, Ph.D. in Law.
** Assistant Professor, Police Science and Security. College of Law, Gachon University.
*** Professor, John Jay College of Criminal Justice, City University of New York
**** Professor, School of Criminal Justice, Michigan State University
***** Assistant Professor, Criminology Department, School of Economic, Political and Policy Science, The University of Texas at Dallas
as laws and press releases. Through analysis, this research provides a comprehensive and comparative review of current status and trends in cyberterrorism, its types and characteristics, its issues with conceptualization, international efforts for cooperation, use of the Internet for terrorist purposes, and legal, governmental response and crisis management systems regarding cyberterrorism in major countries.

Based on this analysis and its findings, this research proposes various recommendations. Among these recommendations, particular emphasis is given to the necessity for legal provisions that can continue to change and improve in response to the ever-evolving nature of cyberterrorism and the necessity for improving cooperation, coordination, information sharing and other forms of interaction between nations, governmental agencies, the private sector and the public.
Cyberterrorism: Trends and Responses

발 행 / 2012년 12월
발행인 / 김일수
발행처 / 한국형사정책연구원
서울특별시 서초구 태봉로 114
(02)575-5285
등 록 / 1990. 3. 20. 제21-143호
인 쇄 / (주)이환기획인쇄
(02)764-1116
보고서 내용의 무단복제를 금합니다

정가 원