

**Strategic Philanthropy for Cyber Security:  
An extended cost-benefit analysis framework to study cybersecurity**

Yiseul Cho

**Working Paper CISL# 2012-06**

**June 2012**

Composite Information Systems Laboratory (CISL)  
Sloan School of Management, Room E62-422  
Massachusetts Institute of Technology  
Cambridge, MA 02142

**Strategic Philanthropy for Cyber Security:  
An extended cost-benefit analysis framework to study cybersecurity**

by

Yiseul Cho

M.S Energy Strategies  
École Nationale Supérieure des Mines de Paris, 2010

B.S Computer Science  
Korea Advanced Institute of Science and Technology, 2008

Submitted to the Engineering Systems Division  
In partial Fulfillment of the Requirements for the Degree of  
Master of Science in Technology and Policy

at the  
Massachusetts Institute of Technology

June 2012

© 2012 Massachusetts Institute of Technology. All rights reserved.

Signature of Author: \_\_\_\_\_  
Technology and Policy Program, Engineering Systems Division  
May 22, 2012

Certified by: \_\_\_\_\_  
Stuart Madnick  
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management &  
Professor of Engineering Systems, MIT School of Engineering  
Thesis Supervisor

Accepted by: \_\_\_\_\_  
Joel Clark  
Professor of Materials Systems and Engineering Systems  
Acting Director, Technology and Policy Program

(THIS PAGE INTENTIONALLY LEFT BLANK)

# **Strategic Philanthropy for Cyber Security: An extended cost-benefit analysis framework to study cybersecurity**

by

**Yiseul Cho**

Submitted to the Engineering Systems Division  
on May 22, 2012 in Partial Fulfillment of the  
Requirements for the Degree of Master of Science in  
Technology and Policy

## **ABSTRACT**

The international climate of cyber security is dramatically changing and thus unpredictable. As such, agile yet sustainable solutions are needed, along with an effective and a pragmatic evaluation framework to assess and demonstrate the value and efficacy of international development collaboration. Currently, no mature frameworks are available for evaluating such non-conventional, new, and complex international activities as they exist today, and thus this study aims to provide an innovative and pragmatic approach to study cybersecurity.

This study recognizes the lack of institutionalized solutions, and aims to provide a novel framework with which to evaluate emerging solutions. In particular, this study evaluates the effectiveness of international development activities and public-private partnerships as a way to improve cyber security.

Guided by literature on strategic philanthropy and international development, this study develops an extended cost-benefit analysis framework and applies it to an in-depth case study of a Korean security agency, its Computer Emergency Response Team (CERT.) This newly extended framework can be used for assessing international programs and activities aimed at improving cyber security, where the costs and benefits are not restricted by traditional boundaries. Unlike conventional approaches, this study explicitly includes three additional critical aspects, which are neglected in the conventional cost-benefit analysis framework: 1) synergic effect (such as public-private partnership), 2) indirect impact, and 3) shared value. An in-depth case study with field interviews and technology reviews was conducted to test the applicability of this extended framework. Based on the application to the case of the international development activities of the Korean CERT, this study presents two findings. First, private companies can benefit from participating in government-led international development programs. Second, international development activities are effective solutions to improving global and local cyber security.

Repeated applications of this framework to other cases will further assess the generalizability of the framework. Cumulated evidence from evaluating the effectiveness of international development activities will also inform the development of future activities for establishing partnerships of strategic philanthropy to improve cyber security.

**Thesis Supervisor:** Stuart Madnick

**Title:** John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

(THIS PAGE INTENTIONALLY LEFT BLANK)

## **Dedication**

This thesis is dedicated to my family,

**My father-Kyungho Cho, My mother-Jungryun Park, and My sisters- Yuree Cho**

## Acknowledgments

I am grateful to my Thesis advisor and a true leader, Prof. Stuart Madnick, for his guidance, support, and patience as I had spent quite long time in pivoting around research questions and approaches. Prof. Madnick taught me how to ask the right questions, and showed immense understanding and patience during my difficult times. Thanks to Prof. Yang Lee of Northeastern College of Business Administration and Prof. Changsu Kim of Youngnam University, from whom I have received salient advice and feedback; and to Skype for making our virtual meetings possible.

The fine staff, faculty, and students of the Technology and Policy Program kept me focused and joyful during my time at MIT. Special thanks to Krista Featherstone and Ed Ballo of TPP. Thanks to my fellows in research group Xitong Li, Gihan Dawelbait and Aadya Shukla with whom I have been able to talk about my ideas and receive helpful feedback whenever I hit a dead end. I am also thankful to Allen Moulton, Raphael Yahalom, and Michael Siegel from the COIN Group.

I am grateful to Taekyu Shin and Wanseock Lee of Korean Cyber Emergency Response team and Eunhee Kang of Winitech, who agreed to interview with me, and occupied a Chapter in my Thesis. Finally, I would like to acknowledge my inspirational parents Kyungho Cho and Jungyeon Park, amazing siblings Yuri Jo, who encouraged me along the entire path, never showed anything but confidence in me, and taught me the most important things I know.

This research is performed under the Explorations in Cyber International Relations (ECIR) project. ECIR project is a collaborative effort involving the MIT Political Science department, the MIT School of Management, the MIT Electrical Engineering & Computer Science department, the Harvard Law School, and the Harvard Kennedy School of Government.

## Table of Contents

<b>EXECUTIVE SUMMARY</b>	<b>12</b>
<b>CHAPTER 1. INTRODUCTION</b>	<b>19</b>
1.1. FIRST MOTIVATION: INTERNATIONAL COOPERATION FOR CYBERSECURITY	19
1.2. SECOND MOTIVATION: JUSTIFICATION FOR CYBER SECURITY INVESTMENT	20
1.3. THIRD MOTIVATION: INCENTIVES FOR PRIVATE SECTORS	20
1.4. PROPOSITIONS	21
1.5. THE STRUCTURE OF PAPER	22
<b>CHAPTER 2. BACKGROUND</b>	<b>23</b>
2.1. CYBERSECURITY	23
2.1.1. EMERGING THREAT FROM CYBERSECURITY	23
2.1.2. KEY INITIATIVES TO COMBAT CYBER SECURITY THREATS: NATIONAL LEVEL CERTS	25
2.1.3. INTERNATIONAL COOPERATION AMONG CERTS	26
2.1.4. DIFFICULTIES OF THE INSTITUTIONALIZATION FOR INTERNATIONAL COOPERATION ON CYBERSECURITY	27
2.2. FOREIGN AID/FOREIGN DIRECT INVESTMENT	28
2.2.1. MOTIVE OF FOREIGN AID/FOREIGN DIRECT INVESTMENT: DONOR'S PERSPECTIVE	28
2.2.2. EVALUATION OF EFFECTIVENESS: RECIPIENT'S PERSPECTIVE	29
2.2.3. PROBLEMS ASSOCIATED DESIGNING FOREIGN AID PROGRAM	30
2.2.4. PUBLIC-PRIVATE PARTNERSHIP FOR INTERNATIONAL DEVELOPMENT	31
2.3. STRATEGIC PHILANTHROPY: DESIGNING AIDS IN STRATEGIC WAY	31
2.3.1. BRIEF IDEAS FROM ALCOA FOUNDATION CASE	32
2.3.2. PORTER'S IDEA : STRATEGIC PHILANTHROPY AND CREATING SHARED VALUE	33
2.3.3. STRATEGIC PHILANTHROPY IN GOVERNMENT (NON-PROFIT ORGANIZATIONS)	35
2.3.4. STRATEGIC PHILANTHROPY AND INTERNATIONAL DEVELOPMENT IN CYBERSPACE	35
2.4. COST-BENEFIT ANALYSIS (CBA)	37
2.4.1. A BRIEF GLANCE AT CBA	37
2.4.2. CBA MODEL	39
2.4.3. CONTROVERSIAL POINTS OF APPLYING CBA TO ENVIRONMENTAL ISSUES	40
2.4.4. CYBERSECURITY AND CBA	40
2.4.5. CONTROVERSIAL ISSUES OF CBA MODEL IN CYBERSPACE	42
2.4.6. STRATEGIC PHILANTHROPY AND EXTENDED CBA	43
2.4.7. CYBER ISSUES IN EMERGING COUNTRIES	43
2.5. CONCLUSION OF CHAPTER 2	44
<b>CHAPTER 3. RESEARCH METHODOLOGY</b>	<b>46</b>
3.1. METHODOLOGIES	46
3.1.1. LITERATURE REVIEW	46
3.1.2. INTERVIEWS AND SITE VISIT	46
3.2. SITES & DATA	47
3.2.1. KOREA CERT	47
3.2.1.1. SITE INFORMATION	47
3.2.2. WINITECH	48
3.3. SUMMARY OF RESEARCH METHODOLOGY	49
<b>CHAPTER 4. KOREAN CYBER EMERGENCY RESPONSE TEAM (CERT)</b>	<b>50</b>
4.1. KOREAN CYBER SECURITY FRAMEWORK	51



<b>4.2. KOREAN GOVERNMENT: INTERNATIONAL COOPERATION IN CYBERSPACE</b>	<b>54</b>
<b>4.3. PRELIMINARY COST-BENEFIT ANALYSIS</b>	<b>57</b>
<b>4.4. GLOBAL G2G COOPERATION PROCESS OF KOREAN CERT</b>	<b>58</b>
<b>4.5. CASE: KOREAN CERT AND MALAYSIAN CERT</b>	<b>58</b>
<b>4.6. COMMENTS ON CHAPTER 4</b>	<b>59</b>
<b>CHAPTER 5. EXTENDED COST-BENEFIT ANALYSIS</b>	<b>60</b>
<b>5.1. EXTENDED BENEFITS WITH SHARED VALUE</b>	<b>60</b>
5.1.1. INTRODUCTION OF SHARED VALUE AND DEFINITIONS OF TERMINOLOGIES	60
5.1.2. DIAGRAM OF STAKEHOLDERS AND BENEFIT CREATION	61
<b>5.2. THE EXTENSION OF COST-BENEFIT FRAMEWORK</b>	<b>62</b>
5.2.1. EXTENDED COST-BENEFIT FRAMEWORK: GLOBAL CSR	62
5.2.2. EXTENDED COST-BENEFIT FRAMEWORK: FOREIGN DIRECT INVESTMENT / FOREIGN AID	63
5.2.3. EXTENDED COST-BENEFIT FRAMEWORK: CYBERSECURITY INVESTMENT	64
<b>5.3. COMPLETED COST-BENEFIT FRAMEWORK: INTERNATIONAL DEVELOPMENT BY PUBLIC-PRIVATE PARTNERSHIP TO ADDRESS CYBER SECURITY</b>	<b>65</b>
<b>5.4. SUMMARY OF CHAPTER 5</b>	<b>66</b>
<b>CHAPTER 6. APPLICATION TO KOREAN CERT CASE</b>	<b>67</b>
<b>6.1. VERIFICATION THROUGH EXTENDED COST-BENEFIT ANALYSIS</b>	<b>67</b>
<b>6.2. EXPECTED AND UNEXPECTED COSTS &amp; BENEFITS</b>	<b>68</b>
<b>6.3. VISUALIZATION OF DIFFERENT INFLUENCE OF COST &amp; BENEFIT ELEMENTS</b>	<b>69</b>
<b>CHAPTER 7. CONCLUSION</b>	<b>71</b>
<b>7.1. SUMMARY</b>	<b>71</b>
<b>7.2. LIMITATIONS &amp; FURTHER WORKS</b>	<b>71</b>
<b>7.3. POLICY RECOMMENDATIONS</b>	<b>72</b>
<b>7.4. CONCLUSION</b>	<b>73</b>
<b>REFERENCE</b>	<b>74</b>
<b>APPENDIX</b>	<b>81</b>
<b>APPENDIX 1. SUPPLEMENTARY DESCRIPTION ON 2009 KOREA DDOS ATTACK</b>	<b>82</b>
<b>APPENDIX 2. INTERVIEW NOTES AND SCRIPTS</b>	<b>83</b>
<b>2.1. INTERVIEWS OF CYBER SECURITY RELATED GOVERNMENT AGENCIES IN KOREA</b>	<b>83</b>
<b>2.2. INTERVIEW WITH KOREAN CERT</b>	<b>84</b>
<b>2.3. INTERVIEWS WITH WINITECH</b>	<b>86</b>
<b>APPENDIX 3. CYBER SECURITY DASHBOARD</b>	<b>92</b>
<b>3.1. DATA SOURCE DESCRIPTION (MARCH 25, 2011)</b>	<b>94</b>
<b>3.2. HOW TO ACCESS CERT DATA</b>	<b>103</b>

## List of Figures

Figure 1. The Architecture of DDos attack and the Globalization trend of Cyber Security issues.....	13
Figure 2. Synergic benefits of Public-Private partnership .....	14
Figure 3. Corporate Strategic approach for international development programs .....	15
Figure 4. Spillover of benefits created from Cyber security activities of a Public-Private Partnership .	16
Figure 5. Extension of Cost-Benefit Analysis Framework for assessing true benefits of cyber security activities including benefits which have been overlooked by traditional analysis.....	16
Figure 6. Extended benefit elements .....	17
Figure 7. The Architecture of DDos attack and a trend of the Globalization of Cyber Security Problems (Source: self-created, The detail of this crisis is described in Appendix 1).....	19
Figure 8. Related laws to international institution building .....	28
Figure 9. Strategic methodology for designing international development programs (Adopted from (Porter & Kramer, 2002) .....	37
Figure 10. Core Buisness activity of Winitech.....	49
Figure 11. Total CERT reported incidents from 2000 to 2009 of India, Malaysia, Pakistan, Brazil and Republic of Korea .....	50
Figure 12. Korean Cyber security framework (IT security policy in Korea, 2011).....	51
Figure 13. Intrusion detection system of Korean national security framework .....	52
Figure 14. Information support to operate integrated emergency response system with related organizations for cyber attack .....	53
Figure 15. Incident response system of Korean CERT .....	54
Figure 16. Explanation of Korean CERT's Government to Government cooperation process.....	58
Figure 17. Korean IT companies benefiting from the government led IT training programs.....	59
Figure 18. How Korean IT learning program lead to economic benefits.....	59
Figure 19. Benefit diagrams of international development programs operated by Public-Private Partnership.....	61
Figure 20. Data input table of Dashboard (three variables, country, period and normalization attribute can be controlled) .....	93
Figure 21. Visualized chart of Total CERT reported incidents divided by population in Korea from 2000 to 2009 .....	93
Figure 22 Yearly Data and its provenance .....	94

## List of Tables

Table 1. Six Categories of Cyber incidents of US CERT .....	25
Table 2. Principle Policy Instruments to enhance information security.....	25
Table 3. Porter's Structured Method of Listing Social Issues categorized in terms of 1) Generic social issues, 2) Value chain Social impacts, and 3)social dimensions of competitive context.....	33
Table 4 Corporate Involvement in Society: A Strategic Approach.....	34
Table 5. Definition of Strategic Philanthropy, Cases and Intrinsic Characteristics .....	36
Table 6. Types of Cost-Benefit Analysis .....	38
Table 7. Average insurance costs for death and disabilities.....	39
Table 8. Trend of recent research on economic evaluations of cybersecurity investments and limitations .....	41
Table 9. Comparison of IT Investment Success Studies .....	42
Table 10. Reasearch Cooperation with Korean CERT.....	47
Table 11. Korean Five key ICT international development programs (Two programs, Korea IT Learning program and IT policy assistance program, run by KISA, which is a higher organization of CERT, are related to international activities of CERT) .....	55
Table 12. Global G2G cooperation .....	56
Table 13. Preliminary Cost & Benefit elements of International development programs .....	58
Table 14. Cost-benefit analysis table for Global CSR .....	63
Table 15. Cost-benefit analysis table for foreign direct investment or foreign aid.....	63
Table 16. Cost-benefit analysis table for cyber security investment.....	64
Table 17. Extended Cost-Benefit analysis framework specialized in International development programs by Public-Private partnership .....	66
Table 18. Interviewed costs and benefits of Korean CERT and IT company, Winitech .....	67
Table 19. Expected and Unexpected costs & benefits .....	69
Table 20. Visualization of different influence of cost & benefit elements in program assessment and decision making (↑:Strong ↓:Weak ○:Medium) .....	70
Table 21 CERT information access-from the left, CERT website address (english site and local language site), and third column is for direct link for the webpage of statistical data and publication, and the last column specifically describes how to access specific data value from the statistic & publication webpage. ....	105
Table 22 Matching table of CERT terminologies--Table2 helps find what terminology which each country uses, matches Dashboard terminology. For the input word for the function, you can use this table to find a proper term for a target country.....	106

## Abbreviations

**CERT** : Cyber Emergency Response Team

**CERT/CC** : The CERT Coordination Center

**ECIR** : the Explorations in Cyber International Relations project.

**CBA**: Cost Benefit Analysis

**DOS** : Denial of Service

**IT** : Information Technology

**FDI** : Foreign Direct Investment

**OECD/DAC** : The Organisation for Economic Co-operation and Development/The Development Assistance Committee

**RCT** : Randomised Control Trials

**PPP** : Public-Private Partnership

**CSR** : Corporate Social Responsibility

**ITU** : International Telecommunication Union

**MOU** : Memorandum Of Understanding

**IEMS** : Integrated Emergency Management System

**RFID** : Radio-Frequency IDentification

**USN** : Ubiquitous Sensor Networks

**ICT** : Information Commuication Technology

**KISA** : Korea Internet & Security Agency

**KCC** : Korea Communications Commission

**APISC** : Asia Pacific Information Security Center

**IDC** : International Data Corporation

# Executive Summary

The threat of cyber security has become real, evolving to actual crimes and cyber wars. Many problems in cyber security are becoming complicated and global.

## **New Evaluation Tool for understanding International activities for Cyber security**

Agile yet sustainable solutions are needed, along with an effective and a pragmatic evaluation framework to assess and demonstrate the value and efficacy of international development collaboration. Currently, no mature frameworks are available for evaluating non-conventional, new, and complex international activities for combatting cyber security threat. This newly extended framework includes three additional critical aspects, which are neglected in conventional cost-benefit frameworks, to simple cost and benefit categories: 1) synergic effect (such as public-private partnership), 2) indirect impact, and 3) shared value.

## **International Development Program of Public-Private partnerships**

Guided by literature on strategic philanthropy and international development, we found that 1) private companies can benefit from participating in government-led international development programs and that 2) international development activities are effective solutions to improving global and local cyber security.

## **Current International Climate of Cyber Security**

**The threat of cyber security is not virtual.** On September 6, 2007, a construction site in Syria where North Koreans were working disappeared in a less than minute. Several F-15 Eagles and F-16 Falcons sent from Turkey crossed the border between Turkey and Syria and dropped bombs on the site. However, no one noticed what was going on until they saw blinding flashes. This is the reality of cyber war. Syria's multibillion-dollar air defense systems had been paralyzed by Turkey's hired hackers and reported that the skies over Syria seemed safe and largely empty, when the Eagles and Falcons penetrated Syrian airspace (Clarke & Knake, 2010).

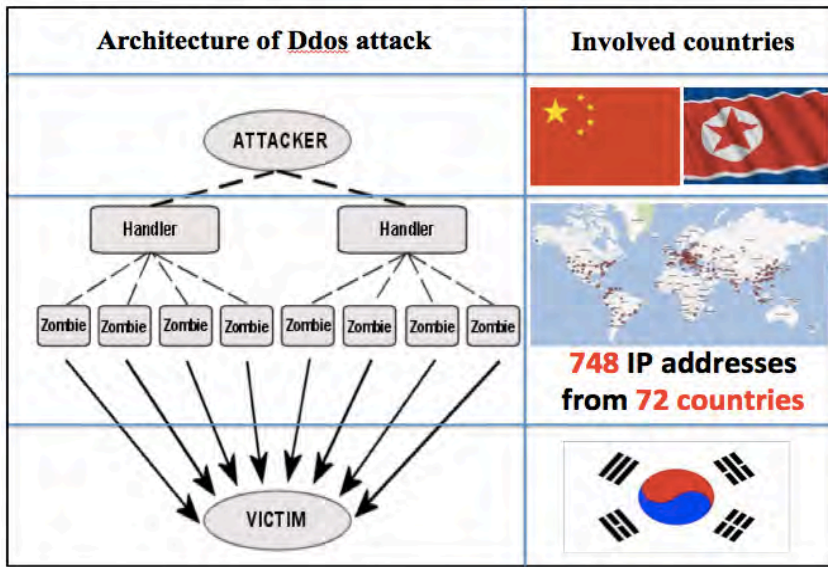


Figure 1. The Architecture of DDos attack and a trend of the Globalization of Cyber Security Problems

Many problems in cyber security are becoming complicated and global. In July 2009, one-third of South Korea’s websites were knocked out over a period of a week by distributed cyber attacks. This attack was sophisticatedly designed with a series of hierarchy. This single crisis involved computers over 75 countries and is one of the most common types of cyber attacks, DDos (Distributed Denial of Service).

**International activities for improving cyber security have been underinvested.**

This is because the benefits of the activities are mostly spillover effects and easily overlooked. Public sectors are still searching for strong justifications to take actions and need more financial and human resources. Private sectors lack incentives to participate in public good projects because (Porter & Kramer, 2002).

**Challenge #1: Not-Enough Resources for International activities**

From the interviews with several countries’ national cyber security agencies, the most common answer to the question, “what is the most difficult challenges to expand international activities?” was “lack of resources (human and financial resources).” Currently, 48 countries are operating national Computer Response Emergency Team (CERT), which are government agencies to control national cyber security problems and the most active actors in International climate of Cyber security (Ferwerda, Choucri, & Madnick, 2010), and only few CERTs can afford to investing in international activities. However, cyber security issues, as infrastructure, cause significant spillover effects over communities and across countries. International cooperation to address problems together is necessary.

**Solution #1: Partnership with Private sectors**

To cover the lack of resources of government agencies, securing the support from private companies can be of great help. Not only do public sectors solve the lack of resource issues, but also private companies can benefit from participating in government-led international activities in cyber security.

Korean IT companies supported Korean CERT led

training sessions. Those sessions are designed to give lectures and consulting about how to establish and

control national cyber security system to developing government officers. The participating companies could gain opportunities to introduce their solutions to government officers; some of which eventually participated in the public procurement projects of the countries and entered the market of emerging countries such as Malaysia.

	<b>Synergic benefits</b>
<b>Public</b>	<b>Leveraging</b> resources <b>Increasing</b> the sustainable momentum of programs
<b>Private</b>	<b>Network opportunities with</b> government officials of targeting countries <b>Creating</b> a community-wide coalition

Figure 2. Synergic benefits of Public-Private partnership

**Challenge #2: Ineffectiveness of current Programs**

**How can we drive the voluntary participations of private sectors in international development programs for cyber security?** If the solution is not strategically beneficial to participating actors, no private entities want to be involved. In addition, if the solution is not sustainable, all the time and effort invested in the solution will end up as “hit and run” or ad-hoc events, which may solve short-term issues but not touch the core of the problems.

**Solution #2: Strategic Design of International Development Program**

A new perspective on societal issues for private companies was suggested by Michael Porter (Porter & Kramer, 2002). Porter suggested that it is possible for a corporation to design social responsibility activities to support its core business and increase long-term sustainability. He also emphasized that companies should see philanthropic activities not as sunk costs but as business opportunities or new business solutions to solve longstanding problems. From the Porter’s idea and framework, a strategic design methodology for international development program can be suggested (Figure 3).

- First, public and private actors can understand both interests and identify their convergence areas.
- Second, they thoroughly research their context to understand internal and external contexts

through and value chain analysis and competitive advantage analysis.

- Third, listed emerging social issues from the first step can be categorized and prioritized based on the result from second step analysis.
- Fourth, social issues, whose required solutions are aligned with the core competences of public and private actors, can best perform needs can be selected out.

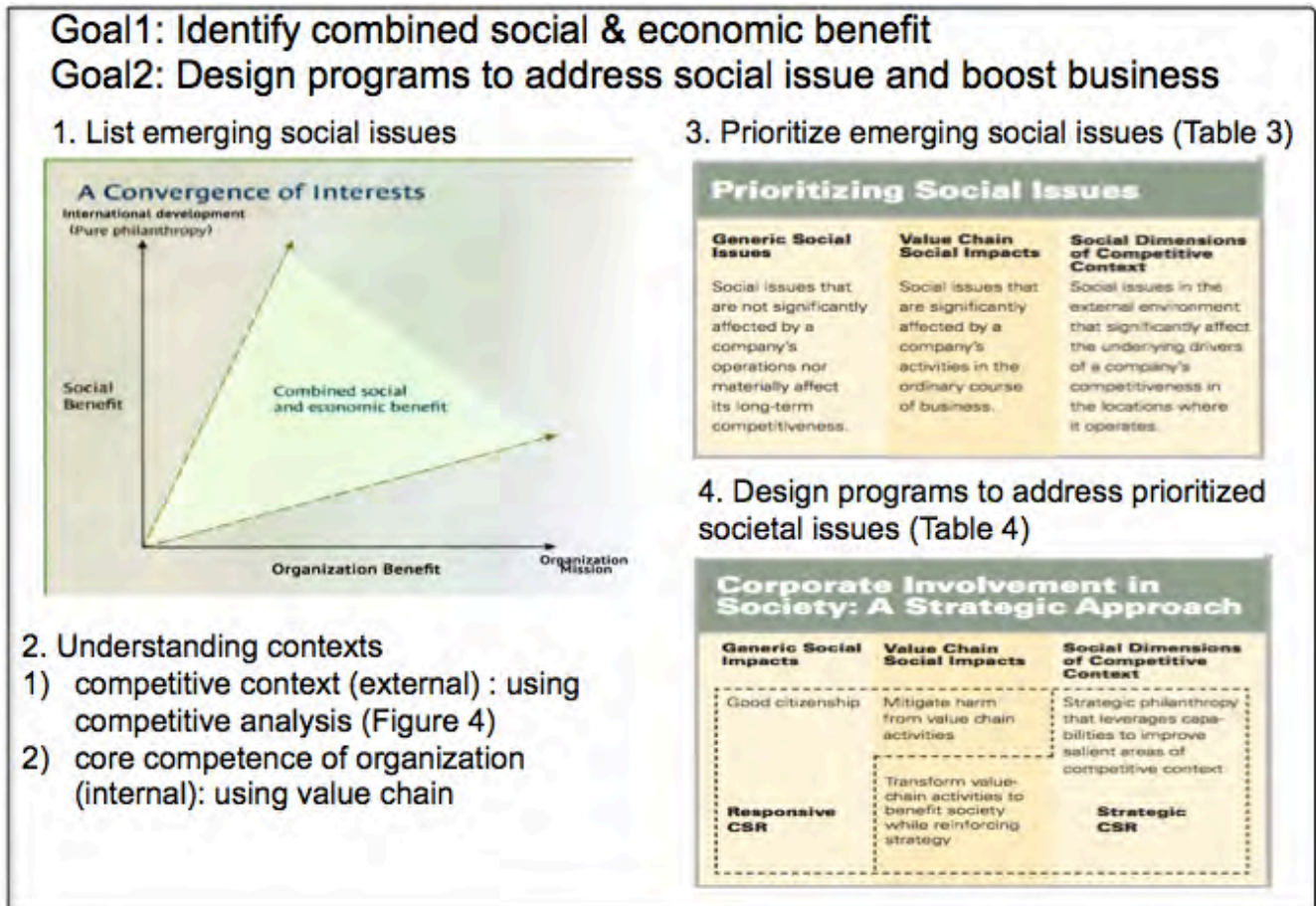


Figure 3. Corporate Strategic approach for international development programs

Sources: Adopted from (Porter & Kramer, 2002)

**Challenge 3: Underestimated Benefits and Insufficient Justification discourage investments in International programs and Cyber Security**

Both international philanthropic activities and Cyber security area have intrinsic limitations on engaging other actors because their benefits are largely distributed and the costs concentrated. Those underestimated benefits and cost burdens discourage the participation of private companies and weaken the justification of public sectors for launching international initiatives in the Cybersecurity area. **How can we assess the true benefits of cyber security considering spillover effects?** The diagram in Figure 4 shows the benefits generated from the public projects operated by public-private partnership.



The arrows marked number 3,4 and 5 are spillover effects and have been overlooked in the traditional assessment framework.

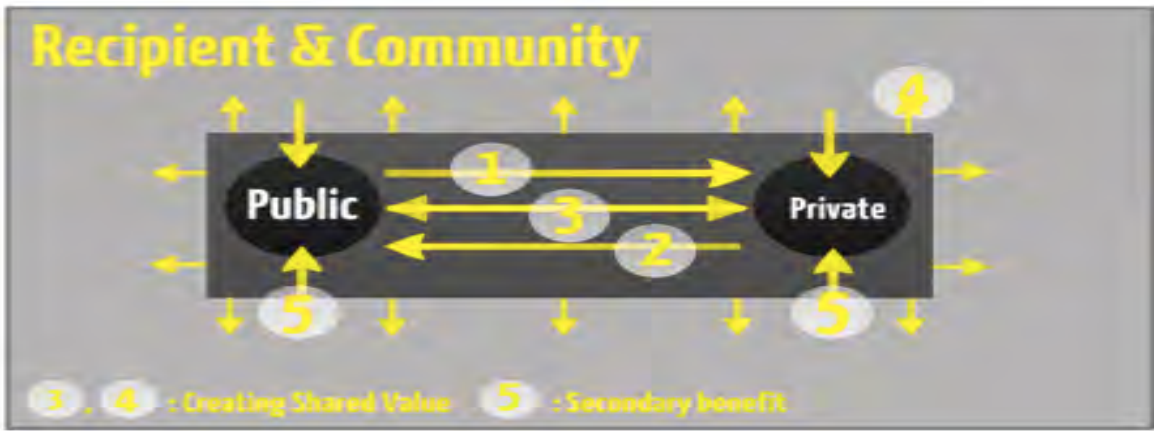


Figure 4. Spillover of benefits created from Cyber security activities of a Public-Private Partnership

**Solution 3: New Evaluation tool to assess true benefits of the effort for International activities in Cyber security**

As Figure 5 suggests, the newly extended framework includes three additional critical aspects, which are neglected in the conventional cost-benefit framework: 1) synergic effect (attained by public-private partnerships), 2) indirect impact (gained through long-term operations), and 3) shared value (benefits influencing participating actors, communities and countries). Its detailed elements collected from rigorous literature reviews are presented in Figure 6.

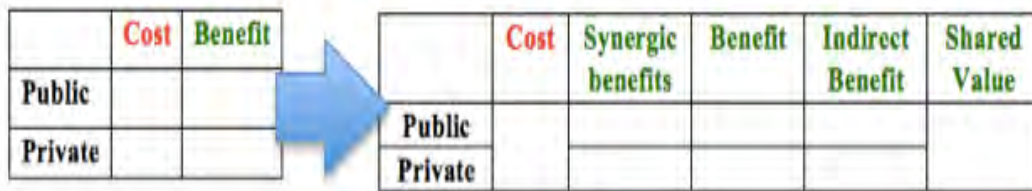


Figure 5. Extension of Cost-Benefit Analysis Framework for understanding true benefits of cyber security activities including benefits which have been overlooked by traditional analysis

	<b>Synergic benefits</b>	<b>Benefit</b>	<b>Indirect Benefit</b>	<b>Shared value</b>
<b>Public</b>	<b>Leveraging</b> resources <b>Increasing</b> the momentum of program	<b>Meeting</b> the political mandate for international development finance <b>Achieving</b> the large scale accomplishments	<b>Strengthen</b> political linkages <b>Targeting</b> trading partners <b>Raising</b> the international reputation among countries <b>Increasing</b> annual budget	<b>Knowledge</b> sharing -> improvement of employee skills and overall productivity <b>Improving</b> supplier quality, the overall quality of life of community people

<b>Private</b>	<b><u>Network opportunities</u></b> with government officials of targeting countries <b><u>Creating</u></b> a community-wide coalition	<b><u>Entering</u></b> 3rd/emerging country market under official/unofficial protection	<b><u>Marketing</u></b> effect; <b><u>License</u></b> to operate <b><u>Sustainability</u></b> based on infrastructures and customer base <b><u>Meeting</u></b> moral obligation	<b><u>Providing</u></b> job opportunity to community <b><u>Providing</u></b> infrastructure and appropriate training <b><u>Improving</u></b> International Cyber security
----------------	---	---	--	---

Figure 6. Extended benefit elements

## Policy Recommendations

This study proposes two recommendations that are of interest for developed countries with well-funded CERTs and competitive IT industries:

The first recommendation is that when designing international development programs to address global issues, Porter's strategic philanthropy framework makes it possible to identify combined benefits, which can occur from the project and persuade and involve private companies.

The second recommendation is that when the effectiveness of the projects is assessed, extended cost-benefit analysis framework can prevent spillover benefits from being overlooked and include collective benefits from partnership.

From the international development programs of public-private partnership, there are numerous benefits. Public agents can benefit from the participation of private agents by acquiring financial and human resources from the private sector. In addition, the programs can be more sustainable. Private companies have more incentive to keep running the initiatives, once those activities are connected to their business. Private agents can enter into emerging markets under governmental supports, which can help the companies easily navigate around complicated regulations pertaining to business activities in the developing countries. In partnership with local organizations, government, and citizens, the private companies in the partnership can greatly benefit from the creation of a community-wide coalition focused on enhancing the local economy and the environment (Porter & Kramer, 2002).

The extended cost-benefit framework can help us understand and encourage participating in the new global challenges likely to face nations in the 21st century. Addressing this growing agenda of common concerns will require fresh thinking, further research efforts and new political instruments. But it is evident that more research and cases are needed to refine the idea presented in this paper. I hope that this study can be a start.



# Chapter 1. Introduction

## 1.1. First Motivation: International cooperation for cybersecurity

Many problems in cyber security are becoming complicated and global. In July 2009, one-third of South Korea’s websites were knocked out over a period of a week by distributed cyber attacks. This attack was sophisticatedly designed with a series of hierarchy--a 'host computer' which sent attack commands to infected computers, 748 intermediate 'handlers' over 72 countries, which are infected by the host and distributed the infection, and 'agents' which are a large number of zombie PCs. Along with this chain of command, a hacker could control 130,000 zombie PCs and ordered them to attack target servers in Korea. This single crisis involved computers over 75 countries and is one of the most common types of cyber attacks, DDos (Distributed Denial of Service) <sup>1</sup>. The story shows that cyber crimes are becoming complicated and globalized. **We are connected and cyber security problems are border-less.** To address those types of the emerging cyber problems, we need internationally cooperative solutions.

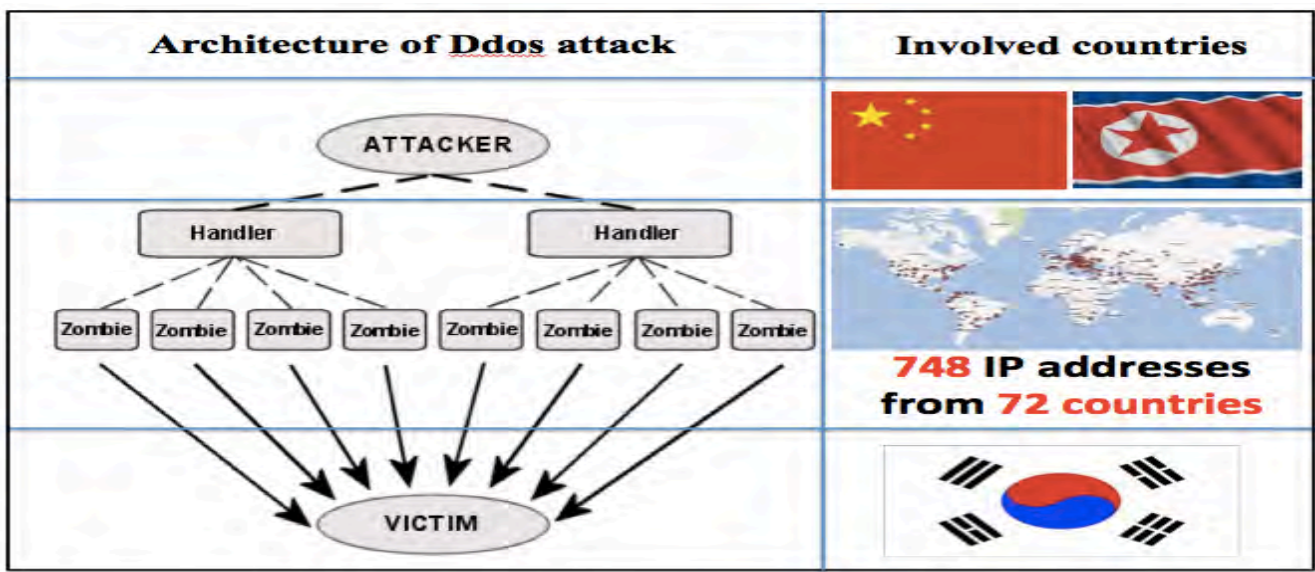


Figure 7. *The Architecture of DDos attack and a trend of the Globalization of Cyber Security Problems* (Source: self-created, The detail of this crisis is described in Appendix 1)

<sup>1</sup> distributed denial-of-service attack (DDos Attack) is an attempt to make a computer or network resource unavailable to its

## 1.2. Second Motivation: Justification for cyber security investment

To reduce the damage of cyber security crimes and incidents, simply monitoring traffic in a country is not helpful. Cyber security issues are not only public goods but also ‘*global public goods*’<sup>2</sup>, whose externalities span the world. Its impacts bring enormous spillover externalities but are widely distributed over the countries. With concentrated cost and diffuse benefit, no entity will volunteer to solve this problem. Given their limited resources, most organizations should optimize their operations by choosing the most effective solutions. Decisions, either for policy or business, need to be the ‘right decisions.’

**How can we evaluate decisions?** The most traditional method is cost-benefit analysis, used in conventional business as well as international development programs, notably by World Bank. In addition, cost-benefit analysis has evolved to deal with ever-changing issues such as environmental problems; the cost-benefit analysis tries to include and internalize new context and value systems. Cybersecurity problems share many common characters with environmental problems. **As cost-benefit analysis has been adapted to the environmental domain, this paper suggests an extended cost-benefit analysis framework for cybersecurity.**

There has been insufficient investment in cybersecurity. With the traditional cost-benefit analysis, the benefits of international activities in cybersecurity have been overlooked because they bring not only benefits as public goods but also as global public goods.

This paper reveals overlooked benefits and shared value for public agents and private companies to attain through international involvement in cybersecurity. With the extended cost-benefit framework, we can verify the effectiveness of cybersecurity investment and encourage more organizations to participate in cybersecurity. More players and more activities will strengthen IT infrastructure and improve cyber security, thereby creating greater shared values all over the world.

## 1.3. Third Motivation: Incentives for Private Sectors

According to Kaul (1999), individual actors often consider as the best and most rational strategy to let others provide the good—and then to enjoy it, free of charge. In addition, “government and civil society have often exacerbated the problem by attempting to address social weaknesses at the expense of business” and “the presumed trade-offs between economic efficiency and social progress have been

---

<sup>2</sup> “...with globalization, the externalities—the “extra” costs and benefits—are increasingly borne by people in other countries. Indeed, issues that have traditionally been merely national are now global because they are beyond the grasp of any single nation” (Kaul, Grungberg, & Stern, 1999)

institutionalized in decades of policy choices” (Porter & Kramer, 2011). Therefore, the private sector lacked incentives to participate in public good projects, and the approaches that governments have used are not effective because they have required the sacrifice of companies.

**How can we suggest solutions to encourage the voluntary participations of private sector for cybersecurity problems?** If the solution is not strategically beneficial to the implementing agents, no private entities want to be involved. In addition, if the solution is not sustainable, all the time and effort invested in the solution will end up as “hit and run” or ad-hoc events, which may solve short-term issues but not touch the core of the problems.

A new perspective on societal issues for private companies was suggested by Michael Porter (Porter & Kramer, 2002). Porter suggested that it is possible for a corporation to design social responsibility activities to support its core business and increase long-term sustainability. He also emphasized that companies should see philanthropic activities not as sunk costs but as business opportunities or new business solutions to solve longstanding problems. In this paper, Porter’s idea will be applied to international cooperation for cybersecurity.

#### **1.4. Propositions**

This paper assumes that Computer Emergency Response Teams (CERT)s can play key roles in international cooperation in cybersecurity. National Computer Emergency Response Teams are generally government agencies formed to combat cyber security threats. It proposes that international development programs are an effective solution to international cybersecurity problems and that public-private partnerships increase the likelihood of implementing development programs.

To verify the effectiveness of proposed solutions, the paper introduces an extended cost-benefit analysis framework. The main idea of framework is adapted from Porter’s strategic philanthropy research, and the benefits in the framework are collected through extensive literature reviews.

The extended cost-benefit framework will be applied to an international development program run by Korean CERT (Computer Emergency Response Team) to see which of theoretically proposed benefits actually emerge. Data and information from ten interviews and site visit support the framework application and its analysis.

## **1.5. The structure of paper**

Chapter 2 reviews the literatures in four areas: 1) cyber security, 2) foreign aid / foreign direct investment, 3) strategic philanthropy and 4) cost-benefit analysis. Chapter 3 introduces research methodologies used in this paper to explain how data and cases were collected. Chapter 4 presents the case of Korean Cyber Emergency Response Team (CERT) collaborating with Malaysian CERT and the success of Korean IT companies. This case is greatly interesting in that this paper sees this international development program as one of the most effective solutions to cybersecurity problems.

Chapter 5 focuses on extended cost-benefit analysis framework. In Chapter 6, the framework will be applied to the Korean CERT case to identify benefits and assess the effectiveness of cyber security training program of Korean CERT targeting developing Asian countries. Chapter 7 summarizes the findings and draws conclusions.

## Chapter 2. Background

What matters most in deriving the most meaningful result from cost-benefit analysis is determining cost and benefit elements. The sustainability friendly analysis includes sustainability related elements in the calculation. In addition, it might define the scope of impact created by an issue wider than traditional analysis by including broader range of beneficiaries, who benefits from the analyzed program and long-term benefits. Secondly, depending on which areas we apply the analysis, the structure and elements of analysis become different. Environment area and cybersecurity area should consider different costs and benefits.

Cybersecurity issues cause significant spillover impacts spreading over communities, which sometimes are borderless. This is because cyber security is the infrastructure on which most modern businesses rely. In addition, cyber space or networks are based on people's interactions; this interactive character of the Internet accelerates the spread. Traditional cost benefit analysis (CBA) frameworks have missed the spillover impacts, thereby leading to underestimated calculation. Understanding the intrinsic characters of cyber space and long-term effects, a new cost benefit analysis (CBA) model should be considered to precisely evaluate cybersecurity programs.

The extended cost-benefit analysis (CBA) model can also be important for business decision makers. The public demand for corporation social responsibility has become higher than ever. Porter changed the entrenched perspective on corporation's social responsibility, where people think that to create social benefit, a business should sacrifice profits. He recommended that corporations strategically design their social programs to boost their business bottom line. To measure this strategic philanthropy of corporations, the extended CBA can be applied.

Lastly, this study sees emerging countries as the best context in which to apply our extended CBA. Investing in cybersecurity issues in emerging countries can create more impact than investment in developed countries because of non-existent or insufficient IT infrastructure, the high speed of penetration of its service and first-mover effect.

### 2.1. Cybersecurity

#### 2.1.1. Emerging Threat from Cybersecurity

**Cyberwar:** On September 6, 2007, a construction site in Syria where North Koreans were working disappeared in a less than minute. Several F-15 Eagles and F-16 Falcons sent from Turkey crossed the



border between Turkey and Syria and dropped bombs on the site. However, no one noticed what was going on until they saw blinding flashes. This is the reality of cyber war. Syria’s multibillion-dollar air defense systems had been paralyzed by Turkey’s hired hackers and reported that the skies over Syria seemed safe and largely empty, when the Eagles and Falcons penetrated Syrian airspace (Clarke & Knake, 2010),

Clarke derived five lessons from the incident:

- 1) Cyber war is real.
- 2) Cyber war happens at the speed of light.
- 3) Cyber war is global.
- 4) Cyber war skips the battlefield.
- 5) Cyber war has begun.

In other words, the impact of cyber security is real, global, explosive and changing the entrenched system. Particularly, this characteristic of cyber war adds a new dimension of threat to the instability of national security (Clarke & Knake, 2010).

**Cybercrime & Cyber incidents:** Cybercrime and incidents are another important emerging threats facing governments and corporations. Those cyber crimes are usually governed at the national level by law enforcement agencies such as police, and cyber incidents are monitored by Computer Emergency Response Team (CERT). The actual instance of cyber crimes that CERT monitors and collects their data are listed below:

In US CERT, there are six categories of computer incidents (Madnick, Xitong, & Choucri, 2009):

Category	Description
CAT 1 <i>Unauthorized Access</i>	An individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource
CAT2 <i>Denial of Service (DoS)</i>	An explicit attempt by attackers to prevent legitimate users of a service from using that service
CAT 3 <i>Malicious Code</i>	Successful installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application)
CAT 4 <i>Improper Usage</i>	Violation of acceptable usage policies as established by the organization
CAT 5 <i>Scans, Probes, or Attempted Access</i>	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, services, or any combination for later exploit. This activity does not directly result in a compromise or denial of service

CAT 6 Investigation	Unconfirmed incidents of potential malicious or anomalous activity deemed by the reporting entity to warrant further review
---------------------	---

Table 1. Six Categories of Cyber incidents of US CERT

Source: (Madnick, Xitong, et al., 2009)

The Korean CERT also monitors and collects data on seven categories: 1) malicious code, 2) hacking, 3) spam relay, 4) Phishing, 5) attempted access, 6) defacement and 7) bot (“Korea Internet Incident and Phishing Report,” 2012). To prevent and respond to those incidents, CERT and cyber security related business have invested in developing technologies.

### 2.1.2. Key Initiatives to Combat Cyber Security Threats: National Level CERTs

Bauer and Van Eeten summarized the policy instruments that a governmental entity can use to enhance information security with the four categorizations: legal and regulatory measures, economic measures, technical measures and informational and behavioral measures. These practices are listed in the Table 2:

**Table 2**  
Principal policy instruments to enhance information security

Predominant policy vector	Cybercrime	Information security
Legal and regulatory measures	<ul style="list-style-type: none"> <li>● National legislation</li> <li>● Bi- and multi-lateral treaties</li> <li>● Forms and severity of punishment</li> <li>● Law enforcement</li> </ul>	<ul style="list-style-type: none"> <li>● National legislation/regulation of information security</li> <li>● Legislation/regulation of best practices to enhance information security</li> <li>● Liability in case of failure to meet required standards</li> <li>● Tax credits and subsidies</li> </ul>
Economic measures	<ul style="list-style-type: none"> <li>● Measures that increase the direct costs of committing fraud and crime</li> <li>● Measures that increase the opportunity costs of committing fraud and crime</li> <li>● Measures that reduce the benefits of crime</li> </ul>	<ul style="list-style-type: none"> <li>● Level of financial penalties for violations of legal/regulatory provisions (compensatory, punitive)</li> <li>● Payments for access to valuable information</li> <li>● Markets for vulnerabilities</li> <li>● Insurance markets</li> </ul>
Technical measures	<ul style="list-style-type: none"> <li>● Redesign of physical and logical internet infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>● Information security standards</li> <li>● Mandated security testing</li> <li>● Peer-based information security</li> </ul>
Informational and behavioral measures	<ul style="list-style-type: none"> <li>● National and international information sharing on cybercrime</li> </ul>	<ul style="list-style-type: none"> <li>● National and international information sharing on information security</li> <li>● Educational measures</li> </ul>

Table 2. Principle Policy Instruments to enhance information security

Source: (Bauer & van Eeten, 2009)

Those suggested practices are implemented by law enforcement agencies and CERT Coordination Center CERT/CC)<sup>3</sup> combined with cooperation from the private sector. Law enforcement agencies govern cyber crimes, which are “attacks on private entities with the intent of gaining profit or inflicting damage” (Ferwerda, Choucri, & Madnick, 2010). CERT/CC focuses on cyber threats, which are “the exploitation of infrastructural weaknesses and security vulnerabilities” (Ferwerda et al., 2010). While national governments have the authority and the jurisdictional power to prosecute criminals, cyber threats can be mitigated by organizations with the technical capability to improve the security, not only by CERT/CC (Ferwerda et al., 2010).

This paper focuses on the activities of CERTs, according to papers analyzing data of Cyber Emergence Response Team (Madnick, Choucri, et al., 2009; Madnick, Xitong, et al., 2009), the activities of CERT are defined as:

- 1) organizing responses to security emergencies,
- 2) promoting the use of valid security technology, and ensure network continuity
- 3) identifying vulnerabilities and fostering communication between security vendors, users, and private organizations, and

Through those core activities CERT, in general, produces three products:

- 1) a reduction in unaddressed security vulnerabilities,
- 2) improved understanding of the nature and frequency of cyber threats
- 3) improved methods of communicating and reporting these threats to other security teams and the general public.

### **2.1.3. International Cooperation among CERTs**

CERTs are generally government organizations (one national CERT per country), and CERT/CC and some of established CERTs have provided other countries, which plan to establish CERTs, with technical supports and educations. For those reasons, CERTs have similar organization structures and monitoring and response systems, so they can interact and form parallel coordination networks, such as the Forum of Incident Response and Security Teams (FIRST) (Ferwerda et al., 2010). FIRST was to enhance information sharing among disparate security groups (« FIRST.org /

---

<sup>3</sup> CERT/CC is the ordination hub for all global CERTs and is responsible for setting standards, best practices, and policies (Madnick, Xitong, & Choucri, 2009)

FIRST Members », 2011). It is composed of more than 200 organizations, and is notable for its influential annual conferences and its extensive integration of national, academic, and private CERT teams (« FIRST.org / History », 2011).

#### **2.1.4. Difficulties of the Institutionalization for International Cooperation on Cybersecurity**

With about 30% of the world's population is now using Internet, business has been globally connected with e-commerce, supply chains and workplaces (Greengard, 2012). In addition to its significant role in business, because of its borderless impact, cyber security is global public goods requiring international cooperative frameworks and formalized actions. Relentlessly evolving cyber technologies is changing the way countries approach matters as diverse as international crime and content ownership, and altering business and especially government's legal system (Greengard, 2012).

However, in cyberspace, "the ability to build a legal framework across nations is an increasingly difficult task," states Michael Geist, research chair in Internet and e-commerce law at the University of Ottawa (Greengard, 2012). Particularly in cyber security, Choucri (2009) specified that this domain has not been maintained by formal governmental framework. Companies have assumed the main responsibility of threat detection and mitigation. However, she critiqued "Individual corporations lacked incentives to share information, and more importantly, lacked the legal authority to deal with emerging national threats or to prosecute criminal networks" (Ferwerda et al., 2010).

One of the biggest challenges in the international law in fast-changing digital environment is inconsistency among countries; "What's illegal in one country may not be illegal in another," says Pauline C.Reich, director of the Asia-Pacific Cyberlaw, Cybercrime and Internet Security Institute and co-author of Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization (Greengard, 2012).

The other issue is the lack of international adjustment mechanisms in cyber jurisdiction. "It's up to individual countries to decide whether they want to comply with another country's laws," states Jonathan Bick, an adjunct professor of Internet law at Rutgers University Law School (Greengard, 2012). He also points out that not only among countries, even among companies and between companies and governments, they all use their own courts, which they control (Greengard, 2012).

Despite inconsistency among international laws, to build a global institution to govern cybersecurity, internationally collective efforts and attention are needed. One of these efforts take the

form of legislative enactments to support and justify global institution building. Figure 8 below presents currently valid laws to support institutional institution building.



Figure 8. Related laws to international institution building  
 (Source: excerpts from a presentation material provided by Korean CERT)

## 2.2. Foreign Aid/Foreign direct investment

Most of the literatures about Foreign direct investment examines the factors and motives that determine what type of foreign aids are preferred in giving countries and how effective foreign aids are in receiving countries.

### 2.2.1. Motive of Foreign Aid/Foreign Direct Investment: Donor's Perspective

The motives of foreign aid have been long disputed in the development finance literature. The motives are analyzed in terms of egoistic behaviours and altruistic behaviours (Berthélemy, 2006). According to Berthelemy's rigorous study (2006), most donors participate in foreign aid out of self-interest.

- 1) Strengthen political linkages: those who have particular political linkages with recipient countries aim at reinforcing such ties
- 2) Targeting trading partners: all donors choose target countries which are the most significant trading partners

Dollar and Alesina summarized consensus of what matters for aid giving: poverty of the recipients, strategic interests, colonial history, trade, political institutions of the recipients (Alesina & Dollar, 2000; Lumsdaine, 1993). One of the oldest theories to explain determinants of foreign direct investment (FDI), capital market theory pointed at interest rates as a principal determinant of FDI. Dynamic macroeconomic theory sees FDI as a long-term action of transnational corporations, and gravity approach emphasized that two countries are closer in various senses such as geographically, economically and culturally their FDI flows were higher. Institutional analysis focused on the impact of institutional framework on FDI flows and foreign aid determination.

To determine both FDI and foreign aid, some countries, especially Scandinavian countries, consider 1) political stability reflected in better governance indicators such as democracy, absence of violent conflicts<sup>4</sup> and 2) economic growth (Berthélemy, 2006).

### 2.2.2. Evaluation of Effectiveness: Recipient's Perspective

The definition of the *effect* or *impact* depends on the evaluating agencies. In development cooperation, the OECD/DAC definition has emphasized duration in defining *impacts*: ‘long term effects produced by a development intervention.’ This is not accepted by all agencies; thus, EU defines *impact* as: ‘A general term used to describe the effects of an intervention on society ...’

“Realistically, how to achieve a beneficial aggregate impact of foreign aid remains a puzzle and less importantly regarded.” This difficulty can be attributed to four issues:

- 1) “types of returning impacts are too diverse and broad; some are unrecognizable and evaluators focus only on beneficiaries missing out others
- 2) The balance of evaluative effort can be skewed towards processes unconnected to outcomes

---

<sup>4</sup> Although the levels of attention are different between private flows (FDI) and official aid; private flows seem to pay some attention to corruption, at least more than official aid.



- 3) identifying causality is difficult; methods adopted make little effort to disentangle what works from what is spurious
- 4) The period that programs run is usually too long to accurately measure and initial success is emphasized than longer impact.”

Those inherent challenges of assessing foreign aid have been reflected in the actual implications.<sup>5</sup>

- “1) Aid agencies usually give low priority to evaluating projects after completion  
 2) World Bank reviews only 5% of its loans after three to ten years following last disbursement  
 3) Often: self-evaluation by staff in charge of original projects  
 4) More evaluations by outside scholars should be encouraged”

### 2.2.3. Problems associated Designing Foreign Aid Program

There are four potential problems in how foreign aid program is designed and affects receiving countries.

- “1. Fragmentation (Aid budgets are divided into many tiny, ineffective pieces.)  
 2. Poor selectivity (Aid is given to corrupt and/or relatively wealthy regimes.)  
 3. High overhead (administrative and payroll costs)  
 4. Ineffective aid channels (such as food aid, which harms recipient economies and local farmers, and tied aid, which comes with strings attached that harm the recipient country).”

Lancaster (1999) identified two approaches to analyzing the impact of aid on development:

- (1) Contextual: it suggests that aid impact is primarily a function of the broader economic and political context in which it is provided.
- (2) Instrumental: it evaluates impacts in terms of the success or failure of the programmes and projects it finances.

An approach, which attracts the most credence and popularity is Randomized Control Trials (RCTs) (Prowse, 2009).<sup>6</sup> Abhijit Banerjee and colleagues at the Abdul Latif Jameel Poverty Lab at

<sup>5</sup> Degenbol-Martiniessen et al (2002) argue that it makes little meaning to evaluate aid effects only in relation to the goals set by the donor-financed projects and programmes

<sup>6</sup> A Randomised Control Trial in social science is an evaluation of a public policy intervention. Research is structured to answer a counterfactual question: how would participants’ welfare have altered if the intervention had not taken place?

MIT argue that aid should be subject to the RCT, which focuses less on process and more on outcomes. While this method helps decision makers identify which interventions are most successful and which are failures, it still faces challenges that it cannot tell us precisely why or how success or failure has occurred.

#### **2.2.4. Public-Private partnership for International Development**

Modern public-private partnerships (PPPs), often called joint planning, joint contributions, and shared risk are viewed by many development experts as opportunities. Through involving private actors in development programs, the programs can leverage resources, mobilize industry expertise and networks, and bring fresh ideas to development projects. In addition, international development institutes such as UNICEF and World Bank have taken partnership approaches (Calabrese, 2008). They believe that partnering with the private sector can increase the momentum of program; this is because private actors keep running their business and activities even after government aid has ended. From the private sector perspective, partnering with a government agency can bring development expertise and resources, access to government officials, credibility, and scale (Marian Leonardo Lawson, 2011).

### **2.3.Strategic Philanthropy: designing aids in strategic way**

Along with the Internet linking different countries, business has become global, and no business is unrelated to cyber space. Building this space, establishing rules and making them safe and reliable are all essential to the sustainability of today's business and national security.

However, in the private sector, people have not considered that providing the public goods will pay off individual corporations' effort because of indirect business impact and free-rider problem of other competitors in the cluster. At worst, "government and civil society have often exacerbated the

---

This can involve 'before and after' and 'with and without' comparisons. The former are not dissimilar to more conventional evaluation tools that use baseline data, and may suffer from difficulties in isolating the effects of an intervention from wider societal changes. The latter create a robust comparison group who are not directly exposed to the intervention, and whose outcomes would have been similar to participants if the intervention had not taken place. Such 'with and without' comparisons allow researchers to estimate the average effect of the intervention across the participant group. The main difficulty is in minimising selection bias for the two groups – hence the importance of randomisation. Prowse, M. (2009). Aid effectiveness: the role of qualitative research in impact evaluation.



problem by attempting to address social weaknesses at the expense of business” and “the presumed trade-offs between economic efficiency and social progress have been institutionalized in decades of policy choices” (Porter & Kramer, 2011). Therefore, the private sector lacked incentives to participate in public good projects, and the approaches that governments have used have not required the sacrifice of companies and creating entrenched perception on the trade-offs.

How can we find a solution that delivers both social and economic benefits to community and companies? Porter suggested that companies should pursue strategic corporation philanthropy, named later “shared value” in his paper, “Creating shared value.” (Porter & Kramer, 2002) First, for the private sector, Porter suggested that it is possible for a corporation to proactively design social responsibility activities in order to support its core business and increase the sustainability in the long term, if companies see philanthropic activities not as passive sunk cost but as business opportunity or new business solution to solve.

### **2.3.1. Brief ideas from Alcoa Foundation case**

“It’s no longer enough to write checks to a handful of good causes and local community organizations.” Today, corporate philanthropy departments are aligning their grant making with a strategic business objective, so that their social responsibility activities actually support their bottom-line benefits.

*Harvard Business Review* (December, 2011) introduced the Alcoa Foundation case as an example of strategic corporate philanthropy. Alcoa and the Alcoa Foundation have invested millions of dollars to encourage recycling programs across the United States. The programs run from this investment covered donating recycling bins, developing consumer education programs, and supporting community-recycling efforts. They are not just good for the environment but good for Alcoa’s business as well. (p.139)

The report explains that the first thing to do for strategic philanthropy is to identify a single or few number of key social causes that are closely aligned with a business objective. The company should identify related business concern, unique resources and expertise. For this, Alcoa conducted interviews with corporate executives and regional leaders to understand the business’s top priorities and focus groups with shop-floor employees to understand their social concerns.

### 2.3.2. Porter's idea : Strategic Philanthropy and Creating Shared Value

A long perception on corporate social responsibility is that businesses can maximize their benefits only at the expense of social benefits. In contrast, Porter emphasizes the potential of creating shared value.

To do this, organizations should identify the points of intersection. Organizations affect society by trying to achieve their core missions and long-term visions. Porter notes that this normal course of business and operations harbors “inside-out linkages” (Porter & Kramer, 2006). For example, organizations’ hiring practices, emissions, and health care benefits system have impacted their located communities. Also, organizations including companies are influenced by external social conditions; these are “outside-in linkages” (Porter & Kramer, 2006).

No organization can address all issues in those intersections, but they must select the areas where they can perform best practices and its benefits can most closely be aligned with their core goals. To identify most influential areas in creating shared value, Porter suggested a structured method of listing social issues consisting of 1) Generic social issues, 2) Value chains social impacts and 3) Social dimensions of competitive context. Their definitions are listed in Table 3.

<b>Prioritizing Social Issues</b>		
<b>Generic Social Issues</b>	<b>Value Chain Social Impacts</b>	<b>Social Dimensions of Competitive Context</b>
Social issues that are not significantly affected by a company’s operations nor materially affect its long-term competitiveness.	Social issues that are significantly affected by a company’s activities in the ordinary course of business.	Social issues in the external environment that significantly affect the underlying drivers of a company’s competitiveness in the locations where it operates.
e.g., for a financial service firm like Bank of America, carbon emission is generic social issue.  AIDS pandemic in Africa for Toyota and Home Depot	e.g., Carbon emission for Toyota  AIDS pandemic for a pharmaceutical company like GlaxoSmithKline	e.g., Carbon emission for Toyota  AIDS pandemic for a mining company in Africa like Anglo American, which highly counts on local labor

*Table 3. Porter's Structured Method of Listing Social Issues categorized in terms of 1) Generic social issues, 2) Value chain Social impacts, and 3) social dimensions of competitive context*

*Source: (Porter & Kramer, 2006)*

After brainstorming social issues and their categorization, an organization must select areas of highest priorities. For this, organizations need to think of their competitive advantages, by which they can maximize the effectiveness and efficiency in creating shared value; that is, they can minimize extra cost or investment by using their original competences and achieve better impact than any other organizations who are less competent in the selected domains. In this way, depending on the core competence and strategic positioning in market, companies can take different action. For example, even in the same automotive area, Volvo has focused on safety issue in their operational process, while Toyota has heavily invested on hybrid technology with the focus on environmental issues (Porter & Kramer, 2006).

Organizations can refine the categorization and ranking based on the relevancy of societal issues and their competences, collected through looking inside and outside. Porter re-categorized them as *responsive CSR* and *strategic CSR* Table 4 describes how to do this re-categorization.



Table 4 Corporate Involvement in Society: A Strategic Approach  
 Source: (Porter & Kramer, 2006)

Following these steps, organizations can discover strategic CSR which integrates “inside-out linkage” and “outside-in linkage”; that is, they can design or determine its business practices and directions so that the impact arising from the normal business operations, inside-out linkage, will boost their business bottom line by maximizing the benefits from external conditions, *outside-in linkage*.

In 2011, Porter published a new report (Porter & Kramer, 2011) and described how to design the business practices to achieve the integration. He suggested three ways: 1) reconceiving products and markets, 2) redefining productivity in the value chain, and 3) building supportive industry clusters at the company's locations.

### 2.3.3. Strategic Philanthropy in Government (non-profit organizations)

Porter emphasizes the impact of its application to governmental organizations; “the principles of shared value apply equally to governments and nonprofit organizations.....”, "From society's perspective, it does not matter what types of organizations created the value. What matters is that benefits are delivered by those organizations--or combinations of organizations--that are best positioned to achieve the most impact for the least cost. Finding ways to boost productivity is equally valuable whether in the service of commercial or societal objectives. In short, the principle of value creation should guide the use of resources across all areas of societal concern." and "...Governments and NGOs will be most effective if they think in the value terms--considering benefits relative to costs--and focus on the results achieved rather than the funds and effort expended” (Porter & Kramer, 2011).

### 2.3.4. Strategic Philanthropy and International Development in Cyberspace

Before applying the Porter's model to cyberspace, Table 5 describes the analogy between international cooperation/development activities in cyberspace and Porter's philanthropic activities. This part analyzes the definition of strategic philanthropy and Porter's cases and intrinsic characteristics of international development activities in cyberspace.

<b>Porter's strategic philanthropy</b>	
Philanthropy (corporate social responsibility)	Strategic philanthropy (Creating shared value)
<ul style="list-style-type: none"> <li>• Value: Doing good</li> <li>• discretionary or in response to external pressure</li> <li>• Separate from profit maximization</li> <li>• agenda and priority are determined by external reporting and personal preferences</li> <li>• impact limited by corporate footprint and</li> </ul>	<ul style="list-style-type: none"> <li>• Value: Economic and societal benefits relative to cost</li> <li>• integral to competing</li> <li>• integral to profit maximization</li> <li>• Agenda and priority are determined by companies by themselves</li> <li>• realigns the entire company budget</li> <li>• Application: Alcoa case (Chapter 2.3.1)</li> </ul>

CSR budget • Application: Fair trade purchasing	
<b>International development activities in cyberspace</b>	
Current International development activities in cyberspace	Strategic international cooperation in cyberspace
Discussed in Chapter 6	Discussed in Chapter 6

*Table 5. Definition of Strategic Philanthropy, Cases and Intrinsic Characteristics*

*Source: adopted from (Porter & Kramer, 2006)*

In addition, international development programs will be validated by demonstrating that the impact arising from the normal business operations, inside-out linkage, will boost their business bottom line by maximizing the benefits from external conditions, *outside-in linkage*. Although it is not used in this paper, an additional test, designed to verify that its international development program follow the procedure of 1) reconceiving products and markets, 2) redefining productivity in the value chain, and 3) building supportive industry clusters at the company’s locations, can be greatly helpful to pre-assess the effectiveness of the international development program.

Summarizing the procedure of applying Porter’s idea to preliminary stage of designing international development programs:

- First, public and private actors understand both interests and identify their convergence areas.
- Second, they thoroughly research their context to understand internal and external contexts through and value chain analysis and competitive advantage analysis.
- Third, listed emerging social issues from the first step can be categorized and prioritized based on the result from second step analysis.
- Fourth, social issues, whose required solutions are aligned with the core competences of public and private actors, can best perform needs can be selected out.



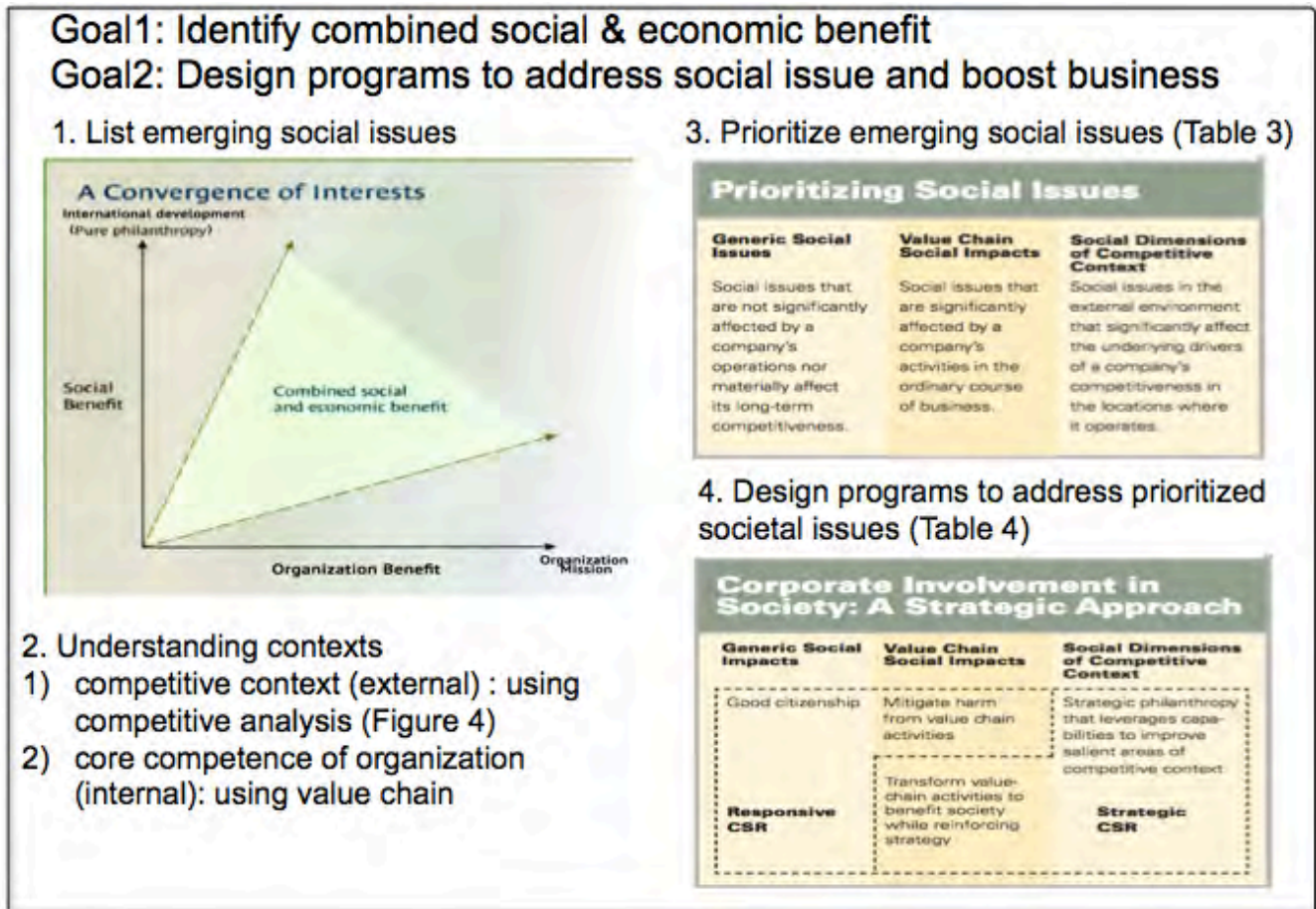


Figure 9. Strategic methodology for designing international development programs (Adopted from Porter & Kramer, 2002)

## 2.4. Cost-benefit analysis (CBA)

### 2.4.1. A brief glance at CBA

“Economic theory has been founded on the notion of a rational individual, that is, a person who makes decisions on the basis of a comparison of benefits and costs. CBA, or strictly social CBA, extends this to the area of government decision-making by replacing private benefits and costs by social benefits and costs” (Brent, 2006).

This “CBA is currently an established technique that is widely used in both governments and international organizations” (Mishan & Quah, 2007). “In addition to being adopted by governments, CBA was also formally adopted by several international organizations – the OECD in 1969, the UN in 1972 and the World Bank in 1975 (Squire, Tak, & Bank, 1976). At the Earth Summit in Rio de Janeiro in 1992, it was agreed that country application of financial support for public sector projects be subjected to passing the cost–benefit test as far as possible” (Mishan & Quah, 2007).

CBA can address the following questions: “whether one or a number of projects or programmes should be undertaken and, if investable funds are limited, which one, two or more among these specific projects that would otherwise qualify for admission should be selected. Another question that CBA sometimes addresses is that of determining the level at which a plant should operate or the combination of outputs it should produce” (Mishan & Quah, 2007).

For a water related public project in 1808, the necessity of evaluating the cost and benefit to implement the project was firstly discussed (Hanley & Spash, 1995). Since then, CBA has been applied to evaluate diverse social issues such as health care (Warner, 1982), airport building (Jorge & de Rus, 2004), environmental standard (Ackerman & Heinzerling, 2001), road safety (Elvik, 2001), energy efficiency regulation making (Clinch & Healy, 2000).

Types of cost benefit analyses	
Type of analysis	When applicable
Formal cost-benefit analysis	Efficiency is the only goal. Both costs and benefits are <i>monetized</i> .
Qualitative cost-benefit analysis	One or more of the impacts (either costs or benefits) cannot be monetized. Orders of magnitude are used instead.
Modified cost-benefit analysis	Efficiency and <i>another goal</i> (e.g., equity) are important. Costs and benefits are <i>weighted</i> .
Cost-effectiveness analysis	Efficiency and the other goal can be quantified but <i>not</i> monetized.
Multi-goal analysis	Three or more goals are relevant.

Source: Weimer and Vinning, *Policy Analysis*, pp. 270–274.

Table 6. Types of Cost-Benefit Analysis

Source: (Weimer & Vining, 2004)

While the general concept of CBA seems simple, most of elements comprising the CBA formula should be redesigned depending on its applying area and dominant value system. Each area defines its own concept of cost and benefit, depending on which, the scope of beneficiaries and elements to measure can become different. Table 6 shows that there are different types of cost benefit

analyses and each has their applicable cases. Also, when measuring elements, particularly unpriced ones, a dominant value system for the period affects its quantified value. Table 7 describes an example of how the cost of unpriced elements such as death and injuries were estimated. Therefore, to describe issues and appraise their impact, CBA has been modified or extended.

For example, when enacting environmental standard, quantifying the value of clean environment can raise subjective so controversial issues. In the case of health care, enormous numbers of research and suggestions have been taken to quantify human lives into monetary value. In addition to considering applying areas, CBA also takes into account prevalent social values and norms. For example, with the social mood to emphasize distribution as political priority, CBA applied a special weight system on its calculation to reflect its social trend (Mishan & Quah, 2007).

Average insurance costs for death and disabilities	
Outcome	Cost
Death	\$1,000,000
Nonfatal disabling injury	\$35,300
Property damage crash (including no disabling injuries)	\$6,500

*Source: National Safety Council: Estimating the Costs of Unintentional Injuries, 2000.*

*Table 7. Average insurance costs for death and disabilities*

*Source: (National Safety Council, 2000)*

### 2.4.2. CBA model

Cost-benefit analysis can be expressed in simple notation form as :

$\sum V_i > 0$  , where  $V_1, V_2, \dots, V_n$  are the net valuations of each of the  $n$  persons affected by the project, where a positive  $V$  valuation indicates a net benefit, and a negative  $V$  valuation a net loss to the person.

The key factors of determining the accuracy of the CBA results are how the cost and benefit elements are defined and who the target people are. Depending on their definitions and scope, CBA can return significant different results. Since the use of CBA became more widespread from 1960s along with the US government's requirement to use CBA before the commencement of projects, CBA has been evolved by eminent economists' the firm theoretical frameworks (Eckstein, 1965; Krutilla & Eckstein, 1958; McKean, 1958).



According to Mishan's comprehensive book on Cost-Benefit Analysis (1976), individual's benefit (gain) can be derived from the concept of consumer surplus (the difference between the willingness to pay and actual spending). In CBA, cost is not the ordinary concept of cost (costs of the materials and productive factors used by the project,) but the opportunity cost, which may refer to the highest value might be created by one of alternative uses. The formula can be rewritten to include the aggregated impact over the period from the project commencement to its termination as:

$V_t = (V_{tb} - V_{tc})$ , where  $V_t$  is the *net* benefit in the year  $t$  (which could be positive or negative),  $V_{tb}$  is the valuation of the benefit in year  $t$ , while  $V_{tc}$  is the valuation of the cost in the year.

### 2.4.3. Controversial points of applying CBA to environmental issues

While the general concept of CBA can be understood, when applying it to real cases, it could not be simply applied to the study of specific issue and some controversial problems should be clarified to derive accurate costs and benefits. By understanding these controversial issues, we can better comprehend the issue specific characteristics of CBA elements. Hanley and Spash summarized in *Cost-Benefit Analysis and the Environment* (1993) about controversial issues that arise when CBA is applied to environmental problem:

- “(i) The valuation of non-market goods, such as wildlife and landscape. How should this be done, and how much reliance should society place on estimates so generated? Are we acting immorally by placing money values on such things?
- (ii) Ecosystem complexity: how can society accurately predict the effects on an aquatic ecosystem of effluent inputs?
- (iii) Discounting and the discount rate: should society discount? If so, what rate should be used? Does discounting violate the rights of future generations?
- (iv) Institutional capture: is CBA a truly objective way of making decisions, or can institutions capture it for their own ends?
- (v) Uncertainty and irreversibility. How will these aspects be included in a CBA?”

### 2.4.4. Cybersecurity and CBA

Since the Internet emerged in the mid-1990s, people have become interlinked in unprecedented ways. There are nearly 2.1 billion Internet users—about 30% of the world’s population (Greengard, 2012). According to the Council of Europe (CoE), global business being transacted in the Internet amounts about US \$10 trillion. It is even expected to rise to US. \$24 trillion by 2020, while the current gross world product is about \$63 trillion, according to World Bank (Greengard, 2012).

Recent studies have applied cost-benefit analysis or cost-effectiveness analysis to justify the IT investment of organizations, to evaluate installed information systems or to compare effectiveness of available security technologies and systems. In Table 8, Kim and Lee summarized (2005) the trend of previous research on economic evaluation of security investments for information systems into three groups (Kim & Lee, 2005):

Research	Limits	Security concern	Methodology concern	Practicality
Evaluation of information systems		Do not consider security related factors and controls	Do not consider economic justification issues	Do not provide benefit criteria of system operations
Investment evaluation of information systems		Do not consider security related factors and controls	Applicable	Lack in provision of practical usage
Investment evaluation of information security systems		Applicable	Only provides high level category of cost factors and benefit factors	Do not provide case studies or practical usage

Table 8. Trend of recent research on economic evaluations of cybersecurity investments and limitations

Source: (Kim & Lee, 2005)

Alpar (1990), Barua (1995), Brynjolfsson (1996), Mahmood (1993), Mitra (1996) and Rai (1997) dealt with the impact of investment in IT on organizational performance and productivity (Alpar & Kim, 1990; Barua, Kriebel, & Mukhopadhyay, 1995; Brynjolfsson & Hitt, 1996; Mahmood & Mann, 1993; Mitra & Chaya, 1996; Rai, Patnayakuni, & Patnayakuni, 1997). Kim and Lee (2005). Stolfo, Wei Fan, Wenke Lee, Prodromidis, and Chan (2000) and Wei, Frinke, Carter and Ritter (2001) introduced their cost-benefit models for network intrusion system. Most of research has focused on internal investments and their returns, and their evaluation factors are summarized by Kim and Lee (2005; Stolfo, Wei Fan, Wenke Lee, Prodromidis, & Chan, 2000; Wei, Frinke, Carter, & Ritter, 2001).

	Delone, et al. 1992	Saarinen, 1994	Grover et. al., 1996	Torkzadeh et. al., 1999
Research method	Literature review	Literature review & statistical verification	Literature review	Literature review & statistical verification
Evaluation factors	System quality, Information quality, Information use, User satisfaction, Individual impact, Organizational impact	Development process, Use process, Quality of the IS product, Impact of the IS on organization	Infusion measure, Market measure, Economic measure, Usage measure, Perceptual measure, Productivity measure	Task productivity, Task innovation, Customer satisfaction, Management control

*Table 9. Comparison of IT Investment Success Studies*

Source: (Kim & Lee, 2005)

#### 2.4.5. Controversial Issues of CBA Model in Cyberspace

The CBA analysis of cyber security investment requires benefits which “are represented as avoided damages expressed in terms of the probability and expected cost of an event occurring also benefits are represented as avoided damages expressed in terms of the probability and expected cost of an event occurring” (Rowe & Gallaher, 2006). Rowe emphasized the difficulties of gathering quantitative data to predict potential damages, the probability of their occurrences and their monetary values. Also, he pointed out that when individuals and organizations try to quantify the vulnerability of networks and the related costs and benefits, “no methodology for such predictions has been widely accepted or implemented” (Rowe & Gallaher, 2006).

Cyber security issues cause significant spill-out impacts spreading over broad communities, which sometimes are even borderless. This is because cyber security plays significant role as the infrastructure on which most of modern business count for the reliability of business environment. Also, this intertwined and borderless character originates in the intrinsic characteristics of cyber security area that cyber space or network itself exists based on people's interactions (signal exchanges). Therefore, when evaluating cybersecurity programs, new CBA model should be considered to avoid missing these spill-out impacts.

#### 2.4.6. Strategic Philanthropy and Extended CBA

Not only governments, but also corporations can use CBA to make business decisions that are interconnected with social issues. This trend has also been accelerated by Porter's idea that a corporation's social responsibility activity can be strategically redesigned to boost its business bottom line rather than ending up giving away money or sacrificing profits.

Porter changed the entrenched perspective on corporation's social responsibility, where people think that to create social benefit, a business should sacrifice its profit. He recommended corporations to strategically see this trend and proactively design their social programs to boost their business bottom line. To measure this strategic philanthropy of corporations, the extended CBA devised above can be applied.

#### 2.4.7. Cyber Issues in Emerging Countries

While there is growing effort to internationally cooperate to fight against cybercrime, its attempts have not achieved significant gains yet. For example, the Council of Europe's Convention on Cybercrime gathers stakeholders from governments, NGOs, corporations, computer scientists, and Internet users. Only half of the participating countries signed, and minimum standards were approved. Emerging countries including Russia and China were not welcome (Greengard, 2012).

However, improving cyber issues in emerging countries can have more impact on global improvement than developed countries. ITU published a guide for developing countries in 2009. It states, "developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run" (Gercke, 2009; World Information Society Report 2007, page 95).<sup>7</sup> In addition, the number of Internet users has increased over several decades, and "In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware and wireless access will enable even more people to access the Internet."<sup>8</sup>

---

7

Regarding cybersecurity in developing countries, see: World Information Society Report 2007, page 95, available at: [http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07\\_full-free.pdf](http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf)

8

See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available

In addition, the ITU report suggested that developing countries are exposed to more associated cybersecurity risks due to their weak protection measures, less strict safeguards and protection (Gercke, 2009). To address those problems, it is important to understand what the issues are when developing countries try to implement strategies, whose effectiveness has already been proved in developed countries. ITU report summarized those difficulties as 1) compatibility of legal systems, 2) the status of supporting initiatives (e.g. education of the society), 3) the extent of self-protection measures in place as well as 4) the extent of private sector support (e.g. through public-private partnerships) (Gercke, 2009).

## 2.5. Conclusion of Chapter 2

Because of lack of incentives of individuals and private organizations, national public goods have been part of the economic theory of government for centuries. The concept that governmental intervention can help society overcome market failures of inequity of resource allocation is hardly new, but recently, global public goods issues such as climate change and cyber security have emerged out, changing the scope of issue from a country to the globe.

Cyber security issues are an emerging global public good in that the issues are deeply related to infrastructures, they are also rooted in information/knowledge sharing, an well-known public goods, and its impacts are across the national frontier. One of the most important factors in addressing global public good issues is participations and collective efforts. How can we encourage countries and private sectors participate in the global movement to address cyber security threats?

Cyber crimes and cyber incidents are globalized and hackers and its victims do not always reside in the same country anymore. The cyber security of a country is becoming deeply related to that of neighboring countries, which implying that narrowing the cyber security gap between developing and developed countries can be an effective approach. This requires the construction of strong domestic cyber security monitoring and response frameworks.

---

at: <http://topics.developmentgateway.org/special/information society>.

Understanding effectiveness and benefits of initiatives for the emerging global public goods, international development programs for cyber security, a new cost benefit analysis (CBA) model should be considered to precisely evaluate the programs. The extended cost-benefit analysis (CBA) model can also be important for business decision makers.

## Chapter 3. Research Methodology

This Chapter introduces research methodologies used in this paper to explain how data and cases were collected.

### 3.1. Methodologies

#### 3.1.1. Literature Review

This review explains the extended cost-benefit analysis frameworks designed for international cooperation in cyber security domain. To do this, this research assembles cost and benefit elements; all of which are closely related to the domain of international cooperation in cyber security and utilize cost-benefit analysis as main analysis tool to assess the effectiveness of their targeting policy or business decisions. The domains are information investment, international development and technology transfer.

#### 3.1.2. Interviews and Site Visit

Since the first phone conversation on April, 18, 2011, the cooperative relationship with Korean CERT for ECIR project has developed. In May, dashboard data of Korean CERT was verified by Korean CERT officers and some of missing data were filled. Also, two phone conversations were completed. I visited Korean CERT on June 6, 2011 and met Taekyu Shin, director of Korean CERT, one legal officer and one technical officer; the meeting lasted 3.5 hours. In addition to the site visit, seven interviews were held with Korean CERT and Winitech, a Korean IT company, which participated in Korean CERT-led international development programs, over 18 months since 2011. For this research, the cooperation and support of Korean CERT is substantial, and over the long time (one and half year,) the several off-record phone calls, emails and interviews were completed. Interview Eunhee Kang, CEO of Winitech was interviewed on April 18, 2012. The interview questions are attached in Appendix 2.2 and 2.3.

<b>Korean CERT</b>	1 <sup>st</sup> Interview	2 <sup>nd</sup> Interview	Site visit	3 <sup>rd</sup> Interview	4 <sup>th</sup> Interview
Date & Time	April 18, 2011 (~1 hour)	April 25, 2011 (~1 hour)	June 6, 2011 (~3.5 hour)	Oct 4, 2011 Oct 15, 2011 (~1 hour)	March 14, 2012 (~1 hour)
Structure	Open interview	Open interview	Open interview	Semi-Structured interview	Semi-Structured

					interview
Record	Scripted	Scripted	Recording	Scripted	Scripted
Contact	Taekyu Shin, Director of Korean CERT	Taekyu Shin, Director of Korean CERT	Taekyu Shin, Director of Korean CERT & Two CERT officers	Wanseok Lee, Manager of performance evaluation team	Wanseok Lee, Manager of performance evaluation team
Key issues	CERT activity: Data sharing	CERT activity: Data sharing	Competence of Korean CERT, Focus of International cooperation	International cooperation activities, AP- CERT Training session	Relationship with Malaysian CERT

**Table 10. Research Cooperation with Korean CERT**

*Source: self-created*

## 3.2. Sites & Data

### 3.2.1. Korea CERT

#### 3.2.1.1. Site information

Korean CERT, founded in July 1996, is located in Seoul, South Korea (135 Jungdaero, Songpa-gu, Seoul, Korea). Composed of four teams—Incident Analysis Team, Network Monitoring Team, Hacking Response Team and Response coordination Team, it is an operational arm of Korean Information Security Agency (KISA). Four main activities of Korean CERT are: 1) promoting the use of valid security technology, and ensure network continuity, 2) organizing and support the responses to cyber security incidents, 3) identifying vulnerabilities and fostering communication between security vendors, users, and private organizations and 4) serving as a unified communication channel for international cooperation activities. Its website is <http://www.krcert.or.kr/> (« KrCERT/CC », 2012). Its upper organization, KISA was established in 1996 under the Act of Promotion of Utilization of Information and Communication Network and Data Protection. (Article 52) Its establishment aimed to create a safe, reliable information distribution climate by reacting effectively to a variety of electronic infringement and intrusion acts. KISA has devoted itself to enhancing the security and reliability of electronic transactions. Its website is <http://www.kisa.or.kr/main.jsp> (« Korea Internet Security Agency », 2012). KISA focuses on seven main working areas below (IT Security Policy in Korea, 2011):

- Internet incidents response & prevention
- Private information and Privacy protection
- Combating illegal spam



- Digital signature(Root CA) management
- Information Infrastructure protection
- IT security products evaluation
- Information security policy/technology development

### 3.2.2. Winitech

Winitech, a Korean IT Company founded in 1997, is an expert of implementing Integrated Emergency Management System (IEMS). Winitech is specialized for 119 Emergency Rescue System. Emergency Rescue System is the main solution of Winitech and this Winitech's solution is now one of the most common Integrated Emergency Management Systems for fire stations in Korea. Winitech successfully installed 119 Emergency Rescue System, which is like 911 systems in USA, in Daegu Fire Department. (« Winitech/About », 2012)

After Winitech installed 119 Emergency Rescue System in Daegu Fire Department successfully, Winitech have been continuously installing the system in many main cities including Jeju, KwnagJu, Ulsan – the main cities of R.O.K. Throughout these projects, we have developed our system based on knowledge and experience in the field of Information Technology and we are continuously trying to develop the effective system that would protect human from disasters.(« Winitech/About », 2012)

Winitech is expanding its areas of business to China, Southeast Asia, Central and South America, Middle East, and etc. As the business gets bigger, Winitech not only stays in firefighting area but also expands to the other areas like police, security, water and sewer service and transportation. (« Winitech/About », 2012)

Winitech is located in 2139-12 Daemyeong-dong, Nam-gu. City, : Daegu. Country, : South Korea. Phone, : 053-659-1703. Fax, : 053-659-1707. Its website is <http://www.winitech.com/Eng/>. The following image summarized their core activities.

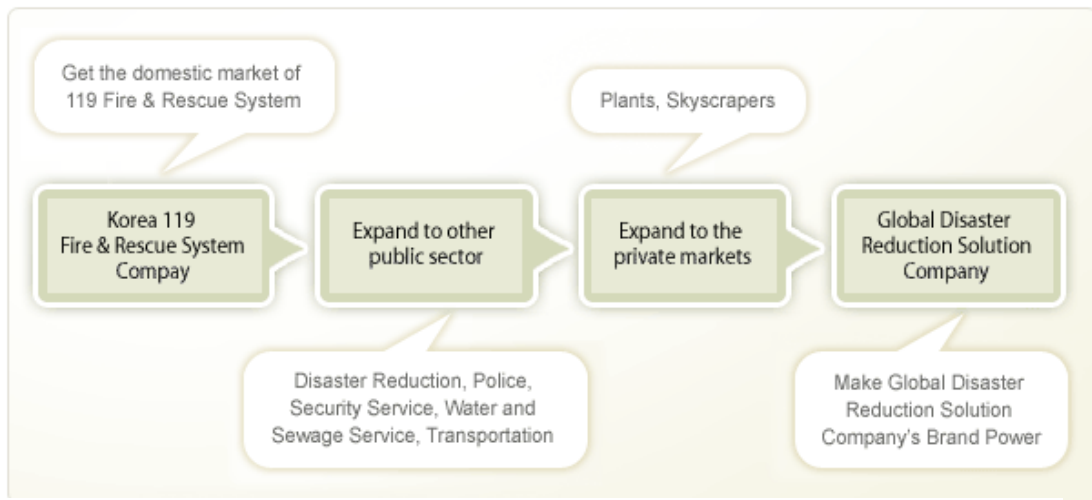


Figure 10. Core Buisness activity of Winitech  
 Source: Excerpts from Winitech website

### 3.3. Summary of Research Methodology

This study suggested a new analysis framework, extended cost-benefit analysis for analyzing emerging global public good issues, cyber security. The analysis framework is established based on literature reviews on the cost benefit analysis studies in three themes: 1) Private companies' Cyber security investment, 2) Governments' foreign aid programs, and 3) Global corporate social responsibility. The devised framework is verified by the data collected from interviews with Korean CERT and a Korean IT company, which participated in government led international development programs.

## Chapter 4. Korean Cyber Emergency Response Team (CERT)

This chapter presents the case of Korean Cyber Emergency Response Team(CERT) collaborating with Malaysian CERT. This case is greatly interesting in that this paper sees this international development program as one of the most effective international cooperation activities for combating globalized cyber security threats..

While numerous countries, which are running national CERT and publish the number of their reported cyber incidents, shows that the number of cyber incidents are increasing, South Korea has successfully decreased the number of incidents. Figure 11 shows the charts from the Explorations in Cyber International Relations (ECIR) Data Dashboard that our research team has operated since 2010. The ECIR Data Dashboard allows you to view and graph various cyber related data (e.g., cyber attacks, number of servers, population) for various countries around the world for the years 2000-2010. Its details, about ECIR project, data sources and how to use it can be found in Appendix 3.

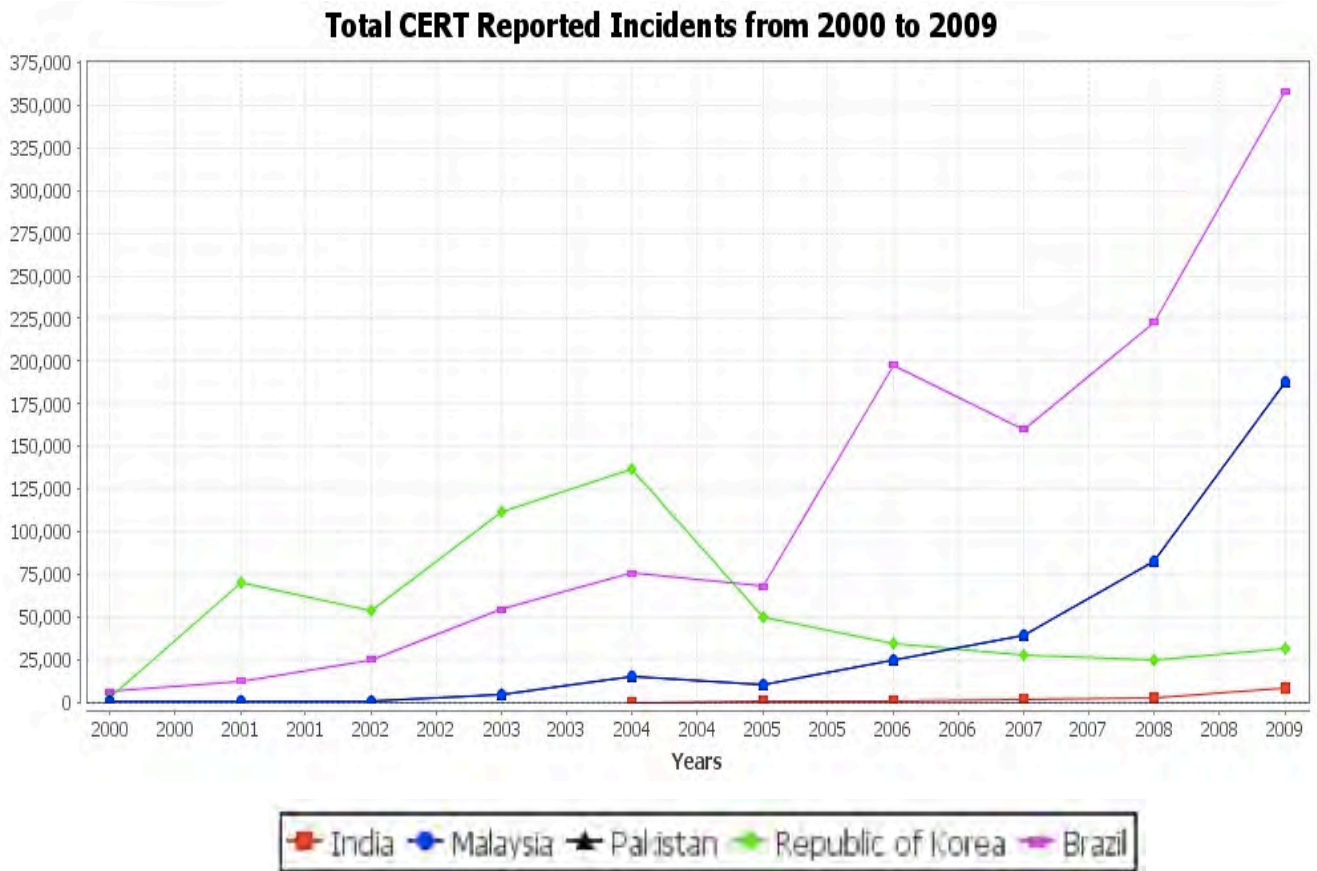


Figure 11. Total CERT reported incidents from 2000 to 2009 of India, Malaysia, Pakistan, Brazil and Republic of Korea

## 4.1. Korean Cyber security Framework

Figure 12 demonstrates the hierarchy of Korean cyber security framework, and CERT is under KISA (Korea Internet & Security Agency).

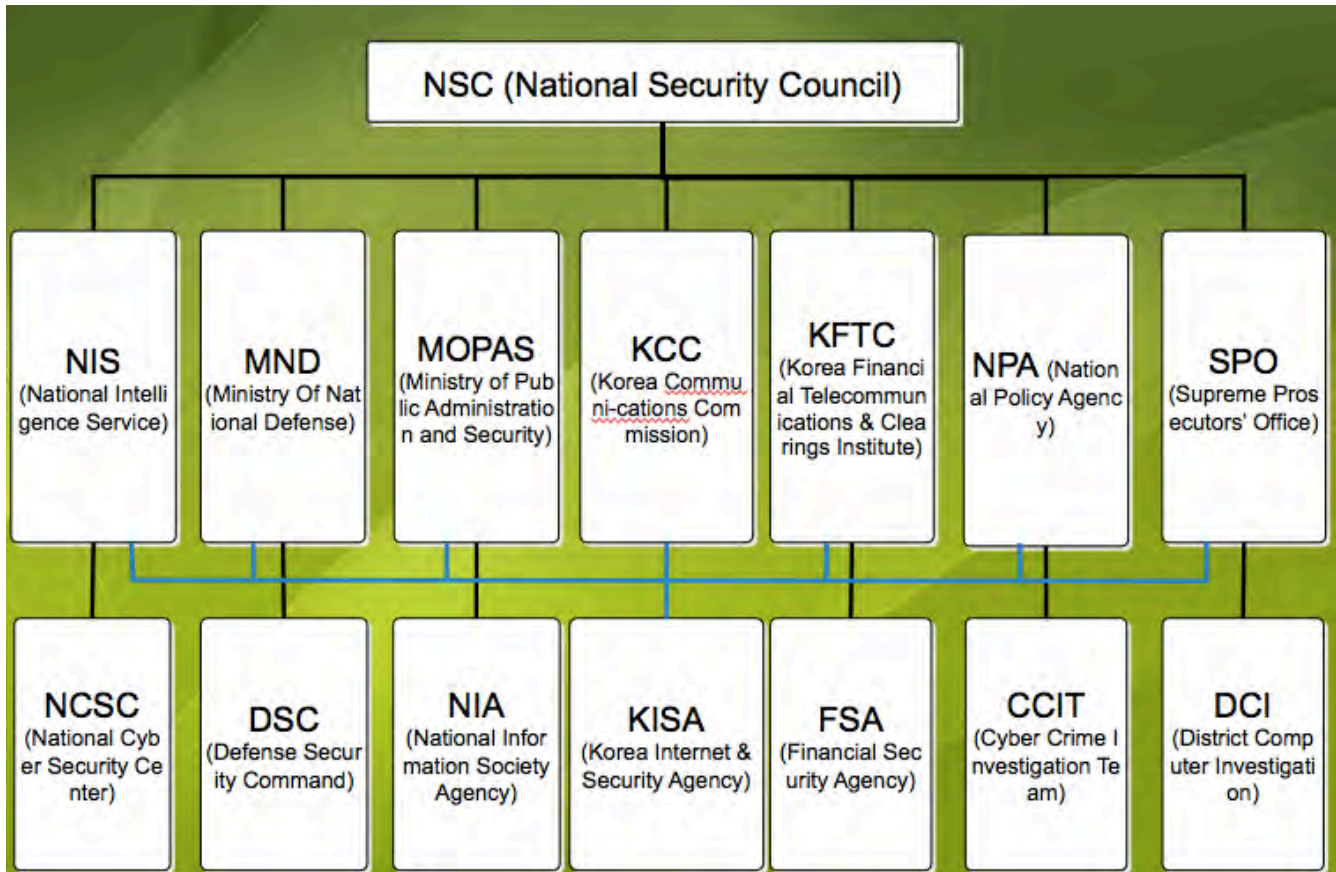


Figure 12. Korean Cyber security framework (IT security policy in Korea, 2011)

(Source: excerpts from a presentation material provided by Korean CERT)

Korean national cyber security framework focuses on four main activities: 1) prevention activities, 2) Intrusion detection, 3) information support and 4) incident support, and Korean CERT plays key roles in those activities. Prevention activities ensure the safety through advising security measures and reviewing corrective actions for government organizations. Korean CERT provides education and publish useful information on its website to reduce the cyber security related problems. The second activity, intrusion detection involves diverse agencies, and those numerous actors require complicated command system. The Figure 13 presents how diverse government agencies cooperate together to detect intrusion and how differently they respond to the incidents of different risk level. In the figure, Korean CERT is referred by a different name, Cyber Incident Response Situation Room. Korean CERT plays fundamental roles in this framework by monitoring abnormal traffic and activities, sharing

information with related organizations and reporting the situation to higher level agency, NCIA (The National Computing & Information Agency).

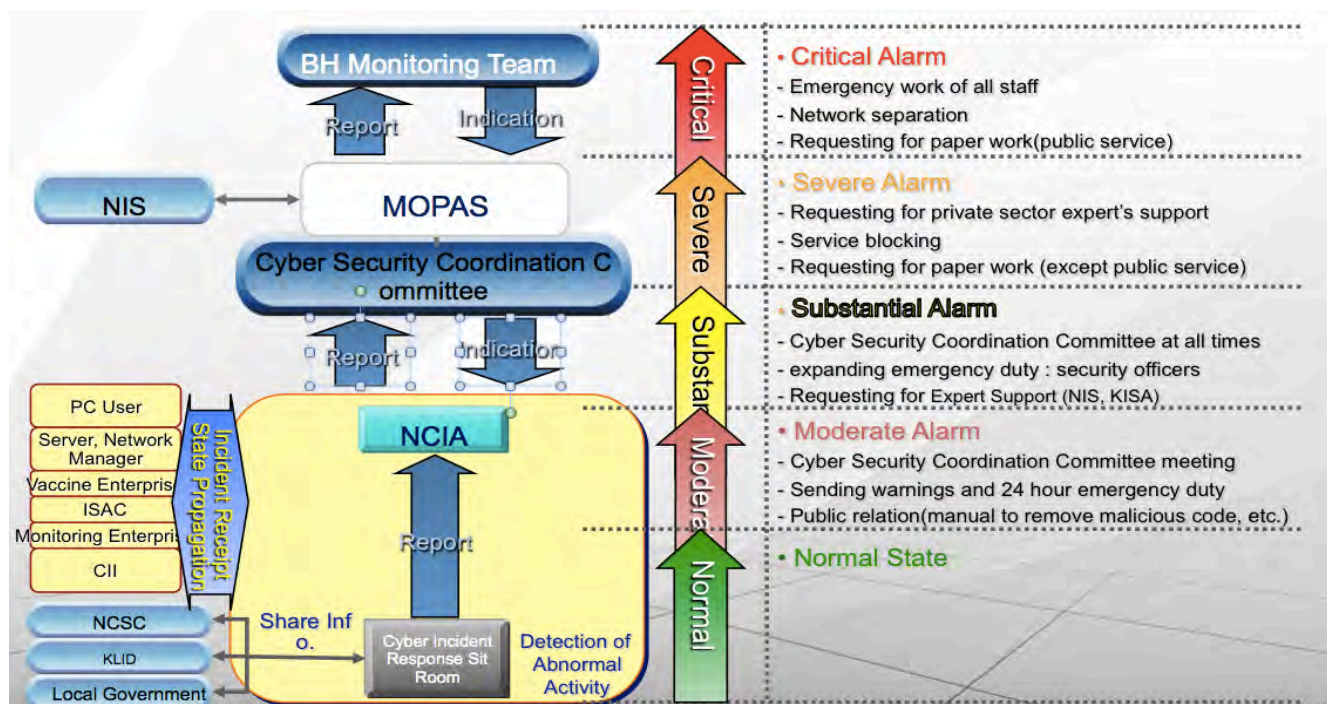


Figure 13. Intrusion detection system of Korean national security framework

Source: (IT security policy in Korea, 2011)

Figure 14 presents the third activity, information support and introduces how Korean cyber security agency shares information with related organizations and operates Integrated Emergency Response System cooperating with the organizations for cyber attacks.



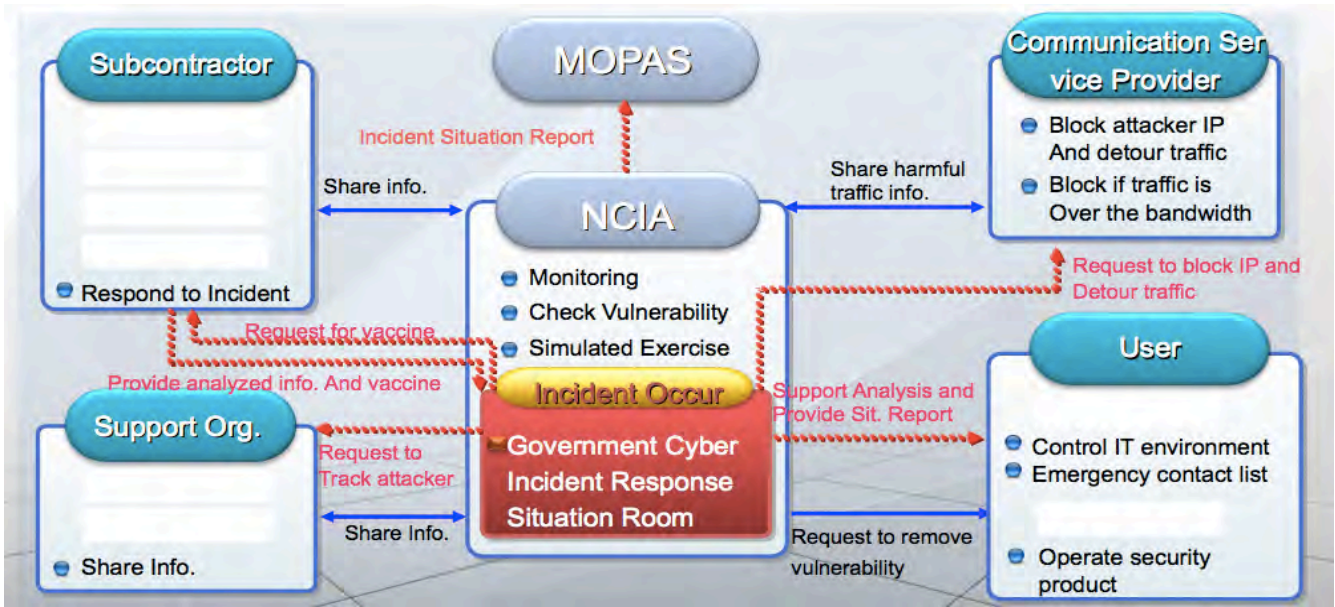


Figure 14. Information support to operate integrated emergency response system with related organizations for cyber attack

Source: (IT security policy in Korea, 2011)

The fourth main activity of Korean cyber security framework is incident response, and it is the task that Korean CERT most focuses on. Incident response is composed of five steps: 1) Initial Response Regarding Incident Report, 2) Scuring and Retention of Evidence, 3) Investigating Incident, 4) Recovering Damage and 5) Analysis Report. The Figure 15 presents incident response system of Korean CERT.

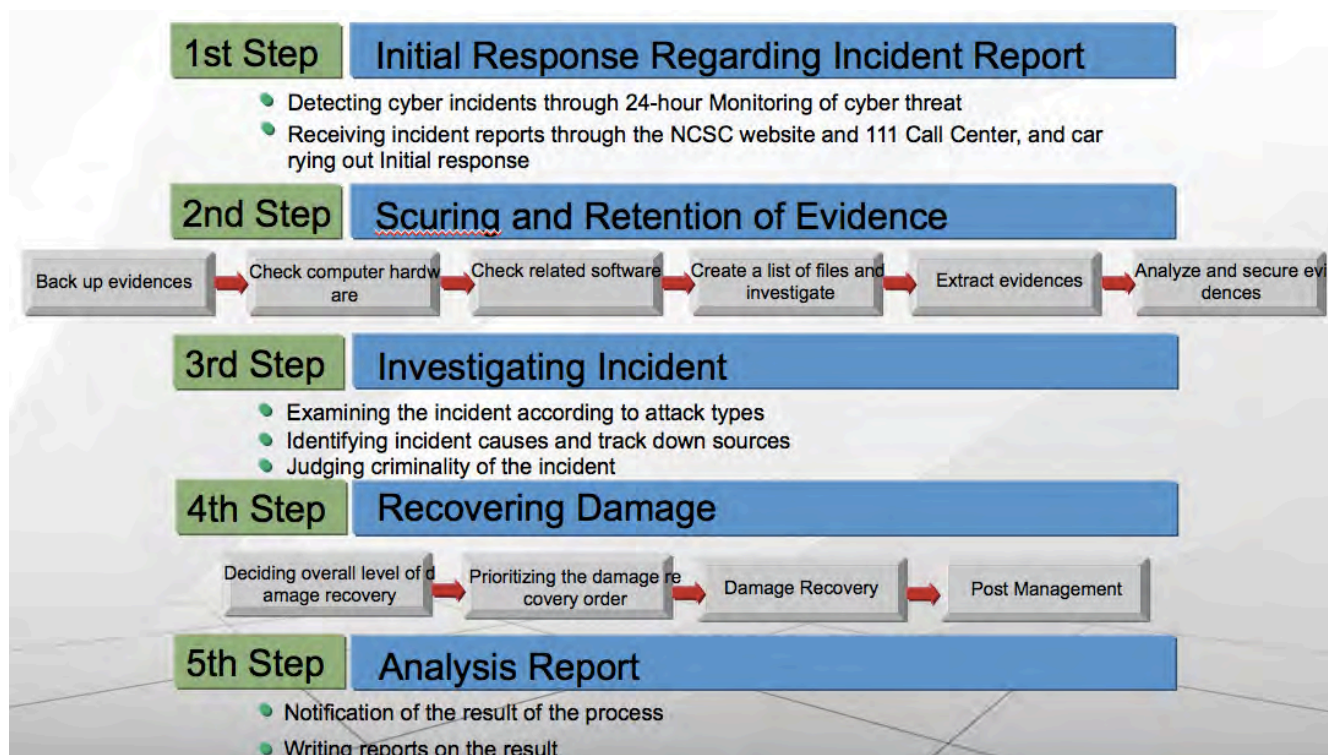


Figure 15. Incident response system of Korean CERT

Source: (IT security policy in Korea, 2011)

## 4.2. Korean Government: international cooperation in Cyberspace

What the most important field of the Korean government’s international cooperation initiative is information technology field. The Korean government allocated the largest portion of bilateral foreign aid in Information communication technology (ICT) field in 2002 as 28.9% of total budget, 212.1 million USD and its trend has continued.

To exercise this ICT international cooperation, two government agents, Korea Communications Commission (KCC) and Ministry of Public Administration and Security collaborate. For cyber security and e-governance related activities, Korea Information Security Agency (KISA), the higher organization of Korean CERT, and National Information Society Agency are the key operational arms. The Table 11 presents ICT focus international cooperation program being operated by the Korean Government.

ICT focus program (Execution agent)	Projects
Information access center (National Information Society Agency (NIA))	Offers an infrastructure with better access and opportunity to use IT for the general public in the partner countries. Established at 22 countries, allowing internet access and IT training to 3 million local residents
Korea Internet Volunteers (Korea Agency for Digital Opportunity and Promotion)	Sends out IT expert volunteers to developing countries From 2001 to 2009, over 3000 KIVs have been sent out to 67 countries to offer IT training courses to 90,000 local residents.
Korea IT Learning program (Korea Information Security Agency (KISA), NIA)	Invites policymakers, public officials, and experts in the IT field to introduce Korea's IT development strategies From 1998 to 2009, about 110 KoIL courses have been offered to more than 2800 participants from 113 countries.
IT Cooperation Centers (NIA)	Korean IT experts and local experts at ITCCs perform joint research, technological knowledge exchange, and IT education. (6 ITCC has been established)
IT & Policy Assistance Program (NIA, KISA)	provides consultations and technical assistance to countries

*Table 11. Korean Five key ICT international development programs (Two programs, Korea IT Learning program and IT policy assistance program, run by KISA, which is a higher organization of CERT, are related to international activities of CERT)*

*Source: self-created based on annual reports of KISA*

Among the five programs of the table above, Korean CERT is contributing mostly to two programs, Korea IT learning program and IT & Policy Assistance program, by providing cybersecurity training courses. Regarding cybersecurity training activities, Korean CERT offered classes to public officials through national projects, named KoIL and also has hosted two training centers of International organizations such as UN ESCAP and World bank's Development Gateway Foundation. Since 2005, APISC (Asia Pacific Information Security Center, **a regional institute of the United Nations Economic and Social Commission for Asia and the Pacific**), located in Korea, has provided training courses to 163 participants from 33 Asian-Pacific countries encompassing Mexico, Malaysia and New Zealand.

International cooperation activities can be described by one country's initiatives to some extent, but to better understand the big picture, government to government cooperation is useful information.



The Table 12 presents the information of international cooperation in the form of government to government (the information including the year, the cooperating countries, the project names and the counterpart agencies of the cooperation projects from 2005 to 2007.)

Year	Nation	Project	Counterpart
'05	Dominican	Local e-Gov Informatization	Liga Municipal Dominicana
		e-Security	Ministry of Home Affairs
	Guatemala	e-Learning	Ministry of Education
	Mongolia	eGov M/P	ICTA
	Vietnam	e-Procurement	MPI
	Mongolia	NID	ICTA
	Pakistan	e-Procurement	EGD
		e-Post	Ministry of Communication
	Uzbekistan	Education Informatization	Ministry of Education
Colombia	Internet Informatization	Ministry of Communication	
Cambodia	Central Bank Informatization	Central Bank	
'06	Nepal	eGov M/P	HLCIT
	Mongolia	e-Customs	Customs Service
	Azerbaijan	Customs Modernization	State Customs Committee
		PKI & RIS	Ministry of Communication & Information Technology
	Egypt	PKI	ITIDA
	UAE	WiBro etc	Etisalat
	Colombia	Education Informatization	Ministry of Education
	Vietnam	Security	VGISC
	Indonesia	Local e-Gov Informatization	Surabaya
Philippines	Marine Disaster Prevention	PCG	
'07	Indonesia	ITS	Ministry of Public Work
		e-Post	POS Indonesia
	Vietnam	GIS	MONRE

*Table 12. Global G2G cooperation*

*Source: (IT security Policy in Korea, 2011)*

### 4.3.Preliminary Cost-Benefit analysis

Analyzing costs and benefits of international cooperation activities allows policy makers identify effective policy programs (e.g., is training program effective than other program?) and develop customized programs for partnering countries. (e.g., different plans should be applied to developing countries and advanced countries) The Korean government generally considers three benefits in evaluating technological international cooperation projects: knowledge flow, diplomatic impact and market penetration. For the cooperation with developing countries, it focuses additionally on achieving ODA mandate and facilitating Korean companies to enter the emerging markets.

The success of Korean E-government Training can be a good example to explain that the international cooperation with developing countries can return economic benefits to the country. As a result of the E-government training, the Korean IT companies successfully won a number of e-government related public contracts such as Mozambique Disaster control system (\$25M), Ecuador E-custom (\$24M), Mongol E-tax (\$5M) and Vietnam IDC (\$100M).

Korean CERT’s cyber security training program also brought back business opportunities in public procurement such as the establishment of Malaysian Integrated Monitoring system & National Security Center Indonesian ICT security R&D center. Table 13. Cost & Benefit elements of international development programs shows the summarized the elements of cost and benefit of international development programs identified in the Korean cases.

COST elements	BENEFIT elements
<ol style="list-style-type: none"> <li>1) Government expenditure to invite &amp; educate related government officials</li> <li>2) Development of education material</li> <li>3) Opportunity cost of free technology transfer</li> <li>4) Official development assistance (ODA) to international organization</li> </ol>	<ol style="list-style-type: none"> <li>1) Public procurement (S/W or infrastructure): Received orders of Mozambique Disaster control system (25M\$), Ecuador E-custom (24M\$), Mongol E-tax (5M\$), Vietnam IDC (0.1B\$)</li> <li>2) Increase of market penetration : Korean private IT companies, who built Korean government systems such as Dream security, Acromate and LG CNS, could enter emerging countries’ market</li> <li>3) Cybersecurity level improvement</li> <li>4) Diplomatic impact</li> </ol>

Table 13. Preliminary Cost & Benefit elements of International development programs

Source: self-created

#### 4.4. Global G2G cooperation process of Korean CERT

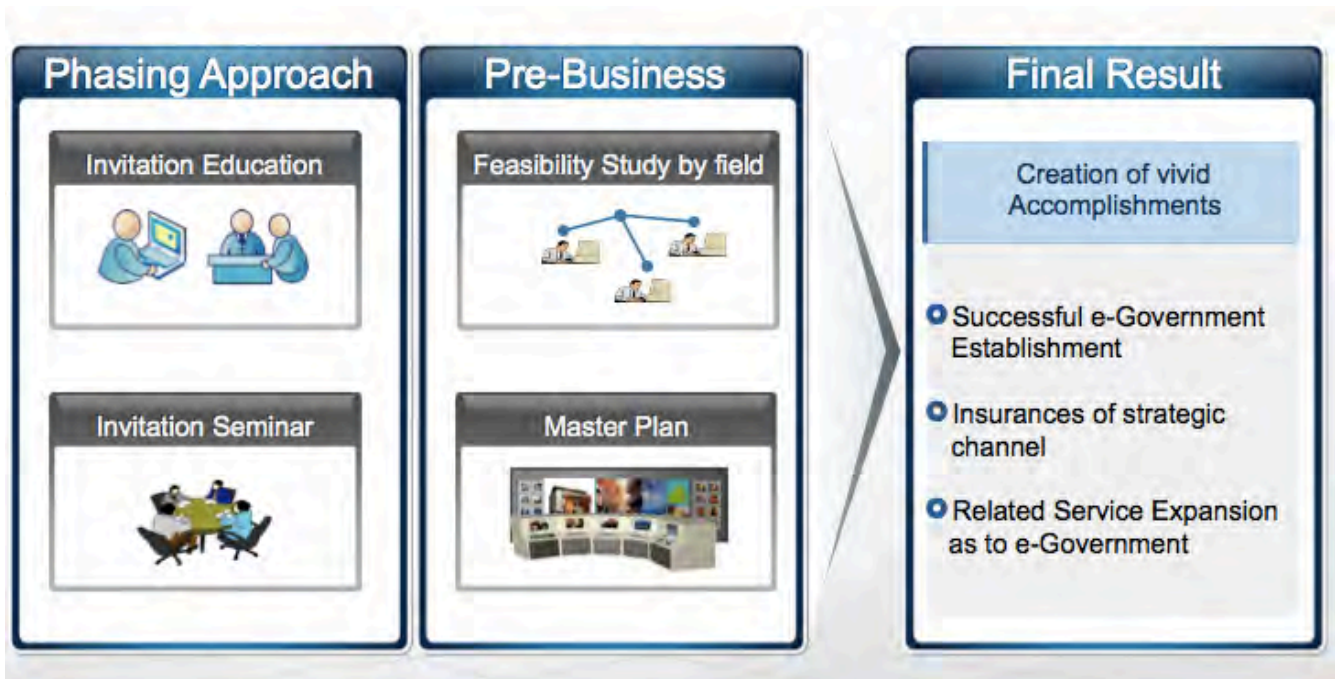


Figure 16. Explanation of Korean CERT's Government to Government cooperation process

Source: excerpts from a presentation material provided by Korean CERT

Figure 16 presents how Korean government establishes the relationship with other countries and relates the relationship to business. As the figure explains, the relationship generally starts from education and seminar activities combined with business feasibility assessment. This implies the participation and influence of private sectors on training session and the potential of more active public-private partnership approach.

#### 4.5. Case: Korean CERT and Malaysian CERT

Malaysian cybersecurity government officers had attended APISC training courses until 2007, and decided to establish National Integrated Monitoring system and National Security Center in Malaysia. Korean private companies, which, as sub-contractors of the comparable projects in Korea

made huge contributions to the establishment of National Integrated Monitoring system and National Security Center, could win some of public procurement projects in Malaysia. The Figure 17 shows those contracting Korean companies of the Malaysian project and their short descriptions.




	Total maintenance solution,
	Security company (CEO is former KR-CERT employee)
	SecureCAST (forecasting system of cyber risk)

Figure 17. Korean IT companies benefiting from the government led IT training programs

Such benchmarking is a classic way of making public policy, so this finding is not a surprise. However, understanding the benchmarking process is important in the potential that its value chain (Figure 18) below can be refined and reinforced, thereby leading to more business opportunities to Korean CERT and companies.



Figure 18. How Korean IT learning program lead to economic benefits

Source: self-created

#### 4.6. Comments on Chapter 4

Analyzing international development activities of South-Korea CERT can provide informative lessons to other countries' CERTs for three reasons. Korea has the fastest average Internet connection speed in the world, 17.5 Mbps, while other leading countries U.S. recorded 6.1 Mbps and Japan 9.1 Mbps. Therefore, Korean CERT has handled lots of emerging crimes and incidents which are not popular in other countries yet. In addition, as we learned from the Figure 11, Korean CERT has successfully addressed the domestic incidents decreasing it by 82% from 2004. Furthermore, the

Korean government allocated the largest portion of bilateral foreign aid in Information communication technology (ICT) field in 2002 as 28.9% of total budget. Based on the advanced system of Korean CERT and strong governmental support of international activities in ICT, Korean CERT could launch several global activities such as training session.

## **Chapter 5. Extended Cost-Benefit Analysis**

This chapter suggests a new evaluation framework, which are designed to analyze international development programs approach in addressing cyber security issues. The framework is formulated by extending traditional cost-benefit analysis framework. Section 5.1 presents the background of shared value and newly defined terms to explain the extended benefits. Section 5.2 will explain how the extended cost-benefit framework is formulated, and section 5.3 introduces the completed cost-benefit framework.

### **5.1. Extended Benefits with Shared Value**

#### **5.1.1. Introduction of Shared Value and Definitions of Terminologies**

The term *shared value* is borrowed from Porter's definition and usage; its definition was initially explored in his paper (Porter & Kramer, 2006). According to Porter, *shared value* is "a meaningful benefit for society that is also valuable to the business." He explains that strategic CSR can unlock shared value by investing in social aspects of context that align with the company's competitive context. The *shared value* from public-private partnership, and the *indirect benefit* (*indirect* because of its characteristics of indirect impact and long-term impact) of private parts were explored and identified through a literature review of Porter's paper and his framework. In this paper, the term *indirect benefit* is used to indicate the benefit that does not emerge in direct response to the investment or activities; they are visible over the long term or manifest "indirectly" (triggered not by an identified factor but by complicated interference of multiple factors). The term *pre-benefit* is used to indicate a benefit resulting not from completing activities, but from the partnership itself between public sector and private sector. The *synergic benefits* imply synergistic effects of the partnerships and facilitates the implementation and completion of programs and activities.



### 5.1.2. Diagram of Stakeholders and Benefit Creation

This paper suggests a diagram to visualize benefits, synergic benefits, indirect benefits and shared value.<sup>9</sup>

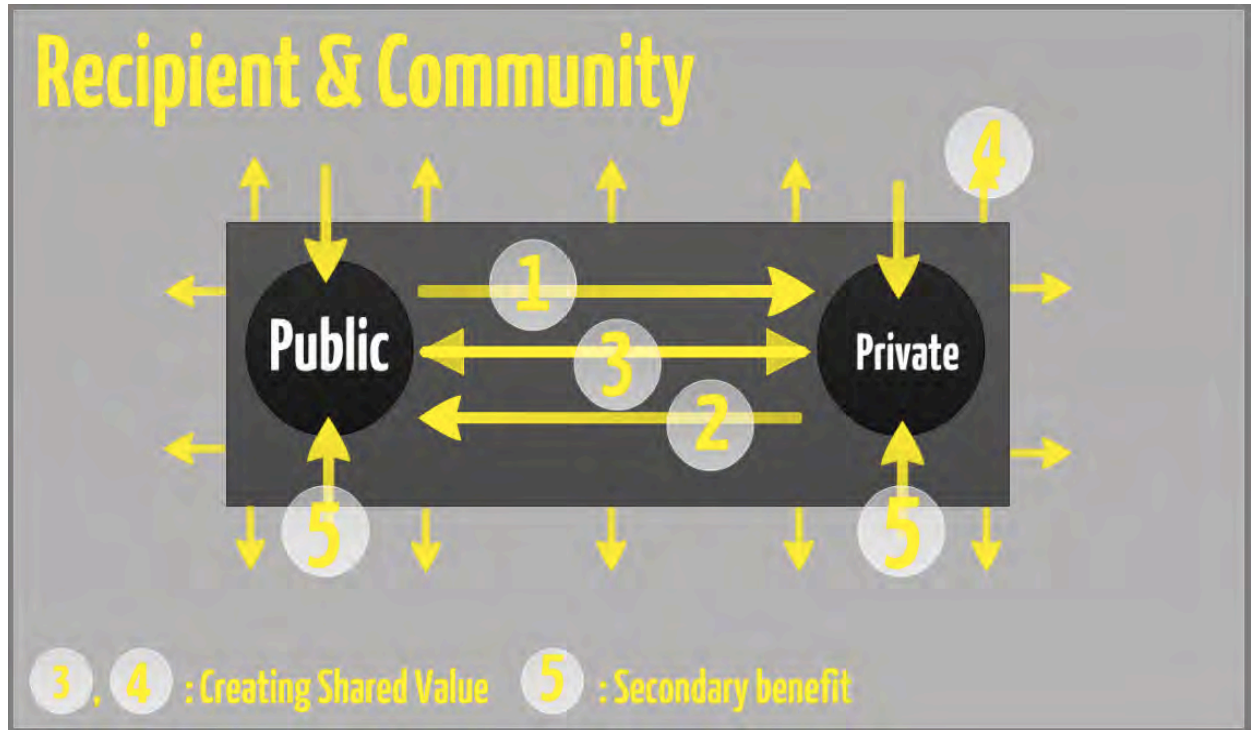


Figure 19. Benefit diagrams of international development programs operated by Public-Private Partnership

Source: self-created

The diagram depicts potential benefits of international development programs operated by Public-Private Partnership: the synergic benefits of public-private partnership (1,2 and 3), shared value (3 and 4), and indirect benefits (5). When public agents and private companies set up a partnership to address social issues, they produce *synergic benefits* (1,2, 3) that facilitate their operations. After the operations are completed, if its investment in time, effort and resources accomplishes the projected goals, they reap the planned *benefits* such as the functions of built infrastructures and the economic benefits from completed projects. They also create *shared values* benefiting both participating actors and broader communities that do not actively participate in the operations (3 and 4); Coca-cola

<sup>9</sup> 1) benefits, originally aimed benefits and created from regular activities, 2) synergic benefits, by-product benefits created from the settings of operation such as relationship of agents, 3) indirect benefits, indirect or long-term benefits and 4) shared value, the benefit applied to broader community, not only to stakeholders who actively involved in the issues.

company has reduced its world-wide water consumption by 9% from 2004, and this reduces its resource use as well as improves global water quality and reduces carbon prints. Take Johnson & Johnson. It helped employees stop smoking through campaigns and support programs and achieved the distinguished result of a two-thirds reduction in the past 15 years. This not only increased the welfare of employees but also helped the company save \$250 million on health care costs and have more present and productive workforce. Likewise, those benefits are not simply spillover, which cause free-rider problems, but return to the implementing agents as long-term benefits, which reinforce the competitiveness of private companies and increase the welfare.

## 5.2. The extension of Cost-benefit framework

The extended cost-benefit framework is established by compiling elements of cost-benefit frameworks used for three domains—1) Global Corporate social responsibility, 2) Foreign direct investment/ foreign aid and 3) Cyber security investment. Those three frameworks were formulated through literature review on the articles found from the search of cost-benefit analysis studies in the three domains.

### 5.2.1. Extended cost-benefit framework: Global CSR

To identify the benefits of Public-Private partnership for international development programs, we should understand the related cost and benefit elements of each party. For private companies, participating in international development programs share numerous common attributes with practicing global Corporate Social Responsibility (CSR) activities. They are both global level activities and aiming for public goods. Understanding costs and benefits of global CSR can help us understand the potential incentives and benefits of private companies in participating in international development programs. Table 14 shows the cost and benefit elements of Global CSR, collected from literature reviews.

Actor	Cost	Benefit	Indirect Benefit	Shared Value
<b>Companies</b>	-Cost of implementing program -Risk of Technology spill-out -Risk of	-Facilitating the entrance of emerging country market (under official/unofficial)	-Marketing effect; community engagement & Reputation -License to operate (by gaining governmental support) e.g. Google and Chinese government case -Sustainability (by establishing	-Building relationship with local administrative agents-> better business environment such as trade conditions and more regulation information. -Knowledge sharing-> improvement of employee skills

dissatisfaction of shareholders with reduced dividend -Opportunity cost of other business activities or R&D	protection)	stable & reliable market and operating environment such as infrastructures) -Meeting moral obligation (do the right things as community members)	and overall productivity Improving supplier quality, the overall quality of life of community people -Providing job opportunity to community -Providing infrastructure and appropriate training
--	-------------	---	--

*Table 14. Cost-benefit analysis table for Global CSR*

Source: self-created based on data collection from (Alesina & Dollar, 2000; Berthélemy, 2006; Chong & Gradstein, 2008; Lumsdaine, 1993; Marian Leonardo Lawson, 2011)

### 5.2.2. Extended cost-benefit framework: Foreign Direct investment / Foreign Aid

To understand the related cost and benefit elements of public parties in public-private partnerships, it is helpful to look at the studies about the cost-benefit elements of Foreign direct investment and foreign aid. Table 15 introduces the Cost-benefit analysis table for foreign direct investment or foreign aid, collected from literature reviews.

Actor	Cost	Benefit	Indirect Benefit	Shared Value
<b>Government Agents</b>	-Cost of implementing program -Human resource -Place to train -Cost of preventing tech spillover to rivals -Wage premium -Secluded production site	-Strengthen political linkages: those who have particular political linkages with recipient countries aim at reinforcing such ties -Targeting trading partners: all donors choose target countries which are the most significant trading partners		-Strengthen political linkages-> better diplomatic relationship and better business environment such as trade conditions and more regulation information. -Knowledge sharing-> improvement of employee skills and overall productivity Improve supplier quality, the overall quality of life of community people -Providing job opportunity to community -Providing infrastructure and appropriate training

*Table 15. Cost-benefit analysis table for foreign direct investment or foreign aid*



Source: self-created based on data collection from (Burke & Logsdon, 1996; Chai Lee Goi & Kah Hian Yong, 2009; Chatterji, Levine, & Toffel, 2009; Dobers & Halme, 2009; Habip et al., 2011; Maas & Liket, 2011; Porter & Kramer, 2002, 2006)

### 5.2.3. Extended cost-benefit framework: Cybersecurity investment

A principal part of information security relates to qualitative and non-financial concerns; therefore, traditional economic approaches are severely constrained in evaluating cybersecurity investment. Many other real world problems require combining quantitative measures with qualitative concerns (Bodin, Gordon, & Loeb, 2005).

Actor	Cost	Benefit	Indirect Benefit	Shared Value
<b>Companies</b>	-Cost of implementing program -Information gathering, installation, debugging, and maintenance costs (labor) -Hardware and software -User inconvenience (monitoring, slowing-down)	-(Expected probability of reducing crimes & incidents) * {(cost of computer crimes) + (cost of viruses, worms, and other attacks) + (cost of Resources (labor) needed to repair damaged systems and data) }	-Reputation	-Cleaner/reliable cyber space -Seamless user experience -Reducing other crimes (otherwise, the systems can be abused as zombie computers)

Table 16. Cost-benefit analysis table for cyber security investment

Source: self-created based on data collection from (Bodin et al., 2005; Rowe & Gallaher, 2006)

As all other infrastructure investment create societal level benefits, the spillover impacts of cyber security investments are huge. Those benefits can be shared by a broad range of beneficiaries even spanning over the world. For example, infrastructure such as train rail and Internet network provide the opportunity to literally whole citizens to benefit from the services. For this characteristics, cyber security should be considered as public goods, and the cooperation with public sector can bring synergy effect. Table16 focuses on cost benefit elements generally involved in private companies' cyber security investment.

### 5.3. Completed cost-benefit framework: International development by public-private partnership to address cyber security

The elements of the tables (Table 14,15 and 16) have been assembled from the widely known cost-benefit elements of Global CSR, foreign aid program, foreign direct investment program and cyber security investment.

The international development program operated by public-private partnership can strengthen political linkages between donor countries and recipient countries, which can alleviate the hurdle of regulations to companies from the donor country. Also, technology transfer under countries' MOU can increase the knowledge sharing, which improve the employee skills and overall productivity. In the long-term, this technology will penetrate into recipient countries and most of companies in the industry will use it. This raised technical standardization will improve the overall quality of suppliers and guarantee the quality of products or services to community people. Newly created industry creates job opportunity. Cyber security as a border-less issue can be highly affected by the improved security of neighborhood countries.

Actors	Cost	Synergic benefits from partnership	Benefit	Indirect Benefit	Shared value
<b>Public agents</b>	<p><b>Cost</b> of implementing program human resource place to train</p> <p><b>Cost</b> related to tech-transfer of preventing tech spillover to rivals</p> <p>1.wage premium to prevent human resource from leaving</p> <p>2.secluded production site</p> <p><b>Cost</b> of communication to gain the justification of abroad</p>	<p>Partnering with private actors, <b>can leverage</b> resources, mobilize industry expertise and networks, and bring fresh ideas to development projects.</p> <p><b>can likely increase</b> the momentum of program; this is because private actors keep running their business and activities even after government aid has ended.</p>	<p>(country-level)</p> <p><b>Meeting</b> the political mandate for international development finance (organization level)</p> <p><b>Achieving</b> the large scale accomplishments</p>	<p><b>Strengthen</b> political linkages: those who have particular political linkages with recipient countries aim at reinforcing such ties</p> <p><b>Targeting</b> trading partners: all donors choose target countries which are the most significant trading partners (country-level)</p> <p><b>Raising</b> the international reputation among countries (organization-level)</p> <p><b>Raising</b> the likelihood of maintaining/ increasing annual budget</p>	<p><b>Strengthen</b> political linkages-&gt; better diplomatic relationship and better business environment such as trade conditions and more regulation information.</p> <p><b>Knowledge</b> sharing -&gt; improvement of employee skills and overall productivity</p> <p><b>Improve</b> supplier quality, the overall quality of life of community people</p> <p><b>Providing</b> job opportunity to community</p> <p><b>Providing</b> infrastructure and appropriate training</p> <p><b>Improving</b> international</p>
<b>Private companies</b>	<p>investment and to reach the agreement with collaborating</p>	<p>Partnering with a government agency <b>can access</b> to government</p>	<p><b>Entering</b> 3rd/emerging country market (under</p>	<p><b>Marketing</b> effect; community engagement &amp; -Reputation</p> <p><b>License</b> to operate (by</p>	

countries / recipient countries Same above	officials, credibility, and scale. Partnering with local organizations, government, and residents, <b>can create</b> a community-wide coalition focused on enhancing the local economy and the environment assisted by the most profound localized knowledge and support.	official/unofficial protection)	gaining governmental support) e.g. Google and Chinese government case <b>Sustainability</b> (by establishing stable & reliable market and operating environment including infrastructures) <b>Meeting</b> moral obligation (do the right things as community members)	security
---	---	---------------------------------	---	----------

*Table 17. Extended Cost-Benefit analysis framework specialized in International development programs by Public-Private partnership*

*Source: self-created based on literature review of*

(Alpar & Kim, 1990; Anderson & Moore, 2006; Barua et al., 1995; Berthélemy, 2006; Bodin et al., 2005; Das, 1987; Glass & Saggi, 2002; Habip et al., 2011; Lumsdaine, 1993; Mansfield & Romeo, 1980; Porter & Kramer, 2002, 2006)

## 5.4. Summary of Chapter 5

Both international activities and Cyber security area have intrinsic limitations that their benefits are largely distributed and the costs concentrated. Those underestimated benefits and cost burdens discourage the participation of private companies and weaken the justification of public sectors for launching international initiatives in the Cybersecurity area. **How can we assess the true benefits of cyber security considering spillover effects?** The diagram in the Figure 19 explains the benefits generated from the public projects of public-private partnership. The arrows marked number 3,4 and 5 are spillover effects and have been overlooked in the traditional assessment framework.

The newly extended framework includes three additional critical aspects, which are neglected in the conventional framework: 1) synergic effect (attained by public-private partnerships), 2) indirect impact (gained through long-term operations), and 3) shared value (benefits influencing participating actors, communities and countries). Its detailed elements collected from rigorous literature reviews are presented in Table 17.

## Chapter 6. Application to Korean CERT case

### 6.1.Verification through extended cost-benefit analysis

Actors	Cost	Synergic benefits from partnership	Benefit	Indirect Benefit	Shared value
<b>Korean CERT</b>	<ul style="list-style-type: none"> <li>-Cost of inviting government officers</li> <li>-Cost of running (training) programs</li> <li>-Developing Prototypes</li> <li>-Demonstration</li> </ul>	<ul style="list-style-type: none"> <li>-Enriched training session based on expert skill and materials from companies</li> </ul>	<ul style="list-style-type: none"> <li>-International relationship with other Asian CERT</li> </ul>	<ul style="list-style-type: none"> <li>-Raising national brand in South-Asia region consistent with IT-Korea image</li> <li>-International project accomplishment can strengthen the position in annual budgeting process</li> <li>-Spreading Korean model to neighboring countries can facilitate the communication with them based on the increased consistency of terminology and system</li> </ul>	<ul style="list-style-type: none"> <li>-Developed government to government relationship</li> <li>-Creating job opportunity (hiring both Malaysian and Korean engineers)</li> <li>-Improving Malaysian security and broadly Asian security</li> <li>-Facilitating emergency response capability based on improved communication</li> </ul>
<b>Winitech (Korean IT company)</b>		<ul style="list-style-type: none"> <li>-Easy to making contacts with Government officers (some of whom are bidding decision makers) and expose products to them</li> <li>-Basic market research data supported by Korean government</li> </ul>	<ul style="list-style-type: none"> <li>-Winning a procurement project</li> <li>-Entered Malaysian market</li> </ul>	<ul style="list-style-type: none"> <li>-Reputation as government project partner</li> <li>-Endorsement of Malaysian government</li> <li>-Increasing the moral of employee who are proud of improving national security and saving people from disaster and crisis</li> <li>-Sustainable momentum based on understanding of Malaysian market</li> </ul>	

Table 18. Interviewed costs and benefits of Korean CERT and IT company, Winitech

Source: self-created based on interviews

Both parties—public agency side, Korean CERT and private companies side, Winitech—agreed the strong synergistic effect from collaborating to prepare for training sessions. CERT could complement the expert skills and materials (such as Software, technical materials and experts who participated in the development of CERT system). This can improve the quality of training combined with practical training sessions. Private companies who supported training sessions emphasized the

importance of building first contact, Government references and Government-led events in that trust is one of the most important factor to win from the bidding, and training session can help companies to build trust on strong G2G (Government to Government) relationship. Winitech also pointed out that “Generally, government to government interaction and communication are more effective than companies’ marketing activity alone because people in government trust the reference, recommendation or introduction from government and both, as government officers of Korea and Malaysia, are speaking in same language based on common context (built on working for national security in government agencies).”

Also about the indirect benefit, Winitech interviewee (the entire interview script is attached in Appendix 2.3) emphasized during the interview on the importance of how the sense of achievement from doing good can change the company’s culture and can encourage people. The interviewee added comments on this that the more employees feel pride and meaning in their works, the more responsibility they are willing to take and the more productivity Winitech can achieve. (This productivity showed up as faster reaction to client’s requests). He also mentioned the indirect benefits of market expansion in emerging countries, not only Malaysia but also South-Asian regions mentioning that “Malaysian market as hub of South-east Asia and stepping stone to Middle East Arabic countries because of geographic location and cultural similarity. Infrastructure projects such as security and disaster control inherently need active international cooperation with neighbor countries; therefore, involving in Malaysian disaster management project can likely lead to the market expansion in neighboring countries such as Thailand, Brunei and Indonesia.”

## 6.2.Expected and Unexpected costs & benefits

Each organizations explained two types of costs and benefits: 1) expected costs and benefits (already expected at the stage of training program design) and 2) unexpected costs and benefits.

<b>Actors</b>	<b>Expected Cost</b>	<b>Unexpected Cost</b>	<b>Expected Benefit</b>	<b>Unexpected Benefit</b>
<b>Korean CERT</b>	-Training session preparation	-Negligible (10 years of experience in running the training session removes the uncertainty)	-Interaction with government officers from other Asian countries	-Korean IT companies’ success in market expansion (to some degree, it is expected) -Increased contribution and in international organization meetings

<b>Winitech (Korean IT company)</b>	-Training session preparation	-Marketing cost (prototyping and demo)	-Introduction of solutions and making contacts with government officers	-Moral motivation (proud of doing good) -Impact in Korean market
-------------------------------------	-------------------------------	--	---	---

Table 19. Expected and Unexpected costs & benefits  
Source: self-created based on interviews

Winitech noted in the interview about the high unexpected cost for marketing mentioning that “we rapidly prototyped and visually demonstrated it several times to help government officers understand what the disaster management/control system and how our solution can support it.” However, he mentioned that this early stage meetings, prototyping, and demonstration, although they were expensive, turned out effective investments to help Winitech win from the project bidding in spite of the competition with global IT companies such as IBM and HP. Unexpected benefits of collaborating with government agencies for international cooperation are identified as global market expansion. It seems obvious, but the created impact is stronger than its expectation. Winitech pointed out the impact of neighboring countries. “From experience, we learned that the systems installed in neighboring countries of similar economic and politic conditions are more benchmark-able than that of most advanced countries” said Winitech.

### 6.3. Visualization of different influence of cost & benefit elements

Actors	Cost	Synergic benefits from partnership	Benefit	Indirect Benefit	Shared value
<b>Public agents</b>	Cost of implementing program ↑	Partnering with private actors, <b>can leverage</b> resources, mobilize industry expertise and networks, and bring fresh ideas to development projects. ↑	<b>Meeting</b> the political mandate for international development finance ↑	<b>Strengthen</b> political linkages: those who have particular political linkages with recipient countries aim at reinforcing such ties ↑	<b>Strengthen</b> political linkages-> better diplomatic relationship and better business environment such as trade conditions and more regulation information. ↑
				<b>Targeting</b> trading partners: all donors choose target countries which are the most significant trading partners ↑	<b>Knowledge</b> sharing -> improvement of employee skills and overall productivity ↑

	<b>Cost</b> related to tech-transfer 1.wage premium	○	<b>increase</b> the momentum of program	↑	<b>Achieving</b> the larger scale accomplishments	↑	<b>Raising</b> the international reputation among countries <b>Raising</b> the likelihood of maintaining/increasing annual budget	○	<b>Improve</b> supplier quality, the overall quality of life of community people <b>Improving</b> international security	○
<b>Private companies</b>	2.secluded production site	↓	Partnering with a government agency <b>can access</b> to government officials, credibility, and scale.	↑	<b>Entering</b> 3rd/emerging country market	↑	<b>Marketing</b> effect	↑	<b>Providing</b> infrastructure and appropriate training	○
							<b>License</b> to operate	○		
	<b>Cost</b> of communication to gain the justification	↓	Partnering with local organizations, government, and residents, <b>can create</b> a community-wide coalition focused on enhancing the local economy and the environment assisted by the most profound localized knowledge and support.	○			<b>Sustainability</b>	↑	<b>Providing</b> job opportunity to community	↑
							<b>Meeting</b> moral obligation	↑		

Table 20. Visualization of different influence of cost & benefit elements in program assessment and decision making (↑:Strong ↓:Weak ○:Medium)

Source: self-created based on interviews

Each cost and benefits are differently taken in account with different weights in evaluating its effectiveness and making decisions. Synthesizing its different influence of elements into the extended cost-benefit analysis table, the table above visualizes two actors' cost and benefit elements.

The study found that public and private agents cooperated from the stage of designing training sessions, of which, Winitech focused on the explanation of technical aspects of how to install system,. The bolded box of cost and shared value in Table20 means that both entities (public and private) are sharing cost and shared value.



## **Chapter 7. Conclusion**

### **7.1. Summary**

The technology and cybersecurity landscapes change quickly. To protect country, business and citizen from the threat to cybersecurity, diverse solutions have been discussed and different actors have searched for their roles. While we are still facing the absence of institutionalized system and solutions to address cybersecurity issues, this report has assessed the effectiveness of international development activities and public-private partnership. To do this, the paper suggested an extended cost-benefit analysis framework.

The cost-benefit analysis framework in this paper has been assembled by the elements of frameworks used cybersecurity investment, foreign direct investment and corporate strategic philanthropy. This extended framework is based on literature reviews, and extended by adding to it 1) the synergic effect of public-private partnership, 2) indirect impact, and 3) shared value.

In Korea, this framework was applied to show that private companies could benefit from participating in government-led international development programs; according to Porter, strategic philanthropy can increase its business. The companies might create more values aligned with their business bottom line by participating in training programs from the earlier stages such as program design stage. In addition, governments could generate sustainable momentum after the program ends because private companies would keep running their business in cybersecurity sectors in developing countries. Expert resources and experience from private sector could reinforce the effectiveness of program. Secondly, the application of the framework to Korean case also show the potential that international development activities can improve global and local cybersecurity. After the training session for developing countries, and with the increased number of CERT installation in some of the countries, the number of related attacks notably decreased.

### **7.2. Limitations & Further Works**

First, the public and private sectors can use Porter's framework to design their strategic philanthropy. This research uses that framework to validate the legitimacy of international development programs, used to address cybersecurity issues. With the lack of time and resources to understand Porter's framework enough to apply it to political programs, this paper is leaving this for future research. Further research can try to address whether this framework can be applied to other public

organizations dealing with international development/cooperation issues, and if so, how it should be modified.

Second, the improvement of cybersecurity in Korea can be quantified by observing quantifiable factors such as the number of cyber-attack on Korea from neighboring countries. For the reliable observations, the experiment environment should be controlled during the observation from the beginning of international initiatives. As alternative experiment, by observing cybersecurity exercises/drills with neighboring countries, we will be able to collect interesting information to prove and measure the improvement of overall cyber security in Korea and the decrease of the threat from neighboring countries.

Third, suggesting international development programs as a potential solution to international cybersecurity problems, other solutions had not been meticulously considered and evaluated. To interpret the effectiveness of the cost-benefit analysis framework, into indicators to identify the most effective programs, the results should be analyzed alongside those of other programs.

### **7.3. Policy Recommendations**

Given their limited resources, organizations should optimize their operations by choosing the most effective solutions. Decisions, either for policy or business, need to prove that the decisions are correct. The benefits of international activities in cybersecurity have traditionally been underestimated because those activities bring not only benefits as public goods but also benefits as global entity; those benefits are broadly distributed. By discovering overlooked benefits and shared value of public agents and private companies, we can convince more organizations to participate in cybersecurity, not only by benefiting participants but also by creating greater shared values all over the world.

The paper proposes two recommendations that are of interest to developed countries with well-funded CERTs and competitive IT industry:

The first recommendation is that when designing international development programs to address global issues, Porter's strategic philanthropy framework makes it possible to identify combined benefits, which can occur from the project and persuade and involve private companies.

The second recommendation is that when the effectiveness of the projects is assessed, extended cost-benefit analysis framework can prevent spillover benefits from being overlooked and include collective benefits from partnership.

From the international development program of public-private partnership, three benefits can be expected: sustainable momentum, expertise, and increased engagements of diverse actors and scope of impact.

Public agents can benefit from the participation of private agents by acquiring financial and human resources from the private sector. In addition, the programs can be more sustainable. Private companies have more incentive to keep running the initiatives, once those activities are connected to their business.

Private agents can access emerging markets under governmental support by navigating complicated regulations and laws pertaining to activities in third countries. In partnership with local organizations, government, and citizens, the private companies in the partnership can greatly benefit from the creation of a community-wide coalition focused on enhancing the local economy and the environment (Porter & Kramer, 2002).

## **7.4. Conclusion**

Cybersecurity should not be overlooked. One newspaper took the words from The Desk of President Obama (A look into the cybersecurity legislation: What does it mean for citizens?, 2012):

We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control... But just as we failed in the past to invest in our physical infrastructure – our roads, our bridges and rails – we’ve failed to invest in the security of our digital infrastructure... This status quo is no longer acceptable – not when there’s so much at stake. We can and we must do better.

With diverse stakeholders involved and borderless impact covered, more research should identify solutions for these unprecedented problems.

## Reference

- A look into the cyber security legislation: What does it mean for citizens? (2012, avril 7). *Boston Information Security*. Consulté avril 9, 2012, de <http://www.examiner.com/information-security-in-boston/a-look-into-the-cyber-security-legislation-what-does-it-mean-for-citizens>
- Ackerman, F., & Heinzerling, L. (2001). Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection. *University of Pennsylvania Law Review*, 150, 1553.
- Alesina, A., & Dollar, D. (2000). Who gives foreign aid to whom and why? *Journal of economic growth*, 5(1), 33–63.
- Alpar, P., & Kim, M. (1990). A Microeconomic Approach to the Measurement of Information Technology Value. *Journal of Management Information Systems*, 7(2), 55-69.
- Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610.
- Barua, A., Kriebel, C. H., & Mukhopadhyay, T. (1995). Information Technologies and Business Value: An Analytic and Empirical Investigation. *Information Systems Research*, 6(1), 3 -23.  
doi:10.1287/isre.6.1.3
- Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10–11), 706-719.  
doi:10.1016/j.telpol.2009.09.001
- Berthélemy, J. C. (2006). Bilateral donors' interest vs. recipients' development motives in aid allocation: do all donors behave the same? *Review of Development Economics*, 10(2), 179–194.
- Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2), 78–83.
- Brent, R. J. (2006). *Applied cost-benefit analysis*. Edward Elgar Publishing.
- Brynjolfsson, E., & Hitt, L. (1996). Paradox Lost? Firm-Level Evidence on the Returns to Information Systems Spending. *Management Science*, 42(4), 541 -558. doi:10.1287/mnsc.42.4.541

- Burke, L., & Logsdon, J. M. (1996). How corporate social responsibility pays off. *Long Range Planning*, 29(4), 495 - 502. doi:10.1016/0024-6301(96)00041-6
- Calabrese, D. (2008). *Strategic communication for privatization, public-private partnerships, and private participation in infrastructure projects*. World Bank Publications.
- Chai Lee Goi, & Kah Hian Yong. (2009). Contribution of Public Relations (PR) to Corporate Social Responsibility (CSR): A Review on Malaysia Perspective. *International Journal of Marketing Studies*, 1(2), 46-49.
- Chatterji, A. K., Levine, D. I., & Toffel, M. W. (2009). How Well Do Social Ratings Actually Measure Corporate Social Responsibility? *Journal of Economics & Management Strategy*, 18(1), 125-169. doi:10.1111/j.1530-9134.2009.00210.x
- Chong, A., & Gradstein, M. (2008). What determines foreign aid? The donors' perspective. *Journal of Development Economics*, 87(1), 1–13.
- Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It* (First Edition.). Ecco.
- Clinch, J. P., & Healy, J. D. (2000). Cost-benefit analysis of domestic energy efficiency. *Energy Policy*, 29(2), 113-124. doi:10.1016/S0301-4215(00)00110-5
- Das, S. (1987). Externalities, and technology transfer through multinational corporations A theoretical analysis. *Journal of International Economics*, 22(1-2), 171–182.
- Dobers, P., & Halme, M. (2009). Corporate social responsibility and developing countries. *Corporate Social Responsibility and Environmental Management*, 16(5), 237-249. doi:10.1002/csr.212
- DOD Funds New Views on Conflict With Its First Minerva Grants. (2009, janvier 30).AAAS.
- Eckstein, O. (1965). *Water-resource development: the economics of project evaluation*. Harvard University Press.

- Elvik, R. (2001). Cost–benefit analysis of road safety measures: applicability and controversies. *Accident Analysis & Prevention*, 33(1), 9-17. doi:10.1016/S0001-4575(00)00010-5
- Ferwerda, J., Choucri, N., & Madnick, S. (2010, septembre). Institutional Foundations for Cyber Security: Current Responses and New Challenges. Composite Information Systems Laboratory (CISL), Sloan School of Management.
- FIRST.org / FIRST Members. (2011). Consulté avril 2, 2012, de <http://www.first.org/members/teams>
- FIRST.org / History. (2011). Consulté avril 2, 2012, de <http://www.first.org/about/history>
- Gercke, M. (2009). Understanding Cybercrime. A Guide for Developing Countries. *International Telecommunication Union (Draft)*, 89–93.
- Glass, A. J., & Saggi, K. (2002). Multinational firms and technology transfer. *The Scandinavian Journal of Economics*, 104(4), 495–513.
- Greengard, S. (2012). Law and disorder. *Commun. ACM*, 55(1), 23–25. doi:10.1145/2063176.2063184
- Habip, A., Pigdon, J., Galante, J. M., Green, C. H., Holowicki, E., Gouillart, F., & Porter, M. E. (2011, avril). Creating Shared Value: Interaction. Harvard Business School Publication Corp.
- Hanley, N., & Spash, C. L. (1995). *Cost-Benefit Analysis and the Environment*. Edward Elgar Pub.
- Jorge, J.-D., & de Rus, G. (2004). Cost–benefit analysis of investments in airport infrastructure: a practical approach. *Journal of Air Transport Management*, 10(5), 311-326. doi:10.1016/j.jairtraman.2004.05.001
- Kaul, I., Grunberg, I., & Stern, M. A. (1999). Global public goods. *UNDP*, 450.
- Kim, S., & Lee, H. J. (2005). Cost-Benefit Analysis of Security Investments: Methodology and Case Study. In O. Gervasi, M. L. Gavrilova, V. Kumar, A. Laganà, H. P. Lee, Y. Mun, D. Taniar, et al. (Éd.), *Computational Science and Its Applications – ICCSA 2005* (Vol. 3482, p. 1239-1248). Berlin, Heidelberg: Springer Berlin Heidelberg. Consulté de <http://www.springerlink.com.libproxy.mit.edu/content/wlj3ge20ytgmmf6t/>

- Korea Internet Security Agency. (2012). Consulté avril 2, 2012, de <http://www.kisa.or.kr/eng/main.jsp>
- KrCERT/CC. (2012). Consulté avril 2, 2012, de [http://www.krcert.or.kr/english\\_www/](http://www.krcert.or.kr/english_www/)
- Krutilla, J. V., & Eckstein, O. (1958). *Multiple Purpose River Development: Studies in Applied Economic Analysis* (Reprint.). RFF Press.
- Lancaster, C. (1999). *Aid to Africa: So much to do, so little done*. University of Chicago Press.
- Lumsdaine, D. H. (1993). *Moral vision in international politics: the foreign aid regime, 1949-1989*. Princeton Univ Pr.
- Maas, K., & Liket, K. (2011). Talk the Walk: Measuring the Impact of Strategic Philanthropy. *Journal of Business Ethics*, 100(3), 445-464. doi:10.1007/s10551-010-0690-z
- Madnick, S., Choucri, N., Camina, S., Fogg, E., Li, X., & Fan, W. (2009). Explorations in Cyber International Relations (ECIR) - Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System. *SSRN eLibrary*. Consulté de [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1477618](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1477618)
- Madnick, S., Xitong, L., & Choucri, N. (2009, septembre). Experiences and Challenges with using CERT Data to Analyze International Cyber Security. Composite Information Systems Laboratory (CISL), MIT Sloan School of Management.
- Mahmood, M. A., & Mann, G. J. (1993). Measuring the Organizational Impact of Information Technology Investment: An Exploratory Study. *Journal of Management Information Systems*, 10(1), 97-122.
- Mansfield, E., & Romeo, A. (1980). Technology transfer to overseas subsidiaries by US-based firms. *The Quarterly Journal of Economics*, 95(4), 737.
- Marian Leonardo Lawson. (2011, juin 13). Foreign Assistance: Public-Private Partnerships (PPPs). Consulté de <http://www.fas.org/sgp/crs/row/R41880.pdf>



- McKean, R. N. (1958). *Efficiency in government through systems analysis: with emphasis on water resources development*. Wiley.
- McWilliams, A., Siegel, D. S., & Wright, P. M. (2006). Corporate Social Responsibility: Strategic Implications. *Journal of Management Studies*, 43(1), 1-18. doi:10.1111/j.1467-6486.2006.00580.x
- Mishan, E. J., & Quah, E. (2007). *Cost-benefit analysis*. Psychology Press.
- Mitra, S., & Chaya, A. K. (1996). Analyzing cost-effectiveness of organizations: the impact of information technology spending. *J. Manage. Inf. Syst.*, 13(2), 29–57.
- National Safety Council. (2000). Estimating the Costs of Unintentional Injuries. Consulté mai 2, 2012, de [http://www.nsc.org/news\\_resources/injury\\_and\\_death\\_statistics/Pages/EstimatingtheCostsofUnintentionalInjuries.aspx](http://www.nsc.org/news_resources/injury_and_death_statistics/Pages/EstimatingtheCostsofUnintentionalInjuries.aspx)
- Porter, M. E., & Kramer, M. R. (2002). The Competitive Advantage of Corporate Philanthropy. *Harvard Business Review*, 80(12), 56-69.
- Porter, M. E., & Kramer, M. R. (2006). Strategy & Society: The Link Between Competitive Advantage and Corporate Social Responsibility. *Harvard Business Review*, 84(12), 78-92.
- Porter, M. E., & Kramer, M. R. (2011). CREATING SHARED VALUE. *Harvard Business Review*, 89(1/2), 62-77.
- Prowse, M. (2009). Aid effectiveness: the role of qualitative research in impact evaluation.
- Rai, A., Patnayakuni, R., & Patnayakuni, N. (1997). Technology investment and business performance. *Commun. ACM*, 40(7), 89–97. doi:10.1145/256175.256191
- Rowe, B. R., & Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis \*. Consulté de <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.78.1588>

Squire, L., Tak, H. G., & Bank, W. (1976). *Economic analysis of projects*. World Bank Publications.

Stolfo, S. J., Wei Fan, Wenke Lee, Prodromidis, A., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: results from the JAM project. *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings* (Vol. 2, p. 130-144 vol.2).

Présenté à DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings, IEEE. doi:10.1109/DISCEX.2000.821515

Warner, K. E. (1982). *Cost-Benefit and Cost-Effectiveness Analysis in Health Care: Principles, Practice, and Potential*. Health Administration Pr.

Wei, H., Frinke, D., Carter, O., & Ritter, C. (2001). Cost-Benefit Analysis for Network Intrusion Detection Systems. Consulté de <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.5607>

Weimer, D., & Vining, A. R. (2004). *Policy Analysis: Concepts and Practice* (4<sup>e</sup> éd.). Prentice Hall.

Wikipedia contributors. (2012, avril 30). Denial-of-service attack. *Wikipedia, the free encyclopedia*. Wikimedia Foundation, Inc. Consulté de [http://en.wikipedia.org/w/index.php?title=Denial-of-service\\_attack&oldid=489748107](http://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=489748107)

Winitech/About. (2012). Consulté avril 2, 2012, de <http://www.winitech.com/Eng/>

Winitech/NewsRoom. (2012). Consulté avril 7, 2012, de [http://www.winitech.com/bbs/bbs\\_list.jsp?b\\_id=news\\_en](http://www.winitech.com/bbs/bbs_list.jsp?b_id=news_en)



# Appendix

## Appendix 1. Supplementary Description on 2009 Korea DDoS attack

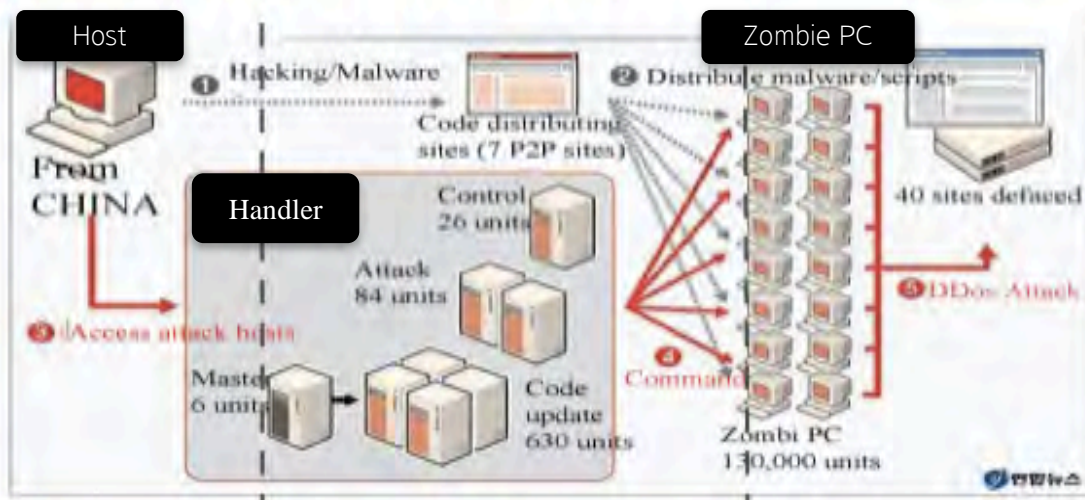
### Box. The Technical Description of DDoS and July 2009 Crisis in Korea

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, a hacker (or, if you prefer, cracker) begins by exploiting a vulnerability in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple -- sometimes thousands of -- compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service.

The July 2009 cyber attacks were a series of coordinated cyber attacks against major government, South Korea and United States. Hackers in China, whose computer is called *host* in the figure, began the attack process by infecting agents/zombie PC through seven P2P sites or 746 handlers. Handlers, directly infected by host and operational arms of host to accelerate the infection, deliver malwares and bots to other computers, which become zombie PC, and control infected zombie PCs. With the existence of handlers, the scope of infection can be broader than a host tries to infect PCs and the attack can be distributed. In Korean case, the number of zombie pc recorded 130,000, the origins of which were identified 72 countries.

### July 2009 cyber attacks in Korea



## Appendix 2. Interview Notes and Scripts

### 2.1. Interviews of cyber security related government agencies in Korea

#### Interviews of Cyber security related government agencies in South Korea

Yiseul Cho ([Yiseul@mit.edu](mailto:Yiseul@mit.edu))

May 13, 2011

- 4/18-4/21
  - Introduction of our projects on the phone with the director of monitoring & emergent reaction team
  - Talk with researchers for our Explorations in Cyber International Relations (ECIR) Data Dashboard Report #1 Korean related question (Korea has a much lower rate of piracy per computer than the US)
  - No conclusion yet, but make an another appointment of talking with another relevant expert
- 4/25-4/29
  - Talk with Taekyu Shin in CERT
    - Questions in email are internally being discussed and relevant data being collected. ([+82-2-405-5620/tkshin@kisa.or.kr](mailto:+82-2-405-5620/tkshin@kisa.or.kr))
  - Talk with Eungjae Lee in National Internet Development Agency of Korea; (+82-2-405-6730)
    - Regarding the question, why Korea shows lower software piracy losses compared to other countries, such as US, Germany, Malaysia, and China ,etc. , he was not surprised at the result. He rather supported it by providing examples such as strict Korean SW IP protection policy and government routinely investigation that exposes pirated SW among installed SW in public agency
    - He also explained a SW that scans all installed SW and tell whether the scanned computer includes pirated SW or not.

- He commented that public data is likely to be gathered from public sector which has virtually the least motivation in using pirated SW and is being more strictly monitored compared to private sector and Home PC.
  - Talk with Hohyun Jung in Korean Copyright Commission (+82-2-2660-0143/[jhh@copyright.or.kr](mailto:jhh@copyright.or.kr))
    - Calculated statistical figures of damage dollar loss and piracy rate are sensitive to diplomatic relationships and can cause conflicts with US Chamber of Commerce or foreign SW companies. Therefore, figures can be inaccurate
    - Government-led SW piracy investigation systems in Korea
  - Talk with Yongbum Kwon in IDC Korea (+82-2-550-4323)
    - IDC's methodology to estimate Korean SW market size, which is a key variable in BSA's formula to calculate SW piracy rate and dollar loss
    - No relationship or collaboration with BSA, and only the IDC headquarter is involved with the BSA's study (I would like to talk with people in BSA and IDC USA to better understand their methodology beyond publicly open data on their websites)
  - Talk with Kibong Kang in Korea Software Property Right Council (+82-2-567-2567-503)
- 5/2-5/13
    - Follow-up calls to check whether the requested data collection is done or not.

## 2.2. Interview with Korean CERT

\*(Documentation formats:

#number. Questions

(clarifying points by posing questions)

{expected questions}

-> *actual response.*

)

### [Introduction]

1. What's your name and current role/position in CERT?



(When was the signing date of the MOU with MY-CERT?)

2. What was your role then?

3. Who were the principal researchers/players, who were involved in this MOU?

### **[Justification of international cooperation activities of CERT]**

1. What is the budget of CERT's international cooperation team (or activities)?

2. Is that relatively significant size of budget in CERT? (What is the most sizable task/project in CERT in terms of budget?)

(Decrease in budget and break-up of special task team for international cooperation.)

3. What was the behind story of those changes?

{because of the poor result on those tasks by cost-effectiveness analysis, critiques from politic examination or the pressure on those activities}

4. Along with those changes of budget & team break-up, have (has) you (CERT) experienced any overall changes in projects or in activities? (To verify whether its cutback was targeted only on international cooperation activities and teams)

{less active? less coherent activities}

5. Do you know that one of three missions of KR-CERT is international cooperation among CERTs?

Why? What's the behind story?

### **[Specialization of cyber security international cooperation task]**

1. What are their core competences to be assigned to international cooperation tasks?

2. Do you know that one of former employee of CERT left KR-CERT to start a company, a subcontractor of MY-CERT?

(What happened behind?)

3. Do you have any training program for cyber security international cooperation experts?

{No, learning over shoulder}

### **[Case related questions]**

1. How long have you worked/known MY-CERT people?

2. Do you think what was the first initiator of this MOU? {Training session/personal contact or relationships}
3. What were the criteria of the procurement process of this establishment?
4. Have you performed pre-analysis before initiating training programs for developing countries CERT officers? (to understand how they build up justification of international cooperation activities of CERT)

**[Effectiveness/impact analysis and follow-ups]**

(to understand that KR-CERT perceived those initiatives as success or not.)

1. Do you perform cost-benefit analysis on your organizations' tasks?
2. How's the relationship with MY-CERT nowadays?
3. Is there other procurement successful cases besides MY-CERT

### **2.3. Interviews with Winitech**

#### **Interview on cyber security, international development and the roles of private companies**

The emergence of internet has caused a variety of problems such as the infringement of intellectual property, the change of monetary transaction, the emergence of a new type of cyber crimes and the distribution of porno. Cyber security issues are emerging phenomena and borderless because of intrinsic characters of the Internet, connectivity. None of issues listed above can be effectively addressed by a country without international cooperation.

This research sees international development programs as a potential solution to address cyber security problems and focus on the roles of private companies and its impact on the planning and implementation of the development program. This interview is composed of questions related to private companies' participation in international development projects in cyber security area.

Your answers will be used only for research purpose. Thank you for taking your time on this interview.

April 2012

Researcher : Yiseul Cho, Graduate student at MIT (yiseul@mit.edu)

Research supervisor: Stuart Madnick, Professor of MIT Sloan school

Contact : +1-617-817-8752, e-mail: yiseul@mit.edu

### **1. Basic questions (e.g., Demographic questions)**

---

1.1. What is your name and role/position in Winitech?

Kukhee Han, Deputy chief of Winitech.

1.2. How long have you worked for Winitech?

6years

### **2. Questions on the training session program run by Korean Cyber Emergency Response Team (CERT).**

---

Brief introduction of Korean CERT led training session program: Since 2005, Korean CERT has run a cyber security training session targeting on cyber security experts from Asian developing countries, the training session, which is supported by UN Asia Pacific Information Security Center.

2.1. Do you know the training session run by Korean CERT? (1)

1) Yes

2) No

2.1.1 (In case of yes to the question 2.1) How do you know the session? (2), (3), (4)

1) I attended before

2) Winitech (or I) designed the training session

3) Winitech (or I) sponsored the program

4) Winitech (or I) know people from the Korean CERT and heard it from him/her

5) Other path (Please specify) \_\_\_\_\_

### **3. Questions on the procurement of installation of Malaysian security system project**

---

(Han): The project where Winitech is participating is a MKN-National Security Counsel lead project to build a national disaster/crisis management system.

3.1 When did Malaysian security system project start? Specific schedules (the first announcement about the procurement, starting date of signing date and starting date of installation)

(Han): This project launched as an official task in 2011 and will end in August 2012, and requires Winitech to serve 2 years of maintenance service. I have constantly worked for this project since 2009, 1.5 year before the official bidding announcement. This preparatory period of 1.5 year focused on networking, service demo, requirement discussion and negotiations, and site exploration and selection.

Preparatory period (1.5 years) -> Bidding announcement-> Bidding -> Official task launch (1-1.5 years)-> Maintenance (2 years)
--

3.2 Since when, have **you been involved in this project? At which stage?**

(Han): I have worked for this project since 2009, 1.5 year before the official bidding announcement in 2010. The stage that I joined was before the bidding announcement.

3.3 What is your role and position in this project and which roles have you assumed?

(Han): The entire project is composed mainly of four divisions: interior & building, infrastructure, operating system and storage system. Winitech is mostly working for operating system, and hardware and infrastructure are being progressed by local partner company, whose principal shareholders include Malaysian people. My jobs as project manager widely range from planning to software development, quality control and human resource management.

3.4 When did Winitech/you firstly heard about the Malaysia project?

(Han): There are various channels to meet government officers and learn government projects. Unofficially Winitech heard of it from local partner company and Korean government host training programs.

3.5 What was the motivation of Winitech participating in the procurement bidding process?

(Han): International project experience was the first motivation. Then working experience in Malaysia makes us envision market expansions in South-east Asian region. Winitech sees the Malaysian market

as hub of South-east Asia and stepping stone to Middle East Arabic countries because of geographic location and cultural similarity. Infrastructure projects such as security and disaster control inherently need active international cooperation with neighbor countries; therefore, involving in Malaysian disaster management project can likely lead to the market expansion in neighboring countries such as Thailand, Brunei and Indonesia. Also, from experience, it seems that the systems installed in neighboring countries of similar economic and politic conditions are more benchmark-able than that of most advanced countries.

3.6 Generally, what kinds of marketing activities are done by bidding participators to win projects?

What activities did Winitech focus on?

(Han): Winitech tried to have contact points and conversations as much as possible by asking Korean government send reference letters, meeting government officers in Korean government lead events and networking with local IT companies. Based on this meetings, we rapidly prototyped and visually demonstrated it several times to help government officers understand what the disaster management/control system and how our solution can support it.

3.7 What do you think of successful factors for Winitech to win the project?

(Han): Aggressive marketing activities, high reputation of Korean e-government system (OECD index) and governmental support. Different from global companies such as IBM and HP, Winitech, a small to medium size company, invests more resource to a single project in customizing solution to requests. Global companies tend to prefer more generic projects to minimize the cost of R&D and customization avoiding prototyping and demo for small project.

3.8 What is the current stage of project?

(Han): In progress of building system in coordination with local partners.

#### **4. Questions on the competitiveness of Korean IT companies in Malaysian security industry**

---

4.1 Do you know other Korean IT companies running their business in Malaysia?

(specific questions:)

(Han): No. Not yet.

4.1.1 how many companies are actively working for Malaysian government project?

4.1.2 What are the name of the companies?

4.1.3 Is any of the companies working for cyber security project?

4.2 What do you think of the competitiveness of Korean IT companies in Malaysia market? (1)

1) Strong

2) Neutral

3) Weak

4.3 Do you know what the initial motivation/opportunities for the companies to enter Malaysian market?

Answered in the question 3.5

## 5. Questions on the competitiveness of Winitech in Malaysia market

---

4.2 What do you think of the competitiveness of Winitech in Malaysia market? (2)

1) Strong

2) Neutral

3) Weak

5.2 Has Winitech made other following contracts after Winitech started working for the current project?

(Han): not yet. Preparing for a project. (Specific information is disclosed at present)

5.3 If you made a contract(s), what do you think of successful factors to win the contract(s)?

N/A

5.4 Has Malaysian government support Winitech in any ways to facilitate Winitech's abroad operation in Malaysia?

(Han): Yes. Generally, government to government interaction and communication are more effective than companies' marketing activity alone because people in government trust the reference, recommendation or introduction from government and both, as government officers of Korea and Malaysia, are speaking in same language based on common context (built on working for national security in government agencies). Korean government hosting events such as expert visits and consulting programs helped us make an initial contact with Malaysian government officers; which ultimately lead to the introduction of Winitech solution.

5.5 Do you think that the record as the partner of Malaysian government influence image/impression of Winitech in Malaysian market?

(Han): Yes. The reputation as a government project operator reduces the concern of uncertainty on solution and company; which lowers the barrier of making first contacts with potential customers. In addition, we benefit more from Korean market after performing international projects, which prove

5.6 Has Winitech participated in other projects of Asian countries? Does Winitech aim to participate in the projects? If so, why?

(Han): Yes. In addition to the benefit explained before, Government projects are attractive to IT companies not taking risk of unexpected project termination and nonpayment.

5.7 What are the main change in relationship with local communities ?

(Han): Hiring local people, required for running sustainable business and meeting regulations, is planned. With the company growing, we could also hire engineers in Korea.

**\*\*\* Thank you for the participation!**



### Appendix 3. Cyber security Dashboard

This research has been performed under Exploration in Cyber International Relations (ECIR) project. Aiming to create a field of international cyber relations for the 21st century, ECIR project is a multidisciplinary project by integrating social sciences, legal studies, computer science, and policy analysis and bringing various personnel from MIT and Harvard. The team includes foreign policy and national intelligence heavy-weights such as Harvard University's Ashton Carter and Joseph Nye, as well as Internet and artificial intelligence gurus such as MIT's David Clark (« DOD Funds New Views on Conflict With Its First Minerva Grants », 2009).

ECIR brings together scientists who haven't had a chance to work on a problem of mutual interest and allow small interdisciplinary groups to expand their activities. To share diverse data and views, effective data share tools are necessary. The cyber security dashboard (<http://coin.mit.edu:8080/Dashboard>), which our research team built, helps to visualize 25 cyber related data (e.g., cyber attacks, number of servers, population) for 17 countries around the world for 10 years of 2000-2010. The dashboard supports simple arithmetic calculations on data and enables the exploration of correlations among diverse factors, thereby facilitating the quantitative understanding of cyberspace. In addition, it collects cyber related data of 17 countries, which can support comparative studies to identify the most effective policy models and develop cybersecurity international standards. Figure 20, 21 and 22 respectively demonstrate 1) how to control input data, 2) how the result will be presented and 3) how the used data and its provenance will be presented.



# MRI Topic 5: ECIR - Explorations in Cyber International Relations DATA DASHBOARD



User Name: ys Login Role: admin Version 3.1  
>> Please set what chart you want to display in the dashboard...

**Choose one or more countries/regions**

- World
- Asia
- China
- India
- Japan
- Malaysia
- Pakistan
- Republic of Korea
- Taiwan
- UAE

**X-Axis: select the observation period**

Start Year: 2000  
End Year: 2009

[Click here for Info on Data Sources](#)  
[Click here for Info on Data Availability](#)

**Y-Axis: select attribute to be observed**

Attribute 1: Total CERT Reported Incidents  
Operator: Divided By  
Attribute 2: Population

Y-Axis Style:  Linear  Logarithmic

[Instruction of Cyber Data Dashboard](#)

Provenance Data:  On  Off [Click Here to Show Chart](#) [Reset](#) [Cancel](#)

Figure 20. Data input table of Dashboard (three variables, country, period and normalization attribute can be controlled)

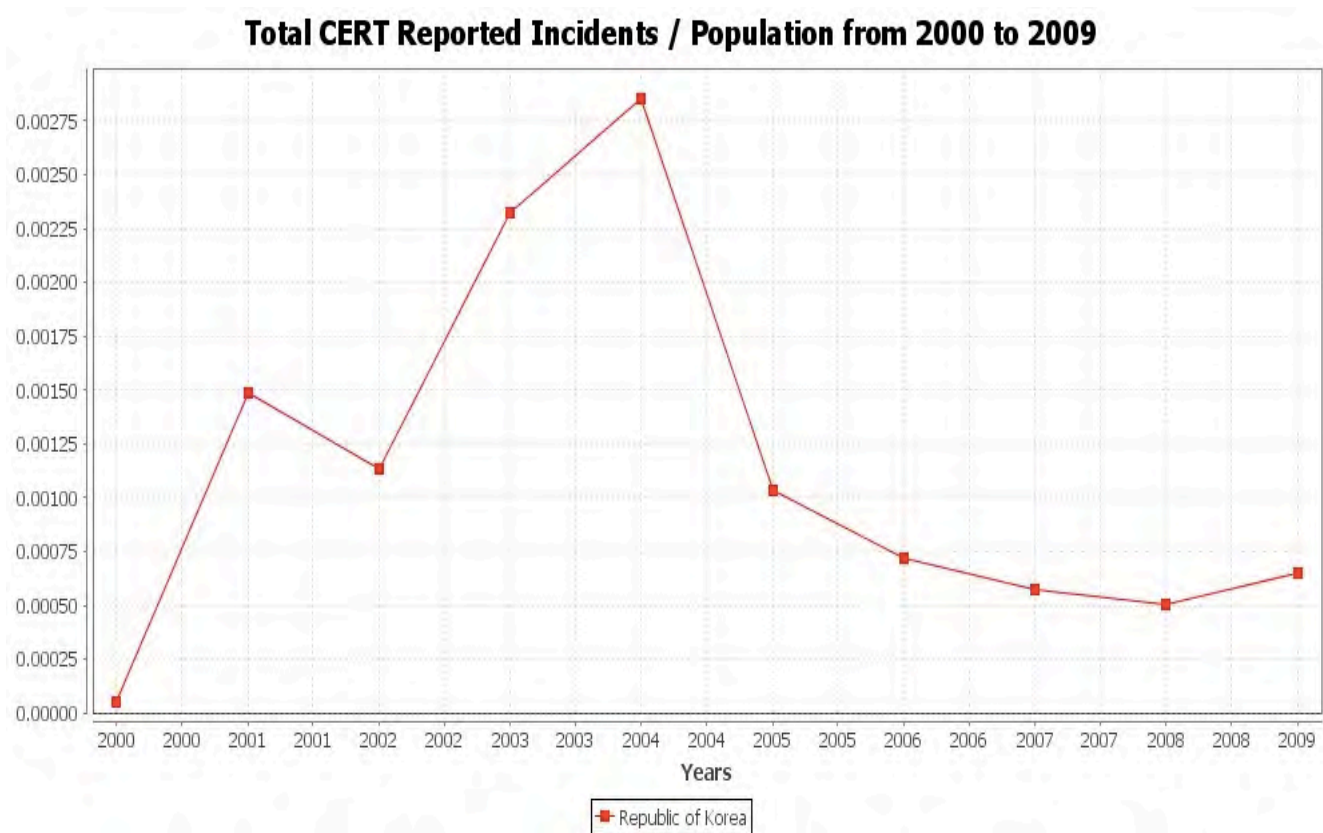


Figure 21. Visualized chart of Total CERT reported incidents divided by population in Korea from 2000 to 2009

Country/Region	Data	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Republic of Korea	Total CERT Reported Incidents / Population	5.4E-5	0.001486	0.001131	0.002324	0.002854	0.001033	7.16E-4	5.72E-4	5.02E-4	6.49E-4
>>OPERANDS in Total CERT Reported Incidents / Population											
Country/Region	Data	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Republic of Korea	Total CERT Reported Incidents	2515.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	70366.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	53869.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	111202.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	137103.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	49726.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	34597.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	27728.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	24409.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>	31625.0 <a href="#">Current Data</a> <a href="#">Saved Data</a>
	Updated	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM	Apr 1,011,:22AM
	Data Collector	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul
Country/Region	Data	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Republic of Korea	Population	4.7008E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.7357E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.7622E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.7859E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8039E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8138E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8297E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8456E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8607E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>	4.8747E7 <a href="#">Current Data</a> <a href="#">Saved Data</a>
	Updated	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM	January 02,2011,10:09:23PM
	Data Collector	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul	yiseul

Figure 22 Yearly Data and its provenance

### 3.1. Data source description (March 25, 2011)

#### 1) Population, Total (Unit: Person)

##### 1. Description

Total population is based on the de facto definition of population, which counts all residents regardless of legal status or citizenship--except for refugees not permanently settled in the country of asylum, who are generally considered part of the population of their country of origin. The values shown are midyear estimates.

##### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of "World Development Indicators" from a list of data sets, and this Database return you data after typing targeted countries, data and time.

#### 2) GDP (Unit: constant 2000 US\$)

##### 1. Description

GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in constant 2000 U.S. dollars. Dollar figures for GDP are converted from domestic currencies using 2000 official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

##### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of "World Development Indicators" from a list of data sets, and this Database return you data after typing targeted countries, data and time.

#### 3) Electric power consumption (kWh)

#### 1. Description

Electric power consumption measures the production of power plants and combined heat and power plants less transmission, distribution, and transformation losses and own use by heat and power plants.

#### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of “World Development Indicators” from a list of data sets, and this Database return you data after typing targeted countries, data and time. In the case that some data are not available, its original source is International Energy Agency (IEA Statistics © OECD/IEA, <http://www.iea.org/stats/index.asp>), Energy Statistics and Balances of Non-OECD Countries and Energy Statistics of OECD Countries.

### **4) Software Piracy Losses (\$M)**

#### 1. Description

The commercial value of unlicensed software is the value of unlicensed software as if it had been sold in the market: the formula is: ( # Unlicensed software Units) x (average system Price).

The average system price is obtained by multiplying a country-specific matrix of software prices — retail, volume license, OEM, free/open source, etc. — by a matrix of products, including security, office automation, operating systems and more.

The number of unlicensed software units is the difference between the total number of software units (total number of PC’s multiplied by the average number of software units on a PC) and the total number of legitimate software units (software Market \$ Value divided by Units average system Price). Most of the data comes from IDC surveys and local analysts. A video presentation of the methodology is available at [www.bsa.org/globalstudy](http://www.bsa.org/globalstudy).

#### 2. Source

BSA & IDC Global Software Piracy Study (Table 3: Pc software Piracy Rates and commercial Value of Unlicensed software). This is the link for the seventh annual study

[http://portal.bsa.org/globalpiracy2009/studies/09\\_Piracy\\_Study\\_Report\\_A4\\_final\\_111010.pdf](http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf)

### **5) School enrollment, tertiary (% gross)**

#### 1. Description

Gross enrollment ratio is the ratio of total enrollment, regardless of age, to the population of the age group that officially corresponds to the level of education shown. Tertiary education, whether or not to an advanced research qualification, normally requires, as a minimum condition of admission, the successful completion of education at the secondary level.

#### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of “World Development Indicators” from a list of data sets, and this Database return you data after typing targeted countries, data and time. In case that this data is not accessible, its source is United Nations Educational, Scientific, and Cultural Organization (UNESCO) Institute for Statistics. (Data label is ‘Gross enrolment ratio. ISCED 5 and 6. Total’)

### **6) # Personal Computers**

#### 1. Description

Personal computers are self-contained computers designed to be used by a single individual. The World Bank raw data is in computers per 100 people, so the calculation that I use is  $\text{Population}(\text{worldbank}) * \text{RawData}(\text{worldbank}) / 100$ .

## 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of “World Development Indicators” from a list of data sets, and this Database return you data after typing targeted countries, data and time. In case this data is not accessible on the World Bank website, its sources are International Telecommunication Union, World Telecommunication Development Report and database, and World Bank estimates.

## 7) International Bandwidth (MB/s)

### 1. Description

International internet bandwidth is the contracted capacity of international connections between countries for transmitting internet traffic. The World Bank raw data is in bits per person, so the calculation that I use is  $\text{Population}(\text{worldbank}) * \text{RawData}(\text{worldbank}) / 1000000$ .

### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>), but currently World Bank stops providing data sets. Therefore, original data for International Bandwidth is not accessible at present time.

If World Bank republishes this dataset, data can be accessed from databank of “World Development Indicators.” This Database returns you data values after typing targeted countries, data and time. In case that this data is not accessible on the World Bank website, its sources are International Telecommunication Union, World Telecommunication Development Report and database, and World Bank estimates.

## 8) # Users w/ Internet Access

### 1. Description

Internet users are people who have access to the worldwide network.

### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of “World Development Indicators” from a list of data sets, and this Database return you data after typing targeted countries, data and time.

## 9) # Secure Internet Servers

### 1. Description

Secure servers are servers using encryption technology in Internet transactions.

### 2. Source

World Development Indicators Database (<http://data.worldbank.org/data-catalog>)

Access databank of “World Development Indicators” from a list of data sets, and this Database return you data after typing targeted countries, data and time.

## 10) # Hosts

### 1. Description

An internet host is a computer connected directly to the internet; normally an Internet Service Provider’s (ISP) computer is a host. Internet users may use either a hard-wired terminal, at an institution with a mainframe computer connected directly to the internet, or may connect remotely by way of a modem via telephone line, cable, or satellite to the ISP’s host computer.

### 2. Source

Source is mainly based on CIA World Factbook. Access publication website of <https://www.cia.gov/library/publications/download/>, then open the pages of every year of Factbook(for the years of 2000-2009) and download Factbook.zip file. Downloaded annual Factbook file is archived

webpages for database in the year. Open index file then find Notes and Definition to look up "Internet Host."

\*The definitions for CERT-Computer emergency response team-variables (number 11 to 20) follow that of Brazilian CERT which currently (on March 10, 2011) reports the most relevant data in public.

### **11) Total CERT Reported Incidents**

#### 1. Description

Total number of reported incidents through the each country's own channels-online form, email, telephone, SMS, Fax-operated by CERT.

#### 2. Source

Described in the document, "Major countries' Computer Emergency Response team information."

### **12) Virus/worm/malicious code/malware**

#### 1. Description

Among total reported incidents, incidents using one of attack type-virus, worm, malicious code or malware-belong to this category, and are counted.

Virus/Worm: Virus and Worms are malicious programs or codes that are inserted into computer systems without the user's permission and operate without the user's knowledge. Unlike viruses, which cannot spread without human intervention, Worms spread automatically from computer to computer. Worms can replicate themselves and send out hundreds or even thousands of copies from each infected computer, tapping into the user's email addresses to spread the infection.<sup>10</sup>

Malicious code/Malware: Any codes or software programs developed for the purpose of doing harm to a computer system or create mischief. The most common are Viruses, Worms, and Spyware.<sup>11</sup>

#### 2. Source

Described in the document, "Major countries' Computer Emergency Response team information."

### **13) Defacement**

#### 1. Description

Among total reported incidents, incidents using defacement attack type belong to this category, and its reported cases are counted.

Defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.<sup>12</sup>

#### 2. Source

Described in the document, "Major countries' Computer Emergency Response team information."

### **14) Phishing/Personal data abuse**

#### 1. Description

---

<sup>10</sup>BSA Online Cyber Safety. Retrived from Cyber Safety Glossary web sites:

<http://www.bsacybersafety.com/threat/worms.cfm>

<sup>11</sup> BSA Online Cyber Safety. Retrived from Cyber Safety Glossary web sites:

<http://www.bsacybersafety.com/threat/malware.cfm>

<sup>12</sup> Wikipedia

[http://en.wikipedia.org/wiki/Website\\_defacement](http://en.wikipedia.org/wiki/Website_defacement)



Among total reported incidents, incidents using phishing attack type belong to this category, and its reported cases are counted.

Phishing also known as ‘Brand spoofing or Carding,’ refers to the process of imitating legitimate companies in emails or creating fake Web sites designed to look like a legitimate Web site in order to entice users to share their passwords, credit card numbers, and other personal information. The perpetrator then uses the information to steal the target's identity or to sell that identity to others. Users need to be educated not to give away personal information in response to an unsolicited email.<sup>13</sup>

#### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

### 15) Scanning

#### 1. Description

Among total reported incidents, incidents using scanning attack type belong to this category, and its reported cases are counted.

Scanning is notifications on computer networks, in order to identify which computers are active and which services are being provided for them. It is widely used by attackers to identify potential targets, because it allows potential vulnerabilities associated with the services enabled on a computer.<sup>14</sup>

#### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

### 16) DoS & Integrity Attacks

#### 1. Description

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service,
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.<sup>15</sup>

#### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

### 17) Total Cyber Crime Cases

#### 1. Description

Computer crime, or cybercrime, refers to any crime that involves a computer and a network. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.<sup>16</sup>

#### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

---

<sup>13</sup>BSA Online Cyber Safety. Retrived from Cyber Safety Glossary web sites:

<http://www.bsacybersafety.com/threat/phishing.cfm>

<sup>14</sup> Brazil national Computer Emergency Response Team. Retrieved from <http://www.cert.br/stats/incidentes/2010-jan-dec/total.html>

<sup>15</sup> CERT operated by Carnegie Mellon University. Retrieved from [http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html)

<sup>16</sup> Wikipedia. Retrieved from [http://en.wikipedia.org/wiki/Computer\\_crime](http://en.wikipedia.org/wiki/Computer_crime).



## 18) Cyber Crime Damage Dollar Loss (millions in \$)

### 1. Description

Self-reported or estimated damage directly caused by cyber crime, compiled by law enforcement agencies.

### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

## 19) Cyber Crime Arrests

### 1. Description

The annual records that cyber criminals are arrested.

### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

## 20) % Cyber Crimes Reported to Police

### 1. Description

### 2. Source

Described in the document, “Major countries’ Computer Emergency Response team information.”

## 21) Political Stability Index

### 1. Description

Political stability and absence of violence measures the perceptions of the likelihood that the government will be destabilized or overthrown by unconstitutional or violent means, including domestic violence and terrorism.

WGI project is based exclusively on subjective or perceptions-based measures of governance taken from surveys of households and firms as well as expert assessments produced by various organizations. An unobserved components model (UCM) is then used to generate the standard normal units of the governance indicator, ranging from around -2.5 to 2.5 (Higher numbers indicating better governance).

### 2. Source

World Bank Governance Indicators. Dataset available in Excel format at

<http://info.worldbank.org/governance/wgi/index.asp>

Please note that there are small changes in the WGIs’ data sources every year. Wherever possible those changes are made consistently for all years in the historical data as well, in order to ensure maximum over-time comparability in the WGI. “Users of the WGI should therefore be aware that each annual update of the WGI supersedes previous years’ versions of the data for the entire time period covered by the indicators”. So in case of any update of this index, all the old values should also be updated (or else, we would be limited to cross-country comparability only).

## 22) Government Effectiveness Index

### 1. Description

Government effectiveness captures perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.

WGI project is based exclusively on subjective or perceptions-based measures of governance taken from surveys of households and firms as well as expert assessments produced by various organizations. An unobserved components model (UCM) is then used to generate the standard normal units of the governance indicator, ranging from around -2.5 to 2.5 (Higher numbers indicating better governance).

### 2. Source

World Bank Governance Indicators. Dataset available in Excel format at

<http://info.worldbank.org/governance/wgi/index.asp>

Please note that there are small changes in the WGIs' data sources every year. Wherever possible those changes are made consistently for all years in the historical data as well, in order to ensure maximum over-time comparability in the WGI. "Users of the WGI should therefore be aware that each annual update of the WGI supersedes previous years' versions of the data for the entire time period covered by the indicators". So in case of any update of this index, all the old values should also be updated (or else, we would be limited to cross-country comparability only).

### 23) Rule of Law Index

#### 1. Description

Rule of law captures perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence.

WGI project is based exclusively on subjective or perceptions-based measures of governance taken from surveys of households and firms as well as expert assessments produced by various organizations. An unobserved components model (UCM) is then used to generate the standard normal units of the governance indicator, ranging from around -2.5 to 2.5 (Higher numbers indicating better governance).

#### 2. Source

World Bank Governance Indicators. Dataset available in Excel format at

<http://info.worldbank.org/governance/wgi/index.asp>

Please note that there are small changes in the WGIs' data sources every year. Wherever possible those changes are made consistently for all years in the historical data as well, in order to ensure maximum over-time comparability in the WGI. "Users of the WGI should therefore be aware that each annual update of the WGI supersedes previous years' versions of the data for the entire time period covered by the indicators". So in case of any update of this index, all the old values should also be updated (or else, we would be limited to cross-country comparability only).

### 24) Polity Index

#### 1. Description

The Polity Index of Democracy/Autocracy is a scale from -10 to +10 measuring the degree to which a nation is either autocratic or democratic. A score of +10 indicates a strongly democratic state; a score of -10 a strongly autocratic state. A fully democratic government has three essential elements: fully competitive political participation, institutionalized constraints on executive power, and guarantee of civil liberties to all citizens in their daily lives and in political participation. A fully autocratic system sharply restricts or suppresses competitive political participation. The chief executives are chosen by an elite group and exercise power with few institutionalized constraints. The Polity index is derived from sub-indices measuring competitiveness of political participation, the openness and competitiveness of executive recruitment, and the constraints on the chief executive.

#### 2. Source

Polity IV Project (Part of the Center for Systemic Peace). The Polity IV Excel time series can be found on the INSCR data page at <http://www.systemicpeace.org/inscr/inscr.htm>.

### 25) Militarization Index (2005) / Militarization Index (2008)

#### 1. Description

Country's military expenditure in US dollars (based on calendar year), at constant (2008 or 2005) prices and exchange rates. It is calculated on the assumption that, where financial years do not correspond to calendar years, spending is distributed evenly through the year

## 2. Source

Stockholm International Peace Research Institute (SIPRI). Dataset available in Excel format at <http://www.sipri.org/databases/milex> .

SIPRI military expenditure data is based on open sources only, including a SIPRI questionnaire which is sent out annually to all countries included in the database. The collected data is processed to achieve consistent time series which are, as far as possible, in accordance with the SIPRI definition of military expenditure. (More info at [http://www.sipri.org/databases/milex/sources\\_methods](http://www.sipri.org/databases/milex/sources_methods) )

## **26) Percentage of gross domestic product (GDP)**

### 1. Description

Country's military expenditure in US dollars as a percentage of GDP (based on calendar year), at constant (2008) prices and exchange rates. It is calculated on the assumption that, where financial years do not correspond to calendar years, spending is distributed evenly through the year

### 2. Source

Stockholm International Peace Research Institute (SIPRI). Dataset available in Excel format at <http://www.sipri.org/databases/milex> .

SIPRI military expenditure data is based on open sources only, including a SIPRI questionnaire which is sent out annually to all countries included in the database. The collected data is processed to achieve consistent time series which are, as far as possible, in accordance with the SIPRI definition of military expenditure. (More info at [http://www.sipri.org/databases/milex/sources\\_methods](http://www.sipri.org/databases/milex/sources_methods) )



### 3.2.How to access CERT data

#### How to access Country CERT(Computer Emergency Response Team) data

Last Updated : 03/17/2011  
 Author: Yiseul (Yiseul@mit.edu)

For the purpose of better understanding and using CERT data of Dashboard website, this paper explains 1) how to access actual data values—data stored in current Dashboard—from country CERT websites (Table 21) and provides 2) matching table to remove confusion possibly being caused when CERTs use different terminologies for the same concepts—eg. South Korea uses “Intrusion” and India uses “Network Scanning and probing” to mean “Scanning.” (Table 22)

	CERT Address (Eng)	CERT Address (Local)	Data provenance	How to access data from webpages(Left Third column)
<b>China</b>	<a href="http://www.cert.org.cn/english_web/overview.htm">http://www.cert.org.cn/english_web/overview.htm</a>	<a href="http://www.cert.org.cn/">http://www.cert.org.cn/</a>	<a href="http://www.cert.org.cn/english_web/documents.htm">http://www.cert.org.cn/english_web/documents.htm</a>	<b>Original data</b> : This is the link for publication website, and user should click each year's report and use Ctrl-F to find keywords <b>Archived data</b> : Saved as pdf file
<b>India</b>	<a href="http://www.cert-in.org.in/">http://www.cert-in.org.in/</a>		<a href="http://www.cert-in.org.in/">http://www.cert-in.org.in/</a>	<b>Original data</b> : Yearly publication pages are accessed via Java script, impossible to attain the specific address <b>Archived data</b> : Annual reports from 2004 to 2009 are collected, but in the 2009 annual report, every data for last 5 years are included
<b>Japan</b>	<a href="http://www.jpCERT.or.jp/english/">http://www.jpCERT.or.jp/english/</a>	<a href="http://www.jpCERT.or.jp/">http://www.jpCERT.or.jp/</a>		
<b>Malaysia</b>	<a href="http://www.mycert.org.my/en/">http://www.mycert.org.my/en/</a>		<a href="http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html">http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html</a>	<b>Original data</b> : Rather than specific yearly web pages, one web page is linked because web address for each year is rather random. <b>Archived data</b> : webpages (2000-2009) are saved in .mhtml files
<b>Pakistan</b>	<a href="http://www.nr3c.gov.pk/(National Response Centre for Cyber Crimes)">http://www.nr3c.gov.pk/(National Response Centre for Cyber Crimes)</a> <a href="http://www.pakcert.org/(Computer Emergency Response Team)">http://www.pakcert.org/(Computer Emergency Response Team)</a>		<a href="http://www.pakcert.org/defaced/stats.html">http://www.pakcert.org/defaced/stats.html</a>	<b>Original data</b> : web address for the left cell <b>Archived data</b> : Statistical data(1999-2008) is saved in .mhtml file

<b>Korea</b>	<a href="http://www.krcert.or.kr/">http://www.krcert.or.kr/</a>		<a href="http://www.krcert.or.kr/english_www/publication/8_1_publication_list.jsp?boardType=PUB">http://www.krcert.or.kr/english_www/publication/8_1_publication_list.jsp?boardType=PUB</a>	<b>Original data:</b> website for the left cell <b>Archived data:</b> saved in pdf file (Korea Internet Incident Trend Report, December 2000-2009).Data values are gained by accumulating monthly data from the graph on page 2
<b>Taiwan</b>	<a href="http://www.twncert.org.tw/">http://www.twncert.org.tw/</a>	<a href="http://www.twncert.org.tw/index.aspx">http://www.twncert.org.tw/index.aspx</a>	No data	
<b>UAE</b>	<a href="http://www.aecert.ae/index-en.php">http://www.aecert.ae/index-en.php</a>	<a href="http://www.aecert.ae/index.php">http://www.aecert.ae/index.php</a>	No data	
<b>Croatia</b>	<a href="http://www.cert.hr/">http://www.cert.hr/</a>		No data	
<b>Estonia</b>	<a href="http://www.ria.ee/28201">http://www.ria.ee/28201</a>		No data	
<b>Germany</b>	<a href="https://www.bsi.bund.de/">https://www.bsi.bund.de/</a>		No data	
<b>Latvia</b>	<a href="http://www.csirt.lv/?lang=en">http://www.csirt.lv/?lang=en</a>	<a href="http://www.csirt.lv/?lang=lv">http://www.csirt.lv/?lang=lv</a>	No data	
<b>Russia</b>	<a href="http://www.cert.ru/en/about.shtml">http://www.cert.ru/en/about.shtml</a>	<a href="http://www.cert.ru/ru/about.shtml">http://www.cert.ru/ru/about.shtml</a>	No data	
<b>USA</b>	<a href="http://www.us-cert.gov/">http://www.us-cert.gov/</a> <a href="http://www.antiphishing.org/phishReportsArchive.html">http://www.antiphishing.org/phishReportsArchive.html</a>	<a href="http://www.us-cert.gov/">http://www.us-cert.gov/</a>	<a href="http://www.us-cert.gov/reading_room/report_archive.html">http://www.us-cert.gov/reading_room/report_archive.html</a>	
<b>Australia</b>	<a href="http://www.cert.gov.au/">http://www.cert.gov.au/</a>	<a href="http://www.cert.gov.au/">http://www.cert.gov.au/</a>	No data	
<b>Brazil</b>	<a href="http://www.cert.br/en/">http://www.cert.br/en/</a>	<a href="http://www.cert.br/">http://www.cert.br/</a>	Annual graph for total incidents (1999-2010) <a href="http://www.cert.br/stats/incidents/">http://www.cert.br/stats/incidents/</a>  Scanning,DOS, invasion: <a href="http://www.cert.br/stats/incidents/2009-jan-dec/total.html">http://www.cert.br/stats/incidents/2009-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incidents/2008-jan-dec/total.html">http://www.cert.br/stats/incidents/2008-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incidents/2007-jan-dec/total.html">http://www.cert.br/stats/incidents/2007-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incidents/2006-jan-dec/total.html">http://www.cert.br/stats/incidents/2006-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incidents/">http://www.cert.br/stats/incidents/</a>	<b>Original data:</b> address left cell <b>Archived data:</b> Data (1999-2010) is saved in .mhtml

			<a href="http://www.cert.br/stats/incident es/2005-jan-dec/total.html">es/2005-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incident es/2004-jan-dec/total.html">http://www.cert.br/stats/incident es/2004-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incident es/2003-jan-dec/total.html">http://www.cert.br/stats/incident es/2003-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incident es/2002-jan-dec/total.html">http://www.cert.br/stats/incident es/2002-jan-dec/total.html</a> <a href="http://www.cert.br/stats/incident es/2001-jan-mar/total.html">http://www.cert.br/stats/incident es/2001-jan-mar/total.html</a> <a href="http://www.cert.br/stats/incident es/2000-jan-dec/total.html">http://www.cert.br/stats/incident es/2000-jan-dec/total.html</a>	
<b>France</b>	<a href="http://www.cert-ist.com/eng">http://www.cert-ist.com/eng</a>	<a href="http://www.cert-ist.com/">http://www.cert-ist.com/</a> (for france industry) <a href="http://www.certa.ssi.gov.fr/">http://www.certa.ssi.gov.fr/</a> (for france administration) <a href="http://www.cert-devoteam.com/">http://www.cert-devoteam.com/</a> (for france comercial) <a href="http://www.renater.fr/">http://www.renater.fr/</a> (for france National Network of Telecommunications for Technology) <a href="http://www.lexsi.fr/">http://www.lexsi.fr/</a> (for france Laboratory of expertise in computer security)		

Table 21 CERT information access-from the left, CERT website address (english site and local language site), and third column is for direct link for the webpage of statistical data and publication, and the last column specifically describes how to access specific data value from the statistic & publication webpage.

	China	India	Japan	Malaysia	Pakistan	Korea	Taiwan	USA	Croatia	Estonia	Germany	Latvia	Russia	USA	Australia	Brazil	France
Total CERT Reported Incidents	Incident Reports																



Virus/worm/malicious code/malware	webpage embedded malicious code	Virus / Malicious Code				Worm/Virus											
Defacement	Web Defacement					Web Defacement											web
Phishing/personal data abuse	phishing	Phishing				Phishing Host											
Scanning		Network Scanning / Probing				Intrusion +other											
DoS & Integrity Attacks																	of
Total Cyber Crime Cases																	
Cyber Crime Damage Dollar Loss (millions in \$)																	
Cyber Crime Arrests																	
% Cyber Crimes Reported to Police																	

Table 22 Matching table of CERT terminologies--Table2 helps find what terminology which each country uses, matches Dashboard terminology. For the input word for the function, you can use this table to find a proper term for a target country

