

University of Texas Rio Grande Valley

ScholarWorks @ UTRGV

Theses and Dissertations - UTB/UTPA

8-2013

Innovation-ICT-cybersecurity: The triad relationship and its impact on growth competitiveness

Manal M. Yunis

University of Texas-Pan American

Follow this and additional works at: https://scholarworks.utrgv.edu/leg_etd



Part of the [Business Commons](#), and the [Information Security Commons](#)

Recommended Citation

Yunis, Manal M., "Innovation-ICT-cybersecurity: The triad relationship and its impact on growth competitiveness" (2013). *Theses and Dissertations - UTB/UTPA*. 874.

https://scholarworks.utrgv.edu/leg_etd/874

This Dissertation is brought to you for free and open access by ScholarWorks @ UTRGV. It has been accepted for inclusion in Theses and Dissertations - UTB/UTPA by an authorized administrator of ScholarWorks @ UTRGV. For more information, please contact justin.white@utrgv.edu, william.flores01@utrgv.edu.

INNOVATION-ICT-CYBERSECURITY: THE
TRIAD RELATIONSHIP AND ITS IMPACT
ON GROWTH COMPETITIVENESS

A Dissertation

by

MANAL M. YUNIS

Submitted to the Graduate School of the
University of Texas-Pan American
In partial fulfillment of the requirements for the degree of
Doctor of Philosophy

August 2013

Major Subject: Computer Information Systems

INNOVATION-ICT-CYBERSECURITY: THE
TRIAD RELATIONSHIP AND ITS IMPACT
ON GROWTH COMPETITIVENESS

A Dissertation
by
MANAL M. YUNIS

COMMITTEE MEMBERS

Dr. K. Koong
Chair of Committee

Dr. J. Sun
Committee Member

Dr. L. Liu
Committee Member

Dr. J. Hughes
Committee Member

Dr. S. Wu
Committee Member

August 2013

Copyright 2013 Manal Yunis
All Rights Reserved

ABSTRACT

Yunis, Manal M., Innovation-ICT-Cybersecurity: The Triad Relationship and its Impact on Growth Competitiveness. Doctor of Philosophy (Ph.D.), August, 2013, 348 pp., 45 tables, 18 figures, 616 references 107 titles.

This study examines the global growth competitiveness of countries using the dynamics of growth, ICT, and innovation. It also introduces a new dynamic, cybersecurity, and argues that within a growth competitiveness framework, ICT, innovation, and cybersecurity mechanisms allow some countries to achieve higher ranks on the competitiveness ladder than others. Based on a theoretical framework that encompasses the economic growth model, the complementarity theory, and the international law theory, a model that integrates ICT, innovation, and cybersecurity, depicts the relationships amongst them and with growth competitiveness, and incorporates complementary factors with possible moderating effect is presented. The model proposed relationships are then tested using PLS-PM. The model proves to have adequate goodness-of-fit as well as predictive validity. Results support most hypotheses showing: (1) a positive relationship between ICT and innovation; (2) a positive relationship between each of innovation and ICT with growth competitiveness; (3) a mediating effect of innovation has in the ICT – growth competitiveness relationship; (4) a positive relationship between ICT and innovation on one hand and cybersecurity on the other; (5) a mediating role of cybersecurity in the ICT – growth as well as the innovation – growth relationships; and the (6) moderating effect that human capital has in the above relationships. Cyber threats, however, do not have a

moderator role in these relationships. These findings are interpreted in relation to the extant body of knowledge related to ICT, innovation, and cybersecurity. Moreover, the theoretical and the practical implications are discussed and the practical significance is shown. Finally, the study limitations are listed, the recommendations are presented, and the direction for future work is discussed.

DEDICATION

This work is dedicated to my most beloved father: you are the best dad that one could have. You are always in my heart, and your smile and encouraging looks and words never leave me. You wanted this accomplishment, and to you I dedicate it the most. I love you so much, and until we meet, you will always be with me. To you, my beloved mother and my angel: your prayers have always glittered my way and eased my worries. Forgive me for every tear you cried for me and forgive me for being away from you all these years. I love you so much Mama. To you, my sister and friend, Joudi: you are always there for me, helping me by all means to dream and to reach my goals. From you and from Adel I learnt that courage does not always growl. Sometimes it is the wisdom to do the right thing at the right time and the tranquil voice that whispers, ‘there is a way... try again tomorrow.’ You are my soul mate, I am so very proud of you, and I love you with all my heart. To you, my beloved husband: you sacrificed a lot to be with me in this journey. You made me smile when I felt down, endured all the pressure, stood by me, and had faith in everything I did. With your kind and loving care, you softened my rough edges and made this endeavor plausible. To you, the love of my life, my wonderful Rani: your smiles, beautiful words, and innocent looks have always pushed me forward. I admit that each page I have written represents some time spent away from you. Without your understanding and patience I could have never completed the journey. You are my wonderful baby, my little gentleman!

ACKNOWLEDGEMENTS

Pursuing higher education can be a challenging and a demanding process. First and foremost, I thank my God, Lord, and Creator for the numerous blessings He has bestowed upon me throughout my dissertation journey. He is the All-Compassionate and the All-Merciful.

Through this project, I have been truly encouraged and blessed by several people along the way. I would like to thank everyone who has contributed to my work and supported me through this lengthy endeavor.

A very big ‘Thank you’ is extended to my outstanding dissertation committee chair, Dr. Kai Koong, and to my esteemed committee members, Dr. Jun Sun, Dr. Jerald Hughes, Dr. Lai Liu, and Dr. Sabin Wu. I greatly appreciate your time and efforts in making my research worthwhile. You are truly role models for me to emulate in the field of education.

In particular, special thanks are extended to my mentor and chair, Dr. Kai Koong, for his continuous guidance and witty sense of humor during my PhD journey, in general, and the dissertation process, in particular. You granted me room to grow independently, yet always provided me with direction when needed. Thank you for believing in me and for having trust in my ideas and work. Your sincere support and interest allowed me to complete this amazing journey.

Dr. Jun Sun, I strongly admire your steadfast knowledge and experience in the world of research. Your invaluable guidance and recommendations related to my study model, data analysis, and statistical techniques were integral in my research.

You were always responsive and helpful with any questions or concerns I had in using the statistical methods I deployed in this dissertation and any previous research. Your accessibility was resourceful and much appreciated.

Dr. Jerald Hughes, your dedication to education shines through all of your efforts and accomplishments. You were my inspiration to get involved with information security in the first place. Thank you for helping me develop a clear focus on how to understand and apply effective and rigorous research methods. You encouraged me to learn and use the tools that added value and depth to my project goals. I am ever grateful. I also thank you for taking time out of your hectic schedule to revise and edit a big part of my work.

Dr. Lai Liu, I admire you for your commitment to excellence in work, for your persistent willingness to help others, for your strong eye for detail, and for your words of encouragement. Thanks for always lending me an ear, easing my worries, and helping me put my thoughts into perspective. Your excitement about my progress always brought me joy.

Dr. Sibin Wu, thank you for being so welcoming and flexible in anything I asked for. Your insights into leadership and relationships have been incredibly helpful, and our discussions have been worthwhile learning experiences. In fact, your encouragement and sincere support throughout this process have made so many things more bearable.

Special thanks are also due to Dr. Joo Jung. Although you were not a member in my dissertation committee, your insights, guidance, encouragement, and concern have always meant

a lot to me. I am lucky I had the nice opportunity of working with you as a research assistant. This was a source of big motivation to me.

I would like to thank Dr. Arturo Vasquez for his enthusiasm, encouragement, and support to me since I took the very interesting “Business Ethics” course with him. I admire you a lot, and I respect your resolute dedication and passion to values in academia and life.

I am very thankful to Dean Teofilo Ozuna for all his help, advice, research, and career guidance. I am lucky I had the opportunity of taking Econometrics II with you. The course encouraged me to think of the economic impact that information systems have at the global level.

A very big and highly appreciated contribution to this dissertation work has been offered by Mrs. Margaret Allison. Despite certain hard conditions she was passing through, Mrs. Allison could complete the editing and the revision of this work on time. Thank you so much, Mrs. Allison: your professional work has added to the value of my work.

To the kind faculty and staff of our CIS and QUMT Department, a very big Thank You! Dr. Andoh-Baidoo, thank you for listening to my concerns all the time, and thank you for your professionalism and understanding. Dr. Ahluwalia, thank you for your encouragement and for all the invaluable pieces of advice. Dr. Midha, thank you for the few but invaluable remarks you gave me concerning a part of my analysis. I admire you for the very kind attitude and support you provide students and colleagues with. Dr. Osatuyi, in a very short time, since your arrival to UTPA, you have become very close to everyone. I admire your very nice character and your knowledge in the field. Dr. Oh and Dr. Xiao, thank you for asking me about my progress all the time, and for showing me a sincere concern about my work. Dr. Wang and Dr. Qin, your smiles, hugs, and sincere support have meant and will always mean a lot to me. You are a source of joy

to our Department. Last, but not least, a sincere thank you is due to Ms. Nora Ramirez. Thank you for your kindness, invaluable support, and prayers.

A special ‘thank you’ is extended to my PhD friends and colleagues: Mohammad, Javier, Madison, Samer, Annie, Juan, and Paul. The past four years were fun with you. Thank you.

A sincere ‘thank you’ is also due to Ms. Sandra Delossantos who, since the very first day I arrived to UTPA , has made my PhD journey smooth and interesting. Thank you for your continuous and kind support.

To our excellent library, our supportive Graduate Office, and our caring International Office, a very big ‘Thank you’! You made my work an exciting one, and you helped in making my time in this great institution a very nice and memorable one.

I would also like to thank my beautiful family for their unconditional love and limitless support. Life is so beautiful because of you, difficulties melt down with your support, and success has a special meaning with you.

In the end, I would like to thank my husband Hussein for his faith in me, his support, and his love. You sacrificed personal time above and beyond what I could ever ask for. Your continuous encouragement and patience made this journey worth it for us and our wonderful Rani. Thanks for the hugs and for wiping the tears. Perhaps I was carried away by the pressure of my studies; too tired, too stressed to appreciate what you always do for me. I’m sorry if I didn’t constantly demonstrate how much you mean to me. I appreciate everything you did for me and the devoted love that you continuously showered me with.

To all of you, I repeat what William Shakespeare said, “I can no other answer make, but, thanks, and thanks.”

TABLE OF CONTENTS

	Page
ABSTRACT.....	iii
DEDICATION.....	v
ACKNOWLEDGEMENTS.....	vi
TABLE OF CONTENTS.....	x
LIST OF TABLES.....	xv
LIST OF FIGURES.....	xviii
CHAPTER I. INTRODUCTION.....	1
Background.....	4
Economic Performance, ICT, and Innovation.....	5
Economic Performance, CIs, and CIIIs.....	7
Cybersecurity.....	11
Need for and Significance of the Study.....	17
Statement of Problem.....	20
Statement of Purpose.....	26
Theoretical Framework.....	29
Study Outline.....	29
CHAPTER II. LITERATURE REVIEW.....	31
Theoretical Framework.....	32

New Economic Growth Theory.....	33
Complementarity Theory.....	37
International Relations Related Theories: National Security and Deterrence Theories.....	42
Literature Review.....	44
Innovation and ICT in the Economic Growth Model.....	46
The Technology Evolving Economy.....	48
Innovation and ICT.....	53
ICT and Growth Competitiveness.....	60
Innovation and Economic Growth.....	71
The Impact of Cybersecurity.....	79
Critical Information Infrastructure Protection.....	80
Importance of Cybersecurity: Cyber Security and the Economy....	88
Cyber Security Requirements and Strategies.....	93
Complementarities.....	96
IT-Related Training.....	96
ICT Human Capital.....	97
Cyber Security Initiatives Estimate.....	98
Legal Measures.....	98
Technical Measures: Secure Infrastructure.....	100
Organizational Structures.....	100
Capacity Building	101
Studies Using or Developing Innovation and ICT Indexes.....	102
Portrayal of the Conceptual Model.....	109

CHAPTER III. RESEARCH DESIGN AND METHODOLOGY	112
Statement of Hypotheses and Research Model.....	113
Theoretical Support for the Statements of Hypotheses.....	115
Design and Methodology.....	118
Research Design.....	118
Methodology.....	119
Data: Source and Size.....	123
Composite Indicators.....	125
Description and Evaluation of Composite Indicators Used in the Study.....	131
ICT Development Index.....	132
The Global Innovation Index.....	140
The Human Development Index.....	143
The Growth Competitiveness Index (GCI).....	146
Computer Threats.....	149
Study Variables.....	151
Data Analysis.....	152
Data Exploration: MVA Assumptions.....	153
Normality.....	154
Homogeneity.....	156
Linearity.....	158
Partial Least Squares (PLS).....	160
Why PLS?.....	162
PLS Assumptions.....	164

Sample Size Adequacy and Power Analysis.....	165
Statistical Power Analysis.....	165
Effect Size Calculation.....	167
Sample Size Estimation.....	169
Fitness of PLS to Study Objectives.....	170
Multi-Group Analysis.....	173
CHAPTER IV. FINDINGS, ANALYSIS, AND DISCUSSION.....	174
Analytical Approach: Triangulation-Based.....	175
Ordinary Least Squares (OLS) Regression.....	177
Partial Least Squares – Path Modeling.....	179
Non-Parametric Methods.....	184
Reading the Countries’ Characteristics: Descriptive Statistics.....	185
The Relationship between ICT, Innovation, and Growth Competitiveness.....	192
Non-Parametric Tests.....	192
Parametric Tests.....	197
Cybersecurity: A Formative Construct.....	204
Cybersecurity Construct: Content Domain and Indicator Specification.....	204
Cybersecurity Construct: Indicator Collinearity.....	206
Cybersecurity Construct: Validity and Reliability Assessment.....	208
ICT-Innovation-Cybersecurity and Growth: Overall Model Relationships.....	212
Non-Parametric Tests.....	212
Parametric Tests.....	219
Mediating Role of Cybersecurity in the ICT-Growth Competitiveness Relationship.....	219

Mediating Role of Cybersecurity in the Innovation-Growth Competitiveness Relationship.....	222
The Overall Model: The Triad Relationship and its Impact on Growth Competitiveness.....	228
Examining the Model Relationships across Country Groups.....	230
Examining the Moderation Impact of Human Capital and Cyber Threats.....	233
Model's Predictive Validity.....	234
Discussion.....	237
Basic Model Relationships.....	238
The Emergence of a New Composite Indicator: Cybersecurity.....	241
Cybersecurity Incorporation in the Basic Model.....	244
The Moderation Effect of Complementarity Variables in the ICT- Innovation-Cybersecurity Relationships with Growth Competitiveness....	248
CHAPTER V. CONCLUSION, IMPLICATIONS, AND RECOMMENDATIONS.....	253
Summary and Conclusions.....	256
Research Implications and Contributions.....	262
Limitations of the Study.....	276
Recommendations.....	279
Future Research Directions.....	282
REFERENCES.....	284
APPENDIX A.....	331
APPENDIX B.....	345
BIOGRAPHICAL SKETCH.....	348

LIST OF TABLES

	Page
Table 1: Cyber Power Metrics and Impact on Vulnerability.....	16
Table 2: Malicious Computer Activity.....	23
Table 3: Summary of Research Articles examining ICT-Innovation Relationship.....	55
Table 4: Summary of Research Articles examining ICT-Economic Growth Relationship.....	69
Table 5: List of some Cyber- attack Weapons against CI: Description and Impact Scope.....	81
Table 6: A List of Some Cyber Threat / Exploitation Types and Exploitation Method.....	86
Table 7: Summary of Research Articles on Developing Innovation and ICT Related Indexes.....	106
Table 8: Hypothesized Relationships and Corresponding Theoretical Support.....	117
Table 9: Secondary Data: Advantages and Disadvantages and their Applicability to the Study	124
Table 10: Pros and Cons of Composite Indicators.....	127
Table 11: ICT Development Index: Subcomponents and Corresponding Indicators.....	138
Table 12: Composite Indicators (Indices) Used in the Study: Compliance with OECD JRC Guidelines for Constructing Composite Indicators.....	150
Table 13: Variable Definitions, Uses, and Source.....	152
Table 14: Research Questions and Analysis Technique Used.....	163
Table 15: Effect Size, Power Level, and Estimated Needed Sample Size.....	169
Table 16: Variable Names and Representation in SPSS and SmartPLS.....	185
Table 17: Little's MCAR Test.....	186

Table 18: Distribution of Countries by Income group.....	187
Table 19: Distribution of Countries by Human Development Level.....	187
Table 20: One-Sample Kolmogorov-Smirnov Test.....	190
Table 21: Descriptive Statistics.....	191
Table 22: Descriptive Statistics across Country Income Groups.....	192
Table 23: Kendall Tau--b Correlations.....	194
Table 24: ICT, Innovation, and Growth Competitiveness: Coefficient of Concordance.....	194
Table 25: Wilcoxon Test of Matched Pairs.....	195
Table 26: Wilcoxon Signed Ranks Test: Innovation-ICT.....	196
Table 27: Wilcoxon Signed Ranks Test: Innovation-ICT-Growth Competitiveness.....	196
Table 28: Coefficient of concordance – Inter Rater reliability.....	206
Table 29: Correlation Analysis: Cybersecurity Indicators.....	207
Table 30: VIF Values pertinent to Cybersecurity Indicators.....	207
Table 31: Indicator Weights.....	210
Table 32: Cybersecurity Indicators: Weights, T-tests, and P-value.....	211
Table 33: Cybersecurity Scores and Country Ranks.....	213
Table 34: Kendall’s-tau-b: Ranking Agreement between Cybersecurity, ICT, Innovation, and Growth Competitiveness.....	215
Table 35: Kendall’s W Coefficient of Concordance – Cybersecurity Ranking with the Rankings of Other Variables.....	216
Table 36: Wilcoxon Test of Matched Pairs.....	217
Table 37: Wilcoxon Signed Ranks Test: ICT-Innovation-Cybersecurity-Growth Competitiveness.....	217
Table 38: ICT-Cybersec-GC: Regression Results and Cybersec Mediation Effect.....	220

Table 39: Innovation-Cybersec-GC: Regression Results and Cybersec Mediation Effect.....	223
Table 40: Overall Model: PLS Analysis.....	229
Table 41: Model Relationships across country groups.....	231
Table 42: Moderation Impact of Human Capital.....	234
Table 43: Cross-validated Redundancy Index (Q^2).....	237
Table 44: Cross-validated Communality Index (Q^2).....	237
Table 45: Support of the Study Hypotheses.....	250

LIST OF FIGURES

	Page
Figure 1: Reliance on Complex Networks of Partners and Suppliers.....	8
Figure 2: Interdependent Critical Assets and Key Resources across the Economy.....	9
Figure 3: The Ripple Effect of Cyber Attacks.....	11
Figure 4: CI Vulnerability Exploitation and Impact.....	15
Figure 5: Virtuous Cycles – Endogenous Growth.....	37
Figure 6: ICT and Complementarities: Impact on Growth.....	41
Figure 7: Application of information security triad to CIIP (Cyber security).....	95
Figure 8: Conceptual Model.....	110
Figure 9: Research Model.....	121
Figure 10: ICT Development Index Indicators.....	135
Figure 11: Component Loadings for the ICT Development Index Indicators.....	137
Figure 12a: Basic Model.....	172
Figure 12b: Model with the cybersecurity formative measure.....	172
Figure 12c: Complete Model.....	173
Figure 13: Model’s Latent and Manifest Variables.....	183
Figure 14: Histograms of Basic and Potentially Moderating Variables.....	189
Figure 15: Overall Model with Path Coefficients and R^2	235

Figure 16: TBI-Cybersecurity-Competitiveness Grid.....	258
Figure 17: CII Reliance on ICT vs. Cyber Threat Vulnerability--Defensive vs. Offensive Strategies.....	261
Figure 18: Country – Level Cyber Threat – Response Model.....	274

CHAPTER I

INTRODUCTION

Since the early dawn of humanity, the human mind has devised ways to make use of natural resources and surmount the challenges of life. As individuals or as groups, human beings always explored, experimented, invented, and learned various means by which to live, support their communities, and defend their possessions and territories from possible threats. This creative ability, known as innovation, is particularly crucial to survive and develop at all levels: the individual, the group, the community, the region, the nation, and the whole globe. Innovation is key to the individual trying to solve problems or make decisions; to the firm aiming to enhance its value chain and attain competitive advantage through differentiation or cost leadership strategies; and to the country following an adaptive approach to cope with a growing population, resource scarcity, global competition, and economic tension.

The critical role that innovation plays in the survival of individuals and nations is highlighted by Peters et al. (2009) who emphasized that, “creativity and innovation is all we have, in the face of the accumulating crisis of our time” (p. VII). In the era of globalization and digitization, innovation proliferation at the organizational and national levels is undertaking new

paths. As a result of globalization, nations and international organizations are setting strategies, establishing policies, and signing agreements aimed at enhancing innovation and achieving a competitive and sustainable economic welfare. In other words, the emphasis is no more merely on inter-firm collaboration (Patrakosol & Olson, 2007; Malhorta et al., 2001; Kumar & Van Dissel, 1996) and collaboration among globally distributed teams (Lee et al., 2006; Kotlarsky & Oshri, 2005) as the means for enhancing innovation. Rather, international R&D agreements, intergovernmental collaborations, and positive externalities are also embraced as pivotal elements in supporting and improving domestic innovation efforts and policies (Fernandez-Ribas & Shapira, 2009; Wagner & Leydesdorff, 2005; Nobel & Birkinshaw, 1998). Moreover, in the era of digitization, where advancements in information and communication technologies (ICT) are taking place at a rapid pace, these advancements may have a crucial role in galvanizing ICT-based innovations (Pilat & Wolfl, 2004; Nambisan, 2003; Corso & Paolucci, 2001).

Accordingly, with a learning and knowledge repository being its foundational base, and being nurtured by flows of information and information exchanges, innovation is influenced by ICT advancements. ICT plays a significant and leading role in sustaining innovation and moving its wheels forward (Ezell & Andes, 2010), although it is not the sole factor. In fact, productivity studies at the firm, industry, and country levels show that the high benefits and returns are realized by entities that not only adopt information technologies (IT), but also implement certain ‘productivity-enhancing’ processes. These include, but are not confined to, structural reforms (Eslava et al., 2004); human capital and an effective institutional framework (D’Costa, 2006); as well as training, empowered and decentralized decision making, and incentive systems (Brynjolfsson & Saunders, 2010). Viewed as complementary resources and processes, the combination of these processes with ICT advancements would probably have a synergistic effect

(Rogers et al., 2011) that outweighs the effect of each single factor on an entity's productivity growth and competitiveness. Accordingly, this paper argues that while ICT can be the source of innovation, the people that will use it and implement it and the prevailing conditions where it will be used are the factors that will drive it forward toward attaining and maintaining competitiveness at the national level.

Nevertheless, ICT advancements bring to the discussion table another crucial factor – that of cyberspace. Based on these rapid advancements, cyberspace has become the main stage of operations for almost every human being, industry, and government in the world. As ICT and cyberspace become sources of impressive innovation, the reliance of organizations, governments, and people on them will greatly increase. However, with this vast reliance on ICT and cyberspace, hazardous vulnerabilities and possible threats have emerged. These vulnerabilities are continuously looked for, examined, and exploited at an increasing rate (Barmin et al., 2011; McConnell & Hamilton, 2002), resulting in information and cybersecurity issues at the national as well as the international levels. This could be the dark side of technology as IT has always been thought of as a double-edged sword (Neumann, 1999; UNESCO, 2005; Mbatha, 2009; Barmin et al., 2011). The worst possible consequences of the harmful edge of the ICT sword would be a failure in a nation's critical infrastructure (CI), such as systems and powerful national assets, the destruction or malfunctioning of which would have a detrimental impact on the economic welfare, social well-being, and the national security of a country (ITU, 2005). In a similar vein, Tiirmaa-Klaar (2011) contends that the most devastating consequences will emanate from information infrastructure destruction or disruption at the national and regional levels. It follows that in a networked, globalized and digitized world economy,

cybersecurity could be envisioned as a critical success factor in a nation's economic growth (ITI, 2011; Romer & White, 2006), and possibly for ICT and innovation to contribute to this growth.

The above-mentioned relationships among ICT, innovation, and economic growth, as well as the emergence of cyberspace security and stability as a cornerstone of economic prosperity (White House, 2011), are the roots of motivation behind the study. Pertinent to this motivation, the objective of this study is to examine these relationships within a framework that derives its support (a) conceptually from relevant theory, scholarly literature, and analyses included in the reports of governments as well as international organizations; and (b) empirically through the application of rigorous and relevant research and statistical methods to country-level data. More specifically, the study aims at:

- Investigating the triad relationship (ICT-Innovation-Cybersecurity) as well as the relationship of each component with national growth competitiveness;
- Proposing a holistic framework that integrates ICT and innovation with new complementary factors, such as cybersecurity;
- Examining the impact that human capital and cyber threats have on the relationship between each of the triad elements and growth competitiveness; and
- Identifying the country-level indicators that are pertinent to cybersecurity, thus paving the way for cybersecurity measures and metrics to be established and tested.

Background

The ground rules of the global economy point to continued ICT advancements and technology-based innovations. A review of the economic growth or global competitiveness of nations would clearly show that some nations have the potential to achieve higher productivity levels and standards of living than others (Acemoglu, 2012; Acemoglu, 2009; Pritchett, 1995).

This raises a question about the possible underlying factors behind such divergence. Extant literature provides various answers, which are elaborated upon in the following sub-sections.

Economic Performance, ICT, and Innovation

While some economists believe the major contributors to competitiveness and productivity improvements lies in the availability of effective institutions, helpful laws, regulations, and education, others have focused on technology and innovation as the major contributors (Brynjolfsson & Saunders, 2010). The authors, however, contend that the effect of ICT on the economy is not confined to its production. Rather, it is the innovative use of these technologies by individuals, organizations, and governments that really matters (Brynjolfsson & Saunders, 2010). This is supported by an earlier view that the impact of a technological innovation will generally depend not only on its inventors, but also on the creativity of the eventual users of the new technology (Rosenberg, 2004). Such innovative uses of ICT could lead to several improvements that are not taken into consideration in the calculation of gross domestic product (GDP), but highly influence the quality of life of the adopting communities (Nordhaus, 1997). Broadly speaking, studies of the economic impact of IT can be classified into two distinct categories: the production function and process-oriented approaches (Lee & Barua, 1999). According to the authors, while the production function approach has solid microeconomic theoretical support, it does not provide details on processes through which IT impacts are created. Thus, the process-oriented approach has more explanatory power, and better articulates the IT impact than does the production function (Lee & Barua, 1999). Studies using growth competitiveness to represent economic growth have indicated that the measure takes into consideration the technological advancements as well as the processes and policies

that underpin economic growth (McArthur & Sachs, 2002). This study follows McArthur and Sachs' approach and thus embraces growth competitiveness as an estimate of economic growth.

In looking at innovation, studies examining the impact innovation has on economic growth have employed the concept of national systems (e.g., Metcalfe & Andrew, 2005; Freeman, 2002). Freeman (2002) discussed the distinction that has been made by Lundvall (1992) between “narrow” and “broad” definitions of national systems of innovation. The narrow approach concentrates on those institutions which deliberately promote the acquisition and dissemination of knowledge and are the main sources of innovation. The “broad” approach recognizes that these “narrow” institutions are embedded in a much wider socio-economic system in which political and cultural influences as well as economic policies help to determine the scale, direction, and relative success of all innovative activities. Still, there is a third approach that links the national systems of innovation to globalization (Archibugi & Michie, 1998). At the core of this approach lies the issue of technological change. This is logical because (a) technology has been a means for information and knowledge flow across borders; and (b) technological advancements have been facilitated and stimulated by market globalization (Carlsson, 2006; Archibugi & Michie, 1998). As for its contribution to economic growth, analysts traditionally contended that investments in R&D and in innovation are the main critical factors for economic growth. This notion has recently been challenged by the view that the globalization of markets for knowledge workers and technology has played the role of a catalyst for strengthening national innovation systems, and in turn enhancing national economic growth (Ernst, 2006). It is this view that the study incorporates in its attempt to identify the relationship between national ICT, national innovation, and economic growth.

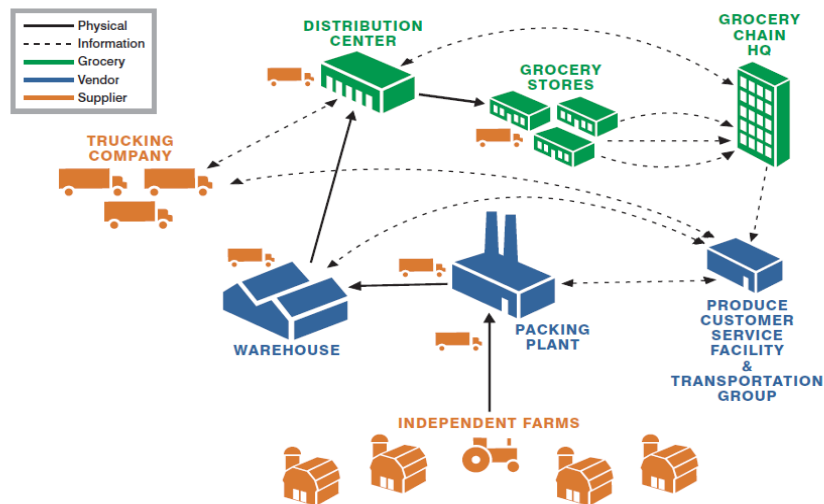
Economic Performance, CIs, and CIIs

Focusing on the role ICTs play in the economic competitiveness of a nation, the analysis will start with a core fact that ICTs, representing the innovation element in the economic growth model, are becoming increasingly intertwined in the daily activities of most, if not all, societies. Some of these ICT systems, services, networks and infrastructures form a vital part of economies and societies, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures (CI) (European Commission, 2009). They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal and economic functions. To grasp the level of these shattering outcomes, consider the complex networks of partners and suppliers that ordinary grocery stores depend upon in today's networked economy. This is portrayed in Figure 1. Notice that the information links among various entities far exceed the physical links. This implies that a cyber-attack targeting; for example, the 'Produce Customer Service Facility' that electronically manages customer orders, delivery, and billing, can affect the overall chain. In this case, the devastating effect may manifest itself in image, reputation, and profitability losses, as well as a shortfall in the stores' value chains and webs.

At a higher and more sophisticated level, a hacker attack on the nation's power grid has the potential for causing blackouts as well as a domino effect of consequent failures in other systems. The domino effect is caused by the high level of interdependencies among these systems and with the power grid (Cavelty, 2008). To illustrate such overwhelming effects resulting from cyber attacks targeting interdependent systems in a nation's critical information infrastructure, it would be useful to envision the impact on intertwined entities across the

economy. Depicted in Figure 2, the illustration visualizes two core points: (DHS and DOE, 2007).

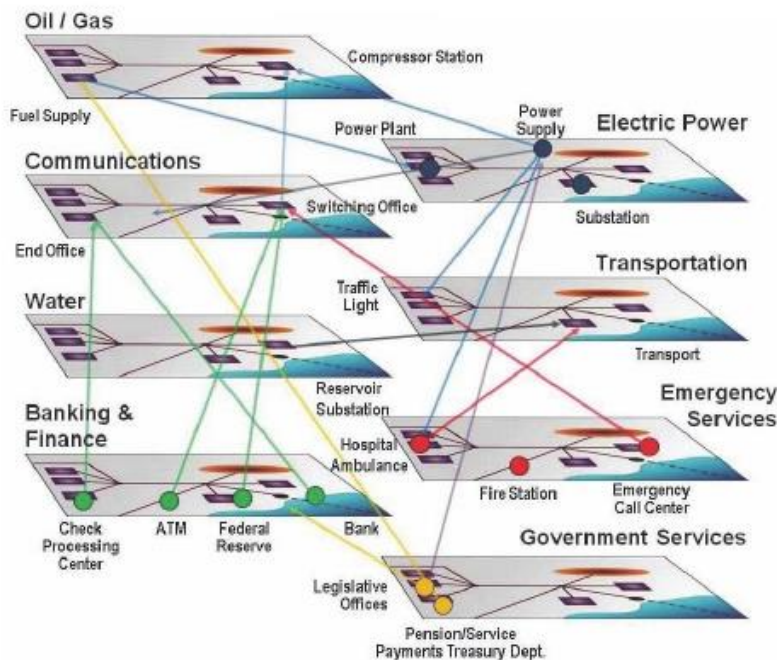
Figure 1 Reliance on Complex Networks of Partners and Suppliers – the case of grocery stores



Source: Institute for Information Infrastructure Protection, 2009.

1. Technical innovations and rapid ICT advancements have markedly linked and increased interdependence among the nation's critical infrastructures. This suggests that harmful attacks directed at a critical asset would have disturbing and possibly amplified effects on the other infrastructures.
2. Infrastructure interdependencies extend beyond the national borders and cross international borders. Besides the dependence of the US on foreign oil, for example, electric transmission lines as well as oil and natural gas pipelines provide the overall North American region with integrated energy systems.

Figure 2 Interdependent Critical Assets and Key Resources across the Economy



Source: Homeland Security and Department of Energy, 2007, 2010. (Note: some relationships are not shown in the figure.)

Analysis of these two points would lead to the inference of the following:

- Because of the interdependencies among the various critical infrastructures (CI) within a nation, a cyber-attack on one CI will have a ripple effect on the other CIs. In other words, the attack can create an adverse situation not only in the target CI, but also in the other intertwined CIs. The ripple effect is used here to describe a situation where an attack vector drops into a critical asset in the nation and momentum builds out externally. This is illustrated in Figure 3. As shown, the adverse impact that the attack vector will cause in one CI will also generate disruptions – that are possibly amplified – in the other critical assets of a critical national infrastructure (CNI).
- The interdependencies of the CIs as facilitated by ICT will enhance the flow of information and knowledge among them. Consequently, innovation in terms of products,

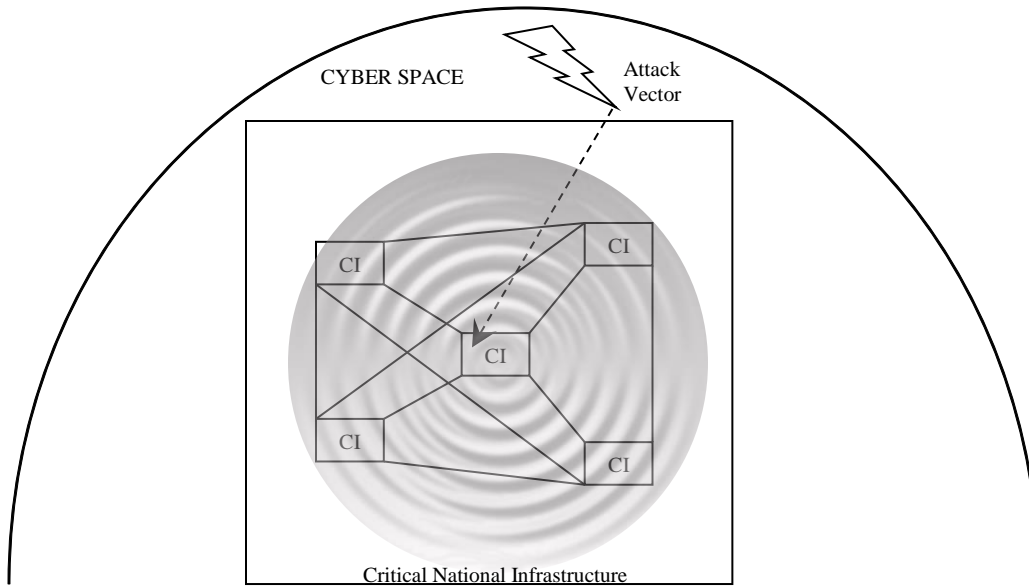
services, and processes, as well as inter-organizational coordination mechanisms and interconnectedness (Zhu et al., 2004; Yeniyurt et al., 2005) will be triggered and enabled.

- The interdependencies and interconnectedness of the CIs along with the ripple effect that the possible disruption of any CI will generate onto other CIs will in turn have an impact on CNI. Consequently, the national economy, which depends on its CNI to a great extent, will also be affected. This is because the digital key resources and the networked critical infrastructures of a nation are increasingly the backbone of sustainable and prosperous economies, transparent government, and better developed societies (White House, 2011).
- The world is becoming more and more networked, with the connections and information flows now reaching far beyond the conventional borders of organizations and even countries. Given the possibility that certain CIs in different nations are integrated and interdependent (e.g., the integrated energy systems in North America), the impact of a disruption attack will probably go beyond the CNI of one nation and affect others. The result is that the conventional information security paradigms are vanishing, opening the way for new models that take into consideration the increasingly important nature of today's information security: it is a borderless security (Van Kessel, 2010).

The above points are visualized in Figure 4. Information systems are prone to failure, as well as attractive targets for rogue actions and malicious attacks (ITU, 2005). Accordingly, a nation's critical assets which are networked and dependent on information systems are vulnerable to cyber threats. If not well-secured, exploitation will take place, leading to an adverse impact on the attacked CI target and disruptions in the other interdependent CIs through the rippling effect. As a result, the impact will reach the CNI and in turn, the national economy and possibly the global economy. An even higher "force-multiplier" effect will take

place if attack vectors target more than one CI. This is denoted by the sum total impact (\sum IMPACT) in Figure 4.

Figure 3 The Ripple Effect of Cyber Attacks



Cybersecurity

Cybersecurity is not a recent phenomenon, as computer data breaches have always been a concern (Goodhue & Straub, 1991; Straub & Welke, 1998; Culnan & Williams, 2009). But what is cybersecurity? The International Telecommunications Union, ITU (2005), defines the term as follows:

“Cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of “cyber-threats” is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors” (p.3).

The term “cybersecurity” is commonly used to refer to three things: (ITU, 2005)

1. A set of technical and non-technical activities and other measures designed to protect computers, networks, stored and communicated information, as well as the overall cyberspace from all types of threats, including threats to national security;
2. The degree of protection generated by the above activities and measures;
3. The associated professional field, including research work aimed at analyzing, developing, and implementing those activities for a better security quality.

Cybersecurity roots extend back to the Cuckoo's Egg incident in the mid-1980s about which Cliff Stoll (1990) wrote a book considered today as one of the most important in the history of computer incident response. The book described and also raised awareness of the incident where foreign spies could obtain highly classified information through computer espionage (Stoll, 1990). Viruses and worms have been active, infuriating actors on the stage of computing for a long time. The term 'virus' was first stated and described in 1983 by Fred Cohen, though John von Neumann initiated the concept in the 1940s in his studies about self-replicating programs (de Villiers, 2009).

This rendered the establishment of reliable trust frameworks and global cybersecurity cultures both prudent and vital (WSIS, 2003). Still, it was only when major cyber-attacks hit an entire nation in spring 2007 that the issue was propelled to the center of attention. The nation was Estonia, and the sustained cyber-attacks that targeted the country were labeled by observers as cyber warfare, cyber terror, or cybercrime (Wilson, 2008). Shortly preceded by a political event where officials in Estonia took down a statue in Tallinn which had been in place since the Soviet-era, which resulted in a huge backlash in Russia against the Estonians. That attack effectively crippled Estonia's government websites, newspapers, police, ministries, media and online banking. The attack came in the form of large Distributed Denial of Service (DDoS)

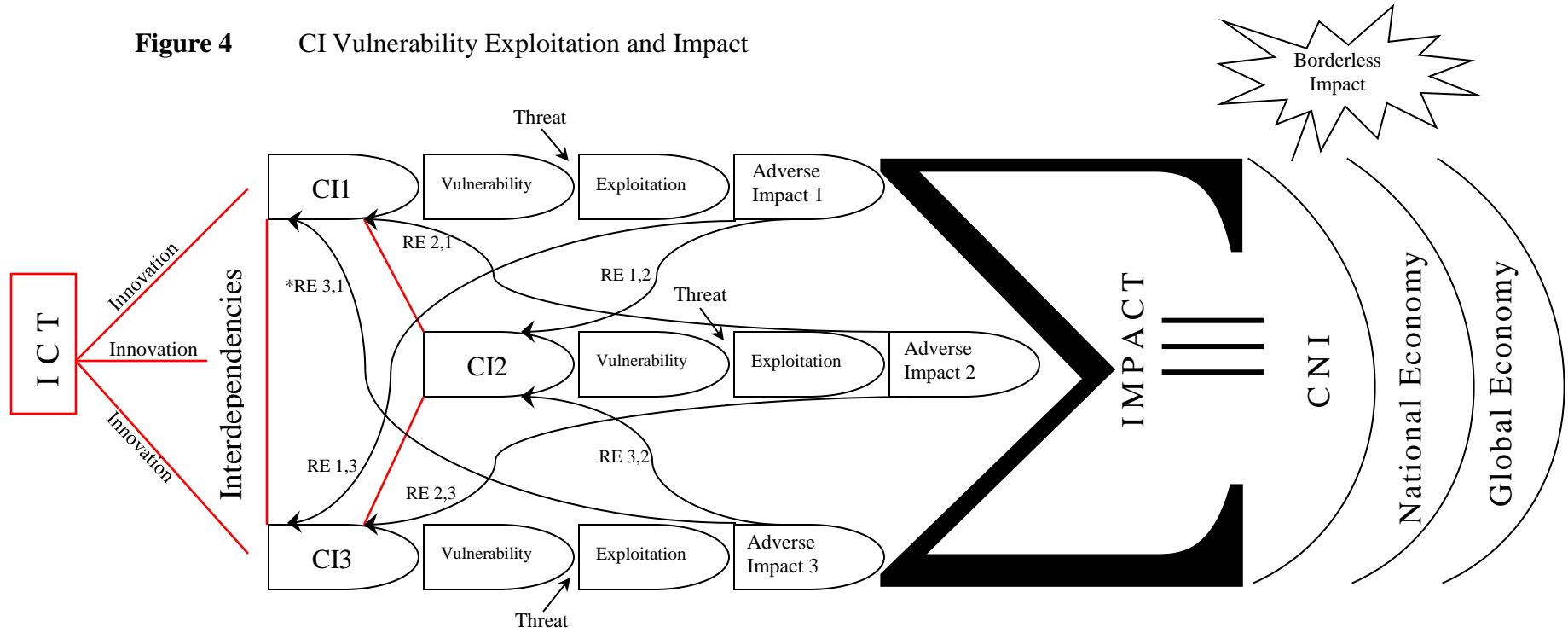
attacks where computers and servers were flooded by multitudes of visits and voluminous e-mails, which blocked legitimate users and caused many websites to shut down for some time. An examination of Estonia's ICT and networkedness level would reveal the following (Collier, 2007; Tiirmaa-Klaar, 2011):

- It is a well-wired, technologically advanced small country;
- There is a high reliance on online services with about 98 % of the banking sector relying on electronic communications;
- Estonia has unique e-government and personal identification systems; and
- There is a high ICT penetration that contributes to economic efficiency through lowering many transaction costs.

However, because of limited resources, there was a lack of proper infrastructure management (Wilson, 2008). This, of course, increased the vulnerability level and intensified the exploitation impact at the social as well as the economic levels (Goodman, 2010). It also demonstrated the potential for similar or even more distressing and destructive attacks on other economies. A case in point could be the wave of cyber-attacks that hit Georgia during the Russian invasion of the country in August 2008. The attack had a devastating impact on the country's media, banking sector, and communications systems (Trustwave, 2011). Later, in 2010, the computers at a nuclear plant in Iran were affected by the 'Stuxnet' worm virus. According to Trustwave's Global Security Report (2011), most of the attacks that hit national CIs were DDoS attacks. These are carried out using 'botnets' – computer networks that "have been hijacked by remote users, often without the knowledge of their owners" (Trustwave, 2011, p.31). An interesting point mentioned in the report is that there are 20 to 30 countries that could be considered 'cyber powers'; i.e., capable of getting engaged in cyber warfare. The list includes:

US, Canada, China, Russia, Israel, Iran, Australia, Taiwan, North Korea, South Korea, India, and Pakistan, as well as several NATO members.

Figure 4 CI Vulnerability Exploitation and Impact



*RE_{x,y} = Ripple effect of the adverse impact resulting from the cyber-attack that hit CI_x on CI_y.

To be a cyber-power, a country is expected to be innovative, technologically advanced, and have sufficient skilled and highly trained computer personnel (Clarke & Knake, 2010). The question that poses itself now is: are these traits attributed to developed countries only because they have both the necessary technological as well as human resources? What about Iran, North Korea, and some others which are also included in the list? This study will ponder these questions in terms of a country's classification as developed/developing, its economic situation, its networked readiness, its computer literacy and training, its innovation capacity, and critical information infrastructures (CII) among other factors. In addition, according to Clarke and Knake (2010), cyber power should be judged according to three metrics: (1) offensive capability; (2) defensive capability; and (3) dependence on computer networks. By these metrics, Clarke contends that North Korea is a top cyber power since, though weak in its offensive capability, it is very strong at the defensive level, and its dependence on computer networks is very low, thus its vulnerability would be expected to be low. In a contrasting situation, we find the US that has a high offensive ability, a low defensive ability, and a huge reliance on computer networks. The last two factors outweigh the first causing the nation to be highly vulnerable to cyber threats and attacks (Clarke & Knake, 2010). Clarke's analysis of the metrics used to identify cyber powers is visualized in Table 1.

Table 1 Cyber Power Metrics and Impact on Vulnerability

Metric Country	Offensive Capability	Defensive Capability	Computer Networks	Vulnerability
USA (Developed and High Technology)	High	Low	High	High
North Korea (Developing and Low Technology)	Low	High	Low	Low

In fact, Clark's metrics and analysis raise other questions regarding: (1) the components of an effective defensive cybersecurity strategy; (2) the relationship between ICT achievement level and a nation's cybersecurity; and (3) the relationship between a nation's economic classification and its ability to implement a defensive and/or offensive strategy.

Need for and Significance of the Study

The need for this study stems from the fact that CIs, which are mostly underpinned by CII, are now pivotal to economies, especially the industrial and developed ones. These economies are as good as these CIs are. Citizens, governments, and businesses are all increasingly becoming reliant on a massive array of intertwined information and physical infrastructure to accomplish daily tasks, solve problems, and make decisions. Also, as mentioned earlier, because of their interdependence, the failure of one is apt to spread and generate a domino effect. It is worth recalling that CI interdependence sometimes extends beyond a nation's borders and crosses into other nations, as is the case with power transmission, oil, gas, and other power sources, or the Internet. This means that failure to attain and maintain safe, resilient, and robust infrastructure in one nation can generate adverse effects on others.

With CI defined as infrastructure whose failure would result in dreadful damages to a nation's society and/or economy (CEPS, 2010), the economic impact of a disrupted CI should be considered (Cashell et al., 2004 and OECD, 2008). This highlights the importance of incorporating the resilience and security of CIs within economic growth and growth competitiveness discussions and frameworks. Major leaps have been achieved since researchers and economists started investigating the contribution of non-conventional factors (such as technology and innovation) in realizing an improved economic welfare and increasing

productivity (Brynjolfsson & Saunders, 2010). The authors mentioned an old joke that economists tell as a way to manifest the importance of these two factors in better examining productivity growth.

The joke talks about a drunk who was crawling on his hands and knees under the light of a lamppost at night. A person passing by asked the drunk what he was doing, to which the drunk answered that he was looking for the keys that he had lost. The passer-by asked him whether he had lost them under the lamppost. Surprisingly enough, the drunk said pointing to the other side of the street, “No, I lost them over there, but the light is better over here”.

The joke indicates the tendency of economics researchers to emphasize the relatively measurable entities of the economy and to focus on quantifiable factors and outcomes (Brynjolfsson & Saunders, 2010). This approach falls short of considering the impact of other important sectors (such as services) as well as increasingly important contributing factors, such as technology, innovation, social welfare, trust, and security, to mention a few, on achieving sustained economic growth. Other studies made a big contribution by moving away from the assumption that technology is only a capital investment to the inclusion of other “complementary” investments, such as testing, IS labor process engineering, and training (Brynjolfsson & Saunders, 2010; Bakos, 1998). This study takes into consideration the importance of cybersecurity in this era of globalization, information, and open economies, and attempts to include it as another complementary factor that helps in better assessing the contribution of ICT and innovations in a nation’s economic and productivity growth. The importance of this approach is underscored by international organizations’ reports and previous theoretical research that emphasized the hampering effect that cyber-attacks on CIs have on a nation’s economy.

The study thus intends to search for the keys where they were lost, deeming it more productive to search in the dark than searching under the lamppost. The significance of the study lies in its examination of various nations' growth with a three-dimensional lens: the ICT dimension, the innovation dimension, and the cybersecurity dimension. Accordingly, not only will the impact of each dimension on a nation's competitiveness be determined and analyzed, but also joint relationships will be examined and discussed. Addressing the topic with this approach will be a good contribution to innovation, ICT, cybersecurity, and nations' competitiveness research streams, especially because:

- Investigating the triad relationship (ICT-Innovation-Cybersecurity) and its impact on competitiveness is the first attempt in the literature;
- A holistic framework integrating ICT with new complementary factors, such as cybersecurity, will add to the body of literature and will extend previous economic growth or growth competitiveness models; and
- The model will open the way for establishing cybersecurity metrics and methods for assessing and controlling the cybersecurity situations in countries based on country-related information.

With the background and the study need in mind, the problem that this research study investigates will be stated and defined. This is elaborated and discussed in the following section.

Statement of Problem

“Make no mistake: Our networks and systems are vulnerable and exposed. Our adversaries are sophisticated, nimble, and organized, and they will stop at nothing to achieve their motives, which include economic gain or damage, espionage, revenge, publicity.”

Gregory Garcia, Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security, RSA Conference, Feb 8, 2007.

Cyberspace, or a nation's ICT, is the information backbone of any country. It links a nation's critical infrastructures across both private and public organizations in various sectors ranging from public health, water supply, food and agriculture, to energy, transportation and financial services. With the exponential growth of the Internet, the increasing use of electronic channels for commerce, governance, health care, and social relationships, and the use of ICT in all forms of utilities, the safety and robustness of these channels are increasingly becoming critical and pivotal matters.

Today, there are over 1.8 billion Internet users, with social networking growing exponentially (CTO, 2010). Innovation in various sectors paved the way for a convergence between telecom, broadcasting, and IT. This has given rise to new and innovative services in the financial, education, government, and healthcare sectors, not only in developed but also in developing countries. Accordingly, the increasing deployment and use of 'e-enabling' in various societies has increased the need for securing the channels of communication. In the globalization era, this security – the security of cyberspace, is deemed crucial, not only within a nation but also between and across nations.

Availability, reliability, and security of communications and information services are essential to the functioning and growth of a modern economy (Dalmini et al., 2009). These

services are collectively termed critical information infrastructure (CII). The distinguishing feature of a CII is that it encompasses and links all the other CIs together; so if it is removed, many other CIs will be down relatively soon (Westrin, 2001).

This tolls the bells regarding the possible risk of exploiting any vulnerability in this vital infrastructure, rendering all the other intertwined CIs vulnerable to exploitation. Within this realm, the World Economic Forum (WEF) estimated in 2009 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years. This is anticipated to have a global economic cost of approximately \$250 billion (World Economic Forum, 2008). In 2011, the same estimation is provided by WEF with a description of the global impact that such a breakdown will bring about: (World Economic Forum, 2011)

- Critical government, communication, energy and financial systems will be severely disrupted.
- Business services will be down, incurring severe economic losses.
- Trust in affected systems will be decreased at both the national and global levels.
- A spillover of devastating effects on other highly interconnected networks will occur.
- Because a CII breakdown hampers emergency responses, there would be potential loss of life.

A finding similar to that of the World Economic Forum was reported by Business Roundtable in 2007. The report suggested that a month-long Internet disruption in the US alone could have an economic cost of more than \$200 billion (Business Roundtable, 2007). As mentioned by CTO (2010), an OECD (Organization for Economic Co-operation and Development) report stated that the estimated annual loss to US businesses caused by malware is \$67.2 billion. In Switzerland, the report estimates, the costs of a major disruption are 1.2% of its

GDP. Moreover, a survey conducted on executives by McAfee in 14 countries (including China, Japan, France, Australia, India, Russia, USA, Germany, Brazil, Mexico, Saudi Arabia, UK, Italy, and Spain) revealed that cyber-attacks are widespread. The conclusion was based on the following survey findings: (McAfee, 2010)

- 54% experienced large-scale DDOS by high-level adversaries (like other nations, organized crime or terrorists) similar to that experienced by Estonia (in 2007) and Georgia (in 2008).
- About 60% believed that other governments have been involved in such attacks to weaken the CII in their countries.

Based on the attacks experienced, the reported cost of downtime due to a major cybersecurity incident exceeds \$6 million per day. Besides this cost, the most feared consequence was loss resulting from damage to their reputation following loss of personal information pertinent to customers (McAfee, 2010). What adds to the problem is that cyber-attacks are not limited to destroying electronic information. For example, power distribution control rooms, which are responsible for supervisory control and data acquisition (SCADA) systems could be hacked and used to damage or disrupt the power distribution in a large area (Branscomb, 2004), thus posing some real threat to citizens (MacEachern, 2011). A case in point is Stuxnet, a malware that facilitates cyber espionage and infrastructure attacks against SCADA systems (Byres, 2011).

All the previously mentioned reported incidents and risk estimations strongly point to the huge impact that an attack may have on a victim, be it an individual, a business organization, a government, or a nation. In all cases, a brief analysis would show the economic impact that such attacks would have on these entities. Simultaneously, one can associate the occurrence of these

incidents with a high dependence on computers, networks, and cyberspace technologies, such as the Internet. With such figures, it is imperative to understand the nature of cybersecurity risks from the perspective of their relationship to a nation's contextual factors as well as a nation's innovation capacity and ICT advancements.

Now consider the ICT adoption and use, the innovation capacity, and the global competitiveness 2009 scores computed by the World Economic Forum (2010) for the following three countries: USA, China, and Canada. Also, consider the 'attack origin rank' and share (%) of 'malicious computer activity' as computed by Business Week/Symantec (2009). These factors and their values are listed in Table 2.

Table 2 Malicious Computer Activity

Factor Country	ICT Adoption Use		Innovation Capacity		Attack Origin rank	Share of Malicious Converter Activity	Global Competitiveness	
	Score	Rank	Score	Rank			Score	Rank
USA	83.4	9	77.5	3	1	23%	5.43	4
China	45.5	79	49.5	65	2	9%	4.84	27
Canada	84.4	8	74.8	7	10	2%	5.30	10

Source: Business Week/Symantec (2009)

Reading through the numbers will open the door for several points/questions to arise:

1. The US is among the top leading countries in innovation. This might be fostered by the country's high ICT capabilities (World Economic Forum, 2009). Both factors have probably contributed to a relatively high rank in global competitiveness, though it fell from previously achieved ranks (Rank number 1 in 2008) (World Economic Forum, 2009).
2. The US ranks first in being the origin of attack. Can this demonstrate that it has more offensive (Clarke & Knake, 2010) than defensive capabilities, particularly since it is the country facing the most cybercrime as the findings show? Is this high risk the reason

behind the decision to invest more in ICT to ensure continuous and uninterrupted services?

3. China has moderate levels of ICT adoption and use, and consequently a low rank (out of 113 countries). However, it has a high attack level and a moderate share of malicious activity. Surprisingly enough, it ranks well in growth competitiveness. What could be the reason behind this? Could it be that the attacks initiated by China are done for economic reasons? Could they be directed at intellectual properties and/or other important information resources available in cyber space?
4. Finally, do the scores and ranks pertinent to Canada reflect better ICT protection levels and accordingly better defensive abilities than those of the US? The country is also displaying high innovation capacity and competitiveness levels.

Despite the importance of such potential relationships, there is a lack of studies that relate ICT, innovation capacity, cybersecurity, and global competitiveness in a comprehensive, integrated, and dynamic form. As important as they are, previous research papers dealt with the ICT/innovation relationship with information security or cybersecurity at the firm level (e.g.: Herzog et al., 2007); they focused only on cybersecurity and analyzed it from the social and motivational aspects (e.g., Cornish, 2009); or devised theoretical models for the assessment of cybersecurity and cyber-attacks or threats (e.g., Ekstedt & Sommestad, 2009). Moreover, studies relating cybersecurity to economic performance were either theoretical (e.g., O'Hara, 2010), or empirical with emphasis on the attitudinal variable (Ponemon Institute, 2010). Of course, there is a huge body of literature on ICT adoption and on innovation that examines the relationship between these two important capabilities and productivity at both the company and the country

levels. However, comprehensive studies of how ICT, innovation, and cybersecurity impact each other and then the overall economy – individually and jointly – have been lacking.

In fact, while the questions: “Why do some countries have better ICT use and higher diffusion levels than other countries?”, “What are the cyber threat trends in various countries?”; “What factors should be considered while setting a cybersecurity strategy?”, “What are the determinants of global competitiveness?”, “How does ICT contribute to global competitiveness?”, and “How does ICT foster innovation?” have been answered by previous research and international survey reports, there are certain questions that have been left unanswered. For example,

- “Why do some countries with valuable ICT resources fail to achieve high levels of global competitiveness?”
- “How can CNI cybersecurity initiatives help nations reap the benefits of their ICT resources and innovation capacities?”
- “While cases related to nations and the cyber-attacks they have been affected by point to an intertwined relationship between ICT, innovation, and cybersecurity, can this relationship be demonstrated?”
- “Can this joint relationship better foster growth competitiveness than each factor alone”?

A holistic and integrated approach is needed to help understand the factors that are most likely to be associated with a country’s vulnerability to cybersecurity threats and to its growth competitiveness. Such an approach will help in the process of setting policies and standards related to innovation, ICT investment, cybersecurity fostering international collaboration, and developing effective security strategies.

This research intends to bridge this gap, model the ICT-Innovation-Cybersecurity triad relationship, define the characteristics of global competitiveness through an analysis that encompasses the triad as well as other complementary factors, and test the model using country-level data. This is discussed more elaborately in the following section.

Statement of Purpose

The purpose of this research is threefold. The first is to present an integrated and comprehensive framework depicting the relationship between ICT and innovation capacity on one hand, and a country's growth competitiveness. This is important given the fact that different countries have different ICT resources (Gassman, 2006), innovation capacities, and diffusion levels. This will also spot the pitfalls that may hamper the efforts to capitalize on the opportunities made possible by cyberspace, ICT capabilities, and global innovations. The synthesis will draw upon a review of both theoretical and empirical research pertinent to the three concepts.

Second is to propose a conceptual model of: (1) the relationship between innovation capacity and ICT on one hand and the nation's cybersecurity (i.e., CII safety and resilience) on the other; (2) the relationship between ICT and innovation on one hand and global competitiveness on the other as mediated by cybersecurity; and (3) the relationship between each of the triad elements with growth competitiveness as moderated by human capital and cyber threats.

Third is to identify the factors that can provide a quantitative estimation of a nation's cybersecurity level using data pertinent to each country's strategies--technical, legal, and international collaboration.

Finally, the fourth is to provide an empirical test for the conceptual model proposed using country-level data. This will help in setting standards that can drive forward the wheels of innovation and ICT as well as potentially increasing their contribution to the nation's social and economic well-being. It will also be crucial for formulating cybersecurity policies with an eye on the country's ICT and innovation capabilities.

Emphasizing a holistic and dynamic framework linking ICT, innovation, and cybersecurity to a nation's competitiveness level will make this study useful for scholars, government analysts, information and cybersecurity specialists as well as ICT developers and strategists. To start with, scholars can use the framework as a foundation for assessing the contribution of each triad element to global competitiveness. They can also build on the cybersecurity estimate that will be based on country-level variables derived and synthesized from pertinent theories as well as the extant body of literature. Moreover, the model is flexible and accommodating. For example, it can be used as one integrated tool, or can be deployed to examine relationships only as it relates to various selected components. In addition to this, the study can help in understanding how different countries are placed along the innovation diffusion curve, or whether ICT and the networked environment of a country have a leapfrog and revolutionary effect on certain countries' levels of global competitiveness. As for government analysts, they will find in this framework a powerful means to identify, based on a country's set of economic and socio-technical resources and dynamic capabilities, the factors that should be emphasized more than others in order to yield higher levels of ICT connectivity and, as a result, better global competitiveness ranks. Government analysts and policy makers may also benefit from the "fair balance" approach (Pagallo, 2010) that the study emphasizes. Since there is a trade-off between a country's dependence on information-based networked economies (as well

as CI interdependencies) and its cybersecurity level, then strategies adopted should take into consideration what is optimal for a given country, considering its resources, abilities, and strengths. Cybersecurity analysts and strategists will be able to consider the various challenges and opportunities posed by the new computing models, including wireless and mobile computing, cloud computing, and social media (Ernst & Young, 2010). Finally, to support the country strategy-technology fit, ICT designers and developers can find the study useful as it allows examining the impact of every innovation/ICT strategy or tool on the ICT performance and on the country's global competitiveness objective.

To summarize, this study will attempt to examine the relatedness of a nation's cybersecurity to its ICT development/deployment and to its innovation capacity. It also intends to examine the impact of this triad on a country's growth competitiveness. More specifically, the study addresses the following questions:

- What is the relationship between a nation's innovation and ICT on one hand and its cybersecurity strategies on the other?
- What is the relationship between a country's ICT and innovation and its global competitiveness levels?
- How does cybersecurity change the ICT-Innovation relationship as it relates a country's competitiveness?
- How do these relationships vary across regions and country groups?
- What are the factors that are most likely to be associated with cybersecurity strategies?

To achieve its objective and address its research questions, this study is based on a rich theoretical foundation. This foundation is briefly introduced in the following section, but will be expanded in the next chapter.

Theoretical Framework

The foundation of this study is a rich theoretical framework that draws its components from a variety of theories related to economic growth, national security, and international relations. The need for such a foundation emanates from the variety of concepts included that are distinct, yet related. Accordingly, the connections among these frameworks will serve as a support for the relationships assumed in this study. The list of theoretical frameworks includes:

- New Economic Growth Theory (Romer, 1990)
- Complementarity Theory (Milgrom & Roberts (1990); Holmstrom & Milgrom (1994))
- International Relations Theory (Waltz, 1979) with its National Security and Deterrence components.

Study Outline

Chapter I, the introduction, presented an overview of the topic, a background that underpinned the triad relationship sought in the study. The background also paved the way for the problem statement which the study addresses, and for the objectives that this study attempts to achieve and the research questions it aims to answer. The chapter also described very briefly the theoretical frameworks that will be used to examine the relationships in question. Finally, a list of definitions for concepts and terms that will be used in the study was also presented.

Chapter II will be an elaboration of the theoretical framework upon which the study is based and a presentation of the literature review pertinent to innovation, information and communication technologies, cybersecurity, and global competitiveness. The research stream of each will be synthesized, analyzed, and related to the other streams in an attempt to probe important

relationships and derive the study hypotheses. Based on the analysis of the literature and the hypotheses derived, a conceptual model will be proposed.

Chapter III presents the study design and methodology. The data used, the variables studied, and the analysis performed to test the study hypotheses and the conceptual model will be presented and discussed.

Chapter IV will report and exhibit the findings reached after the data analysis is performed. Evaluation of each hypothesis in light of the findings, and a discussion of the findings based on an interpretation of results and relatedness to previous work in the area will be completed.

Chapter V will communicate the major study conclusions, linking them to the study problem and purpose. Also, implications for best practices in the field will be conferred. Finally, the study limitations will be assessed and recommendations for future research will be presented.

CHAPTER II

LITERATURE REVIEW

Researchers' interests in economic growth and competitiveness have been manifested in various research themes and directions in the literature. These two constructs have been examined through various perspectives and across myriad contexts with different resources, dynamic capabilities, and characteristics. This study attempts to examine the global growth competitiveness of different countries. The focus is essentially on the dynamics of growth competitiveness and, more specifically, on the ICT, innovation, and cyber security mechanisms that allow some countries to achieve higher ranks on the competitiveness ladder than others. The study therefore draws on national and regional literatures that are concerned with the growth of countries and regions, with the primary purpose of examining such growth in light of the ICT, innovation, and cyber security mechanisms at work, and with the secondary purpose of clarifying which relevant policies ought to be set and applied.

Such literature strands are potentially related, as it can be assumed that ICT and innovation, while related to each other, have the potential to drive forward the wheels of the economy and to contribute to the achievement of sustainable growth. At the same time, with a nation's economy being based on critical information and networked infrastructures, it is logical to assume that the vulnerability of these infrastructures would pose a risk factor for this economy. Moreover, besides all these potentially related factors, the literature related to

contextual factors at the national and regional levels in terms of their relationship to ICT, innovation, and cyber security, as well as to growth competitiveness, cannot be ignored.

This chapter aims at probing these literature streams, with the following objectives in perspective:

- (1) Laying down the theoretical foundation upon which the study will be based.
- (2) Developing a better understanding of the study's main constructs.
- (3) Examining the underlying relationships among these constructs as reported by previous related works.
- (4) Proposing an integrated model that depicts, based on a rich theoretical framework, the potential relationships among the factors being examined.
- (5) Using the theoretical foundation and the literature review to pave the way toward the derivation of the study hypotheses.

This chapter will start with a description of the theoretical framework. After that, a review of all the pertinent literature will be conducted. Finally, the conceptual model, which depicts the relationships among the constructs in light of the literature review conducted, will be presented and analyzed.

Theoretical Framework

The foundation of this study is a rich theoretical framework that draws its components from a variety of theories related to economic growth, ICT and innovation, and cyber security. The need for such a foundation emanates from the variety of concepts included that are distinct, yet related. Accordingly, the connections among these frameworks will serve as a support for the relationships assumed in this study. The three primary theoretical frameworks of the study are:

- New Economic Growth Theory (Romer, 1990);

- Complementarity Theory (Milgrom & Roberts, 1990; Holmstrom & Milgrom, 1994); and
- International Relations Related Theories: National Security and Deterrence Theories (Waltz, 1979; Jablonsky, 2001).

New Economic Growth Theory

The New Economic Growth Theory was developed in the 1980s as an effort to more precisely delineate the attributes of economic growth (Stiroh, 2001). Two important points are incorporated in this theory's view of economy: (Cortright, 2001)

- First, unlike previous theories which viewed technology as a product of non-economic forces or just a given, this theory views technological progress as a product of economic activity. Moreover, the theory internalizes technology into a model depicting how markets function. Accordingly, the New Growth Theory is often termed as an “endogenous” growth theory.
- Second, New Growth Theory deems that knowledge and technology generate increasing returns, which in turn drive the process of growth.

Paul Romer's (1990) paper, “Endogenous Technological Change”, has been considered a seminal contribution to the New Economics Growth Theory. In this paper, Romer stated that technological change: (Romer, 1990)

- (1) is an economic good and is the driving force of economic growth;
- (2) takes place as a result of people's responses to market incentives; and
- (3) is essentially different from other economic goods.

This new theory addresses the fundamental questions about what makes economies grow. Why is the world measurably richer today than a century ago? Why have some nations grown more than others? The New Growth Theory emphasizes the point that knowledge is a main

driver of growth. This stems from the fact that generated ideas can be shared and used in different ways, which leads to their accumulation. Accordingly, the law of diminishing returns will not apply to knowledge. Rather, the increasing returns to knowledge will help propel economic growth. New Growth Theory thus paves the way for a better understanding of the progressive shift from a resource-based to a knowledge-based economy. It emphasizes that the creation and diffusion of new knowledge can contribute significantly to the growth and competitiveness of firms, communities, and nations (Cortright, 2001). Consider, for example, the case of the Internet and computer technologies. Today, these technologies are considered the icons of growth and economic progress. However, it is the idea generation and innovation processes, rather than technologies themselves, that drive forward the wheels of economic growth. This is supported by Romer (1994) who explains that there is nothing new about the theory itself. The central notion behind New Growth Theory is increasing returns associated with new knowledge or technology. The cornerstone of traditional economic models is decreasing or diminishing returns, the idea that at some point as you increase the output of anything (a farm, a factory, a whole economy) the addition of more inputs (work effort, machines, land) results in a smaller increase in output than did the addition of the last unit of production. Decreasing returns are important to consider because they result in increasing marginal costs (that is, at some point, the cost of producing one more unit of production is higher than the cost of producing the previous unit of production). Decreasing returns and rising marginal costs are critical assumptions to understanding the mathematical equations economists use to describe the way the economy settles down to a unique equilibrium.

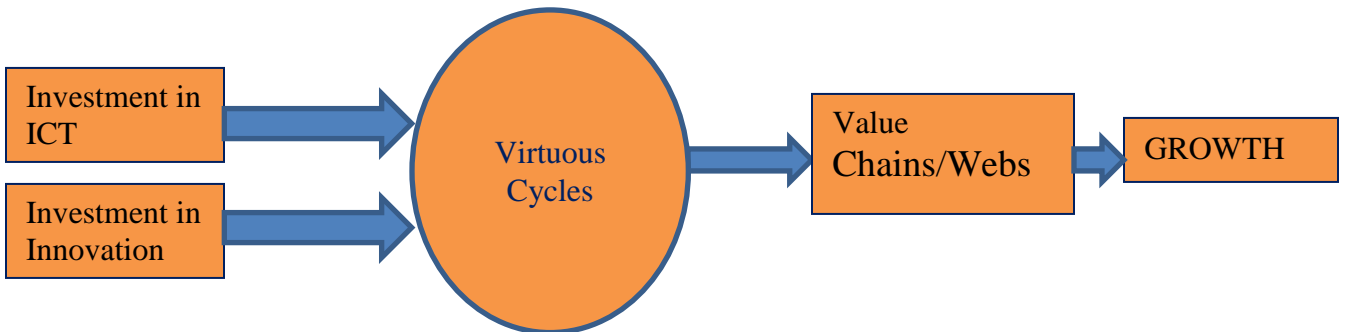
Romer (1990) contended that technology is a partially excludable, non-rival good, rather than a conventional or public good. He considered this an important distinction as private goods

are viewed as provided by markets, while public goods either appear or exist naturally or are provided by governments to counteract some market failure. This distinction between rival and non-rival goods as well as their excludability is a key premise of Romer's model. As an example, technology is considered a non-rival input. It is also seen as partially excludable at least (otherwise the economic incentive to adopt it, develop it, or invent it would be lacking if the free access is not partially limited). On the other hand, as another example, human capital is a rival and excludable good. As stated by the author, mathematical equations can be a free and a non-rival good, but having a person with the skill, knowledge, and ability to do the mathematical calculations is considered rivalrous and, thus, competitive (Romer, 1990). Still another example is the support needed to generate new technology. This is seen as a non-rival, partially excludable factor for production. Governmental support of innovation and technology is a major requirement, especially in imperfect markets (Romer, 1990). Contrary to the New Economics Growth Theory, an earlier model, the Neoclassical Growth Model, assumes perfect competition. Based on this assumption, the theory argues that the market can achieve an optimal allocation of resources including technology investments (actually technology is exogenous, not accounted for within the neoclassical model) (Aghion & Howitt, 1998). In the 1950s, Robert Solow crafted a theory that addressed this problem, building a model that kept diminishing returns to capital and labor, but which added a third factor—technical knowledge—that continued to prod economic productivity and growth (Solow, 1956). Solow's model depicted technology as a continuous, ever-expanding set of knowledge that simply became evident over time—not something that was specifically created by economic forces. This simplification allowed economists to continue to model the economy using decreasing returns, but only at the cost of excluding technology from the economic model itself. Because technology was assumed to be determined by forces outside

the economy, Solow's model is often considered an "exogenous" model of growth. The New Growth Theory challenges the neoclassical model in many important ways. The exogenous growth models developed by Solow and other neoclassical scholars generally did not try to explain what caused technology to improve over time. Implying that technology "just happened" led to an emphasis on capital accumulation and labor force improvement as sources of growth. This approach led Romer to state that the classical suggestion that nations can grow rich by accumulating more and more pieces of physical capital is wrong (Romer, 1986). The underlying reason is that any kind of physical capital is ultimately subject to diminishing returns; economies cannot grow simply by adding more and more of the same kind of capital.

In Romer's New Economic Growth theory, the public-private goods debate is important. Depending upon the theoretical approach, activities that are at the heart of a "value chain" approach, such as public support for innovation and improved business processes can be justified. This new economic growth model had been pivotal to the establishment of the value chain approach (Porter, 1985). The value chain approach is an important development strategy driven by the "virtuous cycles" resulting from ICT and innovation investments and that can positively affect growth (Argyrous, 2001). Such impact is depicted in Figure 5. As the figure shows, both value chains within organizations and value webs across organizations and industries are affected by the virtuous cycles introduced and enhanced by ICT and the innovation waves in an economy. The value chain focus on "virtuous cycles" as embedded in the endogenous growth model underscores the need for investment in technology and innovation, where the resulting improvements in productivity and business processes and the subsequent growing returns are pivotal to promoting economic growth.

Figure 5 Virtuous Cycles – Endogenous Growth



Source: Influenced by Argyrous, 2001 and Porter, 1985.

Complementarity Theory

The “complementarities” concept was introduced by Edgeworth (1881) in which he defined activities as complements, if doing (more of) one enhances the returns of doing (more of) the others. Many researchers have investigated the complementary relationships among various business practices. For example, Black and Lynch (2001) contended that there had been very little explicit or direct analysis of the impact that workplace practices have on productivity. They found some synergies among various workplace practices but concluded that the important issue is not whether an organization promotes or implements a particular work practice, but rather how that work practice is implemented in conjunction with other complementary practices.

While complementarity seems to be a crucial concept in a growth theory, it is seldom clearly defined. Milgrom and Roberts (1995) proposed a general definition, which is followed in this study, albeit at the country level. Assets or activities are perceived as complementary if the marginal return of an activity increases in the level of the other activity. In other words, x and y are complementary if doing (more of) an activity x will cause the marginal benefits of doing (more of) a complementary activity y to increase. For example, when a manufacturer invests in

better quality controls, its product reliability will increase. As a result, extending the warranty will be attractive. Thus, complementarity gives rise to ‘synergy’ among the complementary activities. In synergy, the total value exceeds that of the sum of the elements or parts (Stieglitz & Heine, 2007). Thus, to reap the full potential of corporate activities, managers, strategists, and policy makers have to take into account the complementarities among activities. Failing to do so leads to a loss in value creation, revenues, and, ultimately, in profits for the firm, because it fails to realize its full potential.

The theory of complementarities could be best summarized by stating that to achieve higher returns and better results, it takes more than “just ONE best practice” (Brynjolfsson & Saunders, 2010). In fact, to understand why some entities (firms or nations) use ICT so much more effectively than others, one must understand the economics of complementarities. The model developed by Milgrom and Roberts (1990) delineates the economics of complementarities. To clarify the concept, two practices are complementary if the returns for adopting one practice are greater when the second practice is present. For example, the returns for adopting an e-government or an ERP system may be higher in the presence of training than in the absence of training. In a similar vein, the returns for training may be higher in the presence of these technologies and systems than in their absence (Athey & Stern, 1998).

Rather than looking at complements strictly as inputs, Milgrom and Roberts (1995) examined systems of complementary activities. They demonstrated the chain reaction of business-process redesign that can accompany a change to even one element or piece of technology. They offered an example of the introduction of CAD/CAM engineering software in manufacturing. CAD/CAM software promotes the use of programmable manufacturing equipment, which makes it possible to offer a broader product line and more frequent production

runs. This, in turn, affects marketing, organization, inventory, and output prices. Because customers, domestic and global, also value shorter delivery times, the technology that allowed more frequent production runs gives the firm a substantial incentive to reduce other forms of production delays and to invest in computerized ordering systems (Milgrom & Roberts, 1995).

Milgrom and Roberts (1990, 1995) argued that it is important to adopt systems of complementary activities, rather than adopting one individual best practice. The authors' insights have been demonstrated by many case studies and empirical papers focusing both on the United States and on other developed countries. Some of these cases are highlighted below:

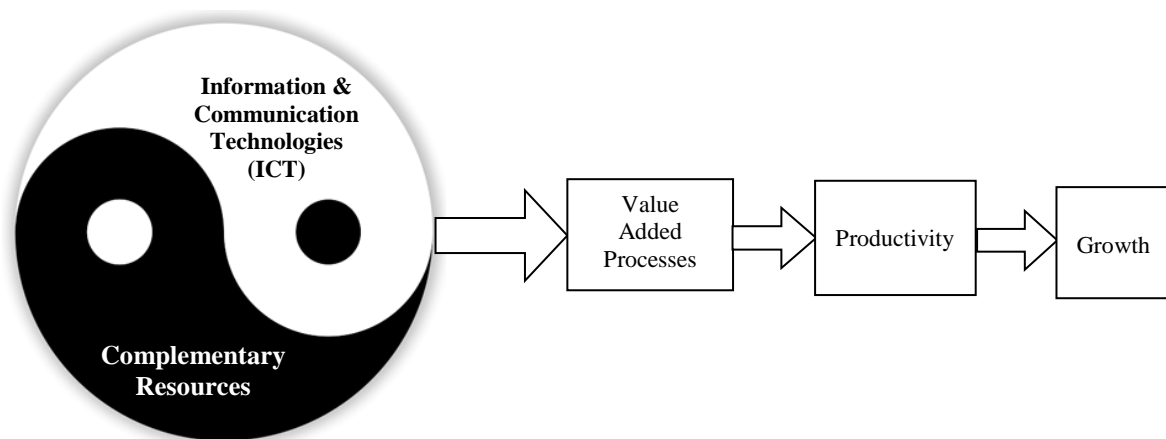
- In a recent study about how information technology (IT) may complement other key firm resources such as human capital in today's environment, Siqueira and Fleury (2011) found that the use of IT services is positively related to firm productivity and that this relationship is positively moderated by entrepreneurs' management education. Their findings indicate that firm productivity is associated with a combination of human and technology resources. The authors contended that this has become a common situation that is particularly critical for small businesses operating in developing countries with emerging economies.
- An empirical paper concerning the relationships between complementarities and productivity, Bresnahan et al. (2002) conducted a firm-level study of about 300 large American manufacturing and service firms. Studying the organizational complements to technology and their impacts on productivity, the authors found that “increased use of IT, changes in organizational practices, and changes in products and services taken together are the skill-based technical changes that call for a higher skilled-labor mix” (p.

341). Furthermore, they found that interaction of IT workplace organization and human capital are good predictors of productivity.

- In another recent study at the national level, successful IT deployment in Least Developed Economies (LDEs) was examined (Prasad, 2011). The author contends that this requires a complementary presence of related resources. Isolated IT investments do not improve organizations' business processes. Organizations can achieve better payoff from IT investments when other complementary factors such as decision authority, training and development, and investment policies change in a coordinated direction.
- In conformity with Prasad (2011), national productivity gain studies show that developing countries do not experience desired gains associated with IT investments (e.g., Pohjola, 2001, Dewan & Kraemer, 2000), because of insufficient investment in complementary assets to permit them to enjoy IT-related productivity benefits (Dewan & Kraemer, 2000, Shih et al., 2008). Coordinated changes in organizational resources will first help organizations and nations attain specific business objectives at the process level (Alter, 2003). This means that assessment of the business value of IT investments should reflect a direct path from IT and IT-related investment to specific metrics that reflect the business objectives being sought (Dehning et al., 2007). IT and complementary factors also affect overall organization-level performance, albeit indirectly (Dehning & Richardson, 2002). The measures of IT-related value at the process level capture the direct effect of IT investments and related complementarities. Relating the process-level performance to organization-level performance captures the indirect effect of IT and IT-related investments. This theoretical framework defines the basis for the hypotheses development in the next section.

The above cases show that there are two ways in which complementarities reveal themselves empirically. First, complementary practices often are correlated with each other. If managers, strategists, or policy makers know that training is complementary to ICT investments, then training expenditures and other human capital development aspects will tend to be higher when ICT investments are higher, and vice versa. Second, performance often is higher when complementary practices are adopted together than when they are adopted separately (Brynjolfsson & Saunders, 2010). Indeed, this is the definition of complementarity. At the same time, it draws attention to the crucial role of governments, strategists, and policy makers in setting effective strategies at the national level so as to encompass all the related complementarities in an attempt to better reap the benefits of ICT and innovation toward achieving value-added activities and higher growth competitiveness. This complementarity between ICT and complementary resources is illustrated in Figure 6.

Figure 6 ICT and Complementarities: Impact on Growth



International Relations Related Theories: National Security and Deterrence Theories

Cyber security is a pivotal factor in national security (DHS, 2010). David Jablonsky (2001) defines national security as that part of government policy whose objective is to create national and international political conditions that are favorable to the protection or the extension of vital national values against existing or potential adversaries. Jablonsky defines national security in terms of the respective elements of the power base of the state and the priorities that are seen as of vital and/or national interest.

Nowadays, the protection of critical information infrastructure has reached the international political security agenda. Cyber terror is often mentioned in relation to these threats, but the menace in fact ranges far wider, from more straightforward crime to natural disasters and even basic human error. But comprehensive protection against the entire range of threats and risks at all times is nearly impossible, not only for technical and practical reasons, but also because of the associated costs. What is possible is to focus protective measures on preventive strategies and on trying to minimize the impact of an attack when it occurs (Cavelty, 2008).

Within the growing literature on the topic of cyber security, many authors have addressed technical aspects of this increasingly important concept, providing practical guidance for security experts and infrastructure designers (Lee et al., 2002; Abu Nimeh et al., 2013). Others have focused on deterrence as a governmental organization policy and strategy (Rosenweig, 2010); and still others dealt with the issue from a domestic and international law perspective (Schmitt, 2010). Relatively speaking, few researchers have addressed the cyber security issue using the international relations theory (Waltz, 1979) as a theoretical foundation. Within this framework,

strategies like international cooperation (Cavelty, 2008, 2007) and law enforcement (Neumann, 2002; Lijphart, 1974) are well implied and considered.

Cyber security literature also includes another derivation from the international law theory; namely, deterrence. Deterrence is commonly thought about in terms of convincing opponents that a particular action would elicit a response resulting in unacceptable damage that would outweigh any likely benefit. Rather than a simple cost/benefits calculation, however, deterrence is more usefully thought of in terms of a dynamic process with provisions for continuous feedback. The process initially involves determining who shall attempt to deter whom from doing what, and by what means. Within this frame of reference, deterrence could be in the form of weaponry, and in the case of cyber space, other forms of cyber-attack deterrence may include legislation, international collaboration, and effectively secured communication lines (Kshetri, 2010; Nickolov, 2006; Shue & Lagesse, 2011; Neumann, 2007).

National efforts to combat cyber threats and attacks have to take into consideration the fact that the vulnerability of modern societies, caused by their dependence on a spectrum of highly interdependent information systems, has global origins and implications. The information infrastructure transcends national boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside on the territory of other states. Additionally, cyberspace--a huge, tangled, diverse and almost ubiquitous web of electronic interchange--is present wherever there are telephone wires, cables, computers or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone (Cavelty, 2007). Any adequate protection policy that extends to strategically important parts of the information infrastructure will thus require global solutions: global cooperation and joint law enforcement. According to Cavelty (2008), activity at the international

level should concentrate on challenges that cannot be mastered by a state or region on its own, such as global infrastructures, like the Internet, or truly large-scale interdependencies. By taking such steps, international organizations can help to strengthen the complex and at times overlapping web of national and regional initiatives in the realm of critical information infrastructure protection (CIIP), and can improve the security and dependability of systems, management practices and international policing efforts.

Because it is mainly infrastructure providers that are in a position to install technical safeguards for information technology security at the level of individual infrastructures, national governments depend on cooperation with the private sector to provide the public good of security to their citizens. But national protection measures only go so far: securing the global information infrastructure is a global task. Currently, divergences between national CIIP policies are a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors. However, in consideration of their economic and security interests, industrialized states are working to overcome these temporary obstacles in order to move resolutely toward robust international conventions and mechanisms that protect the global information environment. As for the cyber security measure, this study is adopting the theoretical framework followed by Cavelty (2008); namely, approaching the concept from a national security perspective, considered a sub-field of international relations.

Literature Review

The use of technology has resulted in more reliable power with a reduced need for manpower and resources. Cyber technology provides everyone with immediate global reach and exponential decreases in the constraints of time, distance, and power required. This manifests the

double-edge sword that ICT represents. While technology adoption has provided efficiencies, it also has its limits and challenges. For example, the use of information technology in the power grid has also resulted in weaknesses throughout the national electric grid infrastructure (Assante, 2009). These vulnerabilities allow cyber adversaries to attack the infrastructure without the need to be in close physical proximity.

Cyber security can simply be defined as security measures being applied to computers to provide a desired level of protection. The issue of protection can be defined using the acronym CIA for confidentiality, integrity, and availability. As will be discussed later, cyber security and the protection of critical information infrastructures involve these three basic principles. Nevertheless, cyber security is a complicated process with its details being far from simple (Conklin & White, 2006). In reality, the history of computer security can be viewed as one of regression. Early computer systems offered high security, but relative to today's functionality, very little in terms of availability. As software vendors increased functionality, moving to PCs, then distributed computing and now toward web services, data availability increased by orders of magnitude. But with this increase came issues of confidentiality and integrity. The driving principle behind much of the software being developed was one of features first, other things like security later. In the past few years, an increase in attention to security issues has dominated the software industry (Carter & Belanger, 2005).

The basic design of the Internet was built around shared access and trust, with security measures being an afterthought. There are many protocols in wide use that offer little if any security to their users and instead rely on trust. This model made sense when the Internet was first developed, for the information being transferred was of little value to others than the owners. Today, the Internet is used to transfer information between people, their healthcare

centers, their banks, their businesses, and government entities. This information can be of significant value to others, including criminals, as the current level of cyber-attacks, identity thefts, and phishing attacks attest (Conklin & White, 2006).

With the crucial impact that information has on individuals, entities, and entire societies, it is prudent to examine the relationships between information intensive processes such as innovation and information communication tools such as ICT on one hand and cyber security on the other. It is also important to examine these relationships within the framework of a nation's economic growth or growth competitiveness. With this in mind, the following sections will portray the literature related to these important concepts and relationships.

Innovation and ICT in the Economic Growth Model

Schumpeter's analysis of technological change started with an invention by attributing it to creative thinkers who invent new products or processes; innovation by entrepreneurs who develop means for their implementation; and finally to their adoption and use by a certain sector (Day, 2008). The incorporation of IT into the economic growth theory has occurred throughout the economics body of literature over a long period of time. From the classic growth model of Ramsey (1998) to Cass's (1965) neoclassical growth model all the way to Romer's growth model (1990) which considered technological progress as an endogenous factor, technological change within an analytical growth framework has been progressively refined (Omay & Baleanu, 2009 as adopted from Chiang, 1992).

To elaborate, a brief review of the economic growth literature would reveal that the incorporation of technological change has been different in different models. Solow (1956) viewed technological change as exogenous in his neoclassical economic growth theory. Robert Solow's (1957) modeling of economic growth highlighted the importance of the productivity of

factors, termed as ‘technical change’, in the economic growth process rather than the quantity of input factors (such as labor and capital). Investment in education and effective training programs were pointed out to partly affect labor productivity, whereas investments in R&D that would stimulate innovation were emphasized as important in influencing the fixed capital productivity (Burnham, 2009). The contribution of technical change, rather than the increased use of capital or labor in the enhancement of growth, was demonstrated by Solow (1957) and Dennison (1985), who analyzed the trends in the American Economic Growth from 1929 to 1982.

Nevertheless, using traditional economic growth models, one cannot conduct a comparative analysis of income levels across countries unless TFP – total factor productivity – meaning technical change is assumed constant across all countries. Based on this, differences in economic growth or income levels will emanate from differences in measurable inputs such as investment in R&D or in human capital, with the underlying assumption that the technology available is a common factor for all countries (Burnham, 2009). According to the author, a critical weakness in this assumption is the failure to realize that technology availability doesn’t imply technology use and diffusion. Earlier researchers such as North (1990) and Landes (1998) highlighted the failure of previous economic growth models to incorporate new technology adoption as key in assessing a country’s economic performance.

Later models (e.g., Arrow, 1962 and Rebello, 1991) did not incorporate technological change. A significant contribution to the literature was made by Romer’s (1986) endogenous growth theory, where the technological change was regarded as an endogenous factor determining the economic growth rate while highlighting the importance of research and development (R&D) in the growth process. It also emphasizing that fiscal policy, effective legal framework, sound property rights protection, and proper international trade regulations are

among a multitude of factors that substantive growth depends on. With the increasing importance that technology has gained in growth theory, researchers investigated the spread of technology across countries. Earlier studies (e.g., Grossman & Helpman, 1991) proposed that technological developments achieved by a ‘leader’ country can be imitated by a ‘follower’ country. However, other studies contended that innovations are a distinctive and particular economic concept with both ‘public’ and ‘private’ aspects (Dosi, 1988).

In a similar vein, later studies contended that technological innovation cannot be considered a purely public good since imitating it is costly, and most of it is tacit with only a part of the knowledge pertinent to it codified (Archibugi & Michie, 1998; Zack, 1999; Johnson et al., 2002). While the latter part can be easily transmitted with communication technologies--although it still needs to be understood and used--the former part can only be communicated through experience, which brings human capital into the frame of analysis (Fratesi & Senn, 2009).

The Technology Evolving Economy. Day (2008) portrays an interesting description of the historical and progressive development of a new kind of society or environment that he termed the ‘Technology Evolving Culture’. For thousands of years, the human mind focused on the formation of varied niches and societies through adapting to and challenging natural environments. Later, hard conditions imposed by competitive pressures led to the formation (or innovation) of social organizations, styles of living, and cities/states with resulting cultural, economic, political, and military entities and interactions among them. This also led to work specialization and the formation of the concept of the cooperative organization. According to Day (2008), the impacts of technological transformation have been asymmetric:

“Not all peoples participated in the process. Its incidence, benefits, and costs have been distributed asymmetrically within and among the various regions

and peoples of the world. Some did not attract exploration and commerce by the advancing economies. They continued existence in the pre-civilized state. Others were absorbed, still others simply disappeared ... by the advancing tide of civilized societies.”

The character of this technology-evolving culture could be identified by just examining the changes that occurred over the last five generations. From the telegraph, internal combustion engine, the radio and moving pictures invention to the automobiles, commercial aviation, highways, electrification, and invention of computers, all the way to the Internet, iPods, smart phones, and other wireless technologies, the character of this culture could be analyzed at the micro and macroeconomic levels. At the micro level, transformations took place in farms, factories, and households, and at the macro level, market economies realized high economic growth, increased productivity levels and increasingly better standards of living. At the global level, advancements in information and communication technologies made it possible to bring information from all over the globe and make it accessible to all people regardless of time, place, and income level. This has stimulated a flow of ideas, practices, and cultural aspects across nations and regions (Day, 2008). With all these positive global aspects of the technology-evolving culture comes a negative aspect – that of the destructive potential that technological transformations made possible (Day, 2008) including advanced weaponry, organized terrorism, and the alarmingly increasing risk of cyber threats and attacks.

Economists’ and researchers’ interest in economic growth has been long-established. In *The Wealth of Nations*, Adam Smith (1776) emphasized the concept of ‘the invisible hand’ of the market as the main driver of development, requiring “peace, easy taxes, and a tolerable administration of justice” (Quoted in Burnham, 2009). In fact, looking at development, one can

find that it represents a *transformation* of society, a movement from traditional relations, traditional ways of thinking, traditional ways of dealing with health and education, and traditional methods of production, to more “modern” ways (Stiglitz, 1998). Given this definition of development, it is clear that a development strategy must be aimed at facilitating the transformation of society, in identifying the barriers to, as well as potential catalysts for, change. For example, in East Asia, many of the policies on which the governments focused were simply areas that had been ignored in the past; these included, for example, the heavy emphasis on education and technology, and on closing the knowledge gap between them and the more advanced countries. While the impact of individual policies remains a subject of dispute, the mix of policies clearly worked well. Perhaps had these countries followed all of the dictums of liberalization and privatization, they would have grown even faster, but there is little evidence for that proposition (Stiglitz, 1998). Of course, this emphasizes the importance of taking the complementarity theory into consideration.

In general, and except for very few cases, interest in the issue of long-term economic growth declined over a long period of time, but surged again in the past several decades. In analyzing the reasons behind this renewed interest, Burnham (2009) suggested two major forces:

1. A general consensus that up to the year 1800, there was a period of long stagnation with only very little improvement in the average standard of living in Western Europe and China (considered the world’s major population centers). However, the past 200 years have witnessed significant improvements in the income levels of several countries, but most remarkably in North America, Western Europe and Japan. Also, East Asia, China, and India witnessed some remarkable growth leaps. Consequently, the gap between the

richest and the poorest countries grew to the order of 25:1, but then narrowed significantly because of the growth leaps achieved by East Asia.

2. The post-World War II political situation between the NATO members and the Soviet Union raised interest in the different economic systems applied in the two regions. Of equal interest was the economic growth in the “Third World” countries, particularly those that were under the regimes of Western colonial empires.

In fact, resisting the adoption of new technologies or innovations can bear negative consequences on a firm’s or a nation’s competitiveness level. The disruptive nature of new technologies or work processes could be feared by some parties who may view the ‘new’ entities as a ‘threat’. Here emerges the important role that a country’s institutional body and political system play in facilitating and encouraging ‘innovativeness’. This role includes initiatives like enhancing the freedom of experiment, facilitating easy entry into business, as well as developing an effective legal system that reduces risks on multiple levels (Rosenberg & Birdzell, 1986, Phelps, 2007).

For example, DeSoto (1989) highlighted the importance of entrepreneurship as a powerful means for transferring technology and new ideas into an economy, thus enhancing its competitiveness and growth (DeSoto 1989, as adapted from Burnham, 2009). Burnham (2009) contended that this is possible only when enabled by the prevailing institutions and laws, as regulatory hurdles may make it extremely difficult to start a new business or implement a new idea. In fact, self-imposed constraints such as restricting freedom of experimentation, the adoption of new technologies, and the adoption and implementation of more efficient processes can all be answers to the question of why poor countries don’t use the existing knowledge and available technologies more efficiently (Parente & Prescott, 1994, 1999), that is, to the question

of why asymmetry is observed in technical change and hence economic growth and competitiveness across countries.

Furthermore, using the economics of the transactions costs perspective, Burnham (2009) showed how the telecommunications technology could impact the total factor productivity through sharp reductions in cost, cycle times, and capital investment. Besides cost reduction, the author argued that such developments helped in achieving market extensions, more efficient resource allocation, and increased returns. This implies that telecommunication technologies can contribute to economic development. Evidence from Burnham's (2009) analysis and Parente and Prescott's (1999) discussion, the distinction between technology development and technology deployment is important for public policy, especially in developing countries, where firms can adopt technologies that are developed in other countries without incurring the same high costs of investment. The policy implications of such a distinction would be in governments' initiatives to reduce barriers to entry, enhance the freedom of experimentation, reduce or eliminate unnecessary regulations, and avoid protecting monopolistic market structures as new entrepreneurs seek to introduce new technologies, processes, or business models. A case in point is Turkey, where in 1987, the requests for fixed-line service was huge and remained so until 1994 when two private companies were authorized to provide mobile services under an agreement to share revenues with Turkish Telecom (then the monopolistic government-owned fixed line provider). By 2002, the number of mobile phone subscribers increased, service improved, and the waiting list decreased, thus enhancing sector efficiency. Similar examples could be cited where reduced regulations and barriers to entry of new entrepreneurs have contributed to effective ICT and innovation diffusion.

Innovation and ICT

Innovation and ICT, as main drivers of competitiveness and sustainable growth, enable the reduction of the digital, economic, and social divides within each country, and among countries. A recent analysis made by the European Commission (European Commission, 2010) shows that even before the global economic crisis, Europe was not progressing fast enough relative to the rest of the world, and the productivity gap has widened over the last decade. This was due to many factors, including the insufficient use of ICT, the lower level of investment in R&D and innovation, the “reluctance in some parts of our societies to embrace innovation,” etc. Thus, the importance of *the dynamic relationship between "the use of ICT" and "innovation"* is becoming more and more politically recognized (European Commission, 2010).

The topic has attracted much interest and has been the focus of major research work. Table 3 presents a list of some of the research articles that discuss the relationship between ICT and innovation. The role of ICT as a major catalyst in innovation processes has been an area of investigation of several research papers. Previous research dealt with the topic at the firm level (e.g., Ollo-Lopez & Aramendia–Muneta, 2012; Howells, 1990, 1995; Rosenkopf & Nerkar, 2001; Zander, 1999; Tegarden et al., 1999), or at the country level (e.g., Trajtenberg, 2005; Economou, 2008; ITU, 2008; Tiwari et al., 2007).

At the firm level, Bartel et al. (2007) presented an analysis of 212 manufacturing plants to examine how ICT investments affect business strategies and innovations. The study found that plants that adopted ICT had a shorter setup time in production, and could devise ways to customize production runs in shorter processes and smaller runs, thus avoiding the use of longer batches. Another major finding reported by the study was that the increased use of ICT also leads to the adoption of new workplace practices and raises the demand for more skilled workers.

Studies examining the success and survival of healthcare organizations indicated efficiency and effectiveness of Information technology/systems use or implementation as major factors (Liaw, 2002). Similarly, Thakur et al. (2011) contended that easy to use and effective technology should enhance innovation in healthcare organizations.

Table 3 Summary of Research Articles examining ICT-Innovation Relationship

Research Article	Purpose	Unit of Analysis	Type	Main Outcomes
Tiwari et al. (2007)	Proposing a model for the chances and challenge of global innovation activities based on previous empirical studies.	Country	Conceptual	<ul style="list-style-type: none"> • ICT is one of the major forces that drive global innovation networks • Major barriers (e.g., finding qualified HR, bureaucracy and problem finding the right cooperation partners) as well as major opportunities (such as accessing global expertise and know-how reducing bottlenecks in the R&D pipeline, learning from lead markets and so on) were derived.
Prasad (2011)	Impact of ICT and complementary resources on business value of firms operating in Least Developed Economies.	Firm	Empirical (survey & interview)	<ul style="list-style-type: none"> • ICT investment, along with complementary assets (training and human IT capital) can foster process innovation leading to overall organizational benefits.
Zander (1999)	Proposing and testing a model for the relationship between innovation networks in the multinational corporation and the international dispersion of technological capabilities	Inter-firm	Empirical	<ul style="list-style-type: none"> • Significant references in the structure of international innovation networks across industries and firms in terms of internationalization and diversification of international capabilities
Infodev / World Bank (2007)	Examining the impact of ICT investment and utilization on innovation and then on productivity and competitiveness.	Firm	Empirical	<ul style="list-style-type: none"> • ICT impact on innovation is powerful only when a number of complementarities exist (training, salary structure, new marketing strategy ...) • ICT impact on innovation is different in different sectors (information intensity). • Role of ICT is different for different types of innovation.
OECD (2008)	Examining the relationship between ICT and development via its impact on foreign direct investment (FOI)	Country	Empirical	<ul style="list-style-type: none"> • ICT exerts a positive influence on innovation and entrepreneurship, which are important determinants of FDI.

Ollo-Lopez and Aramendia-Muneta (2012)	Examining the impact of ICT on competitiveness, innovation, and environment in firms operating in the glass, ceramics, and cement concrete industry.	Firm	Empirical	<ul style="list-style-type: none"> • ICT has different effects on product innovation and process innovation. • LAN and wireless LAN have no effect on innovation. • Design software, CAD, has positive effect on product innovation. • CAD and ERP have positive effect on process innovation. • Use of online services has positive effects on process innovation.
Lewin et al. (2009)	Identifying the determinants of offshoring innovation (product development activities such as R&D, product design, and engineering services) by companies searching for talent.	Firm	Empirical	<ul style="list-style-type: none"> • The growing shortage of technical talent and the search for ICT-experienced HR as well as science and engineering talents are major drivers for outsourcing innovation activities.
Trajtenberg (2005)	Providing a framework related to designing innovation policies for development in Israel, with an emphasis on the main levers of innovation policies: skills formation, incentives provision, access to information, and finance availability.	Country	Conceptual	<ul style="list-style-type: none"> • ICT can prompt growth only through “innovational complementarities”. Also, along with the other three innovation levers, access of the information is a necessary condition for innovation to take place.
Belitz et al. (2011)	Developing a composite indicator for measuring the performance of national innovation systems.	Country	Empirical	<ul style="list-style-type: none"> • Drawing on previous literature that examined and assessed the neoclassical models (endogenous model and Schumpeterian theory), the authors generated an innovation index based on the following perspective: innovation is determined by the “interplay” of different economic and social factors more than by technological levels or developments.
Soriano (2007)	Examining the impact of ICT on economic development and poverty reduction.	Country	Conceptual	<ul style="list-style-type: none"> • ICTs can play an instrumental role in generating the means to enhance the access and adoption of livelihood strategies and resources.
Palfrey and Gasser (2007)	Studying ICT interoperability and examining its relationship to innovation.	Firm	Empirical qualitative	<ul style="list-style-type: none"> • Interoperable systems in ICT can lead to innovation. This can be achieved in some cases by reducing lock-in effects and lowering entry.

				barriers.
Tidd (2006)	Reviewing and discussing the various models of the innovation process and their empirical evidence. Discussing the factors that influence the process as well as the 2 main types of innovation: incremental and radical.	Innovation model	Conceptual	<ul style="list-style-type: none"> Effective innovation processes very much depending on complementary assets in production, marketing, and services to complement those in ICT.
Koellinger (2008)	<ul style="list-style-type: none"> Examining the impact and the relationship of IT and innovation on firm performance. Investigating the present situation of innovation to understand the impact of IT implementation to innovate. 	Firm	Empirical	<ul style="list-style-type: none"> IT is positively related to innovation. Innovation is a mediator of IT and firm performance. Innovation is positively associated with firm performance.
Yu and Xin-quan (2011)	<ul style="list-style-type: none"> Exploring the relationship between information technology capability and innovation commitment. Examining the impact (moderation) of learning commitment on this relationship in Chinese firms. 	Firm	Empirical	<ul style="list-style-type: none"> Information technology capability has a positive effect on innovation performance. The interaction between information technology and learning commitment is positively related to innovation performance.
Chen and Tsou (2006)	<ul style="list-style-type: none"> Investigating the impact of IT adoption on service innovation and firm performance in financial organizations. 	Firm	Empirical	<ul style="list-style-type: none"> IT adoption, involving IT strategic alignment, management processes, and individual learning, has a positive effect on service innovation. Service innovation has a positive effect on firm performance.
Johannessen et al. (1999)	<ul style="list-style-type: none"> Examining what companies use IT for and the consequences of these uses for innovation and a variety of performance measures. 	Firm	Empirical	<ul style="list-style-type: none"> IT is positively related to performance. If IT is used to increase effectiveness, improve internal communication, or change existing work processes, then it can lead to successful innovation implementation. If IT is used to reduce costs, it will have a negative effect on successful innovation.

At the country level, researchers have contended that ICT represents a new ‘General Purpose Technology’ that has the potential to create a transformation process that would generate sustainable economic growth through innovation (InfoDev, 2007). Nevertheless, the study found that in transition economies, ICT utilization can substantially affect process innovation, moderately affect product innovation, and marginally affect relational innovation (Infodev, 2007). The same study found that in general ICT by itself is a minor facilitator of innovation. Its contribution will be powerful only in combination with some complementary factors (such as training and organizational change). Another study showed that ICT is pivotal for organizations in developed economies to attain and maintain competitive advantage through fostering continuous innovation of their products and processes (Walsham, 2010). An earlier notable study of the role of ICT in innovation and economic growth is the World Development Report presented by the World Bank and entitled: ‘Knowledge for Development’ (Stiglitz, 1998). The report contends strongly that the information revolution and ICT stimulate the creation and acquisition of new knowledge by giving inventors and innovators wider availability and faster access to knowledge. Several observations could also be derived from the table:

1. Studies examining the ICT-innovation relationship at the firm level outnumber those at the country level.
2. The reported results regarding the ICT–innovation relationship at the firm level were mixed, with some reporting a direct relationship, and with others reporting that ICT can foster innovation only with other complementary assets or resources.
3. Mixed results were also reported by studies examining the relationship at the country level. While some studies found a relationship between ICT and innovation, others

reported that innovation is more a result of social/economic factors than of technological developments/advancements.

Earlier research studying the impact of information technology on innovation introduced the concept of exovation (Johanessen, 1994 as adopted from Clark and Staunton, 1989), which refers to the conditions that should be met to ensure full utilization of the innovation potential. In line with this concept, Johanessen (1994) discussed five elements as being crucial for the relationship between IT and innovation. These are: (1) change agents (or innovation champions as mentioned by Beath (1991) and Rogers (1995); (2) organizational culture; (3) management style; (4) the market; and (5) coordination and service (Johanessen, 1994).

Furthermore, earlier research discussed the growing importance that innovation had gained in the official statistics in Canada and EU Countries during the 1990s. The governments in those countries had aimed at setting a policy for enhancing the economy through the introduction of new processes as well as new or significantly improved products (Gault & Peterson, 2003). As a result, surveys during that period of time found that 33% of innovative firms in those countries got involved in collaborative or cooperative arrangements as part of enhancing the innovation process (Schaan & Anderson, 2001 as adapted from Gault & Peterson, 2003). Innovative ideas were sought from the market, conferences, and the Internet. Of course, such knowledge acquisition and implementation were facilitated to a great extent by the use of ICTs (Gault & Peterson, 2003).

Previous research also has examined innovations with the factor of uncertainty being considered. Uncertainties related to technological innovations are of major concern to all economies, including the high-tech advanced countries for two crucial reasons. First, in high-tech sectors of OECD economies, R&D conduct is highly expensive; and second, there is a big

financial risk related to R&D expenditure (Rosenberg, 2004). According to the author, these financial risks are attributed to the (a) possibility that spending on scientific research may fail to generate useful new scientific knowledge; and (b) the possibility that even if new scientific knowledge emerges, it may not be applicable in terms of new marketable products, or it may not be profitable in terms of cost-effective designs. In addition to this, Rosenberg (2004) discussed other types of uncertainties including: the new innovation's performance, not only at the technological, but also at the economic level; its appropriability (as pertinent to making profit out of the innovation by the innovating entity before it gets imitated by competitors—if it is not patentable); and the threat it faces from the introduction of new competing technologies.

Moreover, examining the role that innovations play in a nation's economic growth or competitiveness requires an understanding of how innovations evolve. Most major innovations start in primitive conditions, and then evolve through a long process entailing cost reductions and technical improvements (Rosenberg, 2004). Merely applying enhanced computer technologies to work patterns and processes that were designed for older and slower technologies is likely to yield very little in terms of enhanced performance and productivity improvement (Rosenberg, 2004). In a similar vein, introducing advanced ICT to nations where outdated and restricted policies prevail is likely to impede its effective diffusion and its potential contribution to the economy of the adopting nation.

ICT and Growth Competitiveness

The question, “Why do some nations succeed and others fail in international competition?” (Porter, 1990) has been since earlier times an interesting question for both scholars and researchers to examine and answer. Nowadays, the rapid growth of economies, technological advancements, and strategic and economic alliances among countries are a few of

many reasons that have made global competitiveness a widely discussed topic. In this study, the emphasis is on the contribution of ICT in the achievement of high scores in the global competitiveness spectrum.

The huge advancements witnessed in the world of IT have been reported to enhance efficiency and rapid access to knowledge and information (Grant, 1996; Berkley & Gupta, 1994). Still, the benefits of IT and its contributions to economic performance were doubted by several earlier researchers (e.g., Sweeny, 1996; Brody & Stabler, 1991). Robert Solow (1987) argued that the computer age could be seen everywhere except in productivity statistics, which has been referred to in the literature as “the productivity paradox” (Jarvenpaa & Ives, 1994; Brynjolfsson and Hitt, 1993).

In response to this argument, other researchers argued that there is little doubt that IT has enormously contributed to performance, although such a contribution is not reflected in macroeconomic measures of productivity (Quinn, 1996). Still others made a further step and suggested that when innovation is emphasized, it would be inadequate to use conventional productivity measures when assessing the impact of IT on business (Johannessen et al., 1999). Also, the role that IT or ICT plays in economic growth should take into consideration the effect of complementary resources (Brynjolfsson & Saunders, 2010).

In the literature, success is often referred to as a low occurrence of incidents leading to undesirable results (Kaplan, 2002). For example, organizations such as healthcare providers, are based on the dimension of high reliability. Managers in such organizations make decisions in a highly dynamic and uncertain environment (Jha-Thakur, 2011). These organizations usually rely on a complex type of interaction between several entities, including patients, physicians, insurance companies, and pharmaceuticals. With such intricate interactions, it is logical to

assume that the success of such organizations is highly likely based on accurate and timely information, processes, and description of conditions (Nemeth & Cook, 2007). Globalization, ICT adoption affordability, the deregulation of the telecommunications sector, and the enabling role that the Internet has played in promoting business and state organizations have all contributed to the increase in ICT use (Gault & Peterson, 2003). “Global ICT application” could be defined as an application that contributes to achieving a global strategy by using ICT platforms to store, transmit, and manipulate data across cultural environments (Ives & Jarvenpaa, 1991).

Misalignment of ICT with global strategies (at the firm as well as the national levels) can drastically hamper efforts to attain and maintain global prominence (Ives & Jarvenpaa, 1991). The authors suggest that at the firm level this alignment requires a shared understanding by IT department staff and the other business staff of the organization’s overall business strategy. This may imply that at the national level, there should be a common understanding of the nation’s overall global strategies by ICT policy makers, ICT designers, as well as private and public organizations across all sectors.

These global strategies are therefore affected by the available and deployed ICTs. Keen (1987) contended that international capabilities are driven to a large extent by telecommunications architectures. This is why the author emphasizes the importance of carefully designing the infrastructure and setting IT international standards (Keen, 1987). Countries like Germany, Japan, and France have long used information policy in order to protect their national computer and telecommunication systems (Lerner, 1984). Moreover, standards for electronic data interchange (EDI) have been established jointly by the United Nations and ANSI—American National Standards Institute (Ives & Jarvenpaa, 1991).

These standards are crucially important with the growing volume of international data sharing, which has gained considerable attention from researchers as well as legislative bodies (Ives & Jarvenpaa, 1991). Much of the focus here has been on data privacy as well as data flows across national boundaries, termed trans-border data flows (TDF) as mentioned by Chandran et al. (1987). TDFs have been classified into four categories: (1) operational data; (2) personally identifiable information; (3) electronic money transfers; and (4) technical and scientific data (Lerner, 1984). This is where the importance of ICT law enforcement comes into the picture, particularly for the second category.

In an attempt to reap the benefits of ICT, governments around the globe are investing huge capital amounts and are establishing plans to ensure widespread connectivity and access (Taylor and Zhang, 2007). The United Nations–Commission on Science and Technology for Development (UNCSTD) described ICT as a general-purpose technology, and accordingly, it contributes significantly to the economy. This is because: (UNCSTD, 2007)

1. ICTs promote GDP growth as a production sector, where the rapid advancement in the production of ICT products and services contributes to an increase in the total factor productivity (TFP) in the sector itself.
2. ICT investments in other sectors contribute to the increase in labor productivity.
3. ICT adoption and use allow for the creation of ‘intangible assets’ such as improved decision-making, managerial processes, and quality. These enhance efficiencies and contribute to increases in TFP.
4. ICTs can be pivotal in the generation of complimentary innovations, which will in turn increase productivity in firms, industries, or sectors using ICTs.

5. The ICTs spillover effect on GDP is very important, especially in industrialized countries. As mentioned by UNCSTD, if the spillover effects are significant, then there will be a big disparity between private and social returns. This may lead to measures toward wider ICT diffusion by the various market participants.

While these points might be referring to radically new technologies, it is worth mentioning that many innovations could be incremental; that is, built on other innovations. Moreover, the benefits of ICT progress cannot be confined to one sector, because there are complementarities associated with the use and generation of knowledge (Taylor & Zhang, 2007).

Other benefits are equally important, though less tangible. For example, increased connectivity to information networks has been recognized as a major contributor to transparency, good governance, and the development of knowledge workers (World Economic Forum, 2008). With all these benefits associated with ICT, Taylor and Zhang (2007) underscored the importance of having an empirically-based policy-guidance. The authors discussed the need for policy studies that would help in the determination of appropriate policies, regulations, and levels of ICT investment in the public and private sectors. According to the authors, these policies should draw on theory-based research as well as empirical research developed from substantial amounts of data (Taylor & Zhang, 2007).

But to what extent can ICT contribute to a nation's growth and development? Does this contribution vary across various economies? Pertinent to the first question is the classical view regarding the 'productivity paradox' as related to investment in ICT (Solow, 1957; Heshmati & Yang, 2006). Relevant to the second question is a suggestion made by research results that ICT return in developed economies could be both significant and positive (OECD, 2005; Jorgenson, 2001, 2002), but this is not the case in developing economies (Fong, 2009; Heshmati & Yang,

2006). Nevertheless, studies in general have shown mixed results, with some researchers reporting differences among developed countries (Colecchia & Schreyer, 2002) and others showing a positive and significant impact of ICT on economic growth in developing countries (e.g., Andrianaivo & Kpodar, 2011). A summarized list of the literature pertinent to ICT-growth relationship is presented in Table 4.

ICT is considered a general-purpose technology (Bresnahan & Trajtenberg, 1995). Based on this, it spreads to the various economic sectors, gets improved and becomes less expensive, enables the creation of new products, services, and work processes, and affects economic growth both as an output component (ICT production) and as an input component (ICT capital services) as well as through the effect of multi-factor productivity gains driven by ICT rapid technological advancements (Jalava & Pohjola, 2007). ICT is also considered a source of labor productivity growth through ICT capital deepening, which is the weighted increase of ICT capital services per hour worked in the income share (Jalava & Pohjola, 2007). The contribution of ICT to economic growth has been further discussed in more recent research work. Vu (2011) examined the positive impact that ICT penetration may have on economic growth through three channels derived from theoretical backgrounds, including:

- Fostering ICT diffusion and innovation;
- Enhancing the quality of the decision-making process; and
- Increasing the output level through increasing demand and reducing production costs.

Besides socioeconomic and technological factors, recent research has examined the role of language barriers on ICT diffusion in a developing country, namely Paraguay (Grazzi & Vergara, 2011). The authors found that the ICT diffusion process is heterogeneous because of differences in socio-economic dimensions. They also found that certain languages in the country

constitute an important cultural barrier to the diffusion of ICT in Paraguay, thus illustrating the cultural barriers that a developing country may face (Grazzi & Vergara, 2011).

The role that ICT plays in the determination of global competitiveness manifests itself in the contribution that ICT has in driving forward the elements that indicate or clearly reveal global competitiveness. For example, knowledge transfer, driven by the increasing size of global competition and the increasing scope of global companies (Niederman, 2005; Baroni de Carvalho & Ferreira, 2001), has been supported by the Internet and the ICT resources. This allows ICT resources to be viewed as major pipelines for knowledge transfer among organizations in various countries (Bathelt et al., 2004).

Moreover, advanced ICT resources have offered companies at various globalization levels the ability to be flexible, more responsive to changing market needs, and more adaptive to rapid changes (Tallon, 2008) through efficient and effective business intelligence systems. As a result, ICT can lead to significant changes in competitive forces (Rivard et al., 2006), more responsive supply chain and customer relationship management, and more efficient, effective, and better coordinated inter- and intra-organizational operations and mechanisms (Yeniyurt et al., 2005 and Zhu et al., 2004).

Analysis of the impact of ICT-related decisions on an organization's or a country's competitiveness level enables executives and country analysts to choose the appropriate strategy to invest in, organize, and manage ICT resources and related activities. In this respect, five key dimensions need to be considered when one is evaluating the impact of networked ICT on an organization's or a country's competitiveness level (Applegate et al., 2003). First, ICT systems are believed to change the core activities of the value chain and value web within and among organizations. This changes the basis of competition among firms at the national and

international levels. Second, using ICT capabilities effectively allows organizations to not only achieve more responsive and efficient supply chain management, but also increases the switching costs of customers. Third, ICT allows companies to increase or reduce barriers to entry in a vast array of markets. Amazon.com is a sound example of a company that could reduce barriers to entry by using Internet capabilities. On the other hand, Merrill Lynch is an example of a company that could increase barriers to entry through its invention of the Cash Management account (Ernst & Young, 1993). Fourth, ICT can change the power dynamics among buyers and suppliers by significantly decreasing costs, increasing responsiveness, enhancing order accuracy, and increasing the speed of delivery. Finally, the rapid advancements in ICT have made possible remarkable improvements in existing products and services (e.g., enhancements in digital cameras and online flight reservation) or the creation of new ones (such as mobile commerce).

Finally, the pivotal role that ICT now has in determining worldwide corporate and national strategies has been revealed in the global IT research stream. For example, this role was confirmed by earlier research (Palvia, 1997) which measured the strategic global impact of IT on an international firm. In a similar vein, the three competitive requirements of a transnational firm--efficiency, responsiveness, and learning--can be met by appropriate and advanced ICTs (Boudreau et al., 1998). Likewise, recent studies show that ICT has a strong impact on operational efficiency and flexibility (Batra, 2006), with flexibility being manifested by enhanced market responsiveness (Gunasekaran & Ngai, 2004), better customer service, and more streamlined business processes. Table 4 presents a list of some of the research articles that discuss the relationship between ICT and economic growth. Of course, these all are manifestations of global competitiveness.

These points portray a dynamic--and potentially causal--relationship between ICT and economic growth /global competitiveness. In reference to the resource-based view model, ICT can be viewed as a resource and as an enabler of dynamic capabilities that have the potential to provide the firm with a competitive advantage at the industry, national, and global levels (Wade & Hulland, 2004). The Global Competitiveness report mentions that the global competitiveness index is a function of 12 factor “pillars”, including among others: institutions, infrastructure, innovation, higher education and training, and technological readiness (World Economic Forum, 2011). Furthermore, ICT capabilities including, for example, safe and secure ICT infrastructure and technically skilled human resources, are sources of competitive advantage (Rivard et al., 2006). These factors are included as enablers of ICT readiness and diffusion, which in turn would lead to global competitiveness.

Table 4 Summary of Research Articles Examining ICT- Economic Growth Relationship

Research Article	Purpose	Sample	Source	Methodology	Main Result
Andrianaivo and Kpodar (2011)	<ul style="list-style-type: none"> Studying the impact of ICT in general, and mobile phone penetration in particular, on economic growth. Testing whether financial inclusion is a means through which ICT enhances growth. 	44 African Countries 1988 – 2007	<ul style="list-style-type: none"> International Monetary Fund (IMF) World Bank International Telecom Union (ITU) 	Econometrics tests: System GMM estimation ¹	<ul style="list-style-type: none"> ICT, including mobile phone penetration, has a significant contribution to the economic growth in African countries. Financial inclusion plays a role in enabling a positive effect of mobile phone diffusion on economic growth.
Colecchia and Schreyer, 2002	<ul style="list-style-type: none"> Comparing ICT capital accumulation impact on output growth among countries 1980 – 2000 	<ul style="list-style-type: none"> 9 OECD Countries: Australia, Canada, Finland, France, Germany, Italy, Japan, UK, and USA 	OECD and Countries' Statistics offices	Weighted Averages of rates of changes	<ul style="list-style-type: none"> Prior to 1990s, ICT contribution to economic growth ranged between 0.2 and 0.5 % /year depending on country. During second half of 1990s, percentage point ICT contribution rose to 0.3 to 0.9 % /year. US was not the only country benefiting from the ICT investment positive effect on economic growth. ICT usage and diffusion play a positive role in economic growth, not only where large ICT productivity sector exists, but rather depends on the availability of right framework conditions.

¹ System GMM estimation = System generalized method of moments. In econometrics, this refers to a generic method for estimating parameters in statistical models. This is usually applied in models that have both parametric and non -parametric components. In this case, the parameter under study is finite-dimensional; however, the shape of the distribution function may not be defined, thus rendering the maximum likelihood estimation method inapplicable (Hansen et al., 1996).

Samoilenko and Osei-Bryson (2008)	<ul style="list-style-type: none"> Exploring whether there is a complementary relationship between ICT investment and ICT human capital. Examining the impact of this interaction on GDP in transition economies (TE) 1993 – 2002. 	25 countries from Europe and former Soviet Union, Classified as TE by IMF.	<ul style="list-style-type: none"> World Bank ITU 	<ul style="list-style-type: none"> Translog formulation Cobb. Douglas production function Multiple Regression 	<ul style="list-style-type: none"> There is a statistically significant interaction effect between ICT and human capital. The human capital is crucial in affecting the economic outcomes of ICT investments. The direction of the interaction effect varies between the leader and follower subgroups in the TEs sample.
Jalava and Pohjola (2007)	<ul style="list-style-type: none"> Analyzing the impact of ICT on output and labor productivity growth in Finland 1995 – 2005. 	Finland: ICT investments and economic indicators during 1995 – 2005.	<ul style="list-style-type: none"> Statistics Finland US Bureau of Economic Analysis (BEA) 	<ul style="list-style-type: none"> A basic computational framework for the balance of aggregate supply and demand. 	<ul style="list-style-type: none"> ICT accounted for 1.87% points of the labor productivity growth, and its contribution to GDP growth is 21% from ICT production and 12% from ICT investment.
Vu (2011)	<ul style="list-style-type: none"> Examining the hypothesis that ICT penetration has positive effects on economic growth 1996 – 2005. 	102 countries from various regions: North America and Western Europe, Latin America and Eastern Europe, Asia, Sub-Saharan Africa, Middle East and North Africa.	<ul style="list-style-type: none"> World Bank ITU 	<ul style="list-style-type: none"> Regression method to identify association between ICT penetration and growth. System GMM to explore the causal link between ICT penetration and economic growth. 	<ul style="list-style-type: none"> There is a strong association between ICT penetration and growth. There is a causal link between ICT penetration and economic growth. For the average country, the marginal effect of Internet penetration is larger than that of mobile phones, which is larger than that of PCs.
Bayo-Moriones and Lera-Lopez (2007)	<ul style="list-style-type: none"> Analyzing the role of environment, human capital, competitive strategy, firm structural characteristics, and internal organization. 	<ul style="list-style-type: none"> 337 Spanish workplaces 	<ul style="list-style-type: none"> Survey 	<ul style="list-style-type: none"> Ordinary least squares (OLS) regression 	<ul style="list-style-type: none"> Results underscore the importance of multinational ownership, and a high-skilled workforce in ICT adoption. Other factors include: quality control systems, teamwork, public support, policies aimed at increasing workforce education and enhancement of ICT-strategic fit.

Innovation and Economic Growth

In advanced economies, productivity growth depends both on technological innovation and on the changes enabled by technological innovation. The increasing computerization of most businesses is a case in point. Rapid technological innovation in the computer industry has led to a quality-adjusted price decline of 20% or more per year for several decades (Gordon, 1999; Brynjolfsson & Hitt, 2003), and these declines are likely to continue for the foreseeable future. Meanwhile, nominal investment in computers has increased even in the face of precipitous price declines, reflecting the myriad new uses that have been found for computers and related technologies. In recent years, companies have implemented thousands of large and small innovations in software applications, work processes, business organizations, supply chain management, and customer relationship management.

Following Schumpeter (1934), innovations are understood as the key drivers of market change and firms have to constantly adapt to a changing environment (Prahalad & Hamel, 1990; Teece et al., 1997). Evolutionary economics has long stressed the Schumpeterian nature of the competitive process and the essential role of firm differences for understanding competitive advantage (Nelson & Winter, 2002). In this perspective, the differing corporate resource bases are a constant source for innovations. Subsequently the new products are tested in the marketplace (Stieglitz & Heine, 2007). As in the resource-based view, the firm's crucial task is to exploit its existing resources and capabilities while simultaneously developing new corporate assets for future business opportunities. It takes time, resources, and managerial effort to create new assets (Dierickx & Cool, 1989). Due to firms having different resources as well as opportunities to innovate and imitate, they differ in their potential strategic paths (Teece et al.,

1997). Established firms are constantly confronted by new threats to the value of their assets. Schumpeter (1934) termed this the process of creative destruction.

To be able to survive creative destruction and to exploit future business opportunities, organizations, governments, and national strategists have to constantly choose which resources and capabilities to develop. As Teece (1986) points out, however, innovations often only diminish the value of technological assets while leaving the potential value of complementary assets untouched. According to Teece's (1986) definition, complementary assets raise the value of a firm's technological innovations. Examples of complementary assets include marketing capabilities, regulatory knowledge, client lists, and so on. Since the values of complementary assets are interdependent, Christensen (1995, 1996) speaks of inter-asset specificity. Given that complementary assets are often not affected by technological innovations, they insulate established firms against the gale of creative destruction. Their resource bases include critical complementary assets and they therefore have the potential to negate early mover advantages of technological leaders. Firms should hence vertically integrate complementary downstream assets (Teece, 1988; Afuah, 2001). On the other hand, complementary assets allow for the innovator's successful appropriation of Schumpeterian rents as they constitute important barriers to imitation. In the resource-based view, Dierickx and Cool (1989) highlight this important role of complementary assets in explaining sustainable competitive advantages by pointing to the interconnectedness of assets that prevent imitation. Correspondingly, gaining access to complementary assets is an important motive for entering cooperative arrangements and corporate networks.

The Internet is a clear example of a technology cluster innovation (Prescott & Van Slyke, 1997 as adopted from Chin & Moore, 1991). It differs from other innovations in being a "highly

dynamic IT innovation.” In fact, as mentioned by Prescott and Van Slyke (1997), the Internet is based on the concerted work of several technologies. According to Rogers, technology clusters could be viewed as “one or more distinguishable elements of technology that are perceived as being closely interrelated (Roger, 1995, p.15). Based on this, adoption of a particular technology may lead to the adoption of another related technology, which means that the diffusion research that deals with each innovation adoption as separate and independent of other innovations is most probably, not realistic (Prescott & Van Slyke, 1997). Examining the history of the Internet (starting with ARPANET in 1969), which was based on packet-switching (that started in 1968), all the way to the Internet where reliable transmissions are enabled by TCP/IP reveals that it fits Rogers’ idea of technology clusters (Prescott & Van Slyke, 1997). According to the authors, the various innovations work together to lead to an easier and more value-added adoption.

Internal and external environments are major determining factors of an entity’s openness to adoption and deployment of innovative ideas (Becker & Whisler, 1967). At the organizational level, an organization would be open to and would adopt an innovation if they perceive and anticipate that the innovation would provide them with a relative advantage, is easy to use, and is compatible with the organizations’ operations and processes (Rogers, 1995).

Traditionally, innovations have been categorized in several ways (Prescott & Van Slyke, 1997): (1) radical vs. incremental (where radical refers to new innovations that require extensive changes in current practices/processes; and incremental refers to innovations that are continuations of previous ones and can be implemented with only minor changes in current processes); (2) product vs. process (with product innovations being perceived of value in themselves, and process innovations being valued as a means to some other objective, as stated by Tornatzky and Fleischer (1990)); (3) voluntarily vs. involuntarily used (where the innovation

being involuntarily used is mandated and has a diffusion pattern different from that voluntarily used); and (4) innovation diffusion occurring due to a technology provider push vs that occurring due to a demand pull (Zmud, 1984). More recent research studying the economic benefits of innovation categorized it as business-focused or technology-focused (Gordon et al., 2006). The authors here found that business-focused innovation produces more economic benefits to citizens of a certain community than a technology-focused innovation, though technology innovations are pivotal in making them possible and in supporting them. This is because business-focused innovations contribute more positively to the economy in terms of more or better jobs and better investment opportunities than the technology-focused ones. In fact, this latter type of innovation (which is mainly directed at providing communication and information access) was found to contribute more to social benefits, including healthcare improvement, education development and consumer benefits enhancement (Gordon et al., 2006). These benefits may overall contribute to a community's growth and development.

At the firm level, previous studies found that innovation contributes to enterprise growth (Wolff & Pett, 2006). Going back to Schumpeter, he viewed innovation as the way resources are utilized in an enterprise as a means to demands (Schumpeter, 1934). Based on this, innovation may be thought of as having a commercialization characteristic (Adams et al., 2006) and could be either technological or business related (Garcia-Muina & Navas-Lopez, 2007). While discussing innovation, it is very important to differentiate between innovation adoption and innovation implementation. The former refers to the decision made to use an innovation, whereas the latter represents the critical bridge between this decision and the actual routine use of innovation (Klein & Knight, 2005). This bridge, according to Klein and Sorra (1996), would be the transition period needed for potential users to become "increasingly skillful, consistent, and

committed in their use of innovation” (p.1057). With this in mind, individuals, organizations, and communities may experience innovation failure due to a failure in implementing them properly (Klein & Knight, 2005). Drawing on literature related to innovation implementation, the authors discussed six major obstacles on the road to innovation (Klein and Knight, 2005):

1. The low quality, unreliability, and imperfect design associated with many innovations in general and technological innovations, in particular. These were reported by earlier empirical research to have negative consequences on innovation use (Klein & Knight, 2005 as adapted from Klein & Ralls, 1995).
2. The complexity associated with many innovations and the higher or the completely new level of skills and knowledge they require of potential users. Earlier research found that complexity was significantly negatively related to the rate at which users became competent in using the technology (Aiman-Smith & Green, 2002).
3. Innovation adoption and implementation decisions are generally made by those at the upper hierarchical levels rather than jointly with the direct users. Accordingly, this low level of involvement may add to the users’ resistance which might lead to slower and lower diffusion levels.
4. Successful innovation diffusion may sometimes require new norms, routines, and roles, such as teamwork or knowledge sharing. This could be difficult for some would-be users, which would negatively influence the overall diffusion process.
5. Effective innovation implementation is often expensive in terms of time and money consumption, especially in new technology, launching, user training, support, and maintenance. This may influence organizational and group performance in the short run. Negative implementation results would most probably occur if, after all these initial

processes are done, managers and users put a lot of effort into restoring the previous performance level rather than investing in the long-term, yet uncertain, benefits of innovation.

6. Successful innovation implementation sometimes requires new work/process designs, norms, or task accomplishment methods. This may lead to what Pfeffer and Sutton (1999) called the “knowing-doing gap”, resulting in a failure to successfully implement, and reap the benefits of, a potentially beneficial innovation.

The obstacles mentioned above draw a lot of attention to the importance, as well as the challenges, of effective innovation implementation (Klein & Knight, 2005). Without effective implementation, the benefits of an innovation will be wasted, and an innovation adoption will be more a cost rather than an asset. In fact, innovation development and progress cannot be limited to internal or domestic sources of knowledge and expertise. Modern innovation management calls for the establishment of “pipelines” to access valuable technological expertise and business intelligence from around the globe (Malmberg & Maskell, 2006). This has been enabled by the following opportunity factors: (Sofka, 2008)

- Political and economic changes in many areas in the world;
- Availability of unexplored markets that could provide huge business and investment opportunities; and
- Major technological breakthroughs and developments (e.g., Internet, telecommunications) in affordable and easy to use communications.

Previous research examined the multinational firms and how they access international knowledge through foreign direct investment, for example (Anand & Kogut, 1997; Von Zedtwitz, 2004). Other researchers have more recently focused on the impact of the transfer of

knowledge across national borders on the enhancement of domestic innovation activities (Sofka, 2008). The researcher examined the impact through studying the firms' absorptive capacity—defined as their ability to identify knowledge, assimilate it, and exploit it from their external environment (Sofka, 2008 as adopted from Cohen and Levinthal, 1990). Different knowledge sources were examined, including foreign customers, suppliers, and competitors. Results showed that promising impulses of foreign innovation come from foreign customers. Moreover, firms using global innovation impulses were found to have higher levels of absorptive capacities represented by higher R&D expenditures, graduate-level education employees, and management support for innovation. They were also found to have a high degree of internationalization (for example, being part of a multinational group). Another important result was related to the relationship between a country's R&D expenditures and its international knowledge sourcing attractiveness. As R&D expenditures decrease, international knowledge sourcing becomes more likely. As for the obstacles impeding innovation activities within the firm and thus leading to international knowledge sourcing, the author reported the following (Sofka, 2008):

1. Pressure from high costs and risks;
2. Regulation and bureaucracy; and
3. Lack of technological information needed for the firm's innovation activities.

A theoretical link relating innovation to economic growth has been examined and discussed since the early days of Adam Smith (1776). Smith's major contribution was not only in articulating the productivity gains from labor specialization and technological improvements, but also in recognizing technology transfer and the role of R&D in the economy. While this contribution was significant, innovation was not formally incorporated into economic growth models until 1957 by Robert Solow. At that time, the prevailing theory was that economic

growth measured in GDP per hour of labor per unit time was attributable to capital increases. However, Solow (1957) found that capital accumulation contributed to less than a quarter of the economic growth. So, Solow (1957) proposed that the remainder of the growth, which represented about 85%, should be attributed to “technical change”. This huge amount of residual could place innovation in a central position in the economic growth analysis.

Since Solow’s model, the link between innovation and growth has been a study focal point for many researchers. For example, Romer (1986) and Lucas (1988) discussed the importance of human capital as distinct from physical capital and emphasized the role of knowledge spillovers and investments in education and training in enhancing economic growth. Romer (1986) developed an endogenous growth model with innovation represented as knowledge spillovers; and Lucas (1988) contended that human capital should be modeled with constant rather than diminishing returns.

The essential role that innovation and creativity play in enabling sustainable growth and economic development has been underscored by several researchers and international organizations (Sener & Saridogan, 2011; LeBel, 2008; Sanidas, 2004; Rosenberg, 2004; Pilat, 2004; and Gould & Gruben, 1996). Yang (2006) found that innovation, both domestic and worldwide, plays a significant role in explaining economic growth in Taiwan. The author concluded that an increase in domestic patenting can result in economic growth in the country. In addition, world-wide knowledge stocks and discovery of ideas can be major drivers to long-run economic growth in Taiwan (Yang, 2006). Innovation was also considered a major force in the economic growth of highly industrialized OECD economies (Rosenberg, 2004). A wider scope comparative study, using panel data related to 103 countries in different geographic regions,

found there is empirical evidence that creative innovation has a positive role in economic growth (LeBel, 2008).

The Impact of Cybersecurity

Along with all the benefits that the Internet, a major part of ICT, provides, it nevertheless has a dark side that has been an issue of concern to organizations, ICT designers and developers, policy makers, and researchers for more than two decades (Schneier, 2005). This dark side of ICT is threatening the very critical infrastructures of nations by increasing their vulnerability to cyber threats and attacks. This growing vulnerability led Richard Clarke (2010) to reemphasize the idea of a ‘digital pearl harbor’ especially after the many reported alarming incidents of cyber espionage and cybercrime. Of course, in this time period, it is more cost-effective to manage infrastructure systems remotely within an internet framework using easy-to-use software and network protocols. Nevertheless, this cost effectiveness and better convenience resulting from the use of ICT to manage critical infrastructures (ICT) are embedded with risk that involves the vulnerability resulting from insufficient or non-robust security measures (Geers, 2009).

While discussing the role that ICT plays in managing critical infrastructures, it is important to emphasize a unique type of infrastructure that provides the essential means for the functioning and the interdependence of the other CIs in this information age. The infrastructure being referred to here is the critical information infrastructure (CII). Since it is the enabler of CI operation as well as the networkedness of the various CIs, its protection becomes a vital requirement. At this point, and before proceeding, examples and definitions of CI, CII, and critical information infrastructure protection (CIIP) will be presented and discussed in the following subsection.

Critical Information Infrastructure Protection. Secure information systems have become a necessity for modern society. This is attributed to two important reasons: (a) the significant social and economic benefits they provide, and (b) the serious consequences of their malfunctioning (Attwood et al., 2011; Nickolov, 2005). In fact, the information society success is assessed by its pervasiveness and correct functioning. However, a look at critical infrastructures in general, and critical information infrastructures in particular, shows that while they are widespread and ubiquitous, they are strongly susceptible to vulnerabilities (Cukier et al., 2005). Such vulnerabilities may be exploited by hackers, criminals, or other groups, using a variety of cyber threat and attack weapons, such as those listed in Table 5. But what is CII? To have an operational definition of the term, it would be a good to start with few examples:

- The telecommunications network drives emergency services, gas distribution, civil aviation, and other critical infrastructures, and is considered a critical information infrastructure (Cukier et al., 2005).
- The power industry depends immensely on ICT for power distribution, power control, and power production optimization, among other things. These are carried out by SCADA (supervisory control and data acquisition) systems, an electronic control system which also enables the integration of electric utility companies into national/regional power grids for efficiency and optimization purposes (Lopez et al., 2007).

Table 5 List of some Cyber- attack Weapons against CI: Description and Impact Scope.

Cyber Threat Weapon	Description	Impact Scope	Source
<ul style="list-style-type: none"> Stuxnet Malware 	A sophisticated software that enhances the potential for cyber espionage and infrastructure attacks.	SCADA	Byres (2011)
<ul style="list-style-type: none"> Zeus 	A malware that enables the theft of valuable intellectual property as well as money.	Critical Infrastructure	Binsalleeh et al., (2010)
<ul style="list-style-type: none"> TDL – 4 	A Bot Trojan that, using command and control servers or peer-to-peer networks, infects machines and adds them to its collection. It is described by Kaspersky Labs as “the most sophisticated threat” today.	Malware dissemination, denial of service, and online fraud.	Greengard (2012)
<ul style="list-style-type: none"> Zero-day 	A virus which takes advantage of a security weakness (hole) that has no patch yet. So, zero-day represents the period of time when there’s nothing that could be done to stop the intrusion which took advantage of a security flaw.	Internet Infrastructure	Acohido and Swartz (2008)
<ul style="list-style-type: none"> Botnet 	A network of compromised computers used to launch internet crimes, with the computer owners unaware of it. The network, mainly comprised of home-based computers, is used to spread spam, Worms, and viruses.	<ul style="list-style-type: none"> Critical Infrastructure Crippled e-society Enterprises 	APCERT (2011); UNODC (2011); and Wilson (2008)
<ul style="list-style-type: none"> Social Engineering 	A technique where the hacker aims at obtaining information that will enable an unauthorized access to valued system information, through the use of clever manipulation of a human nature: the tendency to trust.	<ul style="list-style-type: none"> SCADA Critical Infrastructure 	Granger (2001); Dondossola et al., (2008); Beggs (2010); Parmar (2012).
<ul style="list-style-type: none"> Advanced Persistent Threat 	A sophisticated cybercrime category aimed at political and business targets. To be successful, they require a high degree of stealthiness, as well as prolonged time periods. They go beyond immediate financial gain and are based on various avenues of attack.	<ul style="list-style-type: none"> SCADA Organizations and governments for intellectual property and national secrets. 	Alperovitch (2011) Schneier (2011)
<ul style="list-style-type: none"> Mobile Application Exploits 	Mobile phones are increasingly becoming a threat vector that could introduce a wide range of attacks. Attacks could be launched and data could be stolen through the use of SMS, email, and the mobile web browser. Malware uses root exploits to launch sophisticated attacks on smart phones.	<ul style="list-style-type: none"> Critical Infrastructure Manipulation of online information (including mobile banking) and credential theft. 	Felt et al., (2011)

- The Internet is considered a specific example of CII, as it manages and facilitates essential services in an economy. These include, but are not limited to, financial transactions, communications among government agencies, and community alerts in times of emergency (Landau & Stytz, 2005).

The above examples bring to the picture a point that needs to be recognized: the term ‘Critical’ indicates the need to plan for and cope with new kinds of risks that have emerged with the remarkable ICT advancements (Schultz, 2007). They also make it important to consider the following:

1. Critical Infrastructure (CI) generally depends on an information infrastructure for it to operate. Critical infrastructures, like energy, banking, and communication systems, are now highly reliant on information infrastructures without which they will stop functioning (Christensen et al., 2010).
2. A vast array of pivotal services is provided by CIs to individuals, businesses, and societies, as a whole. This implies that any disruption or damage to a CI could have a ripple effect on other CIs across networked societal and technical systems (Huang & Hsieh, 2010).
3. The previous point is additionally supported by the fact that ICTs encompass all the CIs, thus making them more interdependent and interrelated (Brunner and Suter, 2008).
4. Based on all of the above, studies related to critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP) have considered ICT (which underpins CII) to be a major driver of: (a) Physical interdependence; (b)

Cyber interdependence; (c) Geographical independence; and (d) Logical independence (Bagheri & Ghorbani, 2007; Rinaldi et al., 2001).

With this in mind, the definitions of CI, CII, and CIIP could be stated. Prior to the statement of these definitions, it is important to have a clear understanding of what ‘infrastructure’ is. Of course, defining CII requires first an understanding of the term ‘infrastructure’. According to Merriam-Webster’s Collegiate Dictionary (2003), infrastructure is “the underlying foundation or basic framework”. It also refers to “the resources (as personnel, buildings, or equipment) required for an activity” (Merriam-Webster Dictionary, 2003). Though the definition is broad, it can still be convenient for the physical and information infrastructures that the present study focuses upon--infrastructures that are pivotal to the economic and social well-being of a nation. Proceeding to CI, this refers to the physical infrastructure pertinent to vital critical entities or services (Christensen et al., 2010). It consists of vital service sectors that are needed for the economy, and the overall functioning of a nation, including, but not limited to, (Homeland Security and Department of Energy, 2010):

- Power / Energy
- Communications
- Banking and Finance
- Government Facilities
- Water
- Emergency Services
- Information Technology
- Transportation Systems

In the past many of these CIs were separated. However, IT advancements and the change in market dynamics and business models in the 1970s have paved the way for these CIs to increasingly converge and integrate, and to become progressively reliant on information technologies such as the Internet, wireless networks, and the telephone network for communications, information exchange, management, and control functions. Of course, the

systems' level of interdependence as well as their immense reliance on information infrastructure has a crucial impact on economic progress, government activities, and military operations. In addition, such interdependence among the various CIs and their dependence on IT increases the effects of any malfunction since they are spread across different infrastructures, affecting a wide range of users. This makes CIs and the information systems they depend upon (that is, the CII) both invaluable assets and also lucrative targets to cyber threats. As a matter of fact, cyber security reports describe other infrastructure-related incidents caused by malware, as well as discussing potential cyber targets. For example:

- Spanair flight crash in August 2008: malware was detected. This is believed to have played a role in preventing the computer from detecting some technical problems with the aircraft (Hollis, 2011).
- Modern automobiles have a high vulnerability to cyber-attacks (Koscher et al., 2010). This is caused by the fact that modern automobiles are highly integrated into information technology--a design intended to make them more energy efficient and to contribute to lower CO2 emissions (Brammer, 2011). The attacks could be combined with the ability to leverage several separate weaknesses, including embedding a malicious code that will completely erase any trail of a malware presence after the car crash (Koscher et al., 2010).
- Financial and trading markets, designed to mitigate climate change through rewarding innovation and efficiency, are vulnerable to cyber-attack targets as well. In Europe, these markets faced critical problems due to cyber-attacks, recycling of used credits, and tax fraud (Kanter, 2010). This forced a partial closure of the Emissions Trading Scheme, thus posing legal and political challenges to the European Union (The Guardian, 2011).

- The smart grid, which enables reliability, efficiency and security enhancements, is also subject to critical security concerns (Li et al., 2010). Potential threats include compromising end user privacy, electricity theft, and control of the grid (Brammer, 2011).

The above are a few of the myriad examples that demonstrate the huge vulnerability of critical infrastructures to cyber threats. These threats manifest themselves in a variety of potential exploitations and reported incidents, such as cybercrime and cyber espionage. A list of some of these cyber threats/exploitations is presented in Table 6.

As the table indicates, cyberspace is susceptible to various kinds of attacks that are driven by various kinds of motives and that are launched against different targets. Of course, these cyber threats/attacks are executed through the use of a variety of weapons (such as those listed in Table 6). An example could be the Stuxnet worm, which is thought by some to be developed for cyber warfare since it was aimed at the Bushehr nuclear plant in Iran (Chen, 2010). Following the attack, Iran accused NATO and the US of being involved, while both have denied responsibility (Chen, 2010). Another example is cyber espionage which is achieved through the use of advanced persistent threats (APT) (Twomey, 2010; Schneier, 2011).

Table 6 A List of Some Cyber Threat / Exploitation Types and Exploitation Method

Threat / Exploitation Type	Description	Motivation	Target
Cyber Espionage	An activity which is either foreign sponsored or coordinated intelligence to unlawfully access proprietary economic information (FBI, 1995; Tucker, 1997)	Obtaining economic and political secrets of nations or industries, and stealing intellectual properties (Lewis, 2010).	A nation's government, corporations, establishments, and individuals (Fraumann, 1997).
Cyber Crime	This refers to offenses ranging from activity against data to infringement of content and copyright (Krorie, 2005). It also involves fraud, child pornography, unauthorized access, and cyber stalking (United Nations, 2000)	Financial gain or Economic espionage (PWC, 2011)	Individuals, governments, companies (Twomey, 2010).
Cyber warfare	This refers to the use of exploits in cyberspace as an intentional means to cause harm to economies, people, and assets (Owen, 2008).	Military or political dominance (Twomey, 2010)	Critical infrastructure, economies, military and political targets (Shimeall & Williams, 2002; Chen, 2010; Kelsey, 2008).
Hactivism	Known as a convergence of both hacking and activism, the term refers to the pursuit of political ends through the use of digital means and tools (Vamosi, 2011).	Changing political systems or regimes (Denning, 2000)	Corporations, military sites, governments, and law enforcement agencies (Mansfield-Devine, 2011; Vamosi, 2011).
Cyber Terrorism	This refers to the use of computer network tools by a hostile nation or group to exploit the vulnerabilities of a poorly secured network to disrupt or to stop critical functions (Lewis, 2002).	Changing political/ social systems; Defending a specific cause, ideology, or conviction (Wilson, 2008; Singh & Siddiqui, 2011).	Governments, civilian populations, critical infrastructures (Vatis, 2006).

Recognizing their criticality, countries and international organizations issued acts and reports to protect them and to enhance various stakeholders' awareness about their vital role as well as their vulnerability. In the process, several definitions emerged. According to the Congress of the United States (2001), Critical Infrastructures are "those systems and assets,

whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (U.S. Congress, 2001). Another definition was set by the European Commission, considering Critical Infrastructures: (European Commission, 2004) “those physical and information technology facilities, networks, services, and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of citizens or the effective functioning of governments in the Member States.” While having various definitions set by different entities or governments, CIs have four features in common (Lopez et al., 2007 as adopted from ACIP, 2002):

- Interdependencies: CIs have strong interdependencies across various sectors in a nation and, sometimes, extend to other nations. This implies that a disruption in one CI will negatively affect others. This is the ripple effect mentioned in Chapter 1.
- Private ownership: due to privatization, CIs are mostly operated and owned by the private sector. Nevertheless, this sector is not the only party that exercises influence over CIs.
- ICT dependence: As mentioned earlier, CIs are growing increasingly dependent on ICT. This is due to the fact that they are operated by networked electronic control systems (national and sometimes international) that enable their continuous and reliable operation.
- Global boundaries: Driven by increasing international treaties and commerce globalization, CIs are crossing national boundaries. This makes it prudent for policy makers and security strategists to think of protection methods with both national and international factors taken into consideration.

In reference to the third point mentioned above, one can recognize the interdependent nature of the two infrastructures: CI and CII (Christensen et al., 2010). Previous research has also

contended that CII are components of CI (Walker, 2008; Lopez et al., 2007; Wilson, 2007; Cukier et al., 2005; and Rinaldi et al., 2001) and are influenced by the same legal framework and regulatory policies. Still, several definitions of the term CII were provided separate from those of CI. For example, the Commission of the European Communities (2009) and OECD (2008) provided working definitions of the term. The Commission captured with the CII concept the “ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, Satellites, etc.)” (Commission of the European Communities, 2009). In a similar vein, OECD (2008) referred to CII as “those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.” Besides international organizations, researchers studying CII emphasized the importance of looking at CI and CII as separate terms at least from a conceptual point of view (e.g., Lopez et al., 2007). The authors attributed this need to the fact that there are specific threats that are inherent to information infrastructures, targeting its intangible elements and contents, namely: (1) the information flowing throughout the infrastructure; (2) the knowledge derived from this information; and (3) the services provided. Accordingly, attacks targeting these information infrastructures can result in damages to them as well as to the physical infrastructures. Based on this, Lopez et al. (2007) argue that separating the two concepts allows for a better assessment of the risks and challenges that the CII needs to overcome to achieve better levels of CII protection, or cyber security.

Importance of Cybersecurity: Cybersecurity and the Economy. The modern economy has become increasingly reliant on the safety, reliability, availability, and security of many technology-driven infrastructures (Nickolov, 2005). Nevertheless, the impact of cyber-attacks

targeting critical national infrastructures on economic well-being has been viewed differently by different researchers. While some researchers perceived the negative impact as being limited (Geers, 2009), others considered it devastating (Schneider et al., 2011; Brammer, 2011; Anderson & Fuloria, 2011). The former group based their argument on the assumption that at the nation-state level, governments are not expected to try, basically for their own good. Given the interconnectedness of the world economy today, if state governments undertake cyber-attacks against other states, they would also be harming themselves. As for non-state parties, the author's argument continues, they don't have adequate time and technical resources for this (Geers, 2009). As for the latter group, their argument is based mainly on the following points:

1. The critical infrastructure is of tremendous value as it encompasses and drives crucial segments of an economy. A case in point is the North American energy whose assets are worth more than \$ 1 trillion (Anderson & Fuloria, 2011). Such numbers clearly show why critical infrastructure protection is important and why the huge investments can be justified in this regard (Brammer, 2011).
2. Renewing infrastructure systems can very much depend on new ICT. These new ICT-based designs can generate more efficiency, better flexibility, and higher levels of functionality and performance. An example of this point could be the US power Smart Grid (Brammer, 2011 as adopted from US Department of Energy, 2003). However, according to Brammer (2011), enormous benefits expected from ICT investments could be lost or greatly reduced as a result of the large and growing base of cyber threats.

This risk to which critical national infrastructures are vulnerable, is generated by various types of cyber threats and malicious applications (e.g., the cyber weapons listed previously in Table 5). Security reports (e.g., McAfee, 2011; Hollis, 2011) have reported cyber attacks caused

by these malware threat types. For example, a cyber attack may involve the theft of crucial/sensitive information with crucial financial and competitive value, as the attacks that were conducted against energy, oil, and petrochemical companies in 2010 (McAfee, 2011). The McAfee report states that the attacks involved spear-phishing, social engineering, remote administration tools (RATs), and exploiting the vulnerabilities of Microsoft Windows Operating Systems. The attack, which was referred to as ‘Night Dragon’, targeted and captured sensitive information pertinent to project financing and competitive proprietary operations related to the oil and gas field operations and bids. What raises an alarming concern is the target that these various threats attack; namely, the critical infrastructures that are vital for a nation’s economic and overall security.

These incidents and many others show that information security breaches are common in the modern digital economy. As a result, the literature reveals a new approach being taken by researchers who are studying cyber security economics: applying economic concepts to show the impact of cyber security problems, in the hope of eventually preventing (or at least reducing) their occurrence. This new research agenda is expected to have important implications for organizations and nations around the world. Some of the findings reported by previous researchers include the following:

1. A very recent study showed that information security breaches had a significant impact on firms’ stock market returns. However, the impact of security breaches traced a downward trend in the period following 9/11/2001 as compared to that in the pre-9/11/2001 sub-period (Gordon et al., 2011).
2. At the national level, Lesk (2011), in a study related to cyber security and economics, stated some figures reported by governmental or research agencies that would help shed some light

on the economic impact that cybercrime would have on a nation. The authors mentioned the following as adopted from reports and research articles:

- A large study estimated that cyber fraud and similar types of cybercrime cost between 0.2 percent and 0.4 percent of global GDP, which is approximately \$100 to \$200 billion.
 - The UK government estimates that each year the country loses £27 billion to cybercrime, which extrapolated to the US population and transformed to dollars would be equivalent to \$210 billion. The preventive or mitigation processes will cost the UK about £650 million for cyber security.
 - A few years ago, a cost of \$105 billion per year for cybercrime in the US was suggested.
3. Another recent study provides strong evidence that voluntary disclosures to the SEC concerning information security and incidents are positively related to the stock market value of firms (Gordon et al., 2010).
 4. Moreover, taking into account the indirect costs, as well as the direct costs to the firm, the economic effect of information security breaches on the stock market value of corporations was also examined (Campbell et al., 2003). The study reports that cyber security breaches that have resulted in compromising the integrity of private and confidential information (e.g., the release of medical records or customer credit card numbers to unauthorized parties) significantly and negatively affect the stock market value of the attacked firm. Of a lesser impact are the security breaches related to task disruptions rather than targeting data confidentiality, as for example, causing a temporary shutdown of a corporate website). The costs incurred in such cases are temporary and unlikely to significantly affect shareholder value. This implies that economically rational investment strategies should be based on a

rational discrimination across various types of breaches. This is important for the identification and protection of the most valuable information assets at the organizational as well as the national levels (Campbell et al., 2003).

5. Furthermore, Gordon et al. (2003) discussed the movement fostered by the U.S. federal government aimed at encouraging the sharing of security incidents information. A particular emphasis was placed on protecting CIs largely owned by the private sector. The author presented a model to examine the beneficial economic implications of this movement and showed that information sharing (which enhances cost reductions) provides individual firms and society at large with potential benefits. However, in the absence of appropriate economic incentive mechanisms, some firms will free ride on the security expenditures of other firms, back out from the sharing agreement, and refrain from sharing information (Gordon et al., 2003).

These previous research works indicate that studies pertinent to the economic consequences of cyber attacks have been limited, dealing primarily with microanalyses of the attacks' direct impacts on a particular organization. The indirect impact was not adequately covered (Pfleege & Rue, 2008). Also, the impact at the country level has been mainly confined to descriptive reports from governmental agencies or international/research centers. In other words, having an understanding of what contributes to cyber security and thus better CIIP at the country level can help pave the way to make informed decisions about how much to invest in cyber security and how to ensure that security resources are used effectively (Pfleege & Rue, 2008).

Cyber Security Requirements and Strategies. Security scholars have recently been dwelling on cyberspace because of the vital role it now plays at the individual, organizational, social, and national levels. As noted by some researchers, cyberspace has now developed into a critical sphere of interstate conflict (Goodman, 2010). In 2007, for example, Estonia was a target for a series of cyber attacks that temporarily harmed its economy. Later, in 2008, a similar attack was experienced by Georgia in what some described as an aspect of its war with Russia. Similarly, in 2009, a series of cyber attacks were launched, apparently by North Korea, targeting the United States and South Korea (Olmstead & Siraj, 2009). Some countries, such as China, changed their military strategies to conform to the cyber environment features (Geers, 2010). As observed by the author, the ICT and the internet networked operations are thought to have a strong impact on the nature of warfare to the extent that they have transformed over 2500 years of military philosophy and the path from intensive defense to subjugation of international cyberspace (Geers, 2010 as adopted from Rose, 1999). In general, there are basic information security requirements that are applicable to cyberspace, as they are to physical information systems. These are: confidentiality, integrity, and availability (CIA). As a matter of fact, when the term “computer security” is used, it usually refers to these very important and fundamental elements of any computer or information system (Gordon & Loeb, 2002, Jonsson, 1998). Following is a brief description of each (Pfleeger & Pfleeger, 2011):

- *Confidentiality:* this ensures that computer and information systems are accessed only by authorized users. In other words, those who are supposed to have access to an information resource are the only ones who will actually get that access. Confidentiality is sometimes referred to as privacy or secrecy.

- *Integrity*: This implies that information resources cannot be modified except by authorized users and/or only in authorized ways.
- *Availability*: This means that authorized users can access the information assets they need whenever they need them. That is, with legitimate access, the person or system needing the information should be granted access and should not be prevented. Accordingly, availability is also denoted by its opposite, referred to as denial of service (DoS).

At the national cyber security level, the US National Institute of Standards and Technology (NIST) also proposed these principles as three main cyber security requirements for a critical infrastructure, namely the smart grid (Yang et al., 2011 as adopted from NIST, 2010): availability, integrity and confidentiality (CIA).

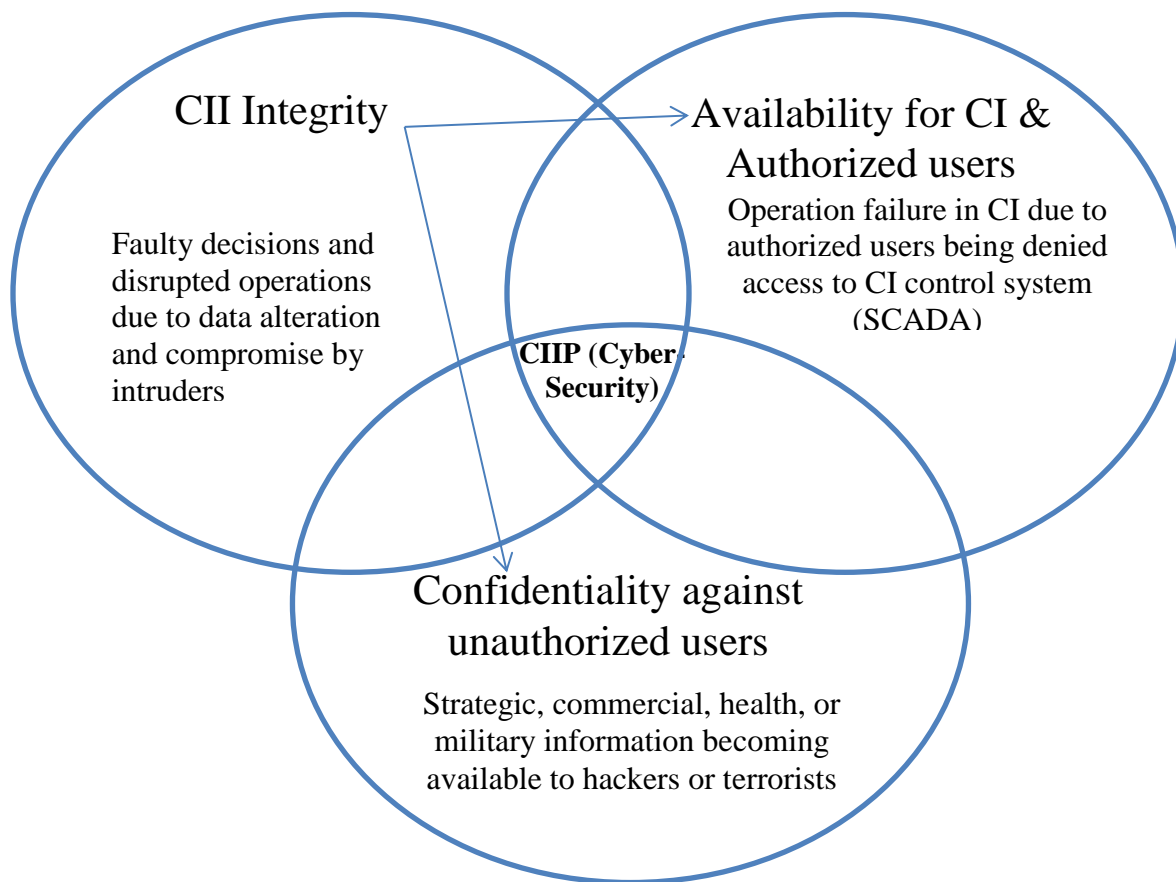
- *Availability*: This requirement refers to ensuring timely and reliable access to or use of information by authorized users. In terms of the Smart Grid, this relates to all cyber systems, for example SCADA, distributed control centers and distribution management system (DMS), as well as the communication networks between these systems and external networks. A loss of availability, such as denial-of-service (DoS) and distributed DoS (DDoS) attacks, may not only lead to economic losses but also result in security problems, for example blackouts or brownouts, as operators may lose the ability to monitor and control the systems. Thus, availability is generally considered the most significant cyber security requirement in the smart grid.
- *Integrity*: This requirement refers to guarding against undetected information modification or destruction by unauthorized persons or systems including ensuring data nonrepudiation and authenticity. Integrity for smart grids applies to information such as sensor values and control commands. A lack of integrity leads to deception that may

cause safety issues. For example, during a potential threat situation, operator judgment may be compromised by unreliable data.

- **Confidentiality:** This requirement refers to preventing disclosure of secret information to unauthorized users. From a Smart Grid perspective, this refers to privacy of customer information, electric market data and critical enterprises information. Violation of confidentiality results from the disclosure of private information. With the increasing accessibility of customer information on the Internet, confidentiality is becoming more and more significant.

These basic principles of information security as applied to CI, CII, and CIIP are presented in Figure 7.

Figure 7 Application of information security triad to CIIP (Cyber security)



Complementarities

Based on previous literature related to ICT and complementarities, this study will emphasize specific factors as complementarities to ICT and innovation in a nation's attempt to achieve high levels of growth competitiveness. These include ICT skills, IT-related training, and the human capital development level.

IT-Related Training. Organizations' and communities' established cultures offer powerful forms of advantage (Downing et al., 2003, Huselid, 1995, Kaarst-Brown, 2004). The human resource factors form an integral part of the unique cultural formations in organizations (Hansen & Wernerfelt, 1989). Human resource performance has implications for organizational and national performance outcomes (Huselid, 1995, Raskin, 1997). Efforts to elicit discretionary performance from employees are likely to provide returns in excess of any relevant costs (Bailey, 1993). This effort is especially important during process transformations where the employees face a varied working environment. Introduction of IT into a country's organizations and institutions will inevitably require some form of transformation on the part of human resources. End-user training is a critical intervention to support successful use of new IT resources in nations, especially the developing nations and the LDEs (Compeau & Higgins, 1995, Galletta et al., 1995, Olfman & Pitsatorn, 2000). IT training is an indispensable complement to investment in IT resources (Powell & Dent-Micallef, 1997).

The sustainable value of IT training emerges from merging ICT with organization-specific and culturally-sensitive training to produce distinctive capabilities at the organizational and national levels (Barney, 1991). This outcome is possible through a set of formal, academic, and on-the-job training initiatives. Training engages end users in cognitive activities, through which they acquire imparted knowledge (Gallivan et al., 2005). End users also acquire

knowledge from other sources, including situated learning, learning-by-doing, and learning-by-using (Sharma & Yetton, 2007). Formal training, however, is an important source of knowledge for them, and an important mediator contributing to the successful use of new IT resources (Powell & Dent-Micallef, 1997). Training also influences new technology adoption benefits through its effects on the beliefs of end users, their attitudes, and their perceptions of usefulness and ease of use (Agarwal & Prasad, 1999).

ICT Human Capital. The existence of human ICT Capital reflects that organizations and/or nations have employees with expertise in the adoption and use of ICT. The human IT capital in developing countries and LDEs is critical and may well represent its most important asset. This asset will not only enable organizational change, but also act as the mechanism through which to achieve greater organizational effectiveness (Wignaraja, 2008, Adam & Urquhart, 2009). The changes in IT in these countries will inevitably have wide-ranging implications for the required skills, behavior, and orientations of ICT staff. In this environment, the need for additional skills for IT professionals will intensify, such as entrepreneurial and change management skills. The presence of IT human capital signifies a proactive approach to creating opportunities by deploying IT to serve the business needs in various countries. The presence of an effective IT workforce in organizations and communities in the LDEs and developing countries will help businesses foster strong partnership skills, a culture of willingness to change, and an environment where the IT staff and the end users act without overt and persistent guidance (Bresnahan et al., 2002). Human IT capital resources will also reduce dependency on vendors and other providers, a major source of IT-related frustration in LDEs (Reijswoud, 2009, Bakos & Brynjolfsson, 1993). The presence of human IT capital in the LDEs will also provide the important fusion between the introduced technology and the business processes. The result will

be a set of refined business processes with an improved level of efficiency and effectiveness. This makes the human IT capital an important complementarity to investments in IT in the LDEs.

Cyber Security Initiatives Estimate

International organizations, such as ITU, recognize that information and technology security are critical priorities for the international community. Cyber security generally is in everyone's best interests and this can only be achieved through a collaborative effort. Cyber threat issues are global and therefore the solutions must be global, also. It is vital that all countries arrive at a common understanding regarding cyber security; namely, providing protection against unauthorized access, manipulation and destruction of critical resources. The ITU believes the strategy for a solution must identify those existing national and regional initiatives in order to work effectively with all relevant players and to identify priorities (ITU, 2010).

ITU established and supported various initiatives within several nations of its 191 member states. These are: (ITU, 2010)

- Legal Measures
- Technical and Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

Legal Measures. The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security. Since

threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.

In fact, the priorities of a nation are reflected in its policies and laws, and these in turn influence its rate of growth and direction of development. This component measures the impact of a nation's policies, laws, and regulations, and their implementation for the development and use of ICT (Dutta & Mia, 2007). Moreover, policy programs must remain coherent and manageable (Poel & Bodea, 2008). Accordingly, the role of the government policy in the process of ICT diffusion enhancement cannot be underestimated. For example, the role of institutional systems in enhancing education and regulatory policies is substantial in global Internet diffusion (Zhao et al., 2007). In conformity with these research findings, in a cross-country study on E-commerce, results corroborated the importance of government policy in firms' level of e-commerce use. Regulatory policies for supporting e-commerce activities, protecting e-commerce transactions, and making ICT and Internet access more affordable to firms and consumers are good drivers for optimal e-commerce use (Gibbs & Kraemer, 2004; Gibbs et al., 2003). Developed and developing countries associate different importance levels to the importance of laws related to ICT usage and security. For example, in certain developing countries, it was found that legislation and regulatory frameworks are still needed in data protection and privacy, cybercrime, computer misuse, and inappropriate web content (Li, 2007). In Denmark, however, the government is committed to digitizing all written communications between citizens, businesses and the public sector and to give all citizens a digital signature to promote the deployment of secure communications for purposes such as e-government and e-business.

Technical Measures: Secure Infrastructure. Discussing the country competitiveness level should include to a large extent the significant role of infrastructure. Infrastructure is defined as the level of availability and quality of the key access infrastructure for ICT within a country. A quality ICT-access infrastructure facilitates the adoption, usage, and impact of these technologies, which in turn promotes investment in infrastructure. Infrastructure thus plays a critical role in influencing the networked readiness of a nation (Dutta & Mia, 2007). In fact, one finds this factor is a common element in nearly all the research work that deals with all kinds of ICT adoption and diffusion. In the context of this study, it refers, among other things, to Internet connectivity, high bandwidth for accessing the network, and sufficiency and competence of the national power grid (Mutula & Brakel, 2006).

Moreover, a country's infrastructure includes the telecommunications facilities, Internet access, dial-up access, bandwidth, and broadband access. As a matter of fact, the role of investment in improving a country's technological infrastructure is very important. For example, investment in fiber networks rather than in telephone hubs can make big differences for bandwidth. A relative advantage in such technology is that it can attract a bigger share of the global economy in one country when compared to others (Fuhr & Pociask, 2007).

Organizational Structures. Individuals, organizations and governments are increasingly dependent on globally interconnected networks. In order to protect network infrastructures and address threats, coordinated national action is required to prevent, respond to and recover from incidents. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and take steps toward remediation (ITU, 2010). Effective incident management also requires considerations of funding, human resources, training, technological capability, government and

private sector relationships, and legal requirements. Efforts are being made to bring together organizational structures at the national and regional level in order to facilitate communications, information exchange and the recognition of digital credentials across different jurisdictions. However, more needs to be done at the global level and international cooperation between these different structures is indispensable (Dutta & Mia, 2007).

At ITU, several regional initiatives are already recommending that member states establish national cyber security response centers, such as computer incident response teams (CIRTs), noting that there is still a low level of computer emergency preparedness within many countries, particularly developing countries, and that a high level of interconnectivity of ICT networks could be affected by the launch of an attack from networks of the less-prepared nations (ITU, 2010).

Capacity Building. Successful training effort on implementation and use of new technologies in certain nations will enhance individual cognitions of application knowledge and business context knowledge, and the inter-individual cognitions of collaborative task knowledge (Yetton et al., 1999). Human resource complementarities, like end-user training, will create embedded advantages that explain significant performance variance among organizations in those nations (Powell & Dent-Micallef, 1997). In developing nations and LDEs, appropriate end-user training will also ensure a coordinated and comprehensive approach to the introduction of new technology. Investment in mature technology in these countries means that the potential of the newly introduced technology is established. In this environment, training will ensure that the end-users are able to capitalize on the opportunities that the new but established technology offers. This fusion will be a source of process-level business value.

Capacity building needs to be promoted in order to develop a sustainable and proactive culture of cyber security. People are the weakest link. One of the key challenges of cyber security is effectively educating the end user. Understanding and awareness of the potential dangers are critical if the end user is to benefit from ICTs safely. This is a matter that concerns all stakeholders from governments and industry to education both at school and at home. With the important role that ICTs play today in providing services in sectors as varied as health, education, finance and commerce, awareness of the opportunities offered by a secure cyber environment and of the threats inherent to cyber space are vital. Programs aimed at creating a level playing field in raising basic awareness and building capacity at all levels are important, and these also need to be undertaken within the international arena (ITU, 2010).

Studies Using or Developing Innovation and ICT Indexes

Composite indicators are used to summarize a number of underlying individual indicators or variables. They are quantitative or qualitative measures derived from a series of observed facts that can reveal or proxy characteristics. A good description is given by Nardo et al., (2005). Because they encompass the multidimensionality aspect of certain constructs, they are used in social science research. However, they are more used in studies entailing comparative analysis across countries (UNDP, 2011; Groh & Wich, 2010). The literature shows that most of these indices were developed by international organizations, such as the UNDP, the World Bank, and the World Economic Forum, to name a few. Other indices were developed by researchers as composite measurement scales for constructs they are studying in specific research works (e.g., LeBel, 2008 & Belitz et al., 2011).

LeBel (2008) proposed an index of creative innovation. He suggested that although R&D expenditures provide a measure of innovation, data could be (sparse and infrequent or sparse

want to rephrase this?) in many cases. So, he developed the index based on two key indicators that may be considered proxies for creative innovation: namely, per capita scientific citations and the ratio of per capita royalty revenues to per capita royalty fee payments (LeBel, 2008). The author justified the choice of the indicators by arguing that while R&D reflects innovation activity, R&D expenditures as well as patents are not well tracked, especially in developing nations: (Do you need more of a connector to link into the following list?)

- Even when the information related to patents (applications and grants) is adequate, the economic impact may be lagged;
- When patents are used as a barrier to entry, they may render the patent innovation-to-economic growth expected positive relationship ineffective; and
- In some countries, patent laws are weak, thus reflecting a weak and ineffective status of property rights. According to the author, building the index based on countries with strong patent laws only will not allow for the examination of the variance in institutional factors.

Based on all of the above points, the authors used scientific citations and net royalties as proxies for research and development and the impact of patents respectively (LeBel, 2008). According to the author, such an index enables the examination of the impact that innovation has on economic growth as well as the effect of institutional factors on that level. The results of the study showed that scientific citations contribute to economic growth more strongly than either savings or trade dependency taken separately. Moreover, the study's creative innovation index was reported to have a strong effect on economic growth (LeBel, 2008).

Along with the creative innovation index, the author also developed a composite index to measure country aggregate risk. Aggregate country risk presents a transaction cost that has a

negative effect on per capita income (LeBel, 2005). In more recent research, LeBel (2008) noted that it is difficult to depend on relative prices as a measure of risk, especially when there are incomplete prices. Since risk is established in many dimensions, the author chose to use a composite index to measure aggregate country risk.

So the index was based on the International Country Risk Guide (ICRG) measure provided by PRS (the Political Risk Services) Group for the countries. The index ranges from a 0 standing for the highest risk level to 100 representing the lowest level. Since the scale doesn't match with the expected inverse relationship between income and risk, the author derived the index complement, and labeled it as RCCRISK (Revised Country Composite Risk). To link risk to the level of innovation, LeBel (2008) used the level of property rights and the degree of judicial independence as the determinants of risk. He justified his approach by explaining that the measures to reduce the risk level are expected to yield positive effects on the innovations level, which in turn is expected to have a positive effect on per capita income. As stated by the author, since markets are incomplete in many countries², the aggregate country risk composite was used in the study to illustrate the linkages between innovation, institutions and economic growth. In other words, the aggregate country risk was used to play the role of a proxy for the efficiency level in institutional governance.

Using this index in the model he proposed to show the relationship between innovation and economic growth, LeBel (2008) found that while trade dependency and savings are

² In Economics, 'incomplete markets' is a term used for markets where there is a shortage of Arrow-Debreu securities – a situation when individuals will be restricted from transferring desired wealth levels among different future assets when confronted with a situation involving risk (Arrow, 1964). An Arrow security, which an individual buys or sells at a certain date t , represents a contract with a promise to yield one income unit in a contingency situation that may occur at some future date $t+1$ (Magill, 1996). The lack of these contracts in such markets would disable optimal risk sharing among agents, thus negatively affecting the economy welfare (Masin & Rahi, 2000). Incomplete markets mainly result from lack of the institutions that enforce contracts as well as from information asymmetry (Marin & Rahi, 2000).

important indicators of per capita income, the aggregate country risk indicator has a higher negative effect than either one separately. Measures that are intended to reduce the country risk level through institutional reform, such as intellectual property rights protection as well as judicial independence, can have an important effect on economic growth. Even when the author examined the impact of foreign direct investment (FDI), he found that its effect is insignificant, though positive. This may imply that the positive effects of FDI are highly related to the institutional regime selection. The study also reported that the aggregate country risk can be offset by a country's production of scientific citations (LeBel, 2008).

Besides the above-mentioned indices, several others were developed by international organizations. Two examples will be given: the Summary Innovation Index (SII) and the Networked Readiness Index (NRI). SII is a composite index that measures the overall innovation performance at the national level.

The SII was created at the request of the European Council in Lisbon in 2000 and since then has been assessed and published annually in the European Innovation Scoreboard (EIS). According to the methodology used since 2008, SII summarizes 7 innovation dimensions grouped into 3 main blocks: "*Enablers*", "*Firm activities*" and "*Outputs*". Each one of the innovation dimensions contains several indicators leading to a total of 29 indicators (European Commission, 2009). Based on a statistical cluster analysis of the SII scores over a five-year period, the EU Member States are divided into four groups: (a) *Innovation leaders*, including countries with innovation performance well above that of the EU average; (b) *Innovation followers*, including countries with innovation performance below those of the innovation leaders but close to or above that of the EU average; (c) *Moderate innovators*, including countries with

innovation performance below that of the EU average; and (d) *Catching up countries*, where the innovation performance is well below the EU average.

The Networked Readiness Index (NRI) has been published annually since 2001 in *The Global Information Technology Report* produced by the World Economic Forum, in collaboration with INSEAD. The index is a composite of 3 components:

- (a) The *environment* for ICT offered by a given country;
- (b) The *readiness* of the economy's key stakeholders (individuals, businesses, and governments) to use ICT; and
- (c) The *usage* of ICT among these stakeholders.

Each of the NRI components contains 3 sub-indexes ("pillars") composed of variable and the total number of variables included in NRI is 68 (World Economic Forum, 2010). Table 7 presents some of the above-mentioned indices along with a few others, including the composites of each as well as the computation method.

Table 7 Summary of Research Articles on Developing Innovation and ICT Related Indexes

Research Article	Index	Composites	Formula
LeBel (2008)	Creative Innovation Index	<ul style="list-style-type: none"> Per capita scientific citation Per capita net royalty ratio 	Per capita scientific citation + per capita = Net royalty ratio / 2
The PRS Group (2013)	International Country Risk Guide	<ul style="list-style-type: none"> Political Risk (12 composites) Financial Risk (5 composites) Economic Risk (5 composites) 	= 0.5 political risk + 0.25 financial risk + 0.25 economic risk
United Nations	ICT – Opportunity Index	<ul style="list-style-type: none"> Degree of a country's info- 	

Conference on Trade and Development (UNCTAD) (Fortin, 2005)		<p>density (productive capacity in terms of overall capital and labor stocks).</p> <ul style="list-style-type: none"> • Level of a country's info-use (i.e., the ICT consumption flows) 	= square root (info-density x info-use)
IDC (2001)	Information Society Index	<ul style="list-style-type: none"> • Computer Infrastructure • Internet Infrastructure • Telecom Infrastructure • Social Infrastructure 	Weighted average of the four indicators
European Commission (2009)	Global Innovation Scoreboard	<ul style="list-style-type: none"> • Pillar 1: Firm activities and output (patents and R&D % of GDP). • Pillar 2: Human Resources (enrolment ratio; education; R&D personnel; and scientific articles per population). • Pillar 3: Infrastructure and absorptive capacity (ICT expenditures per capita; broad band penetration; and public R&D % of GDP) 	= (pillar 1 x 0.4) + (pillar 2 x 0.3) +(pillar 3 x 0.3).
World Economic Forum (2009)	Davos index of international competitiveness	<ul style="list-style-type: none"> • Openness • Government • Finance • Infrastructure • Management 	Weighted average of the eight indicators

		<ul style="list-style-type: none"> • Labor • Institutions 	
Belitz et al. (2011)	Innovation System Indicator	<ul style="list-style-type: none"> • National innovation system (education, R&D, regulation and competition, financing, demand, networking, and implementation in production). • Social Climate of innovation (innovation culture, attitudes towards science and technology, and social capital and trust). 	<ul style="list-style-type: none"> • The indicator was derived based on standardization of sub-indicators and giving them weights suggested by experts. • Difference from the best and worst performer was applied.

Portrayal of the Conceptual Model

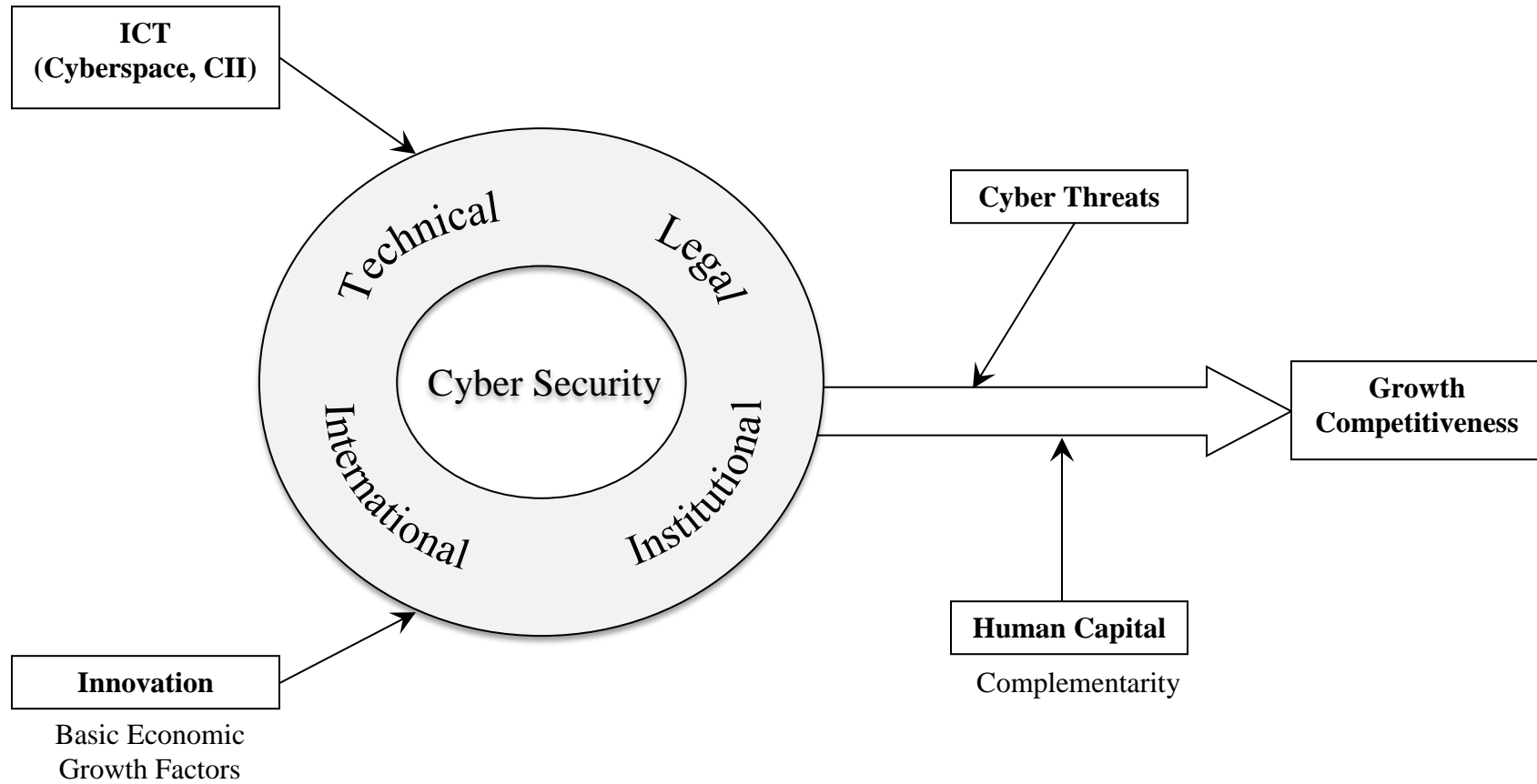
With the previous literature and theoretical frameworks described above, and with all the sets of hypotheses derived, a conceptual model is proposed that is based on all that has been aforementioned and analyzed so far. The model is depicted in Figure 8.

Analyzing the model, one can find that it has three important characteristics:

1. First, it is an integrated socio-technical model. The model synthesizes the majority of the social and technical elements that are mentioned in the literature as being important determinants of ICT and innovation. The Delone and McLean model highlights the ICT system characteristics, such as system quality, information quality, and service quality as major antecedents to system use, which in turn would lead to the realization of certain benefits (Delone & McLean, 2003). Based on this model, ICT and innovation are dependent on a set of country and region characteristics that demarcate the status of these two pillars in a nation's economy from those of other nations. Moreover, the model depicts the relationship between these two pillars and the growth competitiveness, taking into consideration the cyber security status in a country, along with the complementarity resources that shape and influence all the other relationships in the model.
2. Second, it is a dynamic model. ICT, innovation, and cyber security along with the complementarities specific to a certain nation are envisioned as major catalysts that can shape the global competitiveness level of a country. Moreover, working on any of the factors influencing ICT and innovation is expected to influence the other factors as well as the overall growth competitiveness position of the nation.

Figure 8

Conceptual Model



3. Third, it is potentially a proactive model. Understanding the environmental factors--both domestic and global--along with the available resource endowments, a country's strategists can effect certain policies or initiate certain agreements that would improve the ICT, innovation, and cyber security levels and, in turn, realize better levels in global competitiveness of a nation.
4. Finally, it is a pragmatic and sensible model. The impact of the triad on a nation's growth competitiveness could be strongly and negatively affected by the cyber-threats targeting a nation's critical information infrastructures. This impact is influenced to a big extent by the effectiveness of ICT, innovation, and cyber security status in the country, as well as the complementarities available there. The role that the complementarities play can either be proactive or reactive, of course, depending on a vast array of factors ranging from available resources, level of skills, degree of law enforcement, level of cooperation and coordination with other nations, and so on.

This chapter presented the theoretical framework upon which the study is based. It also presented a review of the literature pertinent to the major concepts incorporated in the study as well as the relationships among them. These will support the development of the hypotheses that will be presented in Chapter III and tested later on in the study. Chapter III will clearly show the hypothesized relationships in the research model in light of the variables to be used and the conceptual model presented above. In addition to this, the data to be used, the target population, and the methods of analysis to be deployed will all be incorporated in the next chapter.

CHAPTER III

RESEARCH DESIGN AND METHODOLOGY

This study was conducted with the purpose of investigating the relationships among ICT, innovation, and cyber security at the country level, as well as examining the potential causal impact that the joint relationship among these three constructs may have on countries' growth and competitiveness levels. As outlined in Chapter I, the motivation behind the study encompasses the following: (a) investigating the triad relationship (ICT-Innovation-Cybersecurity) and its impact on competitiveness as a first attempt in the literature; (b) contributing to the body of literature and ICT-Innovation-Growth research streams and models by introducing a holistic framework that integrates these constructs with a new complementary factor; namely, cybersecurity; and (c) paving the way for future research efforts to establish cybersecurity metrics and methods for assessing and controlling the cyber security situations in countries. In light of the study purposes, the following research questions were to be addressed:

- What is the relationship between a nation's innovation and ICT on one hand and its cybersecurity strategies on the other?
- What is the relationship between a country's ICT and innovation and its global competitiveness levels?

- How does cybersecurity change the ICT-Innovation relationship with a country's competitiveness?
- How do these relationships vary across regions and country groups?
- What are the factors that are most likely to be associated to cybersecurity strategies?

This chapter will lay down the initial blocks needed for finding optimal answers to these questions. First, and based on the theoretical framework delineated and the literature review conducted in Chapter II, the statements of hypotheses will be posited and the research model will be proposed. Second, the research methodology that was followed to obtain the data needed will be discussed. Third, the data sets, the constructs to be used, and their operationalization in terms of well-defined variables will be described. Finally, the statistical methods that will be used for data analysis will be stated and explained.

Statement of Hypotheses and Research Model

The review of literature presented in Chapter II has produced essential themes for this study. Some of these emphasized the importance of ICT in driving the wheel of national innovation forward (e.g., Trajtenberg, 2005; Tiwari et al., 2007; Infodev, 2007; and Economou, 2008). Others highlighted the significant role that ICT and innovation play in enhancing the economic growth of nations (e.g., Sweeny, 1996; Rosenberg, 2004; Gordon et al., 2006; Taylor & Zhang, 2007; LeBel, 2008; and Sofka, 2008). In addition, another theme is pertinent to the mediating effect that cybersecurity may have on the relationship between both ICT and innovation as it related to a country's growth competitiveness. Security reports as well as cybersecurity studies indicate that economies with effective cybersecurity measures are better off than those with less effective strategies for defending their cyberspace and critical information infrastructures (Gordon et al., 2011; Brammer, 2011; and Anderson & Fuloria, 2011). Finally,

the impact that human capital may have on the above-mentioned relationships was discussed within the complementarity effect that human capacity may have in fostering the growth resulting from ICT, innovations, and cybersecurity. For such themes, the following hypotheses could be postulated:

ICT and Innovation Relationship to Economic Growth

H1: ICT is positively related to economic growth.

H2: Innovation is positively related to economic growth.

H4: Innovation plays a mediating role in the ICT–Growth relationship (implied hypothesis)

ICT-Innovation Relationship

H3: ICT is positively related to innovation.

ICT-Cybersecurity and Innovation-Cybersecurity Relationship

H5: ICT development (readiness) is positively related to cybersecurity strategies.

H6: A nation's innovation diffusion (or capacity) is positively related to cybersecurity strategies.

Cybersecurity and Economic Growth

H7: Cybersecurity Initiatives is positively related to economic growth.

H7a: Cybersecurity plays a mediating role in the ICT–Growth relationship (implied hypothesis).

H7b: Cybersecurity plays a mediating role in the Innovation–Growth relationship (implied hypothesis).

In addition to the above-hypothesized relationships, the complementarity theory (Milgrom & Roberts, 1990 as adopted from Edgeworth, 1881) brings to the picture some variables that are most likely to impact some of the relationships presented above. Based on Brynjolfsson and Saunders (2010), human capital is a major complementary factor that influences the relationships between (a) ICT and economic growth; (b) innovation and economic

growth; (c) cybersecurity and economic growth; and (d) the triad relationship and economic growth. Accordingly, the following hypotheses are proposed:

Human Capital

H8a: Human Capital has a moderating effect on the Innovation-Growth relationship.

H8b: Human Capital has a moderating effect on the Cybersecurity-Growth relationship.

H8c: Human Capital has a moderating effect on the ICT-Growth relationship.

Finally, with the criticality of national and information infrastructures, their vulnerability, and the devastating impact on the economy in case these entities are attacked (Cukier et al., 2005, Christensen et al., 2010), cyber threats are also introduced as a factor that is anticipated to negatively impact the above-stated relationships. In other words, the following hypotheses are hereby posited:

Cyber Threats

H9a: Cyber threats have a moderating negative effect on the Innovation-Growth relationship.

H9b: Cyber threats have a moderating negative effect on the Cybersecurity-Growth relationship.

H9c: Cyber threats have a moderating negative effect on the ICT-Growth relationship.

Theoretical Support for the Statements of Hypotheses

As previously mentioned, this study is overall based on a rich and comprehensive theoretical framework. To establish more concrete theoretical justification, this section will relate each hypothesis stated above to the theory underpinning its formulation. This is pivotal to provide sufficient evidence of the theoretical validation of the relationships stated. There has always been a criticism against the lack of theoretical perspectives in the information systems (IS) research stream. As stated by Goodhue (1995), “what is needed [in information systems research] is the identification of some theoretical perspective that can usefully link underlying

systems to their relevant impacts” (p. 1828). Similar calls for providing theoretical grounds in IS research have been cited in the literature (e.g., Gable et al., 2008; Lee & Hubona, 2009). The latter contend that while most IS research is a positivist research where authors depict the measures and relationships they are studying in diagrams with boxes and arrows accompanying statistical inference and multivariate analysis, this is not a sufficient approach to build rigor and robustness. “As helpful as mathematical notation can be, however, it must be noted that a theory is necessarily more than just any mathematical representation of it.” (Lee & Hubona, 2009, p. 238). Based on this, the various relationships posited above, their supporting theory, theory choice justification, and citations of previous articles that examined these relationships are all presented in Table 8.

Table 8 Hypothesized Relationships and Corresponding Theoretical Support

Relationship	Theoretical Support	Why?	Example of Relationship Support in Previous Studies
1. ICT – Growth Competitiveness	<ul style="list-style-type: none"> •New Economic Growth Model (Romer, 1990) •Neo-Classical Economic Model (Solow, 1956) 	Both models attributed economic growth to technological changes and investments as opposed to the conventional models that attributed growth to labor and capital accumulation (Romer, 1990; Solow, 1956).	Jalava and Pahjola, 2007; Scarpetta et al., 2000; Wang, 1999; Avegrou, 1998.
2. Innovation – Growth Competitiveness	Value Chain Concept (Porter, 1990) derived from the New Economic Growth Model (Romer, 1990)	It focuses on interactions and mutual interdependency among chain actors, resulting in innovation linkages, trade linkages, and knowledge flow (OECD, 1999). These all lead to the formation of virtuous cycles that positively impact the nation's economic growth (Argyrous, 2001).	Doran and O'Leary, 2011; Linden et al., 2009; Rosenberg, 2004.
3. ICT – Innovation – Growth Competitiveness	Cluster Theory (Porter, 1990) (Johnston, 2003)	ICT facilitates (1) easy exchange of knowledge, information and ideas, (2) access to qualified labor and skilled staff, (3) access to markets, (4) access to new ideas, and (5) access to specialized services or facilities. However, it is the access to highly skilled cluster members that places the ICT into innovative uses and fuels growth (Johnston, 2003).	Hall and Nousala, 2007; Karaev et al., 2007; Simmie, 2006.
4. Cybersecurity – Growth	Resilience Theory (Holling, 1973) (Starr et al., 2003)	Resilience theory has been applied in a wide range of disciplines. In the context of this study, its application to CIIP is considered. Strongly related to the concept of cybersecurity, CIP has a positive economic impact. Resilient CIP, which functions amidst crises, is central to economic growth and social stability (Sinclair, 2009)	Conrad et al., 2006; Croope & McNeil, 2011.
5. Human Capital (moderation effect)	Complementarity Theory (Edgeworth, 1880) (Milgrom & Roberts, 1990)	Human capital, with their tacit skills, knowledge, and use of technologies and innovations, can enhance the effectiveness of the systems used. It is a complementary asset that adds to the impact of ICT and innovation on growth (Brynjolfsson & Saunders, 2010)	Brynjolfsson and Saunders, 2010; Voigtlander, 2008; Bocquet et al. (2007).

Drawing on these hypotheses, and the literature from which they are derived, a research model is now proposed. The model is presented in Figure 9, and it depicts all the above-stated relationships. It also shows the constructs included in the conceptual model proposed in Chapter II in their operationalized form.

Design and Methodology

Research Design

To answer the above research questions and test the stated hypotheses, this study deploys a correlational research design. In general, correlational research investigates the covariation of two or more variables. Correlational research is sometimes considered a type of observational research, as factors are not manipulated by the researcher. It should be emphasized that correlational research is not causal research (Thompson et al., 2005). Statements concerning cause and effect cannot be made on the basis of this research design. This can be done using well-designed experimental studies. Nevertheless, some research questions are best addressed with designs other than experimental. In fact, what is important is to match the research questions with the appropriate research designs (Thompson et al., 2005). According to Cronbach (1957), correlational research and experimental design research use distinct types of samples, measures, analyses, and inferences. Correlational research is often conducted as an exploratory study: it explores relationships to make predictions using a set of subjects (organizations, countries, etc.) with two or more variables (Thompson et al., 2005).

Cohen (1968) considered that in one respect any analysis is correlational. This was also supported by Knapp (1978) and Thompson (2000). This argument is based on the reasoning that since all parametric analyses commonly used (e.g., t-tests and ANOVA) are correlational, as mentioned by Bagozzi et al. (1981), then quantitative studies provide correlational evidence

(Thompson et al., 2005). The authors listed “multiple regression analysis, canonical correlation analysis, hierarchical linear modeling, and structural equation modeling [SEM]” as statistical methods commonly applied with correlational designs (p. 182). As explained in the SEM literature, SEM can either be covariance-based or variance-based, with the latter also termed as partial least squares (PLS) (Reinartz et al., 2009; Haenlein & Kaplan, 2004).

Therefore, and based on the above discussion, this study is designed based on basic correlational research principles since correlational research design allows for the explanation of important behaviors; the analysis of the relationships between two or more variables (Charles, 1995); and the prediction of one variable score based on the values of other scores (Fraenkel & Wallen, 2006). In a similar vein, this study examines the relationship among ICT, innovation, cybersecurity, and global competitiveness. It also uses these relationships to predict the values of the global competitiveness scores.

Methodology

This main and only data source used in the study is secondary data generated by well-known and specialized international organizations. The majority of the data used is in the form of composite indicators, which are used to summarize and synthesize a number of underlying individual indicators or variables. Composite indicators, or indices, are either quantitative or qualitative measures derived from a series of observed facts that can reveal or proxy characteristics (Nardo et al., 2005). The objective is to obtain data for a large number of nations from all regions of the world to assess the relationships postulated above and depicted in the research model.

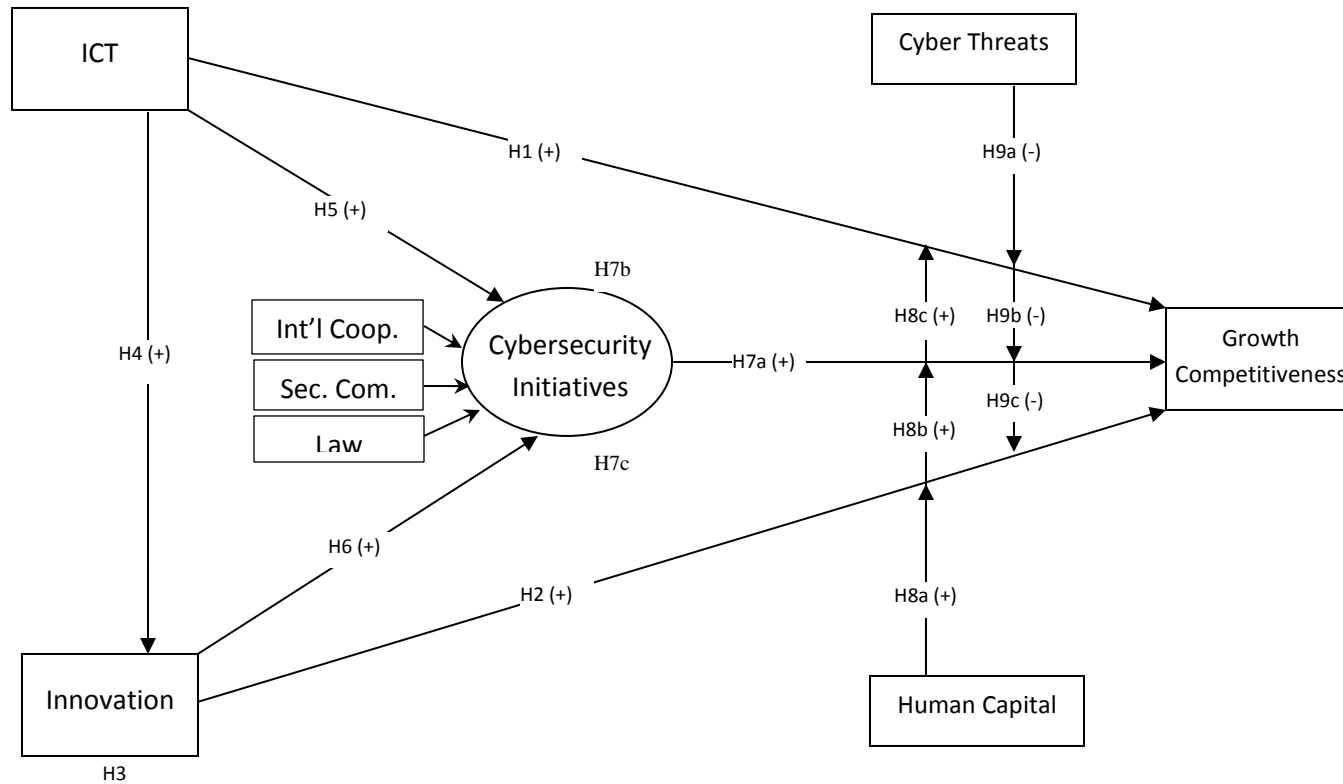
Boslaugh (2007) listed and discussed the benefits and shortcomings of using secondary data. According to the author, the first major benefit is economy: data have already been

collected, thus saving the researcher a lot of resources during this research phase (phase of data collection). Sometimes, even if the secondary data set must be purchased, the cost will most likely be lower than the expenses required for collecting and processing a similar huge data set from scratch (Patzner, 1995). Time savings will also be achieved due to the fact that data are already collected, frequently cleaned, and stored (or published) in electronic format, making it possible for the researcher to devote the bulk of his time to data analysis. In addition to this, secondary data analysis could be ideal for researchers who prefer to think and test hypotheses using existing data sets (Patzner, 1995).

The second major benefit of secondary data usage is the wide scope and extensiveness of data available. In particular, data collected at the national level are important in fields that focus primarily on issues and aspects pertinent more to populations and communities than to individuals. Moreover, some of the data sets comprise data that were collected using a longitudinal design, and others follow a time-series pattern (annual or other regular intervals), allowing researchers to examine population trends, such as economic or development trends, over time (Boslaugh, 2007).

The third advantage in deploying secondary data lies in the expertise and professionalism that often characterize the data collection process, a feature that is sometimes lacking in smaller research projects. For instance, many of the economic, ICT, and innovation surveys use wide scope and complex sample design as well as a vast array of weighting schemes that allow the researcher to compute population-based estimates of the aspects being studied.

Figure 9 Research Model



According to Boslaugh (2007), while a local data collection project could possibly use similar techniques, the tendency is more toward using convenience samples, where generalizability is questionable. Another example could be the federal data sets, where data collection is often performed by specialized and well-experienced staff, in contrast to many smaller research projects, where data are collected by individuals or groups (e.g., students) lacking the adequate experience required in a certain field of study (Boslaugh, 2007).

Besides advantages, secondary data also have some disadvantages. One major disadvantage is inherent in the nature of the secondary data: the data were collected for purposes other than answering the specific research questions of the researcher using the data. Another possibility could be that the data set may not cover the populations, geographic regions, or time periods that the researcher is interested in. A related problem could be in variable definition and categorization, which may not match the researcher's requirements. In addition, data may not be accessible to the secondary researcher for confidentiality or other reasons. For these reasons, careful screening and examination of a secondary data set is crucial to assess its relevance, proper definition, and availability (Boslaugh, 2007).

A second major disadvantage of using secondary data is the lack of knowledge a researcher has regarding how the data collection process took place. More specifically, the researcher using the data may not know whether important aspects related to data quality are met, or the extent to which they are affected by issues such as low response rate. This problem is sometimes alleviated by certain governmental agencies and international organizations that provide extensive explanation of the procedures followed to collect data (Hox and Boeije, 2005) as well as presentation of technical information in the form of documents or reports published on

their websites. In all cases, researchers using secondary data must be well aware of the problems related to the data sets they are using (Boslaugh, 2007).

To assess the applicability of these advantages and disadvantages from the perspective of this study, each point was taken into consideration and analyzed. The result of this analysis is summarized and presented in Table 9. Interestingly, the advantages all apply, and only one disadvantage applies. Based on this, data evaluation is deemed important (Hox and Boeijs, 2005) as discussed later based on the documentation generated by the data publishing organizations.

Data: Source and Size. The development of individual country indices, such as those developed by the World Bank in its large research program and publications compiling information from over 100 countries, facilitates comparative analysis across countries. It can also exert some pressure on poor performers to enhance their growth and competitiveness level (Burnham, 2009) through benchmarking and learning from other nations' best practices. In fact, the data used in the study are mainly composite indicators or indices developed by several international organizations. Because several sources are used, differences in the number of countries across reports from different organizations as well as in reports generated by the same international organization across several years, care should be taken regarding which countries to include and which to exclude because of remarkable missing values for various indicators.

Table 9 Secondary Data: Advantages and Disadvantages and their Applicability to the Study

Features	Applicability	Justification
Advantages		
<ul style="list-style-type: none"> Economy 	✓	Conducting a large-scale project at the global level with many countries involved is not justified cost-wise, time-wise, and effort-wise for one researcher.
<ul style="list-style-type: none"> Breadth of data availability 	✓	An examination of an area like growth competitiveness across nations as well as an investigation of the indicators possibly associated to it, including networked readiness, innovation, and cybersecurity require data focusing on populations rather than individuals for a time period extending over several years.
<ul style="list-style-type: none"> Expertise and professionalism in data collection 	✓	World Economic Forum, the United Nations, the World Bank, and the International Telecommunications Unit are global institutions that enjoy a well-known international reach and reputation at the economic, political, and social levels (Pigman, 2007).
Disadvantages		
<ul style="list-style-type: none"> Particular information needed by the researcher may not have been collected. 	X	Data sets chosen are the ones needed. They can help fulfill the major purpose of the study; namely, examining the relationship between ICT, innovation, and cybersecurity on one hand, and then investigating the impact of this relationship on nations' growth competitiveness.
<ul style="list-style-type: none"> Variable categorization or format is inconvenient for the study. 	X	The study mainly uses indexes rather than raw data.
<ul style="list-style-type: none"> Unavailability of data to the researcher. 	X	Data sets used in this study are available for use on their publishers' websites.
<ul style="list-style-type: none"> Researcher's ignorance of the data collection process due to lack of involvement or participation 	✓	Documentation of data collection procedures, problems encountered, and solutions provided can all be accessed from published reports or are available on the publishers' websites.

The major data sources used were: United Nations Development Program (UNDP), International Telecommunications Unit (ITU), INSEAD, World Bank, and, and World Economic Forum (WEF). The target population consists of 216 countries belonging to all regions, as classified and presented by World Bank (World Bank, 2011). A list of the countries, along with the regional groupings, are shown in Appendix A. As mentioned earlier, countries with complete data sets from all the sources used will be chosen for data analysis. But what are the composite indicators, how were the data originally collected by these organizations, what sampling techniques were used, and what measures were used to ensure the appropriateness of the data? This is elaborately presented and discussed in the following section.

“What we measure affects what we do. We will never have perfect measures – and we need different measures for different purposes”. Joseph Stiglitz (2009, p. 28).

Composite Indicators. A composite indicator is formed of an aggregation of individual indicators compiled into a single index, based on an underlying theoretical framework (OECD, 2004). A theoretical framework allows for the identification, selection, combination, and weighing of individual variables (indicators) in a manner reflecting the dimensions of the phenomenon being measured. An index that combines more than one indicator allows non-experts to use complex information (Castoldi & Bechini, 2010). For example, decision makers and policy makers need a global evaluation of the sustainability of economic growth and global competitiveness in order to define policies, but in some cases they may not have the knowledge necessary to identify the various indicators that may compose national competitiveness and to understand the complexity and trade-offs among the various components, which are easily synthesized by an index. The *Handbook on Constructing Composite Indicators* prepared by the OECD (the Organization for Economic Cooperation and Development) and the JRC (the

European Commission Joint Research Center) discusses the benefits and drawbacks of using composite indicators (listed in Table 10). The functionalities implied from the list of advantages include (Lopez-Claros & Mata, 2010):

1. Provision of support for decision makers, as these indicators enable more considered reasoning and judgment regarding the various policy alternatives available;
2. Enabling international comparison, benchmarking, and progress evaluation over time; and
3. Enhancing public debate and promoting accountability.

Table 10 Pros and Cons of Composite Indicators³

Pros	Cons
<ul style="list-style-type: none">• Can summarize complex, multi-dimensional realities with a view to supporting decision makers.• Are easier to interpret than a battery of many separate indicators.• Can assess progress of countries over time• Reduce the visible size of a set of indicators without dropping the underlying information base.• Thus make it possible to include more information within the existing size limit.• Place issues of country performance and progress at the center of the policy arena.• Facilitate communication with general public (i.e., citizens, media, etc.) and promote accountability.• Help to construct/underpin narratives for lay and literate audiences.• Enable users to compare complex dimensions effectively.	<ul style="list-style-type: none">• May send misleading policy messages if poorly constructed or misinterpreted.• May invite simplistic policy conclusions.• May be misused, e.g., to support a desired policy, if the construction process is not transparent and/or lacks sound statistical or conceptual principles.• The selection of indicators and weights could be the subject of political dispute.• May disguise serious failings in some dimensions and increase the difficulty of identifying proper remedial action if the construction process is not transparent.• May lead to inappropriate policies if dimensions of performance that are difficult to measure are ignored.

Source: Giovanni et al. (2008) from OECD and European Commission Joint Research Center Handbook on constructing composite indicators (2008).

³ The usefulness of these types of measures has been widely debated (e.g., Saltelli, 2007; Saisana et al., 2005; Grupp and Mogee, 2004; Freudenberg, 2003). The debate involved technical aspects, methodological questions, as well as the public subjective perceptions, and whether their advantages outweigh their possible disadvantages. It is not the intention of this study to be a part of this debate. Suffice it to say that there has been a notable increase in the development of indices, weighing methods, and rankings by several credible and reputable organizations (Lopez-Claros and Mata, 2010), including the United Nations Development Program, World Bank, World Economic Forum, and International Telecommunications Unit, among others.

With respect to the disadvantages, one may most probably infer that composite indicators (indexes) must be deployed with a keen consideration and evaluation of the methodology followed to develop it. This includes, but is not confined to, the theoretical framework used, the data set chosen, and the aggregation method applied. As widely suggested in the body of literature related to development, competitiveness, technology achievement, and environment sustainability composite indicators, to list a few, country-level indexes stem from the need to rank countries and benchmark their performance against other countries' performance. Composite indicators are commonly used in fields such as economic, business, and human development statistics (e.g., the World Bank and OECD Composite Indicators) and are used in various policy domains, such as quality of life assessment, sustainable development, networked readiness, globalization, and innovation (e.g., Cox et al.; 1992, Huggins, 2003; Wilson & Jones, 2002; Guerard, 2001; Fare et al., 1994; Lovell et al., 1995; and Saisana & Tarantola, 2002, among others). The growing number and wide spread use of these indicators is a clear symptom of their political importance and operational relevance in decision-making. A general objective of these composite indicators is the ranking of countries according to some aggregated dimensions (Cherchye, 2001 and Kleinknecht et al., 2002). A report by OECD clearly summarizes the above discussion, and states that (OECD, 2003, p. 3):

“...The proliferation of composite indicators in various policy domains raises questions regarding their accuracy and reliability. Given the ... nature of their computation, the sensitivity of the results to different ... aggregation techniques, and continuing problems of missing data, composite indicators can result in distorted findings on country performance and incorrect policy prescriptions... [Nevertheless] Despite their many deficiencies, composite indicators will

continue to be developed due to their usefulness as a communication tool and, on occasion, for analytical purposes.” (OECD, 2003, p. 3)

As a consequence, the improvement of the way these indicators are constructed and used seems to be a very important research issue from both theoretical and operational points of view. A typical composite indicator, I , is built as follows (OECD, 2003, p. 5):

$$I = \sum_{i=1}^N w_i x_i, \text{ where } x_i \text{ is a normalized variable and } w_i \text{ is the weight attached to } x_i, \text{ with}$$

$$\sum_{i=1}^N w_i = 1 \text{ and } 0 \leq w_i \leq 1, i = 1, 2, \dots, N.$$

It could be clearly derived from this mathematical notation that a composite indicator entails a weighted linear aggregation rule applied to a set of variables. The main technical steps needed for its construction are the following two: (1) standardization of the variables to allow comparison without scale effect, and (2) weighted summation of these variables. With this in mind, along with the potential disadvantages and challenges outlined by OECD (2003), Munda & Nardo (2003), and Lopez-Claros and Mata (2010), among others, it is prudent to identify and understand the elements required for the construction of effective indices or composite indicators. Previous researchers (e.g., Zhou et al., 2007; Giovanni et al., 2008; and Castoldi & Bechini, 2010) identified three major steps to achieve this objective: (a) normalization and evaluation of the performance of each criterion (indicator), (b) determination of the weights representing the priorities for each criterion, and (c) aggregation (based on additive, multiplicative, or other distributional formalisms). Using a more detailed and explicit approach, the OECD JRC (2008) handbook outlines and discusses the crucial steps needed to construct an effective composite indicator. These are: (Giovanni et al., 2008)

1. Developing a theoretical framework: this provides the theoretical basis upon which the selection and synthesis of variables into a meaningful index take place. In other words, the fitness-for-purpose principle is applied, which makes the involvement of experts and stakeholders at this phase a necessary step. In fact, a sound theoretical framework is the first step toward constructing indexes (composite indicators). The framework should clearly define the phenomenon to be measured, thus facilitating the selection of individual indicators and weights that reflect their relative importance and the dimensions of the overall composite. This process should be based on what should be measured, and not on which indicators are available. This involves defining the concept, defining the subgroups, and identifying the selection criteria.
2. Data selection: this should be based on the analytical soundness, country coverage, measurability, and relevance of the indicators to the concept being measured as well as their relationship to each other. Using proxy variables as substitutes for indicators should be considered when data are not adequately available (involvement of experts and stakeholders is also sought in this phase).
3. Imputation of missing data: data imputation is needed to have a complete dataset. Hair et al. (2006) addressed the missing data issue and discussed various types of imputation methods, including: modeling-based approaches, complete case, all-available subsets, case substitution, hot and cold deck imputation, mean substitution, and regression-based approach (Hair et al., 2006).
4. Normalization: this should be performed to render the variables comparable. Normalization procedures should be selected with respect to both the data properties and the theoretical framework. Care should also be given to the identification of outliers, adjusting scales, and transforming highly skewed indicators (if necessary). In literature a large number of

normalization methods are reported: ranking, Z-score standardization, min–max normalization, distance to a reference measure, categorical scale, transformation of indicators above and below the mean, cyclical indicators, balance of opinions, and percentage of annual differences over consecutive years (Giovanni et al., 2008). Each algorithm differs for the approach used in the handling of the statistical distribution of original data, with advantages and disadvantages in the normalization process (Freudenberg, 2003).

5. Multivariate analysis: applying multivariate analysis is important to assess data suitability, study the dataset overall structure, and guide subsequent methodological choices, including weighting and aggregation. Multivariate analysis at this stage includes principal components/factor analysis, Cronbach coefficient alpha, and cluster analysis.

6. Weighting and aggregation: this involves the selection of appropriate weighting and aggregate procedures that align with the theoretical framework and data properties, the discussion of correlation issues among indicators, and whether they should be accounted for.

7. Uncertainty and sensitivity analysis: this is a very important step that should be conducted to evaluate the composite indicator robustness in terms of inclusion or exclusion of an indicator, the normalization method applied, the imputation method used, the weights selected, and the aggregation method used.

Description and Evaluation of Composite Indicators Used in the Study. As previously mentioned, this study uses four published composite indicators (namely, ICT Development Index, Global Innovation Index, Knowledge Economy Index which draws on Human Capital Index, and Global Competitiveness Index) and one hard data set (cybersecurity threats). Based on the discussion presented in the previous section regarding the challenges posed by using composite indicators, as well as the steps recommended for establishing effective

ones, it is imperative at this stage to assess the indices used in this study in light of the recommended guidelines for index construction and robustness analysis. This will be covered in the following subsections. Note should be taken that most of the description pertinent to the indices are adopted as they are presented in the publishing organizations' reports.

ICT Development Index. Given its leading role in the collection and dissemination of telecommunication and ICT statistics worldwide, ITU developed a statistical tool that would allow countries to benchmark their information societies globally and regionally. With the evolutionary spread of ICTs during the past two decades, and the resulting impact on societies and economies, international calls for monitoring and benchmarking have increased. At the same time, since the turn of the century, the availability of Internet-related data globally has increased, making it feasible to construct a composite index that combines several indicators into one single statistical value and compare it over a number of years. This is when ITU's work on composite indices began.

ICT Development Index is based on a previous index that was developed by ITU, namely, "Digital Access Index (DAI)", which was presented at the first phase of the World Summit on the Information Society (WSIS) (ITU, 2008). The main objective of the DAI was to measure the overall ability of individuals in a country to access and use ICTs. It was thus built around five categories: infrastructure, affordability, knowledge, quality and actual usage of ICTs. It was based on a methodology that used goalposts (or upper value limits), which were averaged to obtain category scores. Categories were then averaged to obtain the overall index value. The DAI included eight indicators and was calculated for 178 economies for the year 2002. Comparative DAI scores for the years 1998 and 2002 were calculated for 40 countries. Although it was published once only, it received considerable interest from governments and other users

and showed that there was a clear international demand for such a benchmarking tool (ITU, 2010).

In 2005, ITU decided to merge the DAI with another index, the Orbicom “Infostate Index” to create the “ICT Opportunity Index (ICT-OI)”. The decision to merge the two indices was taken in order to benefit from the experiences gained in producing the two indices and to avoid publishing two ICT indices that were similar in terms of the data they were based upon. It was also in response to calls from the international community “to develop a composite ICT Development (Digital Opportunity) Index” combining statistical indicators with analytical work (ITU, 2009).

ICT Development Index: Data Collection and Sampling Methods. The ITU presents a detailed description of how data were collected for the development of the ICT Development Index. As a United Nations agency, one of ITU's roles is to identify, define, and produce international official statistics covering the telecommunication/ICT sector. This is in line with other specialized agencies that produce statistics covering their respective field of operations and forms part of the global statistical system of the UN. ITU collects telecommunication/ICT data for about 200 economies worldwide. In fact, ITU targets the overall population of countries with telecommunication technologies and facilities. These can be divided into three key sets of data:

- Telecommunication/ICT infrastructure and access data collected annually through two (one short and one long) questionnaires.
- Tariff data collected through an annual questionnaire.
- Data on access to and use of ICTs by households and individuals, collected annually through a questionnaire. These indicators are the core indicators on access to, and use of, ICTs by households and individuals.

These questionnaires are addressed to the government agency in charge of telecommunications/ICT (ministry, regulatory authority) as well as to National Statistical Offices available in the various countries. The result of the survey-based data collection method was a data set that was treated for certain methodological issues, such as missing data and data normalization.

ICT Development Index: Conceptual Framework. The conceptual framework for the index builds on the basic assumption that ICTs can be a development enabler if applied and used appropriately, as this has been extensively discussed in the literature during the past ten years (for e.g., ITU, 2006a; OECD, 2003, 2005; UNCTAD, 2006, 2007; Oliner & Sichel, 2002; Jorgensen et al., 2002; and Van Ark et al., 2003). ICTs are also critical to countries that are moving toward knowledge-based societies. The index should therefore give an indication of the extent to which countries have advanced in the area of ICT for development and track the progress thereof.

A useful conceptual framework to describe the process countries are going through in their evolution toward information societies is based on the basic three-stage model:

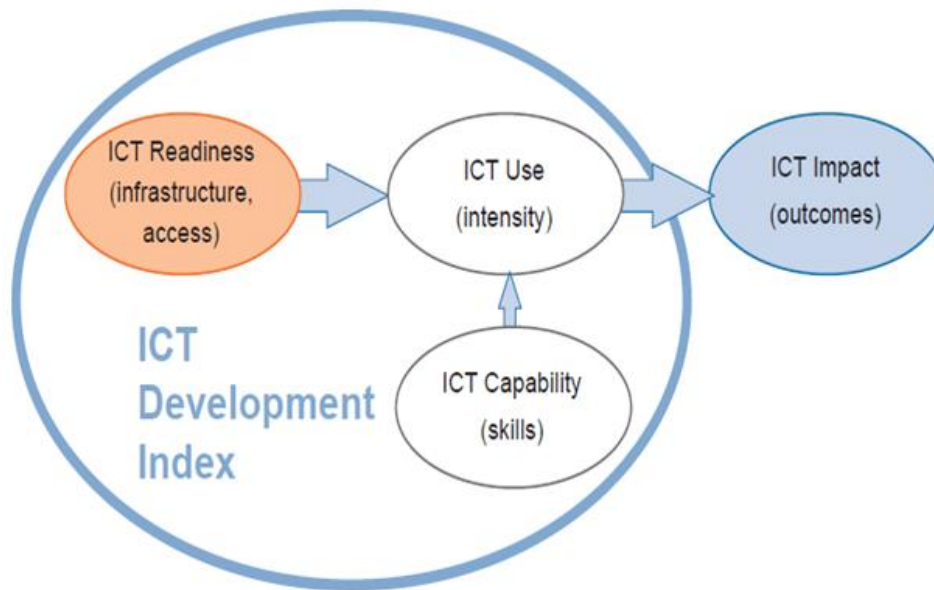
Stage 1: ICT readiness, reflecting the level of networked infrastructure and access to ICT;

Stage 2: ICT intensity, reflecting the level of use of ICTs in the society; and

Stage 3: ICT impact, reflecting the result of efficient and effective ICT use.

These three elements combined measure a country's path toward becoming an information society as depicted in Figure 10.

Figure 10 ICT Development Index Indicators



Source: ITU, 2011

As can be noted from the figure, the approach is a sequential one, where a country's development toward an information society is following a certain sequence of ICT access and its increased use on the path to transformation. Certain indicators in the sequence can be leapfrogged--for example, mobile networks substituting for fixed ones. While the indicators may change, however, the basic stages will still remain.

Based on the above-described framework, the selected indicators should correspond to the following three subcomponents of the index (or sub-indices):

- ICT infrastructure and access.
- ICT use (primarily by individuals, but also households, businesses, others as data becomes available in the future) and the intensity of use.
- ICT skills (or capacity necessary to use ICTs effectively).

For each type of subcategory, a list of potential variables (or indicators) was established, from which a final selection of 11 indicators was made. The selection was based on:

- The availability of the data (and their quality) for a large number of countries, given that the index should be as global in nature as possible. Since the ICT data availability in the majority of developing countries is poor, this was the main restrictive factor in the selection;
- The results of multivariate analyses carried out. Principal components analysis (PCA) was carried out to analyze the underlying nature of the data, to explore whether the different dimensions are statistically well-balanced and to reveal how different indicators are associated and change in relation to each other. Figure 11 shows a copy of the PCA results, as reported by ITU (2009);
- The relevance of a particular indicator for contributing to the main objectives and conceptual framework of the index. For example, the selection of indicators should reflect the situation in all countries (developed as well as developing); and
- The recommendations made by experts and participants at the 6th WTIM (Jensen & Mahan, 2007).

Figure 11 Component Loadings for the ICT Development Index Indicators

	Component loadings	Indicator weights (%)
ICT access indicators		
Fixed telephone line penetration	0.531	7.51
Mobile cellular penetration	0.884	20.84
International Internet bandwidth per Internet user	0.996	26.43
Proportion of households with computer	0.915	22.30
Proportion of households with Internet	0.927	22.91
ICT use indicators		
Internet user per 100 inhabitants	0.842	32.06
Fixed broadband subscribers per 100 inhabitants	0.809	29.61
Mobile broad subscriptions per 100 inhabitants	0.921	38.33
ICT skills indicators		
Adult literacy rate	0.890	28.18
Secondary gross enrolment ratio	0.792	36.20
Tertiary gross enrolment ratio	0.897	35.62

Source: ITU, 2009

The above components are represented by indicators, as shown in the following table (Table 11).

The table also shows the agency that carried out the data collection process.

Table 11 ICT Development Index: Subcomponents and Corresponding Indicators (based on ITU Report, 2009)

ICT-DI Subcomponent	Indicators	Data Collection Agency
ICT ACCESS INDICATORS	<ul style="list-style-type: none"> • Fixed telephone lines per 100 inhabitants • Mobile cellular telephone subscriptions per 100 inhabitants • International Internet Bandwidth (bit/s) per Internet user • Proportion of households with a computer • Proportion of households with Internet access at home 	ICT Access Indicators data were all collected by ITU.
ICT USE INDICATORS	<ul style="list-style-type: none"> • Internet users per 100 inhabitants • Fixed broadband Internet subscribers per 100 inhabitants • Mobile broadband subscriptions per 100 inhabitants 	National Statistical Organizations and ITU.
ICT SKILLS INDICATORS	<ul style="list-style-type: none"> • Adult literacy rate • Gross enrolment ratio 	UNESCO Institute of Statistics (UIS)

ICT Development Index: Imputation and Normalization. For the above listed indicators, ITU applied an imputation method to have a complete data set with no missing data values. The imputation method used was the ‘*hot deck*’ imputation, which uses data from countries with “similar” characteristics. GDP per capita and geographic locations were used as the main criteria in identifying countries with similar characteristics.

Moreover, ITU applied Data Normalization to ensure that the dataset uses the same unit of measurement. This was done, taking three criteria into consideration:

1. The relative performance of countries;
2. The production of index results that allow countries to track progress of their evolution toward an information society over time; and
3. The choice of a method that can be replicated by countries. (These 3 must be parallel)

Based on these three criteria, the *distance to a reference measure* was used as the normalization method. The reference measure is the ideal value that could be reached for each variable. In all of the indicators chosen, this was 100, except for four indicators:

- International Internet bandwidth per Internet user, which in 2007 ranged from 10 (bits/s/user) to more than 1 million. To diminish the effect of the large number of outliers at the high end of the value scale, the data were first transformed to a logarithmic (log) scale. The ideal value was then computed by adding two standard deviations to the mean of the rescaled values, resulting in a log value of 5.
- Mobile cellular subscriptions, which in 2007 ranged from 0.56 to 176 (per 100 inhabitants). The ideal value was computed using the same methodology used for the bandwidth data, by adding two standard deviations to the mean. The resulting reference value was 150 subscriptions per 100 inhabitants.

- Fixed telephone lines per 100 inhabitants ranged between 0.01 and 65 in 2007. The same methodology was used to compute the reference value, resulting in a rounded value of 60 per 100 inhabitants.
- Fixed broadband subscribers per 100 inhabitants. This is a fairly recent indicator and values range from zero to over 40 per 100 inhabitants. In line with main fixed telephone lines, the ideal value was defined at 60 per 100 inhabitants.

The Global Innovation Index. The Global Innovation Index issued by INSEAD (2011) is a composite of two sub-indices, one representing innovation input and the other representing the output of the innovation activities and processes in a nation. The pillars on which the Innovation Output Sub-Index and the Input Sub-Index are founded consist of (Dutta, 2011):

1. Five input pillars capture some national economy elements that enable innovative activities. These are: (a) Institutions, (b) Infrastructure, (c) Human capital and research, (d) Business sophistication, and (e) Market sophistication.
2. Two output pillars capture concrete manifestation of innovation outputs: (a) the Scientific outputs and (b) the Creative outputs.

Each of these pillars is composed of many sub-pillars and each sub-pillar consists of individual indicators. Sub-pillar scores are computed as the weighted average of individual indicators, and pillar scores are the simple average of the sub-pillar scores. Based on this, three measures are then calculated:

- The Innovation Input Sub-Index, calculated as the simple average of the five pillar scores listed in (1).
- The Innovation Output Sub- Index, computed as the simple average of the last two pillar scores mentioned in (2).

- The overall GII, computed by simply averaging the Input and Output Sub-Indices.

In addition to these, an Innovation Efficiency Index was calculated as the ratio of the computed Output Sub-Index to the computed Input Sub-Index. To audit the data collection and index building processes, INSEAD referred to the services provided by the Joint Research Centre (JRC). JRC of the European Commission has researched extensively concerning the complexity of composite indicators' ranking countries' performances along policy lines. For the 2011 edition, the JRC agreed to perform a thorough robustness and sensitivity analysis of the Global Innovation Index (Dutta, 2011). A previous version of the GII model was submitted to the JRC in April 2011. The recommendations and flexibilities allowed on the basis of the JRC preliminary audit were taken into account in the final version of the Global Innovation Index model.

The Global Innovation Index: Data Collection and Sampling Methods. The 2011 Global Innovation Index (GII) covers 125 countries, which were selected on the basis of the availability of data. The criteria used were to keep those countries with a minimum indicator-coverage of 50 indicators (63%) and with scores for at least two sub-pillars per pillar. This flexibility was allowed by the JRC after the first audit, on the basis of the high correlations between sub-pillars within each pillar; after the second audit, five countries with unreliable rankings were dropped from the rankings. The last record available for each country was considered, with a cut-off at year 2000. Survey questions are drawn from the World Economic Forum's Executive Opinion Survey (EOS) and were used to capture subjective perceptions on specific topics. An effort was made in this year's edition to replace soft data with hard or index data, when possible. The GII gained in objectivity, consistency over multiple periods, comparability, and transparency. Nonetheless, 6 EOS questions were kept or added in this year's GII to capture phenomena

strongly linked to innovative activities for which either there are no hard data or existing statistics have low country coverage.

The Global Innovation Index: Conceptual Framework. According to INSEAD and the World Intellectual Property Organization (WIPO), the assessment of conceptual and statistical coherence of the Global Innovation Index (GII) and the estimation of the impact of modeling assumptions on a country's performance are necessary steps to ensure the transparency and reliability of the GII and enable policy makers to derive more accurate and meaningful conclusions and potentially guide choices on priority setting and policy formulation (INSEAD and WIPO, 2012). Modeling the versatile concepts underlying innovation at a national scale around the globe, as attempted in the GII, raises practical challenges related to the quality of data and the combination of these into a single number.

The Econometrics and Applied Statistics Unit at the European Commission Joint Research Centre (JRC) was invited for a second consecutive year by INSEAD and WIPO to audit the GII along two main issues: the conceptual and statistical coherence of the structure, and the impact of key modeling assumptions on the GII 2012 scores and ranks. To ensure conceptual consistency, candidate indicators were selected for their relevance to a specific innovation pillar (based on literature review and expert opinion) and timeliness. To represent a fair picture of country differences, indicators were scaled (by GDP, population, total goods, or others), as appropriate and where needed, either at the source or by the GII team.

The Global Innovation Index: Imputation and Normalization. For the sake of transparency and replicability of results, no additional effort was made to fill missing values. Missing values are indicated with 'n/a' and are not considered in the sub-pillar score. Potentially problematic indicators with outliers that could polarize results and unduly bias the rankings were

treated following the recommendations of the JRC. This affected 28 hard data indicators. This was done in two stages: selection and treatment. As for selection, the 28 problematic indicators were identified by a combination of skewness and kurtosis statistics: absolute value of skewness greater than 2, and kurtosis greater than 3.5. The second stage was treatment. Here, treatment series with one to four outliers (26 cases) were winsorised: The country values distorting the indicator distribution were assigned the next highest value, up to the level where skewness and/or kurtosis entered within the ranges specified above. For series with five or more outliers (2 cases), skewness and/or kurtosis entered within the ranges specified above with transformation by natural logs. The 80 indicators were then normalized into the [0, 100] range, with higher scores representing better outcomes. Normalization was made according to the min-max method, where the min and max values were given by the minimum and maximum indicator sample values respectively, except with index and survey data, for which the original series' range of values was kept as min and max values (for example, [1, 7] for the World Economic Forum Executive Opinion Survey questions, [0, 100] for World Bank's World Governance Indicators, [0, 10] for ITU indices, etc.).

The Human Development Index. The Human Development Index (HDI) is a summary measure of human development. It measures the average achievements in a country in three basic dimensions of human development: a long and healthy life, access to knowledge and a decent standard of living. The HDI is the geometric mean of normalized indices measuring achievements in each dimension.

The Human Development Index: Data Collection and Sampling Methods. Since the HDI relies on country-level aggregates such as national accounts for income, the HDI must draw on alternative sources of data to obtain insights into the distribution. The distributions have different

units—life expectancy is distributed across a hypothetical cohort, while years of schooling and income are distributed across individuals. Inequality in the distribution of HDI dimensions is estimated for:

- Life expectancy, using data from abridged life tables provided by UNDESA (2010). This distribution is grouped in age intervals (0–1, 1–5, 5–10, ..., 85+), with the mortality rates and average age at death specified for each interval.
- Mean years of schooling, using household survey data harmonized in international databases, including the Luxembourg Income Study, EUROSTAT’s European Union Survey of Income and Living Conditions, the World Bank’s International Income Distribution Database, the United Nations Children’s Fund’s Multiple Indicators Cluster Survey, ICF Macro’s Demographic and Health Survey, the World Health Organization’s World Health Survey and the United Nations University’s World Income Inequality Database.
- Disposable household income or consumption per capita using the above-listed databases and household surveys--or for a few countries--income imputed based on an asset index matching methodology using household survey asset indices (Harttgen and Vollmer 2011).

The Human Development Index: Conceptual Framework. The conceptual framework for an HDI-based assessment of sustainability reflects the human development concept of intergenerational equity based on principles of global justice and rooted in the premise that choices made today should not limit choices available to people in the future. The people-centered, HDI-based approach to assessing sustainability also incorporates the idea of planetary thresholds, showing how climate change in particular is already posing severe long-term human development risks, most acutely in poor nations and poor communities.

The HDI-based itself on three development-linked concepts, and then chose indicators to represent each concept. The HDI measures are comprised of: life expectancy (as a proxy for health), adult literacy (as a proxy for education) and purchasing-power-adjusted dollar income (as a proxy for access to a decent standard of living). The purchasing-power-adjusted GNP per capita figure was taken from the International Price Comparison Project, jointly run by the UN Statistical Office, the World Bank, EUROSTAT and the OECD (UNDP, 1990). International bodies such as the World Bank, representing the interests of investors, were thus included in the project. The educational indicators were soon expanded with adult literacy being supplemented by ‘mean years of schooling’, for 1991-94, then by ‘combined gross enrolment’ at primary, secondary and tertiary levels, in 1995 (UNDP 1990-1995). From 1995 to 2009 the HDI indicators remained stable (UNDP 2009).

The Human Development Index: Imputation and Normalization. For a small number of countries that were missing one of our indicators, the HDRO filled the gap by estimating the missing value using cross-country regression models. Moreover, until 2010, the HDI had been defined as a simple arithmetic average of normalized indices in the dimensions of health, education and income:

$HDI = (1/3) * (H_h + H_e + H_{ls})$; where H_i denotes the sub-index for dimension I , with $i = \{h, e, ls\}$ respectively denoting the health, education and living standards dimensions. Each of these indices was in turn estimated as (or derived from) normalized indicators of achievements in each of these dimensions. Life expectancy and GDP per capita were the proxies for health and living standards respectively, whereas the education dimension used two indicators: literacy and the gross enrollment ratio. The indices were normalized using (given stated?) upper and lower bounds.

As important as it is, the human development index stresses education, health, and living standards without taking into consideration the ICT skills or their use by the people of a nation. Based on this, the index presented by the World Bank, namely Knowledge Economy Index (KEI), was developed based on HEI but also taking into consideration the ICT use dimension, which cannot be ignored in this information age. Accordingly, the KEI has been used in this study. It includes the measures of HDI but also incorporates the institution regime and the ICT use in terms of computer and Internet access. The advantage of this index is that it takes into consideration the abilities of individuals (education), their ICT skills, and the opportunities provided to them (institutional regime). The variables included in the index were standardized using the process of normalization (World Bank, 2012).

The Growth Competitiveness Index (GCI). For more than three decades, the World Economic Forum's annual Global Competitiveness Reports have studied and benchmarked the many factors underpinning national competitiveness. From the onset, the goal has been to provide insight and stimulate discussion among all stakeholders on the best strategies and policies to overcome the obstacles to improved competitiveness (Sala-I-Martin et al., 2012). In the current challenging economic environment, nations should take into account the consequences of certain actions, strategies, and policies on future prosperity based on sustained growth.

The Growth Competitiveness Index: Data Collection and Sampling Methods. To measure the concept of global competitiveness, the GCI uses statistical data such as enrollment rates, government debt, budget deficits, and life expectancy, which are obtained from internationally recognized agencies, notably the United Nations Educational, Scientific and Cultural Organization (UNESCO), the IMF, and the World Health Organization (WHO). Furthermore,

the GCI uses data from the World Economic Forum's annual Executive Opinion Survey (Survey) to capture concepts that require a more qualitative assessment or for which internationally comparable statistical data are not available for the entire set of economies.

The Growth Competitiveness Index: Conceptual Framework. There are many determinants driving productivity and competitiveness. Understanding the factors behind this process has occupied the minds of economists for hundreds of years, engendering theories ranging from Adam Smith's focus on specialization and the division of labor to neoclassical economists' emphasis on investment in physical capital and infrastructure, and, more recently, to interest in other mechanisms such as education and training. The GCI is a composite of twelve pillars; namely, training, technological progress, macroeconomic stability, good governance, firm sophistication, and market efficiency, among others. While all of these factors are likely to be important for competitiveness and growth, they are not mutually exclusive—two or more of them can be significant at the same time and, in fact, that is what has been shown in the economic literature (WEF, 2012).

In line with the economic theory of stages of development, the GCI assumes that, in the first stage, the economy is *factor-driven* and countries compete based on their factor endowments—primarily unskilled labor and natural resources. Companies compete on the basis of price and sell basic products or commodities with their low productivity reflected in low wages. Maintaining competitiveness at this stage of development hinges primarily on well-functioning public and private institutions (pillar 1), a well-developed infrastructure (pillar 2), a stable macroeconomic environment (pillar 3), and a healthy workforce that has received at least a basic education (pillar 4).

Yet as a country becomes more competitive, productivity will increase and wages will rise with advancing development. Countries will then move into the *efficiency-driven* stage of development when they must begin to develop more efficient production processes and increase product quality because wages have risen and they cannot increase prices. At this point, competitiveness is increasingly driven by higher education and training (pillar 5), efficient goods markets (pillar 6), well-functioning labor markets (pillar 7), developed financial markets (pillar 8), the ability to harness the benefits of existing technologies (pillar 9), and a large domestic or foreign market (pillar 10).

Finally, according to the Global competitiveness Report, as countries move into the *innovation-driven* stage, wages will have risen so much that they are able to sustain those higher wages and the associated standard of living only if their businesses are able to compete with new and unique products. At this stage, companies must compete by producing new and different goods using the most sophisticated production processes (pillar 11) and by innovating new ones (pillar 12).

It is worth mentioning that the GCI takes the stages of development into account by attributing higher relative weights to those pillars that are more relevant for an economy given its particular stage of development. That is, although all 12 pillars matter to a certain extent for all countries, the relative importance of each one depends on a country's particular stage of development. To implement this concept, the pillars are organized into three sub-indexes, each critical to a particular stage of development.

The Growth Competitiveness Index: Imputation and Normalization. Cross-country and yearly comparisons are meaningful only if, for any given indicator, all the data points capture the same concept over the same period. According to the report (2012), given the extensive country

coverage of the GCI—a record 142 economies this year—it is not always possible to obtain all the data points for an indicator from a unique source. In order to address missing data points, which can also lead to less reliable results, sometimes other sources are used and/or previous years' data are taken, assuming that the time-sensitivity of the particular indicator is not too great. The Forum's Partner Institutes assist with data collection. As a result of these efforts, the percentage of missing data points is usually below 0.5 percent.

The data used to generate GCI are derived from surveys as well as from governmental reports. Based on this, variables that are not derived from the Executive Opinion Survey (Survey) are normalized. To make the aggregation possible, these variables are transformed onto a 1-to-7 scale in order to align them with the Survey results. The min-max transformation was applied. This was used to preserve the order of, and the relative distance between, country scores. A summary of the above composite indicators, along with their compliance with the construction guidelines mentioned earlier, are presented in Table 12.

Computer Threats. The data pertinent to computer threats were obtained for a certain monetary price from RISI, the Repository of Industrial Security Incidents. RISI is a database of cybersecurity incidents that have or could have affected process control, industrial automation or Supervisory Control and Data Acquisition (SCADA) systems. RISI's primary objective is to collect, investigate, analyze, and share important industrial security incidents among its members to enable them to learn from the experiences of others.

Table 12 Composite Indicators (Indices) Used in the Study: Compliance with OECD JRC Guidelines for Constructing Composite Indicators

Composite Indicator	Compliance with Construction Guidelines						
	Theoretical Framework	Data Selection	Imputation	Normalization	MV Analysis	Weighing & Aggregating	Robustness Test
ICT Development Index	✓	✓	Hot Deck imputation method	Distance to a reference measure	✓	✓	Sensitivity analysis
Global Innovation Index	✓	✓	No treatment for missing data	Min-Max method	✓	✓	Uncertainty and sensitivity analysis using Monte Carlo simulation
Human Capital Index	✓	✓	Cross-country regression models	Upper and lower bound methods	✓	✓	Sensitivity analysis
Growth Competitiveness Index	✓	✓	Previous years' values	Transforming non-survey data into a 1-to-7 scale.	✓	✓	Inter-year robustness test

RISI includes accidental cyber-related incidents, as well deliberate events, such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations that did or could have resulted in loss of control, loss of production, or a process safety incident (e.g., fire, explosion, chemical release, injuries, fatalities, etc.). Data is collected through research into publicly known incidents and from private reporting (Luallen and Hamburg, 2010). The database logs security incidents in process control, SCADA, and manufacturing systems, and gathers voluntary submissions from victim companies as well as from news or other reports (Higgins, 2010). Based on this, the data pertinent to threats represents the overall number of incidents that organizations with SCADA systems have encountered in various countries. It is soft data, and will be used to represent the cyber threats measure.

The Security Incidents Organization (SIO) operates the Repository of Industrial Security Incidents (RISI), an industry-wide repository for collecting, investigating, analyzing, and sharing critical information regarding cybersecurity incidents that directly affect SCADA, manufacturing, and process control systems. RISI members receive reliable incident information that allows them to learn from others' experiences, understand the risks associated with industrial cyber threats, and adapt their current security policies in step with changing industrial cybersecurity dynamics (Hollis, 2011).

Study Variables

Preliminary to our analysis, time series and cross-sectional data from various sources were obtained from a variety of sources, including but not restricted to: World Bank, World Economic Freedom, ITU, and the Heritage Foundation. Moreover, since the study is also concerned about determining the indicators that are most likely to be associated to cybersecurity, other sources such as Nation Master for Collaboration Index as well as the Corruption

Perceptions Index, Inc., were also used. A list of these variables, their usage in the study, and their source are listed in Table 13.

Table 13 Variable Definitions, Uses, and Sources

Variable	Description	Usage in Study	Source
ICT Development/Readiness	Ability of a country to make use of networks and ICT.	Independent	World Economic Forum (WEF)
Cybersecurity	Cybersecurity initiatives and strategies	Independent	ITU
Cyber Threats	The reported number of cyber threats/attacks on an economy CI or its SCADA	Independent	RISI
ICT Human Capital and Knowledge Economy	Knowledge use and ICT Skills in an economy	Independent	UNDP and World Bank
Growth Competitiveness	A measure of economic growth	Dependent	WEF
Secure Communication	A measure of the information infrastructure security	Independent	WEF
Collaboration	A measure of the extent of collaboration a nation builds with other nations	Independent	World Bank
Law Enforcement	The legal measures and acts intended to enforce laws related to ICT use as well as information and privacy	Independent	World Bank

Data Analysis

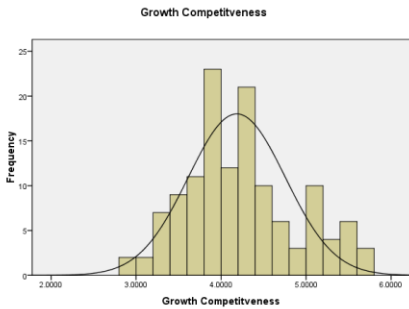
To achieve its objectives and answer the above-stated research questions, the data sets for the variables described in the previous section will be analyzed through the application of several statistical techniques. The study will use PLS-SMART, G*Power 3, and SPSS (the Social Package for Statistical Analysis) to apply various techniques in order to: (1) explore the composite indicator scores in terms of multivariate analysis assumptions; (2) compute the effect size and conduct power analysis to assess the adequacy of the sample size; and (3) test the relationships among the study constructs for exploratory, confirmatory, and predictive purposes. The confirmatory part is related to the basic model of the study, where the relationship between

ICT and innovation on one hand and growth competitiveness on the other is examined (this will be termed the basic model of the study). As for the exploratory part, it examines the changes in the relationships just stated when cybersecurity is introduced. Finally, the goodness-of-fit of the model and the extent to which it can predict growth competitiveness scores will be assessed. In addition, cybersecurity will be considered a formative indicator that will be assessed and built following the approach presented by Diamantopoulos and Winklhofer (2001). Finally, the moderating effect that human development and computer threats play in the above relationships will be gauged. As for the statistical techniques, a variety of descriptive and inferential tests will be applied. To start with, descriptive statistics will be deployed to explore country profiles and characteristics as well as develop a preliminary comparison of the various country groups. In addition to this, bivariate and multivariate parametric and non-parametric techniques, such as multiple regression, PLS and multi-group path analysis, as well as rank correlation methods will be applied. Next will be an exploration of the data used in the study in terms of multivariate analysis (MVA) assumptions. Following this, a description of the multivariate analysis techniques deployed in the study, mainly partial least squares, will be presented.

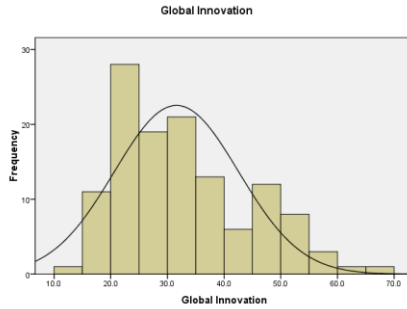
Data Exploration: MVA Assumptions

Multivariate statistical techniques require one or more of the following assumptions about the data. These include: normality of the metric variables, homoscedastic relationships between the dependent variable and the metric and nonmetric independent variables, linear relationships between the metric variables, and absence of correlated prediction errors (Hair et al., 2006).

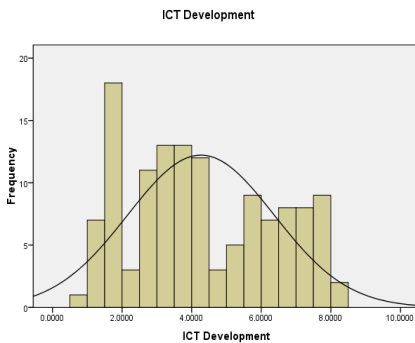
Normality. Determining whether or not the distribution of values for a metric variable complies with the definition of a normal curve is tested with histograms, normality plots, and statistical tests (Hair et al., 2006). In this study, the normality of the distribution of the indices and indicators used was assessed. The graphical and statistical tests yielded the following results:



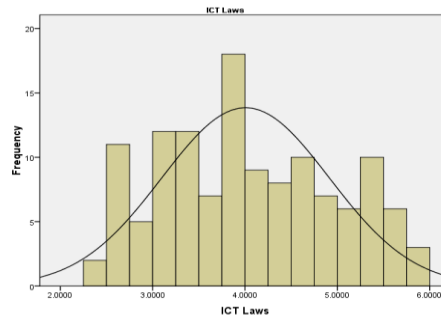
Skewness = 0.389



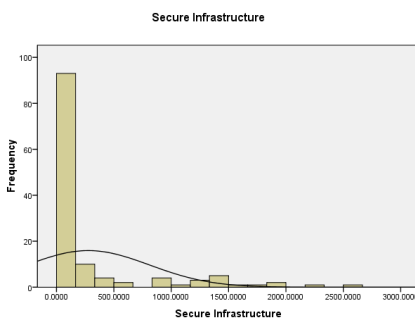
Skewness = 0.727



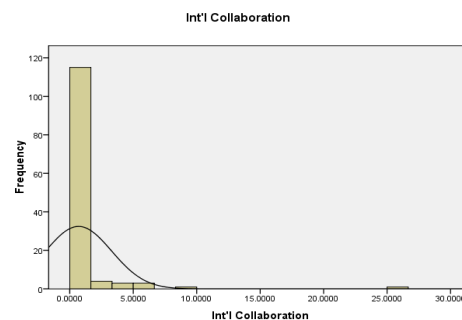
Skewness = 0.240



Skewness = 0.181



Skewness = 2.300



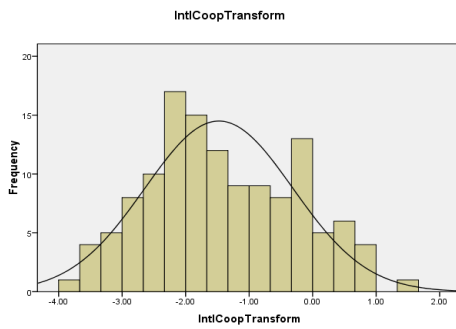
Skewness = 7.629

The normal distribution charts and the skewness coefficient values presented above clearly show that the composite indicators have somewhat of a normal distribution, except for secure infrastructure and international collaboration. According to Hair et al. (2006), if the skewness is greater than 1.0 (or less than -1.0), the skewness is substantial and the distribution is far from symmetrical. To verify this result, a non-parametric Kolmogorov-Smirnov test is run.

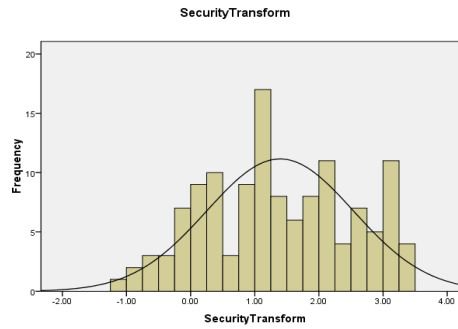
One-Sample Kolmogorov-Smirnov Test

	Growth Competitiveness	Global Innovation	ICT Development	ICT Laws	Secure Infrastructure	Int'l Collaboration
Kolmogorov-Smirnov Z	1.071	1.291	.961	.839	3.755	4.415
Asymp. Sig. (2-tailed)	.202	.071	.314	.483	.000	.000

The K-S test statistics, as shown in the above table, support the previous graphical and skewness tests. Here, the p-values for the K-S test are all higher than the significance level of 0.05, except for those of secure infrastructure and international collaboration. Hence, for these two variables, the alternative hypothesis that the data comes from a normal distribution is rejected (Hair et al., 2006). Taking into consideration the fact that these two variables are not index scores, but rather percentages (secure infrastructure is the number of secure communication lines per one million people as measured by the World Bank) and international cooperation is the percentage of a country's co-authorship and international agreements to that of the world (as suggested by ITU), a transformation procedure should be applied. Hair et al. (2006) and several statistics' articles and books suggest three kinds of transformation in this case: Log (10), square root, or the inverse transformation (1/X). The log transformation was applied on the two variables, and the results came out as follows.



Skewness = 0.193



Skewness = -0.009

Therefore, the transformed values of international collaboration and secure infrastructure could attain a normal distribution. A K-S test was also run here for better verification, and the result is:

One-Sample Kolmogorov-Smirnov Test

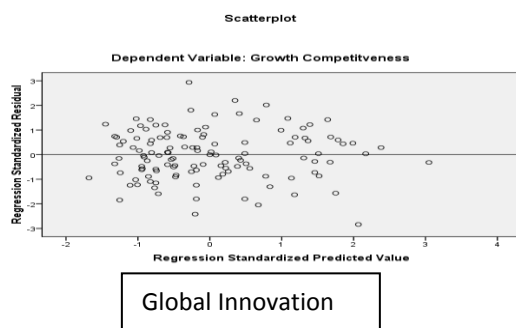
	IntlCoop Transform	Security Transform
Kolmogorov-Smirnov Z	.760	.652
Asymp. Sig. (2-tailed)	.610	.790

Thus, with a p-value higher than 0.05, it can be concluded that the test fails to reject the null hypothesis (that the data for the two variables are normally distributed), which is the desirable outcome in this case.

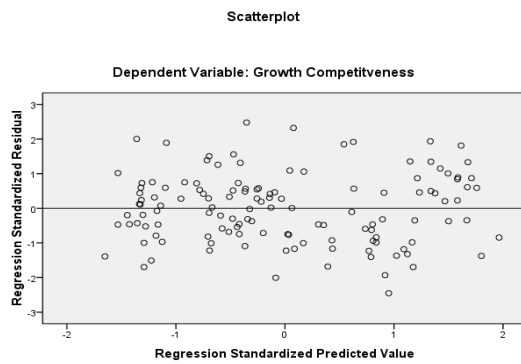
Homogeneity. Known as homoscedasticity, refers to the assumption that the dependent variable will have equal amounts of variance across the range of an independent variable values (Hair et al., 2006). Usually, according to the authors, this assumption is tested using the Levene test for homogeneity. However, this test requires the dependent variable to be metric and the independent variable to be non-metric. In situations where the dependent and independent variables are metric, the assumption is evaluated as part of the residual analysis in multiple

regression. According to Hair et al. (2006), using this method can be used to check for both the linearity and the homoscedasticity assumptions. Hence, if the two assumptions are met, the plot of points will take the form of a rectangular band in the scatterplot graph. A narrow band will indicate a strong relationship, whereas a broader band symbolizes a weaker relationship. If the points show a curved rather than a rectangular pattern, the assumption of linearity is violated. However, if the set of points is narrower at one end and broader at the other end (funnel-shaped), the assumption of homogeneity of variance is violated.

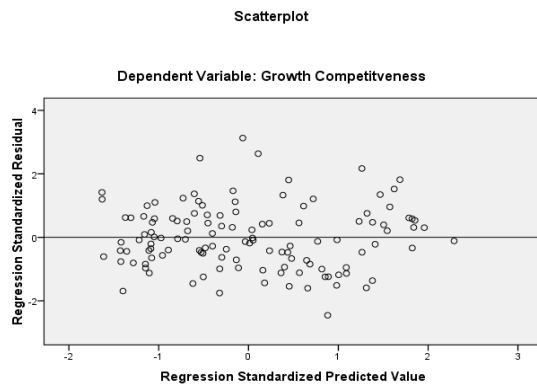
Before proceeding with the test, it is important to have a preliminary estimate of the cybersecurity measure from the three indicators used in the study with the intention to formulate this variable⁴, namely ICT laws, secure infrastructure, and international cooperation following the definition of the variable by ITU (ITU, 2009) and the theoretical basis explained previously. To maintain consistency among measures (Hair et al., 2006), a log transformation was also applied on ICT laws. Cybersecurity measure was then computed as the sum of the three log variables. Based on this, the homogeneity test was performed on global competitiveness (as a dependent variable) and ICT, innovation, and cybersecurity as independent indicators. The results came out as follows.



⁴ The validity and reliability of this formulation will be assessed in Chapter IV when the PLS model is built and tested.



ICT Development

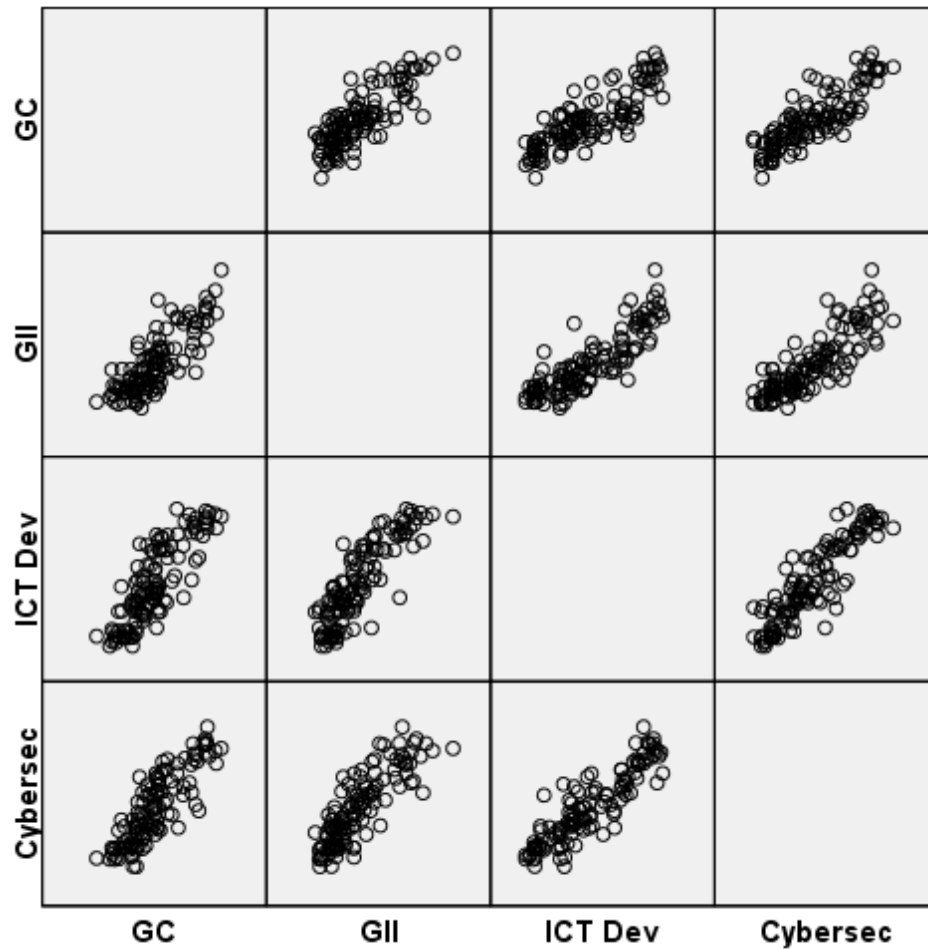


Cybersecurity

Based on the above scatterplots, it seems that the homogeneity of variance assumption is somewhat met in the dataset used in the study.

Linearity. This assumption required for multivariate analysis focuses on the relationships between pairs of metric variables. Linearity is tested through scatterplots, which show the pattern of the relationship between two variables (Hair et al., 2006). The pattern can show a linear, curvilinear, or no relationship. A matrix scatterplot was generated and the result showed the following. As the figure shows, the trends depicted between pairs of variables indicate that none

of the relationships in this scatterplot matrix indicates any serious problem with the assumption of linearity.



The MVA assumptions checked above are a requirement before any multivariate statistical method. Although the statistical method chosen for the study is PLS, which is considered a “soft distribution” modeling approach (Gefen et al., 2000) and doesn’t require an emphasis on these assumptions, still meeting these assumptions can be thought to enhance the rigor of the study and its results.

Partial Least Squares (PLS)

Wold's (1975, 1982) partial least squares structural equation modeling (PLS-SEM) approach and the advanced PLS-SEM algorithms by Lohmoller (1989) have enjoyed growing popularity as a key multivariate analysis method in management information systems (MIS) research (Gefen et al., 2011). Chin's (1998) scholarly work and technology acceptance model (TAM) applications (e.g., Gefen & Straub 1997) are milestones that helped to incorporate PLS-SEM in MIS research.

A key argument for employing PLS-SEM relates to the use of formative measurement models since PLS-SEM readily handles both reflective and formative measures. Technically and implicitly, researchers accept the underlying assumptions of the PLS-SEM method, as for example, predictor specification (Lohmoller 1989; Wold 1982), which allows for the possibility of formative measurement models. However, automatically relying on PLS-SEM, when using formative measures, is not without its own problems. This is particularly because PLS-SEM is restricted to estimating formative constructs without error terms (Diamantopoulos, 2011). In practice, this circumstance is hard to defend because scholars cannot really be certain that all possible causes related to the latent variable are accounted for by the indicators (Diamantopoulos, 2006).

This study incorporates the estimation of a formative construct; namely, Cybersecurity Initiatives. Despite the limitation mentioned above regarding lack of error terms and difficulty of assuring that the indicators used comprise all the possible explanations of the construct in question, this will be alleviated by two types of validity assessments:

- a. Content validity, through seeking the opinion of experts in the field of cybersecurity; and

- b. Nomological network, through a solid theoretical framework and reference to pertinent literature. As for the theoretical framework, the International Relations Theory, and its related concept of national security will be applied. The theory and its perspectives were elaborately discussed in Chapter II. Here, the support that the theory provides to the formative construct estimation will be presented.

Previous literature pertinent to adopting the IR theory in the field of politics and national security within the context of digitalization, information flow, networking, and the Internet support the use of three factors: technological, legislative, and international collaborations. Starting with the technological factor, previous studies that adopted the IR theory noted that with respect to technological advances, the dependency on cyberspace has given rise to new strategic vulnerabilities. This vulnerability has been dramatized by the specter of a “cyber Pearl Harbor” and the realization that the existing cyberspace is vulnerable to a variety of adversary attacks (e.g., denial of service attacks; potential corruption of sensitive data; cyber espionage). In addition, due to the diffusion of low-cost cyberspace technology, the power of non-states (e.g., individuals, corporations, terrorists, transnational criminals,) has been greatly enhanced, thus contributing to more vulnerabilities and potential exploitations (Starr, 2009). Following this argument, recent research suggested the technological measure for combatting the impact of possible cyber attacks. For example, it was suggested that the trend toward cloud computing has a direct impact on cybersecurity: rather than securing user machines, preventing malware access, and managing removable media, a cloud-based security scheme must focus on enabling secure communication with remote systems. This change in approach will have profound implications for cybersecurity research efforts (Shue & Lagesse, 2011). Corroborating with this view, Yan et al. (2012) noted that upgrading an existing power grid into a smart grid requires significant

dependence on intelligent and secure communication infrastructures. This requires security frameworks for distributed communications, pervasive computing and sensing technologies in a smart grid. However, as many of the communication technologies currently recommended for use by a smart grid are vulnerable in cybersecurity, it could lead to unreliable system operations, causing unnecessary expenditures, and even consequential disaster to both utilities and consumers (Yan et al., 2012).

As for international cooperation, it is important as it can resolve the conflicts generated by the dark side of ICT, including cyber threats and vulnerabilities, cyber space militarization, cyber espionage and cyber crime, and cyber warfare. The cooperation will result in global cybersecurity agenda, such as the ITU Cyber Security Agenda (ITU, 2009); global cyber commons, such as those established by CERT (Computer Emergency Response Team) (ITU, 2010); Internet governance; and global cyber norms (MIT & Harvard, 2010).

Finally, previous literature emphasized the importance of law enforcement (domestic and joint) for dealing with cybersecurity issues. However, it was observed that the distinction between law enforcement and national security is blurred by the new threats (Yan et al., 2012). Dealing with this issue requires the expertise of a number of departments and agencies in areas such as international diplomacy with nations where terrorists have been operating, foreign intelligence operations, military planning, domestic law enforcement, and security and prevention activities in the nations (Newmann, 2002).

Why PLS? The most prominent argument for choosing PLS-SEM is the use of small sample sizes. This issue has been debated over the last years (e.g., Goodhue et al., 2006; Marcoulides & Saunders, 2006) with Gefen et al., (2011) noting that there is an “apparent misuse of perceived leniencies such as assumptions about minimum sample sizes” (p. iii).

Prior studies appearing in scholarly journals (e.g., Reinartz et al. 2009), including those more critical of the PLS-SEM method (e.g., Lu et al. 2011), indicate that PLS-SEM overcomes problematic model identification issues and that it is a powerful method to analyze complex models using smaller samples. Nevertheless, like any other statistical technique, PLS-SEM is not immune to threats from data inadequacies and researchers should make every effort to provide support for its statistical power in the research setting at hand. If commonly known standards of collecting adequate sets of empirical data have been met (e.g., the identification and treatment of outliers and other influential observations or the handling of missing values), PLS-SEM can indeed be a “silver bullet” in certain research situations (e.g., when models are relatively complex and representative sets of data are rather small) (Hair et al. 2011; Reinartz et al. 2009). Table 14 lists the study research questions, and the analysis techniques that will be used to address each.

Table 14 Research Questions and Analysis Technique Used

Research Question	Analysis Technique
1. What is the relationship between a nation’s innovation and ICT on one hand and its cybersecurity strategies on the other?	PLS Analysis.
2. What is the relationship between a nation’s ICT and innovation and its global competitiveness level?	PLS Analysis.
3. How does cybersecurity change the ICT-Innovation relationship with a country’s competitiveness level?	PLS Analysis for assessing the mediation effect.
4. How do these relationships vary across regions and country groups?	Multi-group path analysis.
5. What are the factors that are most likely to be associated with cybersecurity strategies?	Formative measure assessment using PLS Analysis.

With the analysis roadmap being outlined here, data examination and analysis can now be done toward shedding light on the ICT-Innovation-Cybersecurity relationship as well as the potential impact of the triad on the nations' economic growth.

PLS Assumptions. As previously mentioned, there are two approaches to estimate the parameters of an SEM; that is, the covariance-based approach and the variance-based approach. The covariance-based approach “attempts to minimize the difference between the sample covariance and those predicted by the theoretical model....Therefore, the parameter estimation process attempts to reproduce the covariance matrix of the observed measures” (Chin & Newsted, 1999, p. 309). Like any SEM, a PLS model consists of a structural part, which reflects the relationships between the latent variables, and a measurement component, which shows how the latent variables and their indicators are related; but it also has a third component, the weight relations, which are used to estimate case values for the latent variables (Chin & Newsted, 1999). Nevertheless, unlike covariance-based SEM, PLS is considered an approach that is used in situations with limited information. Hence, being a limited information approach (Dijkstra, 1983), PLS has the advantage that it “involves no assumptions about the population or scale of measurement” (Fornell & Bookstein, 1982, p. 443) and consequently works without distributional assumptions and with nominal-, ordinal-, and interval-scaled variables.

However, one has to bear in mind that PLS, like any statistical technique, also requires certain assumptions to be fulfilled. Beyond those known from the standard (i.e., Gaussian classical linear ordinary least squares) regression model, the most important assumption is predictor specification (Chin & Newsted, 1999). This requirement states that the systematic part of the linear regression must be equal to the conditional expectation of the dependent variable and can be considered as fulfilled in most cases. Furthermore, by using a Monte Carlo

simulation, Cassel et al. (1999) showed that PLS is quite robust with regard to several inadequacies (e.g., skewness or multicollinearity of the indicators, misspecification of the structural model) and that the latent variable scores always conform to the true values.

Sample Size Adequacy and Power Analysis

The primary product of research inquiry is one or more measures of effect size, not ρ values.
(Jacob Cohen, 1990, p. 1310)

Using the rule of thumb, multivariate analysis techniques generally require 5 to 10 cases per indicator (Hair et al., 2006). Given a total of 9 variables used in this study, the sample size needed according to this rule is $n = 90$. The number of countries (i.e., sample size) in the study is about 174, which means that the sample size herein is adequate. Beside the rule of thumb, one can also use power analysis to derive the sample size needed to achieve that power.

Statistical Power Analysis. Statistical power, in technical terms, describes the probability that a study will reject a null hypothesis when it is false; that is, when it correctly identifies a genuine effect (Hair et al., 2006). It is worth mentioning here, and before proceeding with further discussion, that a study involves two types of errors, Type I error (denoted by α) and Type II error (denoted by β)⁵. The two types of error are related; as one goes up, the other goes down. A test's statistical power is inversely related to β , and is denoted by: $1 - \beta$.

Accordingly, statistical power is the probability that an estimate of the effect size will be

⁵ The two errors researchers may make when drawing conclusions emerge from the fact that an empirical research comprises two competing hypotheses: the null (H_0) and the alternative (H_1). Type I error (α) corresponds to the probability that a researcher wrongly concludes that H_0 should be rejected, and thus; there is an effect, when in fact there isn't. Type II error (β), however, refers to the probability that the researcher will not find an effect (rejects H_1) when there is **one** (Hair et al., 2006). Of course, only one type of error is possible since the null hypothesis cannot be both true and false, and thus both should be taken into consideration when research is conducted. This is very important, especially **because** most researchers pay more attention to minimizing α than trying to find a balance (Ellis, 2010) between both types of errors (i.e., a balance between a study's statistical significance and its power).

statistically significant when, in fact, it represents a real effect that actually exists (Ellis, 2010). Being a probability, power ranges between 0 and 1 in value. Therefore, a power of 0.5 represents a study that has a 50% chance of being successful, i.e., of finding something.

The importance of power analysis stems from the opportunity it makes available to answer two very important questions (Ellis, 2010): (a) how much statistical power does a study have? and (b) how big the should sample size be to detect the minimal real effect in terms of differences or associations? Power analysis requires an examination of four parameters (Ellis, 2010; Hair et al., 2006; Murphy & Power, 2004):

- (1) The effect size, describing the degree to which the results of the study reflect the phenomenon present in the population. As stated by Cohen (1988), “the degree to which the null hypothesis is false” (p. 10).
- (2) The sample size used to conduct the study’s tests, though sample size is one factor, yet the most important of many factors affecting a test sensitivity is that to which power is related (Mazen et al., 1987)⁶.
- (3) The alpha statistical significance criterion (α), which describes the risk related to committing a Type I error. Normally, this is set at the value of $\alpha = 0.05$.
- (4) Statistical power, referring to the suggested Type II error (β) of the test conducted. If, for example, the acceptable level of β is 0.20, then the desired power set for the study is 0.8⁷.

⁶ Other factors include the type of test being deployed, reliability of measures, and the use of controls (Ellis, 2010).

⁷ The literature doesn’t indicate an appropriate power level. However, Cohen (1988) reasoned that power level should be set at 0.8. Cohen contended that this would attain an acceptable balance between α and β risks, taking into consideration the ‘conventional scientific view’ that takes into account Type I error more seriously than Type II error (Ellis, 2010). According to Cohen (1988), the values set were merely guidelines aimed at making researchers think about the importance of and the need to balance the two types of errors.

Based on the aforementioned discussion, and the type of statistical analysis chosen for the current study; namely, Partial Least Squares Path Modeling, a power analysis will be now presented based on:

- (i) A calculation of effect size according to the guidelines presented by Cohen (1988) and Vinzi et al. (2010);
- (ii) Alpha significance criterion of $\alpha = 0.05^8$; and
- (iii) Beta Criterion of $\beta = 0.20$, and thus a power of 0.8.

The power analysis is used mainly to identify the effect size of the study and, equally important, to determine the sample size needed to realize the derived effect and the desired power. Since the study is based on secondary data, the concern would be about the adequacy of the sample size of the data obtained. Following (would be is?) an explanation of the method followed to calculate the effect size, which along with α and the desirable power of 0.8 will be used to derive an estimation of the minimum sample size required.

Effect Size Calculation. An effect size refers to the magnitude of a study's result as it occurs, or as it would be discovered, in the population (Hair et al., 2006). It is a standardized measure of the differences between groups as a result of a treatment introduced (hence, a treatment and a control group), or it can describe the level of association between related variables (Ellis, 2010). In general terms, effect size is the strength of the theoretical relationship found in an analysis and provides an estimation of the degree to which a phenomenon exists in a population (Chin et al., 2003). Effect size has a direct effect on statistical power: a too small or

⁸ Following Fisher (1925), the conventional critical level of α for determining statistical significance is 0.05. This has been subject to some criticism (e.g., Gigerenzer, 1998 as noted by Ellis, 2010). Nevertheless, despite all criticisms, significance testing is still widely used since it allows for verifying that research results obtained from samples are not because of chance or random fluctuations in data sets (Ellis, 2010).

non-significant power is in general a consequence of low effect size (Hair et al, 2006)⁹. In general, research studies are conducted with the purpose of making comparisons between groups or of examining relationships. Accordingly, Ellis (2010) differentiated between “the d family” for assessing differences between groups and “the r family” for measuring the strength of a relationship. This implies that calculating the effect size of the present study belongs to the second family since it is based on correlational design. Within this family, for tests involving ANOVA and multiple regression, Cohen (1988) recommends using the difference in R^2 to calculate an f^2 effect size.

Since the study is deploying the variance-based SEM, known as partial least squares (PLS), it will follow Cohen’s recommendation similar to the approach followed by Chin (1998). Chin proposed deploying the effect size f^2 of PLS constructs in a similar manner to Cohen’s effect size implementation for multiple regression, with the following values given to various effect size levels (Cohen, 1988):

- Small ($f^2 = 0.02$);
- Medium ($f^2 = 0.15$); or
- Large ($f^2 = 0.35$).

The procedure followed to compute the effect size explored the substantive impact of each independent variable (construct) on the dependent variable. This was done by rerunning

⁹ This implies that computing and reporting the effect size of a study is an important step towards enhancing research quality. Nevertheless, most studies lack the power to detect the desirable effects (Hunter, 1997; Gigerenzer, 1998 as noted by Ellis, 2010). This limitation, especially in social science research, could be attributed to the small effect sizes in several studies (Ellis, 2010). For example, in the field of management, studies that have sufficient power to detect small effect sizes has been reported to be between 6% and 9% (Mazen et al., 1987); in international business 4-10% (Brock, 2003); and in management information systems less than 2% (Baroudi and Orlikowski, 1989). These shortcomings are encountered even when research studies report statistical significance and use the conventional significance (α) levels (Ellis, 2010).

three multiple regressions, including in each run two independent variables and excluding one.

The effect size was then calculated using the following formula (Cohen, 1988):

$$f^2 = \frac{R_{incl}^2 - R_{excl}^2}{1 - R_{incl}^2}$$

The effect size for the three regression runs as well as the R^2 values (corresponding to the inclusion and exclusion of the examined variable) are listed in Table 15.

Sample Size Estimation. Power analysis was conducted using the G*Power (V. 3.0) computer program. This is considered a superior tool for running power analysis (Faul et al., 2007) and getting certain outcomes (such as sample size) by inputting certain parameters (such as α , effect size, and desired power). The results of the power analysis conducted for the data set and the variables used in this study are presented in Table 15.

Table 15 Effect Size, Power Level, and Estimated Needed Sample Size ^a

Construct	R^2_{Excl}	R^2_{Incl}	f^2	Effect Size	Statistical Power Level ^b	Sample Size Needed
ICT	0.757	0.768	0.047414	small to medium	0.8	126
Innovation	0.76	0.768	0.034483	small to medium	0.7	138
Cybersecurity	0.746	0.768	0.094828	somewhat medium	0.8	67

^a The power analysis results for sample size estimations are presented in Appendix B.

^b The desired statistical power was set to 0.8 for all tests; however, for innovation, this power level required a sample size of 181 due to the small effect size. Based on this, and because the sample size of the secondary data used in the study is less than 181 ($n = 139$), the power level was reduced to 0.7, resulting in a lower needed sample size.

In reference to Table 15, ICT and innovation have a small effect magnitude, while cybersecurity has a somewhat medium effect ($f^2 \cong 0.1$). As mentioned before in Chapter II, the New Economic Growth model basically includes technology and innovation (Romer, 1994;

Cortright, 2001). Hence, the model including ICT and Innovation and examining their relationship with Growth Competitiveness will be considered the basic model of the study. It is thus logical to emphasize the effect magnitude of incorporating cybersecurity into the model. This is clearly revealed in the last row of the table. Cybersecurity has the highest effect size among the three variables, and the model incorporating it requires a sample size of 67 to detect this effect at a power level of 0.8. In fact, using the sample size the secondary data set provides ($n = 139$) could increase the power level to 0.9678750. An interpretation of the effect size and a discussion of power analysis in relation to the study results will be presented in Chapter IV.

Fitness of PLS to Study Objectives

The conceptual core of PLS is an iterative combination of principal component analysis relating measures to constructs, and path analysis allowing the construction of a system of constructs (Thompson et al. 1995). The hypothesizing of relationships between measures and constructs, and between constructs and other constructs is guided by theory. The estimation of the parameters representing the measurement and path relationships is accomplished using Ordinary Least Squares (OLS) techniques. PLS can be a powerful method of analysis because of its minimal demands on measurement scales, sample size, and residual distributions (Wold 1985). Although PLS can be used for theory confirmation, it can also be used to suggest where relationships might or might not exist and to suggest propositions for later testing (Chin and Newsted 1999). Chin and Newsted (1999, p. 337) mentioned that PLS method is congruent with a large percentage of research where:

- The objective is prediction, and/or
- The phenomenon in question is relatively new or changing and the theoretical model or measures are not well formed, and/or

- The model is relatively complex with large numbers of indicators and/or
- There is an epistemic need to model the relationship between latent variables and indicators in different modes (i.e., formative and reflective measures) and/or
- The data conditions relating to normal distributions, independence, and/or sample size are not met.

Referring to the nature of this study and its research questions, all these assumptions are verified in our research problem. Therefore, we consider PLS the adequate method to establish the relationship between ICT, innovation, and cybersecurity on one hand and growth competitiveness on the other.

To reflect on the above, this study will use PLS analysis for assessing the proposed interaction effects among ICT, innovation, and cybersecurity as well as the moderation effects of the human capital factor and the cyber threats in the relationships between the triad factors and growth competitiveness. It will also be applied to handle the formative measure of the cybersecurity initiatives. As a matter of fact, the following steps will be applied in the analysis. Step 1 will test the basic model depicting the relationships among ICT, innovation, and growth competitiveness, as shown in Figure 12a.

Following this, the model will be extended to incorporate the cybersecurity formative measure as depicted in Figure 12b. The moderation effect of both the human capital factor and the cyber threats (Figure 12c) will be tested in the third stage.

Figure 12a Basic Model

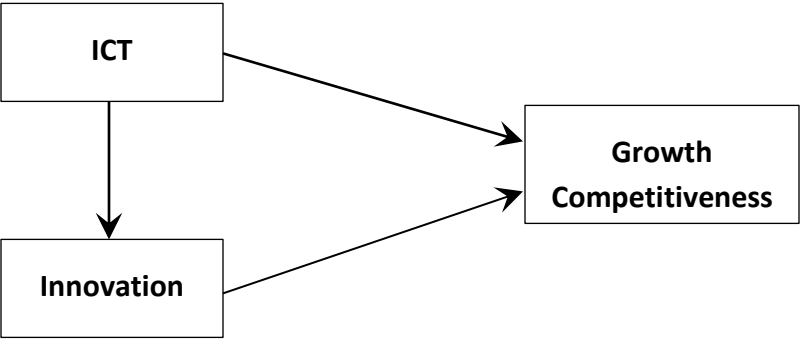


Figure 12b Model with the cybersecurity formative measure

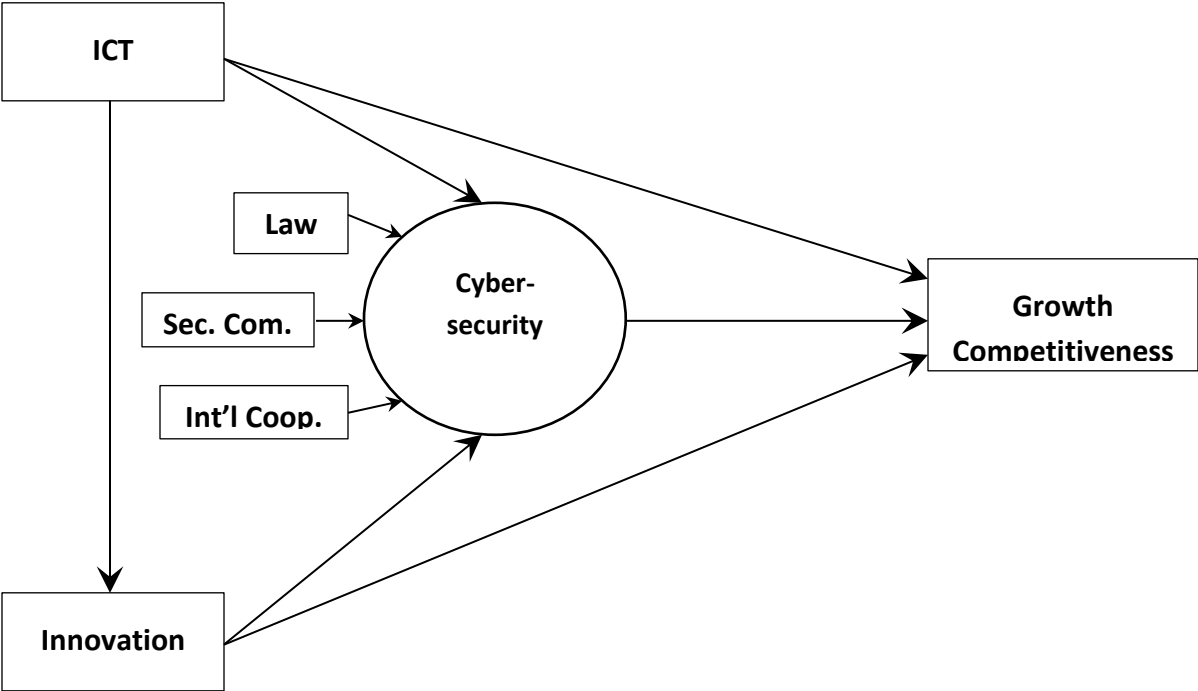
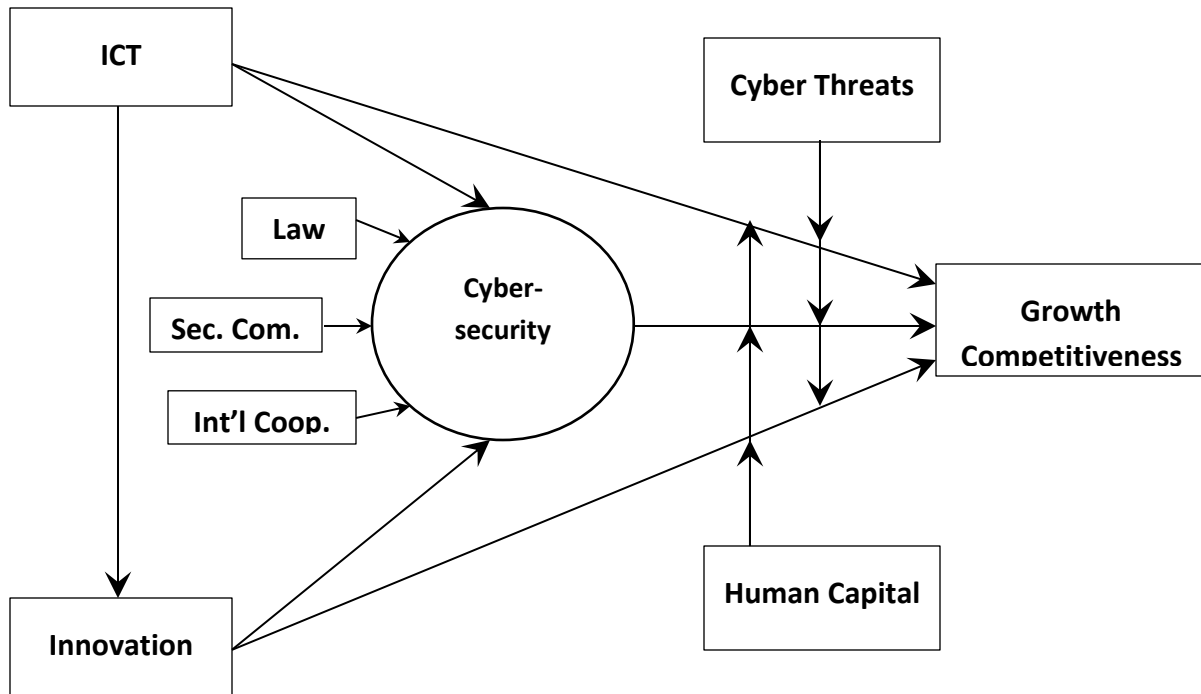


Figure 12c Complete Model



Multi-Group Analysis

This technique will be applied to examine the relationships stated in the above hypotheses across various economy and region groups. The same assumptions and sample size requirement mentioned about PLS apply here.

This, of course, will provide an assessment of the hypotheses stated in this chapter, and will help in finding answers to the research questions addressed by this study. This is what Chapter IV will present and discuss in detail.

CHAPTER IV

FINDINGS, ANALYSIS, AND DISCUSSION

Based on its purpose and motivation as outlined in Chapter I, this study has two core objectives. The first objective is to determine whether or not the ICT, national innovation, and cybersecurity variables are significant predictors of growth competitiveness across countries. As explicitly discussed in Chapter II, while the body of literature discusses extensively the relationships between ICT and innovation on one hand and economic performance on the other, assessing these relationships with the cybersecurity measure taken into consideration within the economic growth model is, to the best of our knowledge, lacking in the literature. The second objective is to formulate a variable that would represent, with adequate theoretical support and methodological robustness, the cybersecurity measure. Therefore, it is essential to choose a data analytical approach that is most appropriate for the given study. The chosen statistical technique should help ensure that results portray the phenomenon of interest as closely as possible, which, in this case, is twofold: to evaluate the constituents of the cybersecurity measure and the impact that this new measure might have on the economic growth or growth competitiveness model.

Chapter III provided an explanation of the chosen statistical technique. This chapter will elaborate more on the analytical approach adopted in this study, as well as present the results and findings of the various data analyses conducted. It will also discuss the results in terms of the study hypotheses and pertinent literature.

Analytical Approach: Triangulation-Based

As explained in Chapter III, the analytical approach followed in this study is based on the use of a variety of statistical tools that would address and attempt to find answers for the study's research questions. In other words, the study adopts the triangulation strategy. Triangulation has been long perceived as a good research practice through which a researcher uses multiple data sources, theories, and methods to enhance the validity of research findings (Mathison, 1988) or to extend or challenge existing findings (Turner & Turner, 2009). Although Campbell and Fiske (1959) introduced the concept in the form of multiple methods, Webb et al. (1966) gave it its name, and Denzin (1978) clearly explained how it can be used and outlined its types, including:

1. Data triangulation, referring to the use of various data sources;
2. Methodological triangulation, which refers to using various research designs or data collection methods (Goodwin & Goodwin, 1984), using a paradigmatic connection, such as qualitative and quantitative methods in data collection and analysis, as well as interpretation of results (Greene & Caracelli, 1997; Barbour, 1998);
3. Investigator triangulation, where multiple experts in the phenomenon of interest get directly involved in the conduct of data collection and analysis efforts. This most probably results in higher reliability levels in data collection (Denzin, 1970); and
4. Theoretical triangulation, which involves the use of several theoretical perspectives and/or multiple working hypotheses (Chamberlin, 1965). The alternative perspectives are theoretically different yet related enough to be considered together and tested using the same dataset. This allows for various theories' testing (Boyd, 2000), decreasing alternative explanation for the phenomenon under study (Mitchell, 1986), and for providing a more profound analysis of findings (Banik, 1993).

In addition to the four types (Denzin, 1970) mentioned above, a fifth type, namely analysis triangulation, was suggested by Kimchi et al. (1991). Data analysis triangulation deploys more than one approach to the analysis of the study data set. This usually involves the employment of different statistical techniques and statistical testing methods for the purpose of determining similarities and validating data (Kimchi et al., 1991). The main task in analyzing findings using data analysis triangulation is to determine whether there is convergence in results (Waltz et al., 2010). If convergence is met, more confidence can be placed in the findings, implying that there is a higher probability that they are the result of the data traits rather than the method variance (Waltz et al., 2010). However, if divergence occurs, then this may prompt an inquiry regarding the methods deployed (Bryman, 2004), the fulfillment of the assumptions of the statistical techniques or tests used, or the model proposed. Nevertheless, it should be emphasized that divergent results may enhance the understanding or explanation of the research problem (Jick, 1979).

In the IS field, triangulation has been deployed by several researchers (e.g., Ammenwerth et al., 1987; Myers, 1997; Tao & Grosky, 1999; Benbasat et al., 1987; and Walczak, 2012). In this study, two of the above -mentioned types of triangulation are applied: the theoretical triangulation and the data-analysis triangulation. The multiple theories used in this study have been elaborately discussed in Chapters II and III. The theories – economic growth, complementarity, national security, and international relations – are vastly different and belong to different disciplines, yet they are related when one considers the factors that are most likely to be associated with growth and competitiveness at the national level. Accordingly, this triangulation theory allowed for several hypotheses to be postulated, thus making it possible to study country-level economic growth from various perspectives.

As for the data-analysis triangulation method adopted in this study, it manifests itself in the variety of statistical techniques and tests used to examine the phenomenon of interest, namely the relationship between ICT, innovation, cybersecurity, and growth competitiveness, as well as the role that human capital and cyber threats may play in these relationships. Triangulation applied in this study, as is often the case, is aimed not only at validation, but also at broadening and deepening one's understanding about the phenomenon being studied (Olsen, 2004; Thurmond, 2001).

With this in mind, this study deploys parametric and nonparametric tests in order to analyze the data used, test the hypotheses, and assess the proposed model and relationships. The tests to be specifically used are: the rank correlation methods (non-parametric), ordinary least squares regression (parametric), and partial least squares (PLS) modeling (parametric). Below is a brief description of the three methods that can help in better reading and analyzing the data analysis results.

Ordinary Least Squares (OLS) Regression

OLS is a statistical method of inference used to assess the causality effect that an independent variable or a collection of variables or a collection of variables (X_i) may have on a dependent variable (Y). It can be represented as: (Hair et al., 2006)

$$Y = B_0 + B_1X_1 + \dots \dots \dots \varepsilon$$

Where:

B_0 = the intercept, the baseline level, the value of Y if $B_1 = 0$

B_1 = an OLS estimate; the coefficient of X_1 ; it represents the change in Y relative to one unit change in X_1 , and the possible causal effect that X_1 may have on Y .

ε = the residual, it is the difference between predicted and actual Y and has a mean value of zero and a variance σ^2 .

OLS is a method whereby the parameters B_i of the model are estimated. It is a linear model whereby a line is fitted to data. This is designed to build the best fit, where the best fit implies a minimization of the sum of squared errors (Hair et al., 2006). In other words, OLS minimizes $\sum \hat{\epsilon}^2$. As with other modeling techniques, when regression analysis is deployed, the main concern would be to assess the overall fit of the model. In general, a regression model is of good fit when it results in predicted values that are close to the observed data values (Hair et al., 2006).

If the predictor variables were not explanatory of the variance in the dependent variable, then the mean model, which uses the mean for each and every predicted value, would generally be used. So, the fit of a proposed model is assessed through comparing it to the fit of the mean model.

In OLS, three statistics are used to assess a model fit: R^2 and adjusted R^2 , the F-test and the Root Mean Square Error (RMSE) (Grace-Martin, 2012). These three tests are all based on Sum of Squares Total (SST) and Sum of Squares Error (SSE). The former measures the distance between the data and the mean; whereas the latter measures the distance between the data and the predicted values.

To start with, R^2 (coefficient of determination) shows the proportional improvement in prediction from the regression model¹⁰, as compared to the mean model, and thus indicates the goodness-of-fit of the model. However, since R^2 tends to increase as the number of predictors increase in number, the adjusted R^2 could be a better reflection of the goodness-of-fit as it incorporates the regression model's degrees of freedom. Based on this, adjusted R^2 will increase as predictors are added to the model only if the new variable improves the model (Montgomery and Morrison, 1973). As for the F-test, it evaluates the null hypothesis: (Hair et al., 2006)

¹⁰ The difference between SST and SSE measures the improvement in prediction from the regression model in comparison with the mean model. Dividing this difference by SST yields R^2 (Grace-Martin, 2012), i.e. the proportional improvement in the regression model prediction.

$H_0: \beta_i = 0$ versus the alternative hypothesis,

H_1 : At least one β is not = 0.

A significant F-test indicates that R^2 is reliable. This F-test determines whether the model relating the predictor variables to the dependent variable is statistically reliable (Grace-Martin, 2012). Finally, the RMSE is the square root of the residuals variance, and it indicates the extent to which the observed data points are close to the model's predicated values. This test can be interpreted as the standard deviation of the residuals, that is, the unexplained variance. RMSE is considered the most important criterion for fit, with lower values indicating a better fit (Hair et al., 2006; Simpson et al., 2001).

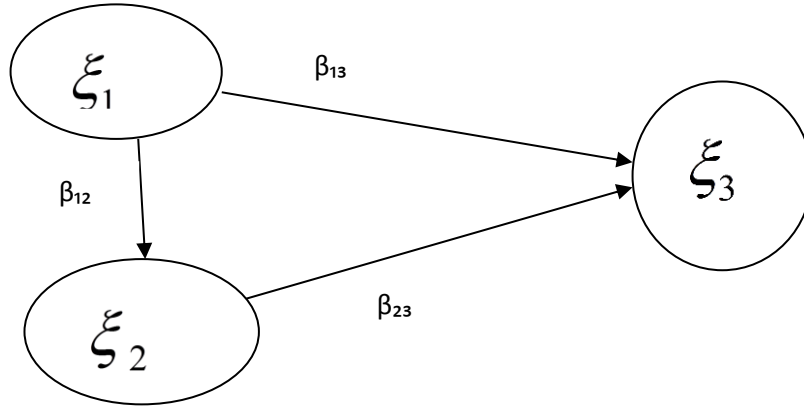
Partial Least Squares – Path Modeling

PLS Path Modeling (PLS – PM), a component-based estimation method (Tenenhaus, 2008), is an iterative algorithm that estimates the model in two steps. It first solves out the various blocks of the measurement model, and then, it estimates the path coefficients of the structural model (Vinzi et al., 2010). It is more an exploratory than a confirmatory approach that is intended to explain most creditably the residual variance of the latent variables in the model's regression runs (Fornell & Bookstein, 1982). Unlike covariance-based SEM, PLS-PM does not reproduce the sample covariance matrix (Vinzi et al., 2010).

In PLS-PM, hypothesis testing procedures are based on resampling methods, such as jackknifing and bootstrapping¹¹ (Tenenhaus et al., 2005; Chin, 1998). Moreover, PLS-PM

¹¹ Jackknifing (Quenouille, 1956) and bootstrapping (Efron, 1979) approaches are iterative procedures, requiring massive numbers of calculations. The attractiveness of jackknifing and bootstrapping lies in providing researchers with an important type of information, namely, estimates of dispersion for statistics of unknown or poorly known distribution. As put by Lanyon (1987), in bootstrapping, the original data set is randomly sampled with replacement to produce "pseudo-replicate" data sets. Since it is 'with replacement', each pseudo-replicate consists of the same number of elements as the original data set but may not include all the original elements (some elements may appear more than once, others not at all). This resampling may be repeated several times (thousands or millions), and each iteration produces a new pseudo-replicate from which statistics may be calculated. In jackknifing, however, a limited number of pseudo-replicate data sets will be produced, each of which contains all of the original data elements except for one. For

emphasizes more predictions optimization, i.e. explained variance, rather than the estimates' statistical accuracy (Vinzi et al., 2010). In PLS-PM, a simple model could be visualized as shown below.



In such model, the structural relations could be represented by the following equations:

$$\xi_2 = \beta_{02} + \beta_{12}\xi_1 + \zeta_2$$

$$\xi_3 = \beta_{03} + \beta_{13}\xi_1 + \beta_{23}\xi_2 + \zeta_3$$

Where β_{0j} ($j=2,3$) is the intercept or the constant term, and β_{ij} ($i=1,2$ and $j=2,3$) is the path coefficient linking latent variable i to the endogenous latent j , and ζ_j represents the error term related to each endogenous latent variable in the model. Based on this, the null and alternative hypotheses related to the PLS-PM model are:

$$H_0: \beta_{12} = \beta_{13} = \beta_{23} = 0$$

$$H_1: \text{At least one } \beta_{ij} \neq 0$$

example, for a data set with 20 elements, 20 pseudo-replicate data sets will be generated, each lacking a different data element. Jackknifing requires far less iterations, thus, it is thought of as a means of approximating bootstrapping (Efron, 1979).

PLS is usually preferred over CBSEM (covariance-based SEM) for several reasons: predictive accuracy, explanation of complex relationships, small sample-size requirements, and lack of need for the assumption of multivariate normality. In this study, it is basically preferred over other methods mainly because of the major aim of building a formative measure for cybersecurity for predicting national cybersecurity levels as well as predicting growth competitiveness levels based on ICT, national innovation, and cybersecurity scores. In fact, it is believed that for analyzing complex relationships and for prediction, PLS is the preferred method (Sambamurthy & Chin, 1994). Multivariate normality is not a requirement for estimating PLS parameters (Barclay et al. 1995), though it is fulfilled in this study. Moreover, PLS is more flexible regarding small sample sizes, though the effect size estimation and the power analysis presented in Chapter III have clearly shown that the sample size used in the study is adequate. In addition, covariance-based SEM software tools, such as AMOS, for example, tests the a priori specified model against population estimates derived from the sample and their main objective is theory testing (Gefen et al., 2000). On the other hand, PLS is intended to explain variance; i.e., “to examine the significance of the relationships and their resulting R^2 , or sample coefficient of determination, as in the case of linear regression” (Gefen et al., 2000, p. 27). PLS is used both for predictive applications and theory building (Chin, 2010; Chin, 1998). In summary, PLS was selected for this study since the emphasis is on theory building by extending the theory of economic growth, and also because of the requirement for a formative construct measure to be developed.

Furthermore, the PLS method has been used by an increasing number of researchers from various fields including organizational behavior (e.g., Higgins et al., 1992), strategic management (e.g., Hulland, 1999), marketing and consumer behavior (e.g., Reinartz et al., 2004 and Fornell & Robinson, 1983). The IS field in this respect has not been an exception. PLS has also been widely

used in IS research (Wasko and Faraj, 2005; Dibbern et al., 2004; Pavlou & Chai, 2002; and Agarwal & Karahanna, 2000). In this study, SmartPLS version 2.0 is used for data analysis and for testing the hypotheses presented in chapter III.

Having decided on using PLS, the data will be analyzed using measurement and structural models as described by Chin (2010). PLS is a statistical technique that uses a combination of principal components analysis, path analysis, and regression to simultaneously evaluate theory and data (Pedhazur, 1997, 1982). PLS estimates parameters for the links between manifest variables with their respective constructs (loadings) and also estimates the links between different constructs (i.e. path coefficients). The loadings can be identified as factor loadings, whereas the path coefficients are standardized regression coefficients. The sign, size, and statistical significance of the path coefficients between constructs in the model can be examined to test the explanatory power of the model (Pedhazur & Schmelkin, 1991).

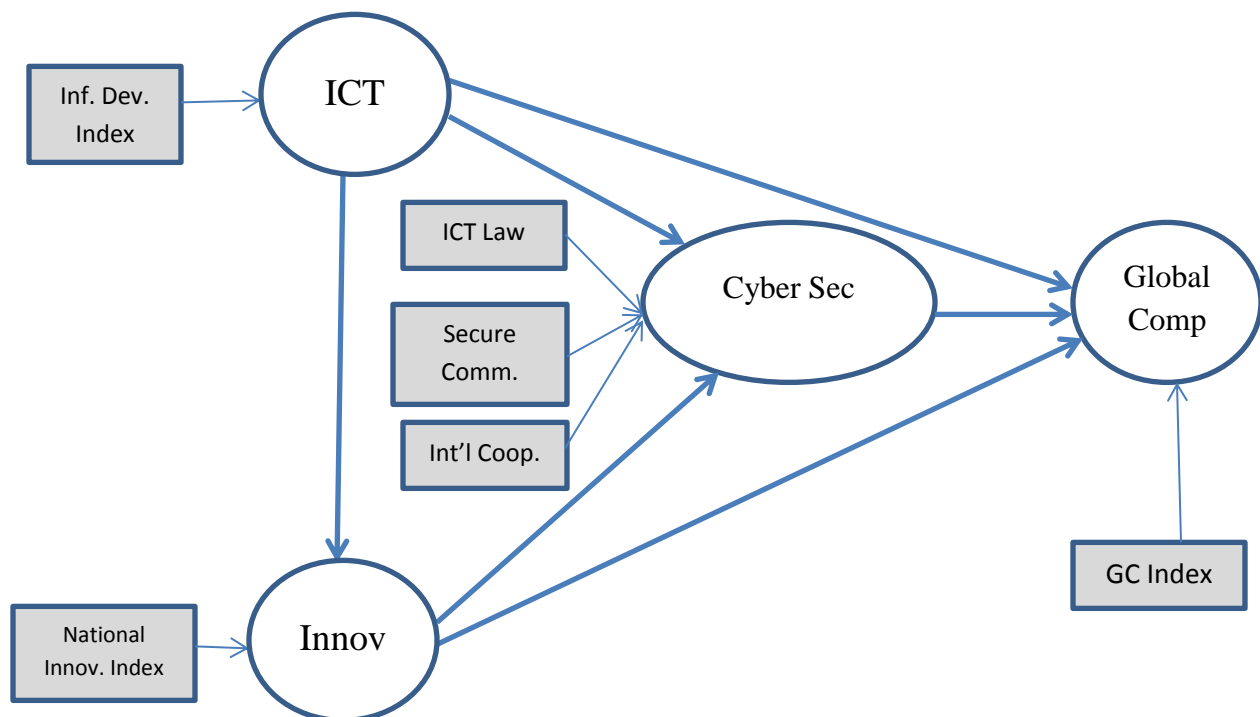
Regarding the model fit, contrary to CBSEM, PLS path modeling does not report any kind of fit indices like RFI, RMSEA or CFI. So, it naturally lacks an index that can provide the user with a global model validation (Tenenhaus et al., 2005). In PLS, the overall model fit is assessed via strong loadings, significant weights, multiple R^2 , substantial/significant structural paths (Chin, 1998), communality index, redundancy index, and goodness-of-fit (GoF) (Amato et al., 2004).

As for the communality index, it measures the quality of the measurement model for each block of manifest variables (MVs) – i.e. the relationship between the manifest variables and the corresponding latent variable (LV). Taking the measurement model into consideration, the redundancy index measures the quality of the structural model for each endogenous block (Tenenhaus et al., 2005). The cross-validated communality (cv-communality) is a kind of cross-validated R^2 between the block MVs and their own LVs, computed by a blindfolding procedure.

This is used to measure the quality of the measurement model for each block. Using the blindfolding process too, the quality of each structural relation (equation) is measured by the cv-redundancy index (i.e. Stone–Geisser’s Q^2). Stone Geisser’s Q^2 is a kind of cross-validated R^2 between the MVs of an endogenous LV and all the MVs associated with the LVs explaining the endogenous LV, using the estimated structural model (Tenenhaus et al., 2005). This index is used for measuring the quality of the path model. The threshold value for Q^2 is zero (Fornell & Cha, 1994), and according to Chin (2010), if Q^2 is greater than 0.5 ($Q^2 > 0.5$), then the model has a predictive fit (Chin, 2010).

In this study, the measurement model consists of formative LV constructs, with ICT, innovation, and growth competitiveness each having one MV, and cybersecurity having three MVs. As for the structural model, it consists of the relationships amongst the latent variables. The model’s latent and associated manifest variables are shown in Figure 13.

Figure 13 Model’s Latent and Manifest Variables



The above figure shows four latent formative variables, three of which- ICT, national innovation, and growth competitiveness, are each a composite of one manifest variable, namely the composite index that it represents. The cybersecurity measure is a formative measure with three manifest variables: ICT law enforcement, secure communication infrastructure, as well as the international cooperation agreements at the level of co-authorship and joint research efforts.

Non-Parametric Methods

The rapid and continuous development of non-parametric statistical procedures is due to several advantages enjoyed by non-parametric techniques (Kendall & Gibbons, 1990). The advantage pertinent to our study is related to a characteristic mentioned by Hollander and Wolfe (1999) that non-parametric procedures are applicable in many situations where ranks, rather than magnitudes, are analyzed.

In practice, ranked material can originate in different forms. These include, but are not limited to the representation of some measurable or countable quality that is capable of practical measurement (Kendall & Gibbons, 1990). An example could be ranking countries, as is the case with the international data set used in this study. The attribute could be population size, gross domestic product (GDP), or laws affecting business. Rank analysis has been recognized as having an importance of its own that may allow it to substitute variate analysis in certain cases (Perry & Lederman, 1999; Kendall & Gibbons, 1990).

This study will deploy three kinds of non-parametric rank correlation methods. First, it will use Kendall's W to assess the inter-rater reliability. Second, it will use Kendall's coefficient of concordance to assess the overall agreement amongst the different rankings across countries. Finally, Wilcoxon's test of matched-pairs will be used to assess the level of convergence or divergence across pairs of ranks pertinent to countries' examined factors.

The following sections provide a detailed description of the data analysis methods used. First, a description of our sample countries will be presented using a variety of descriptive statistics. After that, the results of the structural and measurement models using PLS will be presented. Drawing on the triangulation approach adopted in this study for data analysis, the PLS results will be compared to those of Ordinal Least Squares (OLS) analysis as well as, where applicable, the results of non-parametric rank analysis methods. Finally, an analysis and discussion of the results will be presented.

Reading the Countries' Characteristics: Descriptive Statistics

To describe and summarize data, and to grasp the essence of variables used, descriptive statistics are deployed. Besides the analysis used in Chapter III to understand the distribution shape and identify outliers, descriptive statistics applied here will help in understanding the central tendency and dispersion of the data measuring the variables included in the study. The variable names and their representation in SPSS and SmartPLS are listed in Table 16 below.

Table 16 Variable Names and Representation in SPSS and SmartPLS

Variable Name	SPSS/ SmartPLS Representation
ICT Development Index (BV) ^a	IDI
National Innovation (BV)	GII
Growth Competitiveness (BV)	GC
Human Dev. (Knowledge Economy Index) (MV) ^b	HD
Industrial Security Incidents (MV)	CybThrt
ICT Law Enforcement (CCI) ^c	ICTLaws
International Cooperation (CCI)	Intlcoop
Secure Communication Infrastructure (CCI)	SecureCom

^a. BV = Basic Variable

^b. MV = Potentially Moderator Variable

^c. CCI = Possible Cybersecurity Construct Indicator

The above categorizations are based on the model discussion and variable categorization as portrayed in Chapter III.

Prior to descriptive statistics, the data set was further scanned for missing data. This step had to be taken after introducing the human capital KEI factor. Eight cases contained missing data: three cases with one item missing, two cases with two items missing, and three cases with three items missing. Little's MCAR test (Table 17) revealed that the missing data were missing completely at random (MCAR).

Table 17 Little's MCAR Test

IDI	GII	GC	ICTLaws	HD	IntlCoop	SecureCom
4.382511	3.1900070	4.234383	3.980	5.225213	.718331	256.174508

a. Little's MCAR test: Chi-Square = 162.379, DF = 160, Sig. = .433

As could be noticed in Table 17, the Little MCAR test reveals a chi-square value of 162.379 and a p-value of 0.433. This implies that the null hypothesis of the test stating that the missing data were missing at random cannot be rejected. When the missing data is MCAR, any imputation method can be used (Hair et al., 1998). For this study data, the use of the expectation–maximization (EM) method in SPSS was preferred. The EM approach is an iterative two-stage process where the E-stage makes the best estimates of the missing data and the M-stage makes parameter estimates assuming the missing data are replaced (Hair et al., 1998). This process resulted in a complete data set of 136 countries or cases. Making sure that the little issue of missing data has been solved, the question pertinent to the characteristics of the data set can now be addressed. Table 18 presents the distribution of countries according to income class. Based on the income group categorization provided by the World Bank (2013), a country may belong to the low income group, lower middle, upper middle, high income, or high income OECD group.

Table 18 Distribution of Countries by Income group

Income Group	Frequency	Percent	Valid Percent	Cumulative Percent
Low Income	19	14.0	14.0	14.0
Lower Middle Income	33	24.3	24.3	38.2
Upper Middle Income	41	30.1	30.1	68.4
High Income	14	10.3	10.3	78.7
High Income OECD	29	21.3	21.3	100.0
Total	136	100.0	100.0	

In the countries' data list used in this study, the high income group (OECD and non-OECD) represents the group with the highest percentage of occurrence (31.3%), followed by the upper middle income group (30.1%), lower middle income group (24.3%), and finally the low income group (14%). A similar distribution could be traced for the distribution of countries according to the human development class according to UNDP (2011), with human development indicating education, health, and standard of living. This is shown in Table 19.

Table 19 Distribution of Countries by Human Development Level

Human Development Level	Frequency	Percent	Valid Percent	Cumulative Percent
Low	25	18.4	18.4	18.4
Moderate	32	23.5	23.5	41.9
High	34	25.0	25.0	66.9
Very High	45	33.1	33.1	100.0
Total	136	100.0	100.0	

As one can read from Table 19, the data set used in the study includes 33.1% of countries with very high human development level, 25% with high human development, 23.5% with moderate human development, and 18.4% with low human development.

With this in mind, the second step here is to have a description of the various country-level factors used in this study, namely: ICT, national innovation, growth competitiveness, human capital (knowledge economy), secure communication infrastructure, international cooperation, ICT law enforcement, and cyber threats. This will be done using measures of shape, central tendency, and dispersion.

To start with, Figure 14 and Table 20 show the distributions of these variables, along with the Kolmogorov-Smirnov (K-S) test for normality. As the graphs in Figure 14 clearly reveal, the distributions of all the basic variables in this study are normally distributed, with skewness coefficients $S_k < 1$. These results are supported by the results of the non-parametric test of normality, namely the Kolmogorov-Smirnov (K-S) test, which turned out to be not significant, thus confirming the ICT, innovation, and growth competitiveness normal distribution.

As for the human capital and cyber threat variables, which the study intends to test their moderation effect on the model, they show different distributions. The human capital reveals a normal distribution with a low skewness coefficient and a non-significant K-S test. However, the ‘cyber threats’ variable has a moderate positive skewness and a significant K-S test, implying that this ‘possible’ moderating variable does not have a normal distribution. Based on this, a log transformation was applied, and the resulting values of the transformed variable with the name ‘CybthrtTrans’ revealed a normal distribution. The same procedure was applied to test the normality of the variables intended to be examined as possible indicators for the cybersecurity construct.

Figure 14 Histograms of Basic and Potentially Moderating Variables

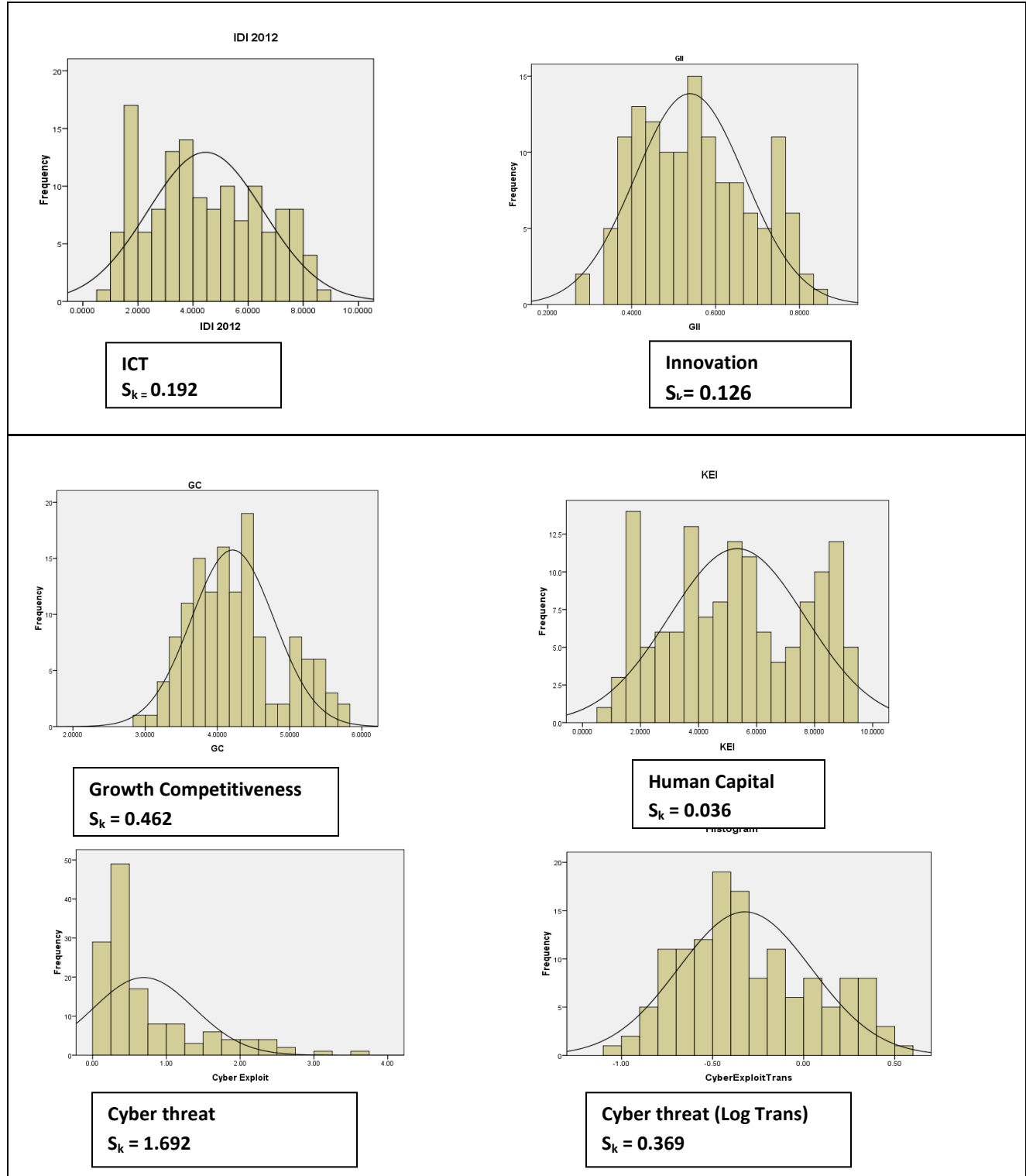


Table 20 One-Sample Kolmogorov-Smirnov Test

	IDI	GII	GC	HD	Cybthrt	CybthrtTrans
Kolmogorov-Smirnov Z	.833	.716	.963	0.992	2.475	1.073
Asymp. Sig. (2-tailed)	.491	.684	.312	0.279	0.000	0.200

As reported in Chapter III, the ‘ICT law enforcement’ variable showed a normal distribution ($S_k = 0.124$; K-S = 0.912 and p-value = 0.377). However, the variables ‘international cooperation’ ($S_k = 5.661$; K-S = 4.220 and p-value = 0.000) and ‘secure communication infrastructure’ ($S_k = 2.402$; K-S = 3.933 and p-value = 0.000) were far from normal distribution. Again here, log transformation was applied, and the transformed variables ‘IntlCoopTrans’ ($S_k = 0.135$; K-S = 0.830 and p-level=0.497)) and ‘SecurityTrans’ ($S_k = -0.011$; K-S = 0.616 and p-level = 0.842) showed normal distribution.

Coming to the measures of central tendency, the two basic measures used herein are the mean and the median. As for the measures of dispersion which refer to the spread of scores around the mean or to the variation in the data set, they are at least as equally important as the central tendency measured, and should be well considered (Tulman & Jacobsen, 1989). Table 21 shows the central tendency and dispersion measures as applied to the variables mentioned above.

The statistics pertinent to central tendency – the mean and the median – of the various measures depicted above can help provide guidance regarding how to address the disparities in national ICT, innovation, competitiveness, and the other important pillars of an economy at the regional or the country levels.

Table 21 Descriptive Statistics

	IDI	GII	GC	HD	CyberExploits	ICTLaws	IntlCoop	SecureCom
N Valid	136	136	136	136	136	136	136	136
Missing	0	0	0	0	0	0	0	0
Mean	4.407380	3.206380	4.242911	5.252751	0.7386	261.561516	3.994	1.707981
Median	4.285000	2.990000	4.165000	5.140000	0.4275	19.864000	3.900	.032700
Std. Deviation	2.0659193	1.1652137	.6424768	2.426830	0.70032	522.1102663	.9694	4.8301551
Range	7.6200	5.5400	2.7500	8.9287	3.50	2529.9470	4.0	42.9463
Minimum	.9400	1.3100	2.9700	0.5013	0.09	.0000	1.9	.0001
Maximum	8.5600	6.8500	5.7200	9.4300	3.59	2529.9470	5.9	42.9464

The median represents the 50th percentile of the distribution, and thus indicates that 50% of the countries included in the data set have ICT, innovation, and growth competitiveness scores higher than 4.285, 2.99, and 4.165 respectively, and 50% have lower scores. The same applies to the other variables. Regarding the ICT laws, one shouldn't be surprised that the mean is larger than the median because the distribution appears to be a bit skewed to the right. Since the mean averages all the values in the data set, it is pulled toward the higher ones (Plichta et al., 2013). As far as the dispersion is concerned, one can find that of all the variables mentioned above, ICT laws and secure communication lines have high dispersion levels as presented by the standard deviation statistic. This indicates high variability in using such security measures across the various countries.

While the general descriptive statistics are informative regarding the various factors included in the study, examining these statistics across the various country groups would provide a better platform for comparison and assessment. The distribution of each of the variables across the various income groups is depicted in Table 22.

Table 22 Descriptive Statistics across Country Income Groups

		Country Factors				
Income Group		ICT	GII	GC	KEI	CyberSec ^a
Low	Mean	2.0425	2.1501	3.6237	2.2284	0.3781
	StdDev	1.6537	0.6472	0.4582	1.5378	0.7179
Lower Mid	Mean	2.8833	2.5200	3.7964	3.4369	0.6315
	StdDev	0.8791	0.5793	0.3245	1.0555	0.4709
Upper Mid	Mean	4.2924	2.9485	4.1891	5.2284	1.2739
	StdDev	1.0636	0.6888	0.3372	1.2563	0.5449
High	Mean	5.9972	3.8357	4.8050	7.0263	1.8769
	StdDev	1.0421	0.9261	0.5353	1.1365	0.6212
High OECD	Mean	7.0862	4.7396	4.9614	8.4786	2.5891
	StdDev	0.7536	0.8806	0.4974	0.5513	0.3392

a. The cybersecurity measure here assumes equal weights for ‘secure communication lines’, ‘ICT laws’, and ‘international cooperation’.

The figures reported in Table 22 indicate an interesting result. The means and spreads are quite different for all the mentioned factors, with the means within the two ‘high-income groups’ being more than twice that within the ‘low-income group’. At the same time, the variability becomes higher as one moves from the higher-income to the lower-income groups. This suggests that the relationships proposed in Chapter III may be influenced by the country development level or income group.

The Relationship between ICT, Innovation, and Growth Competitiveness

The relationship between ICT, national innovation, and growth competitiveness represents the basic relationship in this study. It is the relationship that the Economic Growth model (Romer, 1990) is based upon. To study this relationship, various parametric and non-parametric tools were used.

Non-Parametric Tests

The non-parametric types of analyses used in the study are mainly the rank correlation methods that make use of the rank orders rather than the variates of the dataset (Kendall & Gibbons, 1990). To this effect, the study deploys Kendall’s W, the coefficient of concordance. In practice,

ranked material can originate in different forms. These include, but are not limited to the representation of some measurable or countable quality that is capable of practical measurement (Kendall and Gibbons, 1990). An example could be ranking countries, as is the case with the international data set used in this study. The attribute could be population size, gross domestic product (GDP), or laws affecting business. Rank analysis has been recognized as having an importance of its own that may allow it to substitute variate analysis in certain cases (Perry & Lederman, 1999; Kendall & Gibbons, 1990).

The first non-parametric test applied here is the rank correlation test. To assess the correlation between the ranks of ICT, innovation, and growth competitiveness, Kendall-tau-b is used. The results are reported in Table 23, and they show a significant level of rank agreement across the ranks of these variables.

The correlations across the ranks of these variables are significant and remarkably strong. The correlations are also positive, indicating that higher ranks of one variable are accompanied with higher ranks in the other variables. However, agreement across ranks does not reflect concordance, where concordance refers to the agreement in positive differences in ranks (Sheskin, 1997). In other words, $Y_j - Y_i$ is associated with a similar direction in $X_j - X_i$. To test the level of concordance amongst the ranks of the three basic variables ICT, innovation, and growth competitiveness, Kendall's W test for concordance was used. The results of Kendall's W (the coefficient of concordance) are reported in Table 24.

Table 23 Kendall Tau-b Correlations

			IDIRank	GIIRank	GCRank
Kendall's tau_b	IDIRank	Correlation Coefficient	1.000	.685**	.654**
		Sig. (2-tailed)	.	.000	.000
		N	116	116	116
	GIIRank	Correlation Coefficient	.685**	1.000	.593**
		Sig. (2-tailed)	.000	.	.000
		N	116	116	116
	GCRank	Correlation Coefficient	.654**	.593**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	116	116	116

Table 24 ICT, Innovation, and Growth Competitiveness: Coefficient of Concordance

N	116
Kendall's W ^a	.371
Chi-Square	86.086
df	2
Asymp. Sig.	.000

a. Kendall's Coefficient of Concordance

In this test, Kendall's W is equal to 0.37, implying a moderate level of concordance, with a p-value of 0.000. This indicates that the null hypothesis that there is a lack of concordance among the rank orders could be rejected. At the same time, Wilcoxon test was done to check for rank agreement between matched pairs. The findings reported in Table 25 supported the results of Kendall's W showing agreement between matched pairs of variable ranks.

Table 25 Wilcoxon Test of Matched Pairs

Matched Pairs	Wilcoxon Test (Z statistic)	Significance	Decision
ICT-Innovation	-0.121	0.904	Fail to Reject H_0
ICT-GrowthComp (GC)	-0.105	0.917	Fail to Reject H_0
Innovation-GC	-0.250	0.803	Fail to Reject H_0

The above results indicate a high level of concordance across the ranks of the various variables. Wilcoxon test of matched pairs showed p-values that are far greater than 0.05, implying that the null hypothesis that matched pairs of rank orders are concordant cannot be rejected. Looking into more detail provided by Wilcoxon test for related samples, as shown in Table 26, one can derive more detailed information about the ranked scores (Field, 2009). The table gives the number of negative ranks (the ranks for which ICT scores are higher than those of GII, i.e. innovation, ranks), the number of positive ranks (the ranks for which GII scores are higher than those of ICT), and the number of ties (where the ICT rank is equal to the GII rank).

In Wilcoxon signed rank test, the z-score is based on the lowest mean of the two ranks, and allows exact calculation of significance values based on normal distribution. The table above shows that the z-statistic is based on negative ranks, that the z-score is -0.121, and that this value is far from significance at $P=0.904$. Therefore, although the value is based on negative ranks, meaning that countries with high ICT ranks may have lower innovation ranks, yet this is not significant. This implies that, in general, one can assume an agreement between ICT rank and innovation rank. A similar interpretation of results could be drawn for the rest of ranked variables. Table 27 summarizes the results of the Wilcoxon signed rank test for the remaining matched pairs pertinent to the three core variables: ICT, innovation, and growth competitiveness.

Table 26 Wilcoxon Signed Ranks Test: Innovation-ICT

Innovation and ICT Ranks			
		N	Mean Rank
GIIRank - IDIRank	Negative Ranks	68 ^a	63.84
	Positive Ranks	64 ^b	69.36
	Ties	4 ^c	
a. GIIRank < IDIRank			
b. GIIRank > IDIRank			
c. GIIRank = IDIRank			

Statistics ^a	
	GIIRank - IDIRank
Z	-.121 ^a
Asymp. Sig. (2-tailed)	.904
a. Based on negative ranks.	
b. Wilcoxon Signed Ranks Test	

Table 27 Wilcoxon Signed Ranks Test: Innovation-ICT-Growth Competitiveness

ICT and Growth Competitiveness Ranks			
		N	Mean Rank
GCRank - IDIRank	Negative Ranks	66 ^a	66.86
	Positive Ranks	67 ^b	67.14
	Ties	3 ^c	
a. GCRank < IDIRank			
b. GCRank > IDIRank			
c. GCRank = IDIRank			

Test Statistics ^b	
	GCRank - IDIRank
Z	-.105 ^a
Asymp. Sig. (2-tailed)	.917
a. Based on negative ranks.	
b. Wilcoxon Signed Ranks Test	

Innovation and Growth Competitiveness Ranks			
		N	Mean Rank
GCRank - GIIRank	Negative Ranks	65 ^a	65.96
	Positive Ranks	67 ^b	67.02
	Ties	4 ^c	
a. GCRank < GIIRank			
b. GCRank > GIIRank			
c. GCRank = GIIRank			

Test Statistics ^b	
	GCRank - GIIRank
Z	-.250 ^a
Asymp. Sig. (2-tailed)	.803
a. Based on negative ranks.	
b. Wilcoxon Signed Ranks Test	

The above results show that the z-scores of the two Wilcoxon signed rank tests are based on negative ranks. For the ICT and growth competitiveness ranks, this implies that countries with high ICT ranks do not necessarily have high growth competitiveness ranks. Still, however, this is not significant. Similarly, countries with high innovation ranks may not have high growth competitiveness, but again, this is not significant. The above results imply that there is an overall agreement across the ranks of the basic model variables. Nevertheless since Wilcoxon signed rank test presents precise calculation of significance values, it is useful to analyze the results above based on the significance values presented for each matched pair of variables. With respect to their agreement with growth competitiveness ranks, the above results show that there is more agreement between the ICT and growth competitiveness ranks than there is between innovation and growth competitiveness. This may draw attention to two important points: (1) countries with high ICT development ranks will more likely than not have high innovation ranks and high growth competitiveness ranks; however, (2) countries with high competitiveness ranks may not have high innovation ranks. It seems that ICT-based innovations may have a stronger impact on growth competitiveness than mere ICT developments.

Parametric Tests

Besides the non-parametric tests reported above, two parametric tests were conducted: the ordinary least squares method (OLS) and the Partial Least Squares method (PLS). Regarding OLS, a multiple regression analysis was conducted with growth competitiveness being the dependent variable and both ICT and innovation being the independent variables or indicators. The results can be reported as follows, with ICT alone considered first, and then in the second step both ICT and innovation considered. This was done in order to test the mediation effect of innovation in the ICT-

innovation-growth competitiveness relationship. First, the simple regression model for ICT impact on national innovation and then on growth competitiveness is shown below.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.934 ^a	.871	.870	.0480205

a. Predictors: (Constant), IDI

ANOVA^b

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.095	1	2.095	908.393	.000 ^a
	Residual	.309	134	.002		
	Total	2.404	135			

a. Predictors: (Constant), IDI

b. Dependent Variable: GII

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.287	.010		29.536	.000
	IDI	.060	.002	.934	30.140	.000

a. Dependent Variable: GII

The results show that ICT has a positive and significant relationship with innovation, and it explains 87.1% ($R^2 = 0.871$) of its variance. For this model, the RMSE is the square root of the mean square of the residuals, that is, the square root of 0.002. This yields the value of 0.0447, indicating along with the R^2 value and the significant F-ratio a good model fit. As for the possible effect that ICT has on innovation, the following simple regression model also shows a significant and a positive relationship.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.854 ^a	.730	.728	.3353296

a. Predictors: (Constant), IDI

ANOVA^b

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	40.657	1	40.657	361.570	.000 ^a
	Residual	15.068	134	.112		
	Total	55.725	135			

a. Predictors: (Constant), IDI

b. Dependent Variable: GC

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.072	.068		45.209	.000
	IDI	.266	.014	.854	19.015	.000

a. Dependent Variable: GC

According to the above results, ICT explains 85.4% of the variance in growth competitiveness. Moreover, the F-ratio is significant, and RMSE in this model is the square root of the mean square of errors, 0.112, thus yielding 0.3346. This indicates that the previous model has a better fit than this one. Also, with the two significant and positive relationships reported above, it is important at this stage to identify the possible mediation effect that innovation has in the ICT-growth competitiveness relationship. According to Baron and Kenny (1986), a given construct is considered a mediator if it accounts for the relationship between a predictor and a dependent variable. The following multiple regression model reveals an interesting result.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.873 ^a	.762	.758	.3157538

a. Predictors: (Constant), GII, IDI

ANOVA^b

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	42.465	2	21.232	212.961	.000 ^a
	Residual	13.260	133	.100		
	Total	55.725	135			

a. Predictors: (Constant), GII, IDI

b. Dependent Variable: GC

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.071	.162		12.782	.000
	IDI	.056	.034	.178	1.638	.104
	GII	3.485	.525	.724	6.642	.000

a. Dependent Variable: GC

The findings indicate that ICT and innovation both explain 87.3% of the variation in growth competitiveness. The F-ratio is significant, and RMSE in this case is 0.1362, indicating a far better fit than the previous model (Grace-Martin, 2012). The interesting finding is that when innovation is introduced, ICT shows a non-significant relationship with growth competitiveness. This indicates a partial mediation effect that innovation has in the ICT-growth competitiveness relationship. The mediation effect was further tested using the Sobel test for mediation effect. However, the test requires that there is no multicollinearity risk amongst the variables (Preacher & Hayes, 2004,

2008). The VIF test for multicollinearity diagnostics was done, and the results showed no multicollinearity between the variables included in the model.

Coefficients^a

		Collinearity Statistics	
		Tolerance	VIF
1	IDI	.236	4.244
	GII	.236	4.244

a. Dependent Variable: GC

The above result which showed no multicollinearity risk amongst the variables allowed for the Sobel test of mediation to be conducted. The result, as obtained from the Sobel test calculator, was a mediation effect z score of 6.4813, and a p-value of 0.000. Based on this, Sobel test ascertained the partial mediation effect that innovation has in the ICT-growth competitiveness relationship.

Finally, SmartPLS was used to run a PLS path modeling test to test the above relationships. The first run included ICT-innovation and ICT-growth competitiveness. The path coefficients resulting from the original sample run came out as follows:

Relationship	Path Coefficients
ICT -> Comp	0.8542
ICT -> Innov	0.9335

The path coefficients are both strong and positive. ICT is positively related to innovation, implying that ICT development can foster innovation in a nation leading to new products, services, and operations. The significance of the path coefficients could be tested in PLS using the bootstrapping function previously defined and explained in this chapter. Following Chin's (1998) recommendations, the bootstrapping function was deployed using 1,000 sample runs. The results of the bootstrapping run came out as follows:

Basic Model Path Coefficients (no Med)						
	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
ICT -> Comp	0.8542	0.8538	0.0224	0.0224	38.0848	4.38727E-74
ICT -> Innov	0.9335	0.9334	0.011	0.011	85.0759	3.731E-119

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

The results of the bootstrapping function illustrate the significance of the relationships. Once again, the role that ICT plays in fostering innovation seems to be a big one. With this in mind, the next step now is to test the mediation effect of innovation. The following results show the relationships included in the basic model involving the relationship between innovation and growth competitiveness. As mentioned in the previous step, the bootstrapping function was also deployed here to test for the significance of the path coefficients.

Basic Model Path Coefficients						
	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
ICT -> Comp	0.1789	0.1872	0.125	0.125	1.4315	0.154597984
ICT -> Innov	0.9335	0.934	0.013	0.013	71.9559	1.5153E-109
Innov -> Comp	0.7233	0.7142	0.125	0.125	5.7866	4.78136E-08

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

In this PLS model, R^2 was reported as 0.797, implying that 79.7% of the variance in growth competitiveness could be attributed to ICT and innovation. These results show that there is a positive and strong relationship between ICT and innovation and between innovation and growth competitiveness, but not a strong relationship between ICT and growth competitiveness. Similar to the OLS results, introducing the innovation-growth competitiveness relationship to the model renders the relationship between ICT and growth competitiveness non-significant. Again here, the results illustrate the mediating role that innovation has in the ICT-growth competitiveness

relationship. This, however, is a partial mediation effect, implying that ICT contributes to growth, probably through ICT production, but its major influence comes through innovations; that is, when it is adopted and effectively used in the various sectors of a nation.

Following Preacher and Hayes' (2008) approach, a rigorous method for identifying the significance of the mediation effect could be based on the product of coefficients strategy¹². In PLS, this is very much approximated by the bootstrapping function used above. According to Hayes (2009), bootstrap confidence intervals are preferred to the Sobel test for inference about indirect effects. This was applied here by downloading a macro program developed by Hayes (2009) for mediation effect and running it in SPSS. The result of the bootstrapping method applied in SPSS for testing the validity of the mediation effect claimed above is as follows:

	Value	s.e.	LL95CI	UL95CI	Z	Sig(two)
Effect	.1009	.0242	.0534	.1483	4.1672	.0000

Indirect Effect and Significance Using Normal Distribution

The value figure is the result of the product of the coefficients (ICT-innovation and innovation-growth competitiveness) computed by SPSS, as shown below:

	Coefficient	s.e.	t	Sig(two)
b(IDI-GC)	.2656	.0140	19.0150	.0000
b(IDI-GII)	.0653	.0031	20.8488	.0000
b(GII-GC)in IDI-GII-GC	1.5460	.3631	4.2580	.0000

Direct and Total Effects

¹² Beyond assessing the change in the effect of variable X on a criterion Y upon introducing a possibly mediating factor M, other ways are also used to test the validity of the mediation assumption (Preacher & Hayes, 2004). For example, according to Baron and Kenny (1986), two conditions must be met: (1) there should be no measurement error in M, and (2) Y should not cause M. According to Preacher and Hayes (2004), the product of coefficients strategy is more rigorous than Baron and Kenny's criteria for testing the significance of mediation effects. This strategy deploys bootstrapping confidence intervals. The importance of this method lies in the fact that it allows for the null hypothesis (H_0 : indirect effect = 0) to be tested. This can be done by using a mediation effect macro developed by Hayes (2009) for SPSS.

In other words, the value of 0.1009 is the result of $(.0653 \times 1.5460)$. Referring to the lower limit and upper limit of the 95% confidence interval, one finds that zero does not fall between the resulting confidence intervals of the bootstrapping method. This means one can confidently conclude that there is a significant and validated mediation effect to report (Preacher & Hayes, 2004) in this case. National innovation has a significant mediation effect in the ICT-growth relationship.

Based on the above analysis, the reported results could be summarized as follows: (1) ICT is positively and significantly related to growth competitiveness; (2) national innovation is positively and significantly related to growth competitiveness; (3) ICT is positively and significantly related to national innovation; and (4) the indirect relationship between ICT and growth competitiveness through national innovation is stronger than that of the direct one. The last point signifies the mediating role that innovation plays in the ICT- growth relationship. It also indicates that innovation has the catalyst effect with which ICT propels the wheels of growth.

Cybersecurity: A Formative Construct

One of the main objectives of this study is to develop a formative construct to represent cybersecurity at the national level. To establish the formative construct of cybersecurity, several steps were taken, following the guidelines set by Diamantopoulos and Winklhofer (2001). The guidelines are: (1) content domain definition; (2) indicator specification; (3) indicator collinearity; and (4) reliability and validity assessment.

Cybersecurity Construct: Content Domain and Indicator Specification

To start with, content specification refers to the domain of content the composite measure is intended to capture. This is harder to determine than a latent variable with reflective indicators (Bagozzi, 1994). A critical condition here is to have a 'breadth of definition' (Nunnally &

Bernstein, 1994) since all the construct facets should be included. In this study, the content domain of the 'cybersecurity' construct was specified as the technological, legal, and international cooperation measures or initiatives that a country takes to achieve a secure cyberspace and protect its critical information infrastructure from cyber threats. Such definition has been derived from the literature and from the reports provided by governments and international organizations (e.g., ITU, 2010, 2011). The second criterion, indicator specification is inextricably linked with the previous element. Here a census of indicators is required, and these indicators must capture the technological, legal, and international cooperation aspects mentioned in the content domain. In this study, the content domain of the 'cybersecurity' formative construct was defined and the content validity could be assumed based on theoretical support, literature, and the input and opinion of experts in the area of cybercrime and national security. To start with, the construct indicators are theoretically valid based on the general information security theories as well as the international relations related theories, namely national security and deterrence theories. In addition to the theoretical framework and the literature body based on which the construct is built, expert opinion was sought by referring to information and cybersecurity experts, those involved in the development of composite indexes from the World Bank and UNDP, and others working in the area of cybercrime working in CERT (computer emergency readiness team) units in UAE and Vienna (Austria). Five experts provided their opinions about the measure indicators as well as ranked them in terms of their importance in forming the Cybersecurity construct. All five experts considered the three indicators important for building up the composite construct. Three of them considered secure communication lines as the most important indicator, followed by ICT law enforcement, and then international cooperation; whereas the remaining two declared that international cooperation is

more important than ICT law enforcement while viewing secure communication as the most important indicator.

In order to assess the inter-rater reliability amongst the 5 raters, a non-parametric test, namely Kendall's W, was conducted. The results are reported in Table 28, and show that the coefficient of concordance is relatively high and significant. This suggests that the construct 'cybersecurity' may assume an acceptable content validity.

Table 28 Coefficient of concordance – Inter Rater reliability

N	5
Kendall's W ^a	.760
Chi-Square	7.600
df	2
Asymp. Sig.	.022

a. Kendall's Coefficient of Concordance

Cybersecurity Construct: Indicator Collinearity

After examining the content domain and indicator specification, the indicator collinearity is examined. An issue to be avoided in constructing a formative measure is multicollinearity. Because it is based on multiple regression, the sample size and the indicator inter-correlations can affect, to a large extent, the stability of the indicator coefficients. With this in mind, if indicator collinearity is observed, i.e. an indicator having an almost perfect linear correlation with the other indicators, then this indicator should be considered for exclusion from the construct (Bollen & Lennox, 1991).

The VIF threshold of 3.3 has been recommended in the context of PLS-based SEM in discussions of formative latent variable measurement. A rule of thumb rooted in the use of this software for many SEM analyses in the past suggests an even more conservative approach: that capping VIFs to 2.5 for indicators used in formative measurement leads to improved stability of

estimates. The correlation results for the cybersecurity indicators as well as the VIF values examining their multicollinearity are exhibited in Table 29 and 30 respectively.

Table 29 Correlation Analysis: Cybersecurity Indicators

		SecureCom	ICTLaws	IntlCoop
SecureCom	Pearson Correlation	1	.379**	.377**
	Sig. (2-tailed)		.000	.000
	N	136	136	136
ICTLaws	Pearson Correlation	.379**	1	.354**
	Sig. (2-tailed)	.000		.000
	N	136	136	136
IntlCoop	Pearson Correlation	.377**	.354**	1
	Sig. (2-tailed)	.000	.000	
	N	136	136	136

**, Correlation is significant at the 0.01 level (2-tailed).

The correlation results show that the values of the correlation coefficients are not large, though they are significant. A better indicator of the level of multicollinearity would be the variance inflation factor (VIF) as presented in Table 30. The results show a maximum VIF value of 2.514, which is far less than the common threshold of 10, and also less than the threshold ‘3.3’ recommended in PLS-SEM contexts. The multivariate analysis literature, however, tends to move toward higher thresholds. Also, limiting variance inflation factors to 2.5 may in some cases severely limit the number of possible indicators available.

Table 30 VIF Values pertinent to Cybersecurity Indicators

Model	Collinearity Statistics	
	Tolerance	VIF
IntlCoop	.848	1.180
Secure Com.	.398	2.514
ICTLaws	.406	2.465

Dependent Variable: CyberSecurity

Given this, it is recommended that variance inflation factors be set at 2.5 if this does not lead to a major reduction in the number of indicators available to measure formative latent variables. Even according to this criterion, the indicators for the study cybersecurity formative construct have adequate conformance to this recommended threshold. These criteria are consistent with formative latent variable theory. Among other things, formative latent variables are expected, often by design, to have many indicators. Yet, given the nature of multiple regression, indicator weights will normally go down as the number of indicators go up, as long as those indicators are somewhat correlated, and thus P values will normally go up as well. Moreover, as more indicators are used to measure a formative latent variable, the likelihood that one or more will be redundant increases. This will be reflected in high variance inflation factors (Chin, 2010). For the cybersecurity measure, the VIF values came out to be low, indicating no multicollinearity risks. At the same time, the correlation coefficients amongst the indicators are not high. This demonstrates the multidimensionality aspect of the cybersecurity construct.

Cybersecurity Construct: Validity and Reliability Assessment

Coming to the reliability and validity assessment, this study mainly followed the approach drawn by Straub et al. (2004) and Diamantopoulos and Winklhofer (2001). Starting with reliability assessment, Straub et al. (2004) state that “it is not clear that reliability is a concept that applies well to formative constructs” (p. 400). This statement is also corroborated by Diamantopoulos and Siguaw (2006), who contended that no dimensionality and reliability test are performed on formative indicators. A similar view was provided by Rossiter (2002). These views are attributed to the fact that factorial unity in factor analysis and internal consistency are not relevant in the context of formative measures, which assume multidimensionality rather than unidimensionality. Based on this, previous research in the field suggested that construct reliability of formative measures should

be performed by multicollinearity, test of indicator validity (represented by path coefficients significance), and, if applicable, test-retest (e.g., Andreev et al., 2009 and Petter et al., 2007). Thus, for formative constructs, since unidimensionality cannot be assumed, reliability assessment is mainly based on testing multicollinearity, which is done through VIF, as elaborately discussed above.

Finally, regarding the validity of the formative construct, there is an agreement amongst previous researchers that validity assessment in formative measurement is highly controversial (Diamantopoulos et al., 2008). This is because the applicability of statistical procedures (Hardin et al., 2008) in this context is limited. External validity and individual indicator validity are recommended by several authors (Diamantopoulos et al., 2008; Diamantopoulos & Sigauw, 2006). As for external validity, it examines “how well the index relates to measures of other variables” (Bagozzi, 1994, p.333). However, as noted by Thongrattana (2010), it is unclear as to how this should be done.

In formative measurement models, indicator validity refers to the importance of each individual indicator of the related formative construct (Andreev et al., 2009; MacKenzie et al., 2005). It should critically examine whether a particular indicator should enter into the formative index (Henseler et al., 2009, p.302). The estimation of this validity is performed by the Partial Least Square (PLS) approach with a bootstrapping method to calculate item weights (or PLS scores or outer weights), and t-values of each formative indicator to assess its significance (Bruhn et al., 2008; Diamantopoulos & Winklhofer, 2001; and Chin, 1998).

In this study, the validity of the cybersecurity formative measure is based on the output related to the indicator weights. Indicator weights are provided much in the same way as indicator loadings are, in a table format. In the indicator weights table, all cross-weights are zero, because of

the way they are calculated through PLS regression. This is demonstrated in Table 31. GC (growth competitiveness index score) is the only indicator of the formative measure Comp, and thus has a weight of 1.000. Its cross-weight in Cybersecurity is 0. The cybersecurity formative measure indicators are ICT laws, international cooperation, and secure communication lines with ICT laws having the larger weight, followed by weights for international cooperation and secure communication that are very close to each other. These indicators' cross-weights are zero in the Comp (growth competitiveness) latent variable.

Table 31 Indicator Weights

	Comp	Cybersecurity
GC	1.0000	0
ICTLaws	0.0000	0.6049
IntlCoop	0.0000	0.2295
SecureCom	0.0000	0.293

Based on these weights, the latent variable score is calculated as an exactly linear combination of its indicators, where the weights are multiple regression coefficients linking the indicators to the latent variable. This brings the error term to zero in the regression equation relating the indicators to the latent variable. In fact, a formative construct is a summation or an aggregate of its indicators (Diamantopoulos & Winklhofer, 2001). The only variance, which is treated as error, is the random variance at the construct level (Law & Wong, 1999). Hence the error term is associated with the construct as a whole and not with the individual indicators.

Moreover, as illustrated below in Table 32, P values are provided for weights associated with formative latent variables¹³ based on the T-statistics values provided. In addition to P values,

¹³ Usually, these values can also be seen, together with those for loadings associated with reflective and moderating latent variables, as the result of a confirmatory factor analysis. In research reports, these P values are included as an indication that the formative latent variable measurement items were properly constructed. As in multiple regression analysis, it is recommended that weights with P values lower than 0.05 be considered valid items in a formative latent

variance inflation factors are also provided for the indicators of formative latent variables. These can be used for indicator redundancy assessment. In reflective latent variables indicators are expected to be redundant. This is not the case with formative latent variables. In formative latent variables, indicators are expected to measure different facets of the same construct, which means that they should not be redundant. The VIF values presented above (in Table 15) show that the cybersecurity formative latent variables are not redundant and they show multidimensionality.

With the cybersecurity formative construct formed, the bootstrapping function in Smart-PLS was applied. The indicators' estimated coefficients – i.e. the weights of the outer measurement model – were taken and used in SPSS to compute the new cybersecurity measure. The indicators, their weights, t-test, and computed p-values are shown in Table 32.

Table 32 Cybersecurity Indicators: Weights, T-tests, and P-value

Cybersecurity Indicators			
	Weight	T Statistics	P-value
ICTLaws -> Cybersecurity	0.6049	9.7805	2.08861E-17
IntlCoop -> Cybersecurity	0.2295	4.5462	1.20172E-05
SecureCom-> Cybersecurity	0.293	4.8759	2.99707E-06

According to these results, it seems that 'ICT laws' has the largest and most significant weight in determining the cybersecurity formative measure. This is followed by secure communication lines, and finally by international cooperation. After computing the new cybersecurity measure, the variable was ranked across the various countries so as to assess later its agreement with the ranks of other variables through a nonparametric test. Table 33 presents the scores of the new cybersecurity measure across the various countries, along with the country

variable measurement item subset. Formative latent variable indicators with weights that do not satisfy this criterion may be considered for removal (Diamantopoulos & Winklhofer, 2001).

rankings pertinent to these values. The scores are based on the weights derived from PLS output, and thus, the cybersecurity formative measure scores are based on this formula:

$$\text{Cybersecurity} = 0.293 * \text{Secure Communication} + 0.6049 * \text{ICT Laws} + 0.2295 * \text{International Cooperation}.$$

The resulting scores and derived ranks (Table 33) will be used henceforth in examining the relationships between cybersecurity and the other model variables.

ICT-Innovation-Cybersecurity and Growth: Overall Model Relationships

The basic model relationships were examined and supported, as previously shown. This, along with the cybersecurity construct developed following the guidelines of formative measurement, will make it possible to examine the relationships in the overall model. It is also important to assess the fit and predictive validity of this model, as the major purpose of the study is to develop a prediction model for growth competitiveness based on ICT, innovation, and cybersecurity scores.

Non-Parametric Tests

The new cybersecurity measure has then been used to assess its ranking agreement and concordance with the other three variables of the basic model. Kendall's-tau-b test for ranking agreement was used, and the results came out to be as shown in Table 34. The results indicate a significant and positive agreement in the new construct ranks with all the ranks of the other model constructs. This is an interesting result, and it shows that an increase or decrease in the ranking of ICT and innovation will also be associated with an increase or decrease in cybersecurity ranking, and in turn, an increase or decrease in the ranking of growth competitiveness.

Table 33 Cybersecurity Scores and Country Ranks

Country	New Cybersecurity Score	Rank	Country	New Cybersecurity Score	Rank
Sweden	4.50	1	Turkey	3.19	39
Denmark	4.43	2	Brazil	3.17	40
United States	4.43	3	Lithuania	3.17	41
Switzerland	4.36	4	Bahrain	3.06	42
United Kingdom	4.35	5	Oman	3.06	43
Finland	4.31	6	Panama	3.03	44
Netherlands	4.31	7	China	2.95	45
Singapore	4.31	8	Slovak R.	2.91	46
Australia	4.30	9	Mexico	2.87	47
Canada	4.23	10	Tunisia	2.87	48
Norway	4.22	11	India	2.85	49
Hong Kong SAR	4.21	12	Poland	2.85	50
Korea, Rep.	4.20	13	Croatia	2.84	51
Austria	4.14	14	Bulgaria	2.81	52
New Zealand	4.11	15	Greece	2.81	53
Germany	4.04	16	Latvia	2.78	54
Estonia	4.03	17	Colombia	2.71	55
France	4.00	18	Uruguay	2.71	56
Luxembourg	4.00	19	Barbados	2.69	57
Iceland	3.89	20	Mauritius	2.63	58
Israel	3.83	21	Kuwait	2.61	59
Japan	3.83	22	Costa Rica	2.56	60
Portugal	3.80	23	Russian Fed.	2.55	61
Ireland	3.69	24	Montenegro	2.53	62
Belgium	3.68	25	Romania	2.49	63
Malta	3.64	26	Belarus	2.47	64
Slovenia	3.64	27	Jordan	2.47	65
Spain	3.57	28	Thailand	2.44	66
Malaysia	3.46	29	Jamaica	2.43	67
South Africa	3.46	30	Macedonia	2.38	68
United Arab Emirates	3.42	31	Kenya	2.36	69
Chile	3.40	32	Sri Lanka	2.30	70
Czech Republic	3.39	33	Ukraine	2.30	71
Qatar	3.34	34	Brunei	2.29	72
Cyprus	3.30	35	Argentina	2.28	73
Italy	3.23	36	Azerbaijan	2.27	74
Saudi Arabia	3.23	37	Serbia	2.26	75
Hungary	3.20	38	Egypt	2.23	76

Country	New Cybersecurity Score	Rank	Country	New Cybersecurity Score	Rank
Kazakhstan	2.23	77	Mali	1.37	117
Peru	2.22	78	Bangladesh	1.36	118
Armenia	2.19	79	Paraguay	1.34	119
Georgia	2.18	80	Algeria	1.32	120
Philippines	2.16	81	Zimbabwe	1.31	121
Indonesia	2.14	82	Ethiopia	1.27	122
Rwanda	2.14	83	Cameroon	1.26	123
Guatemala	2.12	84	Nepal	1.24	124
Ecuador	2.09	85	Côte d'Ivoire	1.07	125
Vietnam	2.09	86	Swaziland	1.06	126
Dominican Republic	2.06	87	Benin	1.01	127
Botswana	2.04	88	Mauritania	1.01	128
Morocco	2.04	89	Angola	0.99	129
Trinidad and Tobago	2.02	90	Kyrgyz Rep.	0.96	130
Nigeria	2.00	91	Madagascar	0.93	131
Senegal	1.99	92	Syria	0.91	132
Moldova	1.97	93	Suriname	0.82	133
Cape Verde	1.96	94	Lesotho	0.72	134
Gambia, The	1.95	95	Chad	0.50	135
Albania	1.94	96	Yemen	0.47	136
Namibia	1.94	97			
Nicaragua	1.94	98			
Venezuela	1.91	99			
Iran, Islamic Rep.	1.88	100			
Bosnia and Herzegovina	1.79	101			
Pakistan	1.75	102			
Honduras	1.74	103			
Uganda	1.74	104			
Cambodia	1.73	105			
Zambia	1.71	106			
Ghana	1.67	107			
Mongolia	1.64	108			
Bolivia	1.61	109			
El Salvador	1.61	110			
Tanzania	1.58	111			
Fiji	1.52	112			
Lebanon	1.45	113			
Burkina Faso	1.42	114			
Guyana	1.41	115			
Mozambique	1.41	116			

Table 34 Kendall's-tau-b: Ranking Agreement between Cybersecurity, ICT, Innovation, and Growth Competitiveness

			IDIRank	GIIRank	GCRank	NewCybersecRank
Kendall's tau_b	IDIRank	Correlation Coefficient	1.000	.685**	.654**	.720**
		Sig. (2-tailed)	.	.000	.000	.000
		N	116	116	116	116
	GIIRank	Correlation Coefficient	.685**	1.000	.593**	.667**
		Sig. (2-tailed)	.000	.	.000	.000
		N	116	116	116	116
	GCRank	Correlation Coefficient	.654**	.593**	1.000	.754**
		Sig. (2-tailed)	.000	.000	.	.000
		N	116	116	116	116
	NewCybersecRank	Correlation Coefficient	.720**	.667**	.754**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	116	116	116	116

** . Correlation is significant at the 0.01 level (2-tailed).

As mentioned above, a Kendall's-tau-b of rank agreement does not show the level of concordance amongst the ranks. This necessitates the use of Kendall's W test to compute the coefficient and significance of concordance. The results are reported below (Table 35).

The coefficient of concordance is adequately acceptable as well as significant. From these results, we reject the null hypothesis of mutual independence between the cybersecurity and growth competitiveness rankings for the countries.

Table 35 Kendall's W Coefficient of Concordance – Cybersecurity Ranking with the Rankings of Other Variables

Test Statistics	
N	116
Kendall's W ^a	.625
Chi-Square	217.473
df	3
Asymp. Sig.	.000
a. Kendall's Coefficient of Concordance	

With a two-sided test we are considering the possibility of concordance or discordance (akin to positive or negative correlation). A one-sided test would have been restricted to either discordance or concordance; this would be an unusual assumption. In the case here, it can be concluded that there is a statistically significant lack of independence between cybersecurity and growth competitiveness rankings of the countries. The results tend to demonstrate that countries with apparently higher cybersecurity levels are more competitive in terms of growth than those with apparently less cybersecurity and vice versa.

To show the level of concordance amongst matched pairs, the Wilcoxon test of matched pairs was applied. The results are reported in Table 36, and they demonstrate a significant level of concordance between each two pairs of variables, with cybersecurity being one element of the pair. In fact, this is an interesting and encouraging result as the new measure ranking is in agreement with the rankings of the other variables, meaning a positive difference in cybersecurity ranks will be matched with a positive difference in ICT, innovation, and also growth competitiveness.

Table 36 Wilcoxon Test of Matched Pairs

Matched Pairs	Wilcoxon Test (Z statistic)	Significance	Decision
ICT-Cybersecurity	-0.152	0.880	Fail to Reject H_0
Innovation-Cybersecurity	-0.234	0.815	Fail to Reject H_0
Cybersecurity- Growth Competitiveness	-0.239	0.811	Fail to Reject H_0

As preciously done, the Wilcoxon test for related samples was also applied to derive more detailed information about the ranked scores (Field, 2009). The results are portrayed in Table 37, and they show for each pair of related samples the number of negative ranks, the number of positive ranks, and the number of ties. It is important to recall here that the null hypothesis for the Wilcoxon test of matched pairs is as follows: matched pairs of rank orders are concordant.

Table 37 Wilcoxon Signed Ranks Test: ICT-Innovation-Cybersecurity-Growth Competitiveness

ICT and Cybersecurity Ranks			
		N	Mean Rank
IDIRank – New CybersecRank	Negative Ranks	66 ^a	56.42
	Positive Ranks	65 ^b	55.57
	Ties	5 ^c	
a. IDIRank < NewCybersecRank			
b. IDIRank > NewCybersecRank			
c. IDIRank = NewCybersecRank			

Test Statistics ^b	
	IDIRank – New CybersecRank
Z	-.152 ^a
Asymp. Sig. (2-tailed)	.880
a. Based on positive ranks.	
b. Wilcoxon Signed Ranks Test	

Innovation and Cybersecurity Ranks			
		N	Mean Rank
GIIRank – New CybersecRank	Negative Ranks	54 ^a	57.10
	Positive Ranks	58 ^b	55.94
	Ties	4 ^c	
	Total	116	
a. GIIRank < NewCybersecRank			
b. GIIRank > NewCybersecRank			
c. GIIRank = NewCybersecRank			

Ranks			
		N	Mean Rank
GCRank – New CybersecRank	Negative Ranks	57 ^a	58.98
	Positive Ranks	57 ^b	56.02
	Ties	2 ^c	
a. GCRank < NewCybersecRank			
b. GCRank > NewCybersecRank			
c. GCRank = NewCybersecRank			

Test Statistics ^b	
	GIIRank – New CybersecRank
Z	-.234 ^a
Asymp. Sig. (2-tailed)	.815
a. Based on negative ranks.	
b. Wilcoxon Signed Ranks Test	

Test Statistics ^b	
	GCRank – New CybersecRank
Z	-.239 ^a
Asymp. Sig. (2-tailed)	.811
a. Based on positive ranks.	
b. Wilcoxon Signed Ranks Test	

The above results show that the z-score of the Wilcoxon signed rank test as related to ICT and cybersecurity ranks is based on positive ranks. This implies that countries with high ICT ranks may have lower cybersecurity ranks. However, this is not significant. As for the innovation and cybersecurity ranks, the test is based on negative ranks. This means that countries with high innovation ranks do not necessarily have high cybersecurity ranks. Still, the test is not significant, and the interpretation is merely based on the used rank signs. The last test is pertinent to cybersecurity and growth competitiveness ranks, and is based on positive ranks, implying that countries with high growth competitiveness ranks may not have high cybersecurity ranks. Similar to all the previous results, this test is also not significant. Accordingly, the null hypothesis for all the tests cannot be rejected, and concordance amongst the ranks of ICT, innovation, cybersecurity, and

growth competitiveness could be assumed. Looking at the significance values of the above Wilcoxon signed rank tests for each matched pair of variables, one can find that the levels of agreement vary across the various matched pairs. With respect to their agreement with cybersecurity ranks, ICT, innovation, and growth competitiveness ranks show relatively similar concordance across the three pairs. The lowest agreement is between ICT and cybersecurity, followed by growth competitiveness, and then by innovation. This may allow for the following conclusions to be made: (1) countries with high ICT development scores may face certain cybersecurity issues; (2) countries with high competitiveness may not have high cybersecurity levels; and (3) countries with high innovation may have a chance to effect better cybersecurity levels.

Parametric Tests

The above analysis based on the results of nonparametric tests is now followed by a presentation and analysis of the findings derived from the parametric tests; namely, OLS regression and PLS, as pertinent to the overall model. This will be covered in the following subsections.

Mediating Role of Cybersecurity in the ICT-Growth Competitiveness Relationship. Using OLS, a simple regression analysis was conducted with growth competitiveness being the dependent variable and both ICT and cybersecurity being the independent variables or indicators. The results can be reported as follows, first with ICT considered alone, and then in the second step both ICT and cybersecurity are considered. This was done in order to test the mediation effect of innovation in the ICT-cybersecurity-growth competitiveness relationship. First, the simple regression model for ICT impact on growth competitiveness was shown in the previous parametric test results reported under ‘The Relationship between ICT, Innovation, and growth competitiveness section’. The results showed an R^2 of 0.854, meaning that ICT explains 85.4% of the variance in growth

competitiveness. Moreover, the F-ratio is significant, and RMSE in this model is 0.3346 (i.e. the square root of 0.112).

The second step entailed running a regression analysis with cybersecurity being the dependent variable and ICT being the independent variable. Here, the coefficient of determination, R^2 , came out to be 0.804, meaning that 80.4% of the variance in cybersecurity could be attributed to ICT development. The model proved to be significant with an F-value of 548.56 (sig. =0.000), and a random mean square error (RMSE) of 0.459 ($=\sqrt{0.211}$, where 0.211 is the mean square error).

The last step in assessing the mediation effect of cybersecurity in the ICT – growth competitiveness relationship was to introduce the cybersecurity – growth relationship and examine the effect of this new relationship on the value and significance of the B coefficient in the ICT – growth relationship. In this model, where growth was the dependent variable and ICT and cybersecurity were both independent variables, R^2 was 0.855, meaning that 85.5% of the variance in growth competitiveness could be explained by ICT and cybersecurity. The model proved to be significant, with F-value = 392.573 and a sig value=0.000. The mean square of the model is 0.061, yielding RMSE of 0.2469. These results are shown in Table 38.

Table 38 ICT-Cybersec-GC: Regression Results and Cybersec Mediation Effect

Model	Dep.	R^2	F	Sig	RMSE	Indicators	B Coeff.	Sig.
ICT - GC	GC	.730	361.570	0.000	0.3346	ICT	.266	0.000
ICT-Cybersec	Cybersec	.804	548.560	0.000	0.459	ICT	0.449	0.000
ICT-Cybersec-GC	GC	0.855	392.573	0.000	0.2469	ICT	0.043	0.068
						Cybersec	0.497	0.000

The results in Table 38 clearly illustrate the condition set by Baron and Kenny (1986) that a given construct is considered a mediator if it accounts for the relationship between a predictor and a

dependent variable. While the relationship between ICT and GC reveals a significant coefficient (0.266), the coefficient decreases remarkably (to 0.043) and becomes non-significant (sig = 0.068) when the relationship between cybersecurity and growth competitiveness is introduced. This illustrates a partial mediation effect that cybersecurity has in the ICT-growth relationship. In fact, the result is logical, given that economies are growing increasingly reliant on ICT, with critical infrastructures (CI) operated, monitored, controlled, and linked to each other through ICT which underpins critical information infrastructures (CII). In other words, if these CIIs become a target for any cyber threat, the economy will be negatively affected. Accordingly, the contribution of ICT to the economy hinges upon safe and resilient CIs and CIIs that are protected with effective and optimal cybersecurity measures.

As previously mentioned, the partial mediation reported above had to be further tested for effect and significance using the Sobel test for mediation effect. As the test requires that there is no multicollinearity risk amongst the variables (Preacher & Hayes, 2004, 2008), The VIF test for multicollinearity diagnostics was done, and the results showed no multicollinearity between the variables included in the model.

Coefficients ^a			
Model		Collinearity Statistics	
		Tolerance	VIF
1	IDI	.196	5.094
	NewCybersec	.196	5.094

a. Dependent Variable: GC

The above result showed no multicollinearity risk amongst the variables, and thus allowed for the Sobel test of mediation to be conducted. The result, as obtained from the Sobel test calculator, was a mediation effect z score of 17.86, and a p-value (2-tailed) of 0.000. Based on this,

the Sobel test ascertained the partial mediation effect that cybersecurity has in the ICT-growth competitiveness relationship.

Mediating Role of Cybersecurity in the Innovation-Growth Competitiveness Relationship.

The same steps applied in the previous section were used to test the mediation effect of cybersecurity in the innovation-GC relationship. Using OLS, and as a first step, a simple regression analysis was conducted with growth competitiveness being the dependent variable and innovation being the independent variable. The resulting R^2 was 0.696, meaning that 69.6% of the variance in growth competitiveness may be attributed to innovation. In this regression model, the F-ratio was significant, and RMSE is 0.3549 (i.e. the square root of 0.126, the mean square error).

The second step entailed running a regression analysis with cybersecurity being the dependent variable and innovation being the independent variable. Here, the coefficient of determination, R^2 , came out to be 0.792, meaning that 79.2% of the variance in cybersecurity could be attributed to innovation. The model proved to be significant with an F-value of 509.65 (sig. =0.000), and a random mean square error (RMSE) of 0.473, and the square root of 0.224 (the mean square error).

In the last step, the cybersecurity – growth relationship was introduced to examine the effect of this new relationship on the value and significance of the B coefficient in the innovation – growth relationship. In this model, where growth was the dependent variable and innovation and cybersecurity were both independent variables, R^2 was 0.852. The model proved to be significant, with the F-value = 383.646 and a sig value=0.000. The mean square of the model is 0.062, resulting in an RMSE value of 0.2489. The above mentioned results are portrayed in Table 39.

Table 39 Innovation-Cybersec-GC: Regression Results and Cybersec Mediation Effect

Model	Dep.	R ²	F	Sig	RMSE	Indicators	B Coeff.	Sig.
Innovation - GC	GC	.696	306.651	0.000	0.3549	Innovation	3.476	0.000
Innovation-Cybersec	Cybersec	.792	509.65	0.000	0.473	Innovation	5.967	0.000
Innovation-Cybersec- GC	GC	0.852	383.646	0.000	0.2489	Innovation	0.263	0.390
						Cybersec	0.539	0.000

The results in Table 24 clearly meet Baron & Kenny's (1986) condition and prove cybersecurity as a mediator variable in the innovation-growth competitiveness relationship. The relationship between innovation and GC reveals a significant coefficient (3.476); however, the coefficient decreases noticeably (to 0.263) and becomes far from significant (sig = 0.390) when the relationship between cybersecurity and growth competitiveness is introduced. This again illustrates a partial mediation effect that cybersecurity has in the innovation-growth relationship. The result demonstrates a very important element in fostering innovation and allowing it to contribute positively to growth, namely the protection of innovation output. If intellectual property protection is violated, and if economic espionage takes place, innovation processes will not reach their objectives, and accordingly the innovation efforts in the affected nations may decrease. In conclusion, the contribution of innovation to the economy, just like that of ICT, is contingent upon a safe cyberspace, which depends on effective cybersecurity measures.

Testing the significance of the above mediation effects requires the use of a tool like the Sobel test, which in turn necessitates showing that multicollinearity risk does not exist. The result,

as obtained from the Sobel test calculator, showed a mediation effect with a z-score of 17.406 and a p-value (2-tailed) of 0.000. Based on this, the partial mediation effect that cybersecurity has in the innovation-growth competitiveness relationship is also ascertained.

Finally, SmartPLS was used to run a PLS path modeling test to test the above relationships. The first run examined the relationships of ICT-cybersecurity and ICT-growth competitiveness. The path coefficients resulting from the original sample run were as follows:

Relationship	Path Coefficients
ICT -> Comp	0.8542
ICT -> Cybersec	0.9436

The path coefficients are both strong and positive. ICT is positively related to cybersecurity, implying that ICT development can involve the development of effective and sound cybersecurity technologies. At the same time, ICT contributes positively to economic growth as shown earlier. Using the bootstrapping function, the significance of the path coefficients could be tested in PLS. Here again, Chin's (1998) recommendations were followed, and the bootstrapping function was deployed, using 1,000 sample runs. The results of the bootstrapping run came out as follows:

	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
ICT -> Comp	0.8542	0.8532	0.0224	0.0224	38.1701	3.32729E-74
ICT -> Cybersec	0.9436	0.9443	0.0107	0.0107	88.5443	1.862E-121

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

The results of the bootstrapping function illustrate the significance of the relationships. Once again, high ICT development levels may be associated with better cybersecurity levels. With this in mind, the next step now is to test the mediation effect of cybersecurity. The following results

show the relationship between ICT, cybersecurity, and growth competitiveness. As mentioned in the previous step, the bootstrapping function was also deployed here to test for the significance of the path coefficients.

	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
Cybersec -> Comp	0.8532	0.8733	0.0875	0.0875	9.7555	2.41338E-17
ICT -> Comp	0.0601	0.039	0.0932	0.0932	0.6452	0.519892596
ICT -> Cybersec	0.9307	0.9306	0.0117	0.0117	79.7181	2.0492E-115

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

In this PLS model, R^2 was reported as 0.827, implying that 82.7% of the variance in growth competitiveness could be attributed to ICT and cybersecurity measures or initiatives. These results show that there is a positive and strong relationship between ICT and cybersecurity and between cybersecurity and growth competitiveness, but not a strong relationship between ICT and growth competitiveness. Similar to the OLS results, introducing the cybersecurity-growth competitiveness relationship to the model weakens the relationship between ICT and growth competitiveness and makes it non-significant. Here again, the results illustrate the mediating role that cybersecurity has in the ICT-growth competitiveness relationship. This, however, is a partial mediation effect, implying that ICT contributes to growth, but its major influence comes through supporting a technologically secure critical infrastructure; that is, when it contributes to a resilient and safe cyberspace.

A similar result was derived when the mediator role of cybersecurity was examined in the innovation-growth competitiveness relationship. First, the relationships between innovation and cybersecurity and between innovation and growth competitiveness were examined. The path coefficients and the results of the bootstrapping function related to the significance of these coefficients are shown below.

	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
Innov -> Comp	0.8342	0.834	0.0266	0.0266	31.3505	7.85277E-64
Innov -> Cybersec	0.9027	0.9045	0.0164	0.0164	55.1201	1.95653E-94

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

As can be clearly noticed, innovation has strong and positive relationships with both cybersecurity and growth competitiveness. Innovation can encourage the wheels of growth competitiveness forward. At the same time, innovations in products, services, and processes within the field of cybersecurity are strongly associated to cyberspace safety and security. Now to test the mediating effect that cybersecurity has in the innovation-growth relationship, the cybersecurity-growth relationship was introduced. Interestingly, the cybersecurity-growth relationship has rendered the innovation-growth relationship weak and non-significant. This is shown in the following reported results.

	Original Sample Path Estimate	Sample Mean	Standard Deviation	Standard Error	T Statistics ^a	P-value ^b
Cybersec -> Comp	0.8794	0.8823	0.0707	0.0707	12.4306	4.01636E-24
Innov -> Comp	0.0441	0.0415	0.0787	0.0787	0.5605	0.576067451
Innov -> Cybersec	0.8984	0.8988	0.0176	0.0176	50.9332	5.15301E-90

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $P < 0.05$.

Following Preacher & Hayes' (2008) approach, the product of coefficients strategy was used as a rigorous method for identifying the significance of the mediation effect. In PLS, this is very much approximated by the bootstrapping function used above. Using the macro program developed by Hayes (2009) for mediation effect and running it in SPSS, the result of the bootstrapping method showing the significance of the test as well as its confidence interval for testing the validity of the mediation effect claimed above came out as follows:

	Value	s.e.	LL95CI	UL95CI	Z	Sig(two)
Effect	.2034	.0253	.1538	.2530	8.0380	.0000

Indirect Effect and Significance Using Normal Distribution: Cybersecurity As Mediator In Ict-Growth Relationship

	Value	s.e.	LL95CI	UL95CI	Z	Sig(two)
Effect	2.8179	.3157	2.1992	3.4366	8.9265	.0000

Indirect Effect and Significance Using Normal Distribution: Cybersecurity As Mediator In Innovation-Growth Relationship

The value figures shown above are the result of the product of the coefficients (0.2034: ICT-cybersecurity and ICT-growth competitiveness; 2.8179: Innovation-cybersecurity and innovation-growth competitiveness) computed by SPSS, as shown below.

Cybersec mediator in ICT-Growth	Coefficient	s.e.	t	Sig(two)
b(IDI-GC)	.2656	.0140	19.0150	.0000
b(IDI-Cybersec)	.4149	.0169	24.5090	.0000
b(Cybersec-GC) in IDI-Cybersec-GC	0.4901	.0576	8.5157	.0000
Cybersec mediator in Innov-Growth	Coefficient	s.e.	t	Sig(two)
b(Innov-GC)	3.4760	.1985	17.5115	.0000
b(Innov-Cybersec)	5.4385	.2478	21.9469	.0000
b(Cybersec-GC) in Innov-Cybersec-GC	.5181	.0530	9.7814	.0000

Direct and Total Effects

The value 0.2034 is the result of the product of coefficients (0.4149*0.4901) and 2.8179 is the result of the product of coefficients (5.4385*.5181). Also, the fact that zero does not fall between the resulting confidence intervals of the bootstrapping method means that one can confidently conclude that there is a significant and validated mediation effect to report (Preacher & Hayes, 2004). Cybersecurity has a significant mediation effect in the ICT-growth relationship as well as in the innovation-growth relationship.

Based on the above analysis, the reported results could be summarized as follows: (1) ICT is positively and significantly related to cybersecurity and growth competitiveness; (2) Cybersecurity is positively and significantly related to growth competitiveness; (3) Innovation is positively and significantly related to cybersecurity and growth competitiveness; and (4) the indirect relationship between ICT and growth competitiveness as well as between innovation and growth competitiveness through growth innovation is stronger than that of the direct one. The last point designates the mediating role that innovation plays in the ICT- growth relationship. It also indicates that cybersecurity is an important factor through which ICT and innovation may promote growth at the country level.

The Overall Model: The Triad Relationship and its Impact on Growth Competitiveness

The last step in this section presents the results of all the relationships involved in the model, thus incorporating cybersecurity in the growth framework. The results are very interesting and open a new window through which a nation's growth competitiveness level could be assessed, and probably predicted if the model proves to have a predictive validity and overall fit as will be discussed in a later section. A PLS-PM was conducted and the path coefficients were computed. Also, the bootstrapping function was run with a sample size of 316 and a number of samples equal to 1,000, as recommended by Chin (1998). The results are displayed in Table 40.

Table 40 Overall Model: PLS Analysis

Overall Model: ICT-Cybersecurity-Innovation--> Growth Competitiveness						
	Orig. Sample Path Coef.	Sample Mean	Standard Deviation	Std. Error	T Statistics ^a	P-value ^b
Cybersec -> Comp	0.8275	0.8458	0.0911	0.0911	9.086	1.12955E-15
ICT -> Comp	0.0471	0.038	0.0993	0.0993	0.4738	0.636407883
ICT -> Cybersec	0.5836	0.5822	0.0671	0.0671	8.6966	1.02965E-14
ICT -> Innov	0.8742	0.8743	0.0216	0.0216	40.5622	1.74664E-77
Innov -> Comp	0.0469	0.0376	0.0941	0.0941	0.4982	0.619153742
Innov -> Cybersec	0.3916	0.3931	0.0704	0.0704	5.5612	1.38358E-07

^a T-values were computed by Smart PLS with a bootstrapping function using N=136 and 1,000 samples.

^b P-value computed in Excel; highly significant at $p < 0.05$.

The above results convey a very important finding: cybersecurity is incorporated in the economic growth framework represented by a growth competitiveness model. Cybersecurity is positively and significantly related to growth competitiveness. Its potential impact on growth seems to be high, with ICT and innovation now becoming associated to growth more indirectly through cybersecurity measures than directly. ICT is positively and significantly related to innovation, and both ICT and innovation are positively and significantly related to cybersecurity. One may infer from this finding that there is a two-mediation effect in the ICT – growth relationship. ICT advancements contribute more to the economy when they are well diffused and used in effecting innovative practices and processes in a safe and secure cyberspace than they do by merely producing and selling them. In a similar vein, a creative idea, an innovative system resulting from a well-planned R&D effort, or a new method that emerged as a result of several experiments and tryouts, all these cannot be considered successful in attaining higher competitiveness ranks at the national level unless they contribute to quality enhancement and efficiency realization through putting them in proper use. Of course, this also requires a safe and secure cyberspace that protects

new knowledge and processes from intellectual property right violations, data theft, economic espionage, and other possible threats.

Examining the Model Relationships across Country Groups

Given the significant and positive relationship that cybersecurity proved to have with growth competitiveness, its strong and positive relationship with both ICT and innovation, the agreement and rank concordance between the cybersecurity measure on one hand and the other model major models, and the significant mediating effect that cybersecurity has on the ICT-growth and the innovation-growth relationships, one may argue that cybersecurity is a significant addition to the growth competitiveness model. An interesting question to be answered now is the research question addressing the possibility of change in the relationships across the various economic groups that countries belong to.

Running the model across the various country groups reveals very interesting and important results. As shown in Table 41, in high-income group countries, the mediating role played by cybersecurity is illustrated in both the relationships between innovation and growth competitiveness and between ICT and growth competitiveness.

Table 41 Model Relationships across country groups

High Income Group			
	Path Coefficient	T-Statistics	P-value
Cybersec -> Comp	0.7589	4.6009	9.58595E-06
ICT -> Comp	0.128	0.778	0.437930388
ICT -> Cybersec	0.5996	12.1995	1.54755E-23
ICT -> Innov	0.8386	34.7302	3.5535E-69
Innov -> Comp	-0.1516	1.0121	0.313300783
Innov -> Cybersec	0.3713	6.4994	1.43556E-09
Middle Income Group			
	Path Coefficient	T-Statistics	P-value
Cybersec -> Comp	0.7829	13.7714	1.68783E-27
ICT -> Comp	-0.0037	0.0539	0.957094518
ICT -> Cybersec	0.4129	5.8788	3.07522E-08
ICT -> Innov	0.6213	11.8851	9.72015E-23
Innov -> Comp	0.0912	1.197	0.233404291
Innov -> Cybersec	0.4586	6.066	1.24083E-08
Low Income Group			
	Path Coefficient	T-Statistics	P-value
Cybersec -> Comp	0.88	8.9113	3.05305E-15
ICT -> Comp	0.1248	1.5592	0.121290279
ICT -> Cybersec	0.6346	9.8419	1.4642E-17
ICT -> Innov	0.7979	11.0674	1.16247E-20
Innov -> Comp	-0.1337	2.1088	0.036808916
Innov -> Cybersec	0.3293	4.7524	5.07907E-06

The aforementioned discussion about the overall model applies well here. High-income group countries are majorly industrially developed with knowledge-based economies, where innovation diffusion is high, and where innovation in both new products and services is expected. In such countries, CII is considered the base of most CIs, and the means by which the CIs operate

and communicate with each other. Based on this, and in support of the above discussion, ICT is significantly related to cybersecurity.

At the same time, innovation is positively and significantly related to cybersecurity. Innovation's contribution to growth competitiveness in high-income (most probably the developed and knowledge-based economies) countries is supported by a safe and secure cyberspace marked by intellectual property protection and supportive R&D policies. The same discussion applies to middle-income countries, though the relationship between cybersecurity and competitiveness is higher in these countries.

Given the finding that ICT and innovation are significantly and positively related to cybersecurity and with cybersecurity significantly related to competitiveness, it might be safe to suggest that any ICT development in those countries especially those controlling CIs can lead to a leap frog effect in the economy. The same thing applies to innovation, which may depend a lot on imported inputs or knowledge spillovers, along with innovation programs and efforts. With a secured cyberspace, innovation and ICT developments can strongly influence growth competitiveness. Conversely speaking, if cybersecurity is low, the impact of these developments would be low. In low-income group countries, just like the two other groups, cybersecurity is positively and significantly related to growth. Interestingly, developments in innovation will impact growth with or without a secured cyberspace – though it is more significant with cybersecurity. These countries are sensitive and strongly responsive to any innovation that can contribute to more efficiency and a better quality of life. The examples mentioned concerning the use of ICT-based innovations in Kenya and Sierra Leone prove as good illustrations for this finding (World Bank, 2011).

Examining the Moderation Impact of Human Capital and Cyber Threats

In this study, human capital, represented by knowledge work, ICT use, and education expansion has a significant moderation effect on the relationship between (a) ICT development and growth competitiveness; (b) innovation and growth competitiveness; and (c) cybersecurity and growth competitiveness. The results of the human capital moderation effects are shown in Table are shown in Table 27. This is a quite interesting and important finding, as it highlights the importance of the human capital emphasized by education, ICT skills, and knowledge application in helping the transformation intended by ICT and innovations to take place. The moderation effect on ICT-growth relationship, innovation-growth relationship, and cybersecurity-growth relationship are all positive and significant. This is shown by the significant t-values of the relationships as well as the effect size of the moderation variable, as recommended by Chin (2010). Nevertheless, one can clearly notice that the highest moderation effect is on the ICT-growth relationship. This is probably because it's the cornerstone factor in the model, and if there is a high level of ICT-skilled human capital, then this may be translated into better ICT adoption and use, better allocation of innovative systems, and probably better awareness of cybersecurity measures and possible threats.

Moreover, besides human capital, another factor – negative in nature – was examined for its moderation impact on the above relationships. The factor examined is cyber exploits representing the cyber threat element. Surprisingly, cyber threats didn't have a moderating effect on any of the above relationships. This may be attributed to the possibility that cyber threats are a common concern across all countries and regions. It follows that all cyber threat levels should be taken into consideration to ensure a more secured cyberspace and better ICT and innovation contribution to growth (Ralston et al., 2007). The results of the cyber threats moderation effect results are also shown in Table 42.

Table 42 Moderation Impact of Human Capital

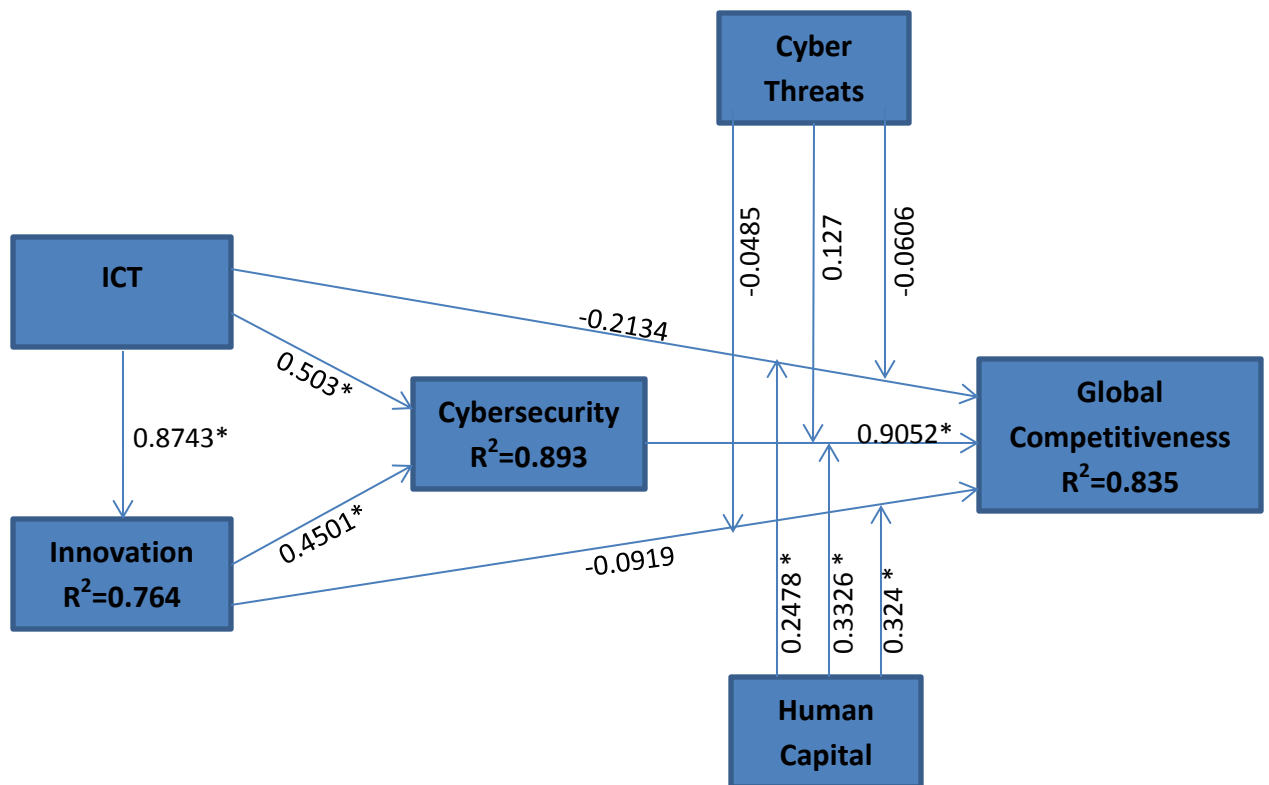
	Original Sample Path Coef	Sample Mean	Standard Deviation	Standard Error	T Statistics	p-value
CybThrt -> Comp	0.0672	0.0691	0.0424	0.0424	1.587	0.114852138
Cybersec -> Comp	0.9052	0.9156	0.0886	0.0886	10.222	1.61358E-18
Cybersec * CybThrt -> Comp	0.127	0.1352	0.1041	0.1041	1.2206	0.224365199
Cybersec * HD -> Comp	0.3326	0.3631	0.1283	0.0926	3.591	0.000460095
HD -> Comp	0.4943	0.4988	0.1227	0.1227	4.0279	9.34477E-05
ICT -> Comp	-0.2134	-0.2174	0.1187	0.1187	1.7979	0.074427729
ICT -> Cybersec	0.503	0.4995	0.0718	0.0718	7.0044	1.06478E-10
ICT -> Innov	0.8743	0.8732	0.0215	0.0215	40.6561	1.30863E-77
ICT * CybThrt -> Comp	-0.0606	-0.0668	0.0739	0.0739	0.8194	0.414002471
ICT * HD -> Comp	0.2478	0.2516	0.0549	0.0549	4.5182	1.3482E-05
Innov -> Comp	-0.0919	-0.1008	0.0844	0.0844	1.0896	0.277830528
Innov -> Cybersec	0.4501	0.4535	0.0748	0.0748	6.0141	1.59827E-08
Innov * CybThrt -> Comp	-0.0485	-0.05	0.0791	0.0791	0.6125	0.54123734
Innov * HD -> Comp	0.324	0.3273	0.0589	0.0589	5.498	1.85575E-07

Based on the above findings, the overall model, along with the R^2 of the various endogenous latent variables and the path coefficients of the relationships between all the latent variables are shown in Figure 15.

Model's Predictive Validity

PLS Path Modeling lacks a well identified global optimization criterion so that there are no universal fitting indexes to assess the goodness of fit of the model. Furthermore, PLS is a variance-based model strongly oriented toward prediction. Thus, model validation mainly focuses on the model predictive capability.

Figure 15 Overall Model with Path Coefficients and R^2



According to the PLS-PM structure, each part of the model needs to be validated: the measurement model, the structural model and the overall model. That is why PLS Path Modeling provides three different fit indexes: the communality index, the redundancy index and the goodness of fit (GoF) index (Vinzi et al., 2010). This is a global criterion of goodness of fit that has been proposed by Tenenhaus et al. (2004). Such an index has been developed in order to provide a single measure for the overall prediction performance of the model by considering the model performance in both the measurement and the structural model. . For this reason the GoF index is obtained as the geometric mean of the average communality index and the average R^2 value. This can be represented as follows: (Tenenhaus et al., 2004)

$$GoF = \sqrt{Com * \bar{R}^2}$$

The PLS results that report the multiple regression and the communality indices for all the model latent variables are shown below:

	R²	Communality
Comp	0.8	1
Cybersec	0.9	0.737
ICT	0.0	1
Innov	0.8	1
Average	0.831	0.934
GoF		0.9

From the table, one can derive the average R², equal to 0.831. The average communality is 0.934. As a result, a production function yields 0.78 (i.e. 0.831*0.934), and thus its square root is 0.9. As a rule of thumb, a GoF value of 0.90 or higher speaks in favor of the model (Tenenhaus et al., 2004). This implies that the study model has a goodness of fit.

Moreover, since PLS explicitly estimates the outer weights to form construct scores, modeling formative indicators is much less problematic. A construct with formative indicators (whether endogenous or exogenously modeled) must be connected to at least one other construct to yield meaningful information since the multiple regression weights that PLS estimates are intended to overlap with neighboring latent variable blocks. Otherwise, without some structural linkage, the weights would end up being identical. This differs from modeling reflective indicators where the weights are meant to form the single best score to maximally predict its own measures (i.e. the first principal component) (Chin, 2010).

The above-mentioned findings meet this requirement for predictive validity. The cybersecurity construct has positive and significant structural linkages with the growth

competitiveness construct as well as with the ICT and innovation constructs. In addition to this, and in line with the extant literature related to PLS and formative measures, the predictive validity of the model is assessed using the cross-validated communality scores, the cross-validated redundancy scores, and Stone–Geisser’s Q^2 index. The results generated by SmartPLS are shown below in Table 43 for the cross-validated redundancy index and in Table 44 for the cross-validated communality index (pertinent only to the cybersecurity measure).

Table 43 Cross-validated Redundancy Index (Q^2)

Total	SSO	SSE	1-SSE/SSO Redundancy Q^2
Comp	136	23.7934	0.825
Cybersec	408	146.4559	0.641
Innov	136	33.2434	0.7556

Table 44 Cross-validated Communality Index (Q^2)

Total	SSO	SSE	1-SSE/SSO Communality Q^2
Comp	136	136	0
Cybersec	408	206.8603	0.6495
ICT	136	136	0
Innov	136	136	0

In both tables, Q^2 is higher than the threshold 0.5. This indicates that the study model has adequate predictive validity in addition to having an acceptable goodness-of-fit.

Discussion

This study proposes and empirically tests a framework that introduces a new lens with which economic growth could be examined, namely the cybersecurity lens. Following an analytical approach based on triangulation, data analysis was performed using non-parametric and parametric

methods. To understand the characteristics of the countries included in the data set in terms of ICT development, innovation, and competitiveness levels along with terms that seem to be indicative of a country's cybersecurity level, the parametric and non-parametric tests were preceded by a descriptive data analysis. This showed the means and dispersion levels in the various country factors examined. The high level of dispersion in ICT law enforcement and secure communication lines may suggest that measures related to cybersecurity are not considered within the same level of urgency or viewed within the same level of threat impact perspective across the various countries.

Moreover, descriptive analysis showed higher and more favorable mean scores and lower variability scores within the higher income groups than within the lower income groups. This could be expected given that countries with higher income levels may have more resources, higher levels of ICT development, higher innovation diffusion levels, better competitiveness levels, more skilled human capital, and more effective security measures – at least at the technological level. The factor that showed the least level of mean differences and of variability across the groups is the national innovation factor. This could be attributed to the possibility that even countries with low innovation performance at the product and performance levels may still benefit from what other countries do through knowledge imitation, transfers, or knowledge spillovers (Fallah and Ibrahim, 2004).

Basic Model Relationships

The study's data analysis started with examining the basic relationship of ICT and innovation with growth competitiveness. In conformity with the New Economics Growth Theory, (Romer, 1990), the study findings showed that ICT is a driving force of growth competitiveness (OLS: $R^2 = 0.730$; $B=0.854$, $\text{sig} = 0.000$ and PLS: $R^2 = 0.730$; $B = 0.266$, and $\text{sig} = 0.000$). This implies that hypothesis H_1 is supported.

However, as emphasized by earlier and more recent literature, ICT contribution to economic growth is to a large extent a result of the way ICT is put into innovative use in the various economy sectors (finance, education, healthcare, government, and so on) rather than of the increase in GDP resulting from ICT production (Romer, 1994; Cortright, 2001; Avegrou, 2003; ITU, 2002; Infodev, 2007; Walsham, 2010; Brynjolfsson & Saunders, 2010; and World Bank, 2011). Fostering innovation and technology diffusion is a channel through which ICT can impact growth (Vu, 2011). This is logical given the fact that the world map has witnessed regions or countries where ICT has the potential to offer an innovative means through which poverty could be reduced (World Bank, 2011) by facilitating information access, enhancing social inclusion, making the markets more responsive and efficient, and providing rural areas with equal opportunities. For example, in a developing, low-income group country, like Kenya, farmers in remote villages use affordable mobile phones to access the latest information and updates about crop prices. Another example could be derived from a similar country, Sierra Leone, where migrant workers in cities no longer depend on high-cost intermediaries, but rather use mobile banking to place money transfers to relatives in their villages. In a developing, low-middle income group country, Sri Lanka, fishermen in rural areas depend on satellite mapping of fish colonies to know where to fish (World Bank, 2011). In more developed countries, developments in ICT could very much contribute to economic growth through enhancing process innovations, enabling the production of new ICT-based product lines and services, and providing innovative solutions to a vast array of economic and social problems in a cost-effective and timely manner. Examples may include smart-phones, social innovations such as e-health and distance learning, e-government, e-trade, e-agriculture (ISTAG, 2011; United Nations, 2012) and all sorts of e-activities and m-activities.

The above discussion supports the reported results in two ways. First, it illustrates the study findings, where ICT is positively and significantly related to innovation, and where innovation has a position and significant relationship with growth competitiveness. The partial mediating effect of innovation was adequately demonstrated by a significant Sobel-test (Sobel-test = 6.4813; p-value = 0.000) as well as by examining the OLS and PLS results, where building a relationship between innovation and growth competitiveness has rendered the relationship between ICT and growth competitiveness non-significant. With national innovation mediating the relationship between ICT and growth competitiveness, $B_{ICT} = 0.056$ with a sig. value = 0.104 according to OLS reported results and a $B_{ICT} = 0.179$ and a t-statistic = 1.551 (not significant) based on PLS results. Whereas innovation has a $B_{innov} = 3.485$ with a sig. value = 0.000 based on OLS, and a $B_{innov} = 0.7233$ with a significant t-statistic value = 7.1789. This implies that hypotheses H_2 , H_3 , and H_4 are supported.

Second, the above discussion draws attention to a very important question: does ICT development lead to higher innovation diffusion levels across all countries? The answer would be probably yes, but certainly not at similar levels. National innovation diffusion can never be merely an outcome of ICT development. It is rather a factor of several elements besides technology, including, but not confined to, research and development initiation, competent education system, knowledge workers, supportive regulatory system, open economy, and tax incentives (Ezell, 2010). This means that ICT developments will not yield similar levels of innovation enhancements, since not all countries provide innovation fostering environments, nor do all countries (even the technologically advanced and industrially developed) share the same sets of enablers and hindrances. This very much supports the lack of concordance in the country rankings of ICT and national innovation, as shown by a low and non-significant coefficient of concordance (Kendall's $W=0.013$; sig. = 0.217).

A similar result was expected regarding the rankings of both ICT and growth competitiveness. While ICT is positively related to economic growth, it can achieve a sustainable and optimal growth mainly through innovation. This translates to an expected concordance between innovation and growth competitiveness rankings and a possible discordance between ICT and growth competitiveness rankings. The study findings confirmed these expectations with concordant innovation and growth competitiveness rankings (Kendall's $W=0.594$, sig. = 0.000) and discordant ICT and growth competitiveness rankings (Kendall's $W = 0.003$, sig = 0.577).

In summary, the above discussion is in conformity with the New Economic Growth Model (Romer, 1990) and the extant literature supporting it (e.g., Brynjolfsson and Saunders, 2010; Cortright, 2001). In other words, ICT drives economic growth forward mainly through fostering innovation, and, to a lesser extent, through the contribution of ICT products and services to a country's GDP.

The Emergence of a New Composite Indicator: Cybersecurity

The reported findings pertinent to the formative measure 'Cybersecurity' suggest that it seems to conform to the guidelines pertinent to the construction of indexes or composite measures based on formative indicators. Examining the thin body of research literature concerning formative indicators reveals the crucial role of the following four elements in the construction of successful composite measures: (Diamantopoulos & Winklhofer, 2001).

1. Content Specification: This refers to the domain of content the composite measure is intended to capture. This is harder to determine than a latent variable with reflective indicators (Bagozzi, 1994). A critical condition here is to have a 'breadth of definition' (Nunnally & Bernstein, 1994) since all the construct facets should be included. In this study, the content domain of the 'cybersecurity' construct was specified as the technological, legal,

and international cooperation measures or initiatives that a country takes to achieve a secure cyberspace and protect its critical information infrastructure from cyber threats. Such a definition has been derived from the literature and from the reports provided by governments and international organizations. (e.g., ITU, 2010, 2011).

2. Indicator Specification: This is inextricably linked with the previous element. Here a census of indicators is required, and these indicators must capture the technological, legal and international cooperation aspects mentioned in the content domain.
3. Indicator Collinearity: An issue to be avoided in constructing a formative measure is multicollinearity. Because it is based on multiple regression, the sample size and the indicator inter-correlations can affect, to a large extent, the stability of the indicator coefficients. With this in mind, if indicator collinearity is observed, i.e. an indicator having an almost perfect linear correlation with the other indicators, then this indicator should be considered for exclusion from the construct (Bollen & Lennox, 1991).
4. External Validity: The nature of formative measurement (especially the multidimensionality of the construct) makes it inappropriate to assess the internal consistency of the indicators. According to Bagozzi (1994), the best approach is to examine how well the formative construct relates to measures of other variables.

Examining the above findings, one can find that the four elements conditions are met. To start with, the content domain of the ‘cybersecurity’ formative construct was defined and the content validity could be assumed based on theoretical support, literature, and seeking the input and opinion of experts in the area of cybercrime and national security. To start with, the construct indicators are theoretically valid based on the international relations related theories, namely national security and deterrence theories. They are also well supported by the general information

security theories that contend that information security is not only a function of technology, but also of other factors, such as people and processes / procedures (Kayworth & Whitten, 2012; Oppliger, 2007; Anderson et al., 2004; Saunders, 2003; and Olivier, 2001). In reference to the Deterrence theory, it was suggested that the technical aspects of communication infrastructure is essential for better cybersecurity levels, and that policies, strategies, and international law could be considered important deterrent factors (Schmitt, 2010; and Waltz, 1979). Within the framework of international relations theory, strategies like international cooperation (Cavelty, 2008, 2007), legislation (Newmann, 2002), and secure communication lines (Yan et al., 2012) are well considered, this implies that the content validity of the construct could be assumed, with support derived from theory and literature. Moreover, the content validity has been more supported by the inter-rater reliability that the findings showed based on Kendall's coefficient of concordance. With a relatively high and significant concordance coefficient (Kendall's $W = 0.760$, $\text{sig.} = 0.022$), one can assume that there is an overall agreement among the raters regarding the relevance and importance of the indicators included for forming up the cybersecurity measure.

Moreover, in line with the guidelines recommended by Diamantopoulos and Winklhofer (2001), a multicollinearity test for the cybersecurity indicators was conducted, and the results suggest that there does not seem to be a multicollinearity problem, with the maximum variance inflation (VIF) being 2.514, which is far below the common cut-off threshold of 10 (Hair et al., 2006; Kleinbaum et al., 1988).

Coming to the validity of the measure, it is worth noting that business research has typically tested formative indicator variable for their validity by referring to a theoretic rationale and expert judgment (Rossiter, 2002) as demonstrated above. This is because the methods used for examining a reflective measure, such as analyzing the values of average variance extracted (AVE) and

correlations, composite reliability, and factor loadings and cross loadings are not appropriate (Chin, 2010). In fact, formative measures are constructed with an expected convergent validity (Chin, 2010), while reflective measures are concerned with unidimensionality (Kim, 2011), rendering the validity and reliability measures used for reflective measurement models inappropriate for formative measures.

The recommendation suggested by Chin (2010) was applied, where a redundancy model is specified based on the original formative construct indicators. The resulting path between the two modes is 0.876, suggesting strong convergence and implying an adequate coverage of the concepts in the formative set. In addition, the communality index and redundancy index were generated leading to GoF (goodness-of-fit) of 0.892. With GoF values ranging from 0 to 1, higher values indicate better validity. Also, the indicator weights for the formative variable were all significant (P-value <0.05). The above discussion of the results related to the cybersecurity formative construct indicates a measure with adequate validity – at the theoretical and the statistical levels.

Cybersecurity Incorporation in the Basic Model

The results suggested that the cybersecurity measure seems to be a valid formative measure. Bearing this in mind, the variable was introduced to the basic growth competitiveness model to examine its relationship with the other latent variables and to examine its predictive ability in forecasting the competitiveness levels of countries.

Interestingly enough, the findings reported indicate that this new formative measure is positively and significantly related to the ICT and national innovation, and has a very strong and positive relationship with growth competitiveness. As a matter of fact, while ICT has a significant and positive relationship with cybersecurity ($B_{ICT} = 0.584$, sig.t-value = 8.9893) and innovation has a similar relationship with cybersecurity ($B_{innovation} = 0.392$, sig. t-value = 5.6494), cybersecurity has

a positive and significant relationship with competitiveness ($B_{\text{cybersecurity}} = 0.8275$, and significant t -value = 8.8293). Introducing the cybersecurity measure to the model has diminished the potential effect that both ICT and innovation have in explaining the variance of growth competitiveness and predicting its scores. The results suggest that cybersecurity is a mediator in the relationship between innovation and growth competitiveness (Sobel effect = 8.9265, sig = 0.000) and a second mediator besides innovation in the relationship between ICT and growth competitiveness (Sobel effect = 8.0380, sig. = 0.000).

The impact of ICT on cybersecurity could be interpreted from two perspectives. First, the ‘technology’ factor is as crucial component of any security system. Secure communication lines are considered one of the dimensions forming the cybersecurity composite construct. Second, ICT is considered the main critical information infrastructure that other critical infrastructure (CI) depend upon. Accordingly, the smooth operation and functioning of the various CIs as well as their contribution to growth competitiveness hinge upon a secure CII. This may provide a logical interpretation of the mediation effect that cybersecurity has in the relationship between ICT and growth competitiveness. The result also concur with previous literature suggesting that CII protection is crucial for the operations of CIs like banking, energy, healthcare, and in turn to their contribution to economic growth (e.g., Merabti et al., 2011; Lopez et al., 2007; and Nickolov, 2005).

Within the same vein, the impact of innovation on growth competitiveness is also mediated by cybersecurity. This is also logical and considered an important finding in the study. A secure cyberspace depends to a large extent on innovative security products and processes that take into consideration possible cyber threats and thus attempt to reduce vulnerabilities in the system as much as possible. At the same time, innovation cannot contribute optimally to economic growth or

competitiveness if the innovation inputs or outputs in terms of new knowledge, processes, or systems are vulnerable to cyber theft, compromising activities, or cyber espionage. It follows that emphasizing intellectual property, an outcome of optimal cybersecurity measures, as well as secure R&D practices can speed up the wheels of innovation, proliferate innovation processes that would contribute better to secure critical information infrastructure and would thus foster growth competitiveness. This discussion falls in line with previous research that analyzes the role that intellectual property and R&D efforts play in enhancing innovation processes in countries, and accordingly, in boosting economic growth (Kumar, 2003). This gives support to hypotheses H5, H6, and H7.

In addition, the findings reported reveal a very important point: in the relationship between each of innovation and ICT with growth competitiveness, cybersecurity is a strong mediator. The mediation effect of this newly operationalized factor brings into the table a new lens with which growth competitiveness could be examined and assessed. The modern economy has become increasingly reliant on the reliability, safety, availability, and security of many interrelated ICT-based critical infrastructures (Brammer, 2011; Anderson and Fuloria, 2011; and Nickolov, 2005). The negative impact that cyber attacks may have on a nation's economy cannot be underestimated, thus presenting cybersecurity as a major element in the growth competitiveness framework. The above discussion serves as a supporting base for hypotheses: H7a and H7b.

Delving deeper in the results, one finds that cybersecurity is relatively a common concern to all countries. Cyberspace is open and no country has its own cyberspace borders. Running the model across the various country groups reveals very interesting and important results. In high-income group countries, the mediating role played by cybersecurity is illustrated in both the relationships between innovation and growth competitiveness and between ICT and growth

competitiveness. The aforementioned discussion about the overall model applies well here. High income group countries are majorly industrially developed with knowledge-based economic, where innovation diffusion is high, and where innovation in both new products and services is expected. In such countries, CII is considered the base of most CIs, and the means with which the CIs operate and communicate with each other. Based on this, and in support of the above discussion, ICT is significantly related to cybersecurity.

At the same time, innovation is positively and significantly related to cybersecurity. Innovation's contribution to growth competitiveness in high-income (most probably the developed and knowledge-based economies) countries is supported by a safe and secure cyberspace marked by intellectual property protection and supportive R&D policies. The same discussion applies to middle-income countries, though the relationship between cybersecurity and competitiveness is higher in these countries.

Given the finding that ICT and innovation are significantly and positively related to cybersecurity and with cybersecurity significantly related to competitiveness, it might be safe to suggest that any ICT development in those countries especially those controlling CIs can lead to a leap frog effect in the economy. The same thing applies to innovation, which might depend a lot on imported inputs or knowledge spillovers, along with innovation programs and efforts. With a secured cyberspace, innovation and ICT developments can strongly influence growth competitiveness. Conversely speaking, if cybersecurity is low, the impact of these developments would be low. In low-income group countries, just like the two other groups, cybersecurity is positively and significantly related to growth. Interestingly, developments in innovation will impact growth with and without a secured cyberspace – though it is more significant with cybersecurity. These countries are sensitive and strongly responsive to any innovation that can contribute to more

efficiency and better quality of life. The examples mentioned about the use of ICT-based innovations in Kenya and Sierra Leone prove as good illustration for this finding (World Bank, 2011).

The Moderation Effect of Complementarity Variables in the ICT-Innovation-Cybersecurity Relationships with Growth Competitiveness

In conformity to the complementarity theory proposition, the relationships between each of ICT, innovation, and cybersecurity with growth competitiveness was also examined taking into consideration a factor that has been regarded as a complementarity factor in many studies at the organizational and country levels namely the human capital factor (e.g., Lucas, 1991; Adam & Urquhart, 2009; Brynjolfsson & Saunders, 2010). In fact, recent theoretical contributions to the growth literature emphasize the role of human capital in the process of economic growth. Several research works seem to indicate that educational expansion does contribute to output growth (Schutt, 2004). There also seems to be grounds, for thinking that human capital has a substantial impact on technological developments, possibly through improving a country's capacity to adopt new technologies, introduce new innovations, diffuse innovations, and make use of knowledge to contribute to better levels of economic growth (Lucas, 1991).

The study findings support what the literature proposed in terms of the important role that human capital plays in translating technological developments and innovations to effective growth catalysts. In this study, human capital represented by knowledge work, ICT use, and education expansion has a significant moderation effect on the relationship between (a) ICT development and growth competitiveness; (b) innovation and growth competitiveness; and (c) cybersecurity and growth competitiveness. This is a quite interesting and important finding. The moderation effect on ICT-growth relationship could be attributed to the fact that educated people with ICT skills can contribute to optimal use of ICT. At the same time, human capital can make a big difference in the

enhancement, adoption, and proper use of innovations. Of course, without adoption and proper diffusion of new ICT-based products and services, innovation's contribution to economic growth would be minimal, if any (Brynjolfsson & Saunders, 2010). Finally, the moderation effect of human capital on the relationship between cybersecurity and growth competitiveness is a logical and important finding. In fact, this finding and discussion conforms to international organizations' reports suggesting the strategic role that knowledge workers with ICT skills – skills related to and needed in today's information intensive societies – is increasingly growing in importance and impact (Lanvin & Passman, 2008). This leads one to conclude that the study findings support hypotheses H8a, H8b, and H8c.

Besides human capital, another factor – negative in nature – was examined for its moderation impact on the above relationships. The factor examined is cyber exploits representing the cyber threat element. Surprisingly, cyber threats didn't have a moderating effect on any of the above relationships. This may be attributed to the possibility that cyber threats are a common concern across all countries and regions. It follows that all cyber threat levels should be taken into consideration to ensure a more secured cyberspace and better ICT and innovation contribution to growth (Ralston et al., 2007). This also implies that hypotheses H9a, H9b, and H9c are not supported by the study data set and findings.

With all the findings in mind, the study has provided an answer to all the posed questions. In addition, as shown in Table 45, all the hypotheses except those related to cyber threats were supported by the data set used and the analysis done.

Table 45 Support of the Study Hypotheses

Hypothesis	Test used			Hypothesis Supported (Yes/No)
	OLS	PLS	Rank Corr.	
ICT and Innovation Relationship with Economic Growth				
H1: ICT is positively related to economic growth.	✓	✓	✓	YES
H2: Innovation is positively related to economic growth.	✓	✓	✓	YES
H4: Innovation plays a mediating role in the ICT – Growth relationship.	✓	✓	NA	YES
ICT-Innovation Relationship				
H3: ICT is positively related to innovation.	✓	✓	✓	YES
ICT-Cybersecurity and Innovation-Cybersecurity Relationship				
H5: ICT development is positively related to cybersecurity strategies.	✓	✓	✓	YES
H6: Innovation is positively related to cybersecurity strategies.	✓	✓	✓	YES
Cybersecurity and Economic Growth				
H7: Cybersecurity Initiatives is positively related to economic growth.	✓	✓	✓	YES
H7a: Cybersecurity plays a mediating role in the ICT – growth relationship.	✓	✓	NA	YES
H7b: Cybersecurity plays a mediating role in the innovation – growth relationship.	✓	✓	NA	YES
Human Capital				
H8a: Human Capital has a moderating effect on the innovation-growth relationship.	✓	✓	NA	YES
H8b: Human Capital has a moderating effect on the cybersecurity-growth relationship.	✓	✓	NA	YES
H8c: Human Capital has a moderating effect on the ICT-growth relationship.	✓	✓	NA	YES
Cyber Threats				
H9a: Cyber threats have a moderating negative effect on the innovation-growth relationship.	✓	✓	NA	NO
H9b: Cyber threats have a moderating negative effect on the cybersecurity-growth relationship.	✓	✓	NA	NO
H9c: Cyber threats have a moderating negative effect on the ICT-growth relationship.	✓	✓	NA	NO

Moreover, the prediction validity of the model has been assessed using the guidelines set by Diamantopoulos and Winklhofer (2001) and Chin (2010). To recall, In the case of formative indicators, there is no emphasis on predicting its own measures. Rather, the objective is to obtain weights that create the best variate or construct score so that it maximally correlates with the neighboring constructs. Thus, PLS-based formative indicators are inwards directed to maximize the structural portion of the model.

In addition, besides looking at the magnitude of the R^2 as a criterion for predictive relevance, we can also apply the predictive sample reuse technique as developed by Stone (1974) and Geisser (1975). This technique represents a synthesis of cross validation and function fitting with the perspective that the prediction of observables or potential observables is of much greater relevance than the estimation of what are often artificial construct-parameters (Geisser 1975, p. 320). The sample reuse technique has been argued as fitting the soft modeling approach of PLS like “hand in glove” (Wold 1982, p. 30).

For the model depicted in Figure 15, the blindfolding process in SmartPLS showed a cross-validated a cross-validated communality Q^2 of 0.6495 and a cross-validated redundancy Q^2 of 0.6410 for cybersecurity and a cross validated redundancy Q^2 of 0.8250 and 0.7556 for growth competitiveness and innovation endogenous latent constructs respectively. In general, a cross-validated redundancy Q^2 above 0.5 is indicative of a predictive model (Chin, 2010). These results, along with the global criterion of goodness of fit (i.e. GoF index) proposed by Tenenhaus et al. (2004) that had a value of 0.892 add to the confidence established in the model as a valid model for prediction with an adequate goodness-of fit.

This Chapter presented the findings and results generated by the data analysis methods – both parametric and non-parametric used in the study. The results reported are satisfactory, well

validated, and supported by a sound theoretical framework and a rich extant body of literature. This leaves the researcher with an eye to the future where new research horizons have been opened and see, to be challenging, yet possible, by the results generated from this current study. With this in mind, Chapter V will present a summary of the findings, draw some conclusions in light of the study contributions, explain the study implications, discuss the study limitations, suggest few recommendations, and set up a road map and directions for future research.

CHAPTER V

CONCLUSION, IMPLICATIONS, AND RECOMMENDATIONS

The purpose of this study was to examine the potential causal impact that ICT, innovation, and cybersecurity may have on the growth competitiveness of nations. The study achieved this objective by proposing and testing a model that:

1. Examined the relationship among ICT, innovation, and growth competitiveness;
2. Developed a formative construct to represent national level cybersecurity initiatives;
3. Incorporated the construct into the growth model and examined the ICT-innovation-growth competitiveness relationships with the cybersecurity lens; and
4. Identified the role that human capital plays in the ICT-innovation-cybersecurity relationship with growth competitiveness.

Chapter IV presented the findings of the study, analyzed them within the scope of the proposed relationships and stated hypotheses, and discussed the results in light of the theories used and the extant literature. The results of the analysis presented therein illustrated the strength of the proposed model as well as its predictive validity. This chapter will provide a summary of the results presented in the last chapter, draw conclusions, discuss the implications of the study, present the limitations, and suggest corresponding recommendations. Finally, possible directions for future research will be proposed.

However, before writing down the study conclusion, it is interesting to assimilate the findings presented and discussed in Chapter IV bearing in mind the literature synthesized and analyzed in Chapter II. Reflecting upon the extant literature pertinent to this study, one can find several trends in relationships that were examined and supported, identify theories that were confirmed, and tap into areas of development that are worth exploring and examining.

To start with, a well-established trend in earlier as well as more recent research involves studying the relationship between technology and economic growth. The extant literature since Solow (1956) to Romer (1990) to Argyrous (2001) and Brynjolfsson and Saunders (2010) have supported the direct relationship between these two crucial constructs. Recent research attributed this kind of relationship between ICT and economic growth to “virtuous cycles” (Argyrous, 2001). High ICT investments have thus been shown to be accompanied by economic growth resulting from improvements in productivity, organizational operations and processes, and then observing subsequent growing returns that are crucial to promoting economic growth. The results reported in Chapter IV support this relationship, as ICT has a positive and significant relationship with growth competitiveness.

Another trend identified in the literature involves studying the relationship between innovation and economic growth. Previous research supported a positive relationship between innovation trends and economic growth (e.g., Sener & Saridogan, 2011, LeBel, 2008; and Rosenberg, 2004). The role that knowledge, new ideas, and creativity play in enabling sustainable growth and economic development cannot be underestimated. This is why ICT-based innovation has been recognized as an important component in the economic growth model. The study findings reported in Chapter IV have also supported this relationship.

Moreover, a prevailing trend in the literature is the argument that the ICT contribution to economic growth is best achieved through innovation. In other words, unless ICT is well adopted and properly used to help generate new products, services, and more effective processes, a country cannot really reap its benefits (e.g., Brynjolfsson & Saunders, 2010; Trajtenberg, 2005). Brynjolfsson & Saunders (2010) considered innovation a major and necessary complementary factor to ICT, without which ICT can never contribute effectively to sustainable growth. This has been a major extension to the economic growth model as supported by the complementarity theory (Milgrom & Roberts, 1990). This trend has also been supported in this study, where innovation proved to have a significant mediation effect in the relationship between ICT and growth competitiveness.

In addition to this, recognizing the importance of having skilled and educated human capital to make better use of technology and to find ways for better diffusion and use of innovations in organizations or nations has been a major trend in research since Lucas (1988). The presence of an effective and well empowered IT workforce signifies a proactive approach to creating opportunities by deploying ICT and innovations to serve the business and community needs in various countries (Bresnahan et al., 2002). Again, drawing on the complementarity theory (Milgrom & Roberts, 1990), the study findings in Chapter IV have supported the significant moderation effect that human capital plays in the relationship between both ICT and innovation as they relate to growth competitiveness.

In addition to the above-mentioned trends, previous research in the form of conceptual papers, international organizations' reports, and governments' documents from so many countries across the globe revealed an important area of research to be tapped and developed; namely, that of cybersecurity. The reader can hardly probe into these articles without finding

strong arguments relating to the impact that cybersecurity may have on the national as well as the economic security of nations. This study represents a pioneering attempt to investigate this impact from theoretical and empirical points of view. The findings reported in Chapter IV strongly supported the mediation role that cybersecurity plays in the relationship between ICT and economic growth as well as in the relationship between innovation and economic growth. Even with this new factor, human capital showed an additional strong moderation effect, that is, between cybersecurity and growth competitiveness.

In conclusion to the above discussion, and based on the literature review presented in Chapter II, this confirms the contributing factor of this study. The supported extension for the economic growth model solidifies the reason for and contribution of this research. Based on outcomes, not only is the body of knowledge richer with these results, but it is also more solidified.

Summary and Conclusions

The study stemmed from a motivation to explore and examine the relationship between a concept that is emerging as a cornerstone of economic prosperity (The White House, 2011) and the factors that have been considered major players on the stage of economic growth for a long time. The study followed McArthur and Sachs' (2002) approach in embracing growth competitiveness as an estimate of economic growth. It also corroborates with the recent approach that in a digitized, knowledge-based economy, the contribution of innovation to economic growth is catalyzed by knowledge workers and ICT investments rather than by mere investments in R&D and in innovation (Ernst, 2006).

Based on theory and data analysis triangulation, this study proposed and tested a new perspective with which nations' growth could be examined and assessed. The findings reported

in Chapter IV revealed important and significant relationships among the various factors incorporated in the model. Today's economy is a knowledge economy, and there are main cornerstones that should be considered in order for it to achieve optimal levels of growth and development. The study's data analysis showed a positive and significant relationship between each of the economic growth key factors: ICT/innovation and growth competitiveness. The results, however, suggest that the growth competitiveness variance is better explained as an indirect rather than a direct effect of ICT. Mediated by innovation, ICT has the potential to play a key role in driving the economic wheels forward and in fostering better competitiveness at the national and global levels.

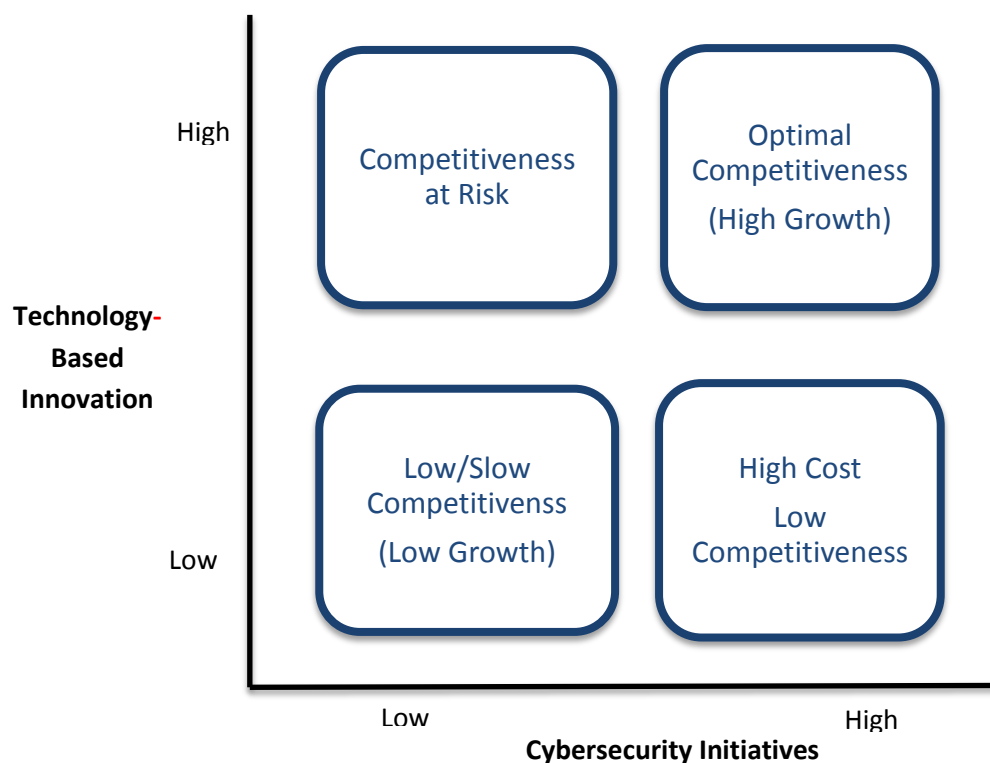
Nations' economies are mainly dependent on their critical infrastructures (CIs). It follows that these economies are as good as their CIs (Tiirma-Klaar, 2011). Being interdependent, the failure of one may trigger other failures because of the domino effect. What adds to the problem is the fact that the CI interdependence sometimes transcends national borders. This poses a probability that the lack of cyber safety or resilience will probably generate adverse effects on others (Cavelty, 2008). This underscores the importance of incorporating CI resilience and security within economic growth or growth competitiveness frameworks.

It follows that one of the major conclusions of the study is that the growth of a powerful, ubiquitous, cyber infrastructure (computing facilities, communication networks, software, and other devices enabling information applications) has propelled innovation as being of enormous value to the national and global economy and society. The mélange of software, hardware, and digital data now comprise a critical infrastructure upon which the smooth functioning of essential sectors such as defense, banking, utilities, transportation, and health depend. While providing dramatic societal benefits, this profound and rich mix has also created a major and growing

complex of risks for many nations around the world. Based on this, the results suggest that while it is true that ICT and innovation are positively and strongly related to global competitiveness, this relationship is strongly mediated by cybersecurity. With this in mind, the study suggests that the relationship between ICT and innovation on one hand and global competitiveness on the other should take into consideration the cybersecurity measures. Such a relationship could be translated into a taxonomy grid (Figure 16) analyzing the relationship between the basic elements of Romer's (1990) economic growth model (technology and innovation) and cybersecurity.

The four cells of the grid show the outcome for each combination pair of levels of both technology-based innovation (TBI) and cybersecurity initiatives, with the outcome representing the growth competitiveness level resulting from such combinations.

Figure 16 TBI-Cybersecurity-Competitiveness Grid



Examining the evolution of the economic growth model throughout the years that embodies the various sets of factors contributing to increased productivity and economic welfare (such as the unconventional factors ‘technology and innovation’), one wonders about the possibility of expanding the framework to include another factor, the lack of which may have a devastating effect on a nation’s economy; namely, cybersecurity. While previous research suggested the importance of including certain complementarity factors such as human capital (Brynjolfsson & Saunders, 2010) in analyzing the technology and innovation contribution to a country’s economic growth, this study takes it one further step and proposes cybersecurity as a pivotal factor in the growth model.

Considering cyberspace as a major environmental element within which ICT, innovation, and the human element interact, the relationship among ICTs, innovation, and the environment is often examined in terms of three distinct kinds of effects: (World Economic Forum, 2011)¹⁴

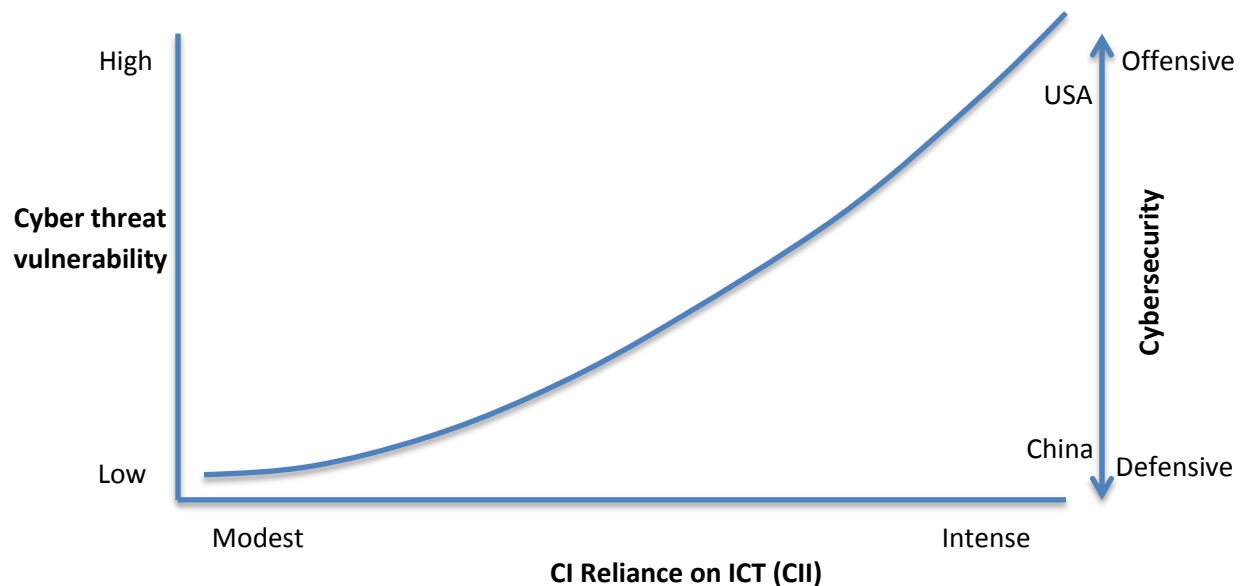
- First-order or direct effects, which arise from the design, production, distribution, maintenance and disposal of ICT goods and services by the ICT industry.
- Second-order or indirect effects, which arise from the application and use of ICTs throughout the economy and society, in government and public institutions, and in the research and academic communities.
- Third-order or systemic and universal effects, which arise from changes in economic and social structures and behavior enabled by the availability, accessibility, application, and use of ICT goods and services.

¹⁴ The Forum for the Future proposed an analytic framework based on a distinction between the first-, second- and third-order effects of ICTs in *The Impact of ICT on Sustainable Development*, European Information Technology Observatory, 2002.

ICT-enabled general effects could dramatically impact economic and social parameters such as the attitudes, expectations and behavior of individuals as consumers, citizens and members of communities; the demand and supply of goods and services; organizational structures; production, distribution and service processes; and governance in the private and public sectors. From this perspective, the large-scale economic and social choices made by individuals, organizations and communities concerning how to use ICTs to change their structures and behaviors will play a potentially significant role in determining whether there is a successful global response to the challenge of achieving sustainable development (WEF, 2011).

Bearing the relationships set by the World Economic Forum (2011) in mind, it follows that society has become dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defense. “The globally-interconnected digital information and communications infrastructure known as ‘cyberspace’ underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security” (White House, 2009). Some countries, including the U.S., are especially vulnerable to cyber insecurity because they depend on cyber systems more heavily than most other nations. The critical information infrastructures (CII) are all ICT-based, which means that the critical infrastructures will not function if a major attack on the CII took place. But cyber insecurity is a worldwide problem, potentially affecting all cyber systems and their dependent infrastructure. Based on this, and in reference to the results reported in Chapter IV, it appears that nations with critical infrastructures that are heavily dependent a lot on ICT (i.e., CII) are more vulnerable to cyber threats. This is illustrated visually in Figure 17.

Figure 17 CII Reliance on ICT vs. Cyber Threat Vulnerability--Defensive vs. Offensive Strategies



Cyber insecurity can result from the vulnerabilities of cyber systems, including flaws or weaknesses in both hardware and software, and from the conduct of nations, groups, and individuals with access to them. It takes the forms of cyber warfare, espionage, crime, attacks on cyber infrastructure, and exploitation of cyber systems. The cyber security measures that a nation develops or adopts to prevent a cyber threat or to alleviate its impact are vast, but in general may range from mainly defensive (e.g., China) to mainly offensive (e.g., US).

Still another major conclusion of the study is the significant role that human capital plays in influencing the relationship between ICT, innovation, and cybersecurity on one hand, and global competitiveness on the other. As discussed by Burnham (2009), differences in economic growth or income levels will emanate from differences in measurable inputs such as investment in R&D or in human capital, with the underlying assumption that the technology available is a common factor for all countries (Burnham, 2009). According to the author, a critical weakness in this assumption is the failure to realize that technology availability doesn't always imply technology use and diffusion. Earlier researchers such as North (1990) and Landes (1998)

highlighted the failure of previous economic growth models to incorporate new technology adoption as key in assessing a country's economic performance. This implies that the contribution of ICT to growth competitiveness will be realized only through effective use of ICT in a manner that would promote efficiency, effectiveness, and a better quality of life in general. Regarding innovation, it can be considered a very important resource at the organizational and national levels. Most of this resource is tacit, and only a part of the knowledge pertinent to it is codified (Archibugi & Michie, 1998; Fisher, 2003). While the latter part can be easily transmitted with communication technologies--although it still needs to be understood and used--the former part can only be communicated through experience, which brings human capital into the frame of analysis (Fratesi & Senn, 2009). Finally, cybersecurity measures cannot be viewed as complete or effective without the human capacity factor. ITU (2010) has considered this element of cybersecurity measures as a critical success factor, without which cybersecurity cannot be achieved. Based on this, the study finding related to the moderation effect that human capital plays in the relationship between each of the model's basic elements and growth competitiveness is quite important from the complementarity theory perspective as well as from the perspective of the international organizations and governments that are emphasizing the unsubstitutable role of human capital.

Research Implications and Contributions

Drawing on the study findings, ITU initiatives (ITU, 2011), and cybersecurity reports generated by the governments of several countries, one can draw several implications at the theoretical, analytical, and pragmatic levels. At the theoretical level, the study seems to contribute well to the economic growth theory. The theory has witnessed a lot of important evolutions throughout the years, with technology and innovation incorporation in its framework

being the most important type of evolution. Nowadays, however, cybersecurity analysts, national leaders, and organizations are associating economic security to the security of the critical infrastructures that the economy is based upon. Based on this, cyberspace safety/security can never be an afterthought. It is a major element in any kind of economic development strategy or discussion. Bearing this in mind, a major contribution of the study is expanding the economic growth model (Romer, 1990), and allowing for growth competitiveness to be assessed and examined through a new lens – that of cybersecurity.

At the same level, a major contribution of this study is the introduction of a cybersecurity formative construct. Using country-level data and rigorous analysis techniques, the construct was developed and tested based on a sound theoretical framework, reference to experts in the field, and the deployment of a variety of parametric and non-parametric techniques. This cybersecurity formative construct may pave the way for an international and systemic cybersecurity index to be developed. Such an index is believed to help gauge nations' performance in terms of ICT, innovation, and cybersecurity initiatives. At the same time, it can help guide the policy setting, legislation process, and cybersecurity technology design toward formulating optimal solutions for:

- enhancing the contribution of ICT to a nation's growth competitiveness level;
- speeding up the wheels of innovation, and ensuring optimal levels of innovation adoption and use; and
- ensuring optimal levels of cybersecurity for efficient and reliable operations in the cyberspace.

Another theoretical implication is pertinent to the finding that the relationship between each of ICT and innovation with cybersecurity is stronger than that with growth competitiveness,

implying that cybersecurity is a main element in the picture. If a country has advanced ICT products and ICT-based critical infrastructures and services, unless these critical assets are well secured and protected, the economic security will be at risk. In a similar vein, a country with cyber violations related to intellectual properties and possible cyber threats in the form of information espionage and data theft will have a low contribution from innovation to the nation's economic growth or competitiveness factor. Finally, emphasizing the role that human capital plays in innovation, ICT advancements, and cybersecurity initiatives also bears an important contribution on the research streams of ICT, innovation, information security, and cybersecurity.

In addition to the theoretical implications and contributions, the study has been based on a rigorous approach based on effect size estimation, power analysis, and triangulation. While these approaches are strongly recommended (e.g., Cohen, 1968, 1988; Straub, 1989) to enhance the validity of the study and the significance of the results, they are rarely applied in social science research. The effect size and the power analysis in this study showed a high power factor (>0.8), thus suggesting study validity and robustness of results.

On the pragmatic level, the implications can be viewed from both the national and the international perspectives. At the national level, a cyber security joint effort bringing together top business, government, and academic experts to frame the key issues for cooperation on cyber threats should be established. These can form a task force to lay the ground for a framework for international cooperation on cyber security—an international cybersecurity regime. As mentioned earlier, ITU considers international cooperation as a pivotal factor in its cybersecurity agenda (ITU, 2011). Moreover, representatives from industry, academia, and government should work jointly to examine gaps in cyber defense to develop new approaches to foster increased resilience to major cyber attacks by developing and strengthening the relationships among cyber

threat analysis and response leaders, organizations and communities, both formal and informal, in these sectors. Cyber disaster response will require new and robust connections between organizations and individuals focusing on cyber security in government, universities, and industry. These connections will most probably extend and strengthen the cyber disaster response communication network giving the country a new capacity to address a large-scale cyber attack. Another implication at the national level would be to increase the cybersecurity awareness level of people at the individual and community levels, of those leading and working in business and government organizations, and those operating in the various public and private sectors. Cybersecurity awareness programs are recommended to be initiated by the various nations' governments as this could be an incentive for all the entities to design and implement optimal cybersecurity measures. Finally, academia can contribute to the enhancement of cybersecurity knowledge and practices through the development of interdisciplinary graduate training programs to prepare the next generation of university researchers to address critical challenges in cybersecurity for industry and government. The program, if properly designed, can be anticipated to bring together faculty in computer science, information systems, information security, political science, international relations, economics, public policy, and law, together with industry and government experts, to train students to examine gaps in cyber defense and develop new approaches to thwart and defeat cybercrime and attacks. In fact, it is vital to have business leaders that are taught to think beyond traditional business risks to ensure that there is greater collaboration between business and IT security to ensure businesses are ready to mitigate cyber risks as well as other risks. As a matter of fact, no country in the world has enough resources. Accordingly, every government and company should be doing more to ensure more people have the basic and specialist skills needed. Alongside these skills, basic training should

include ethics in the cyber world, as this might help in having a better and safer cyber world (Ashford, 2013).

At the international level, international cooperation should manifest itself in serious efforts made by governments to establish a common global understanding that cyber weapons are extremely dangerous and have an agreement to not use them. For example, governments may sign a treaty against the use of cyber weapons in the same way as they have done against nuclear, biological and chemical weapons (Ashford, 2013). This implies that there could be an opportunity opened by such agreements to have greater cooperation among the various national intelligence agencies to share information about threats and attackers in cyberspace (The Economist, 2013).

Moreover, gaining an understanding of how to defend cyberspace in a nation needs an understanding of how ICT (information communication technology) is being used and how it is expected to be used in that particular nation. It also needs to take into account the level of innovation in the country. Outlining the perceived benefits from ICT deployment and innovation diffusion--in both developing and developed nations--helps set the motivation for formulating policies and implementing cyberspace defense. Protecting these benefits from cyber attackers should be one of the objectives for a national strategy and so it is essential to know what they are. This understanding of the motivation is beneficial because it gives an objective to the cyberspace defense strategy. It defines what is to be protected and thus it is possible to target the defense toward particulars instead of generalities. In the future, it will also be a way to evaluate performance by determining if the benefits were protected.

The potential utility of international cybersecurity agreements deserves to be carefully examined. This is because the crucial role that confidence and security play is one of the main

pillars in building an inclusive, secure and global information society and is something that is well recognized worldwide (ITU, 2012). The global nature of the legal, technical and national policy challenges related to cybersecurity can only be properly addressed through a strategy that takes into account the role to be played by all relevant stakeholders in a framework of international cooperation.

Attempts to address these challenges at the national and regional levels are not sufficient due to the fact that the information society has no definite geographical borders.

International agreements covering other transnational activities, including armed conflict, communications, air and sea transportation, health, agriculture, and commerce, among other areas, should be widely adopted by nations to enhance safety and efficiency through processes that could well be useful in regulating cyber activities. Transnational agreements that contribute to cybersecurity will, however, only be possible if they take into account the substantial differences that exist between activities regulated by established international regimes and cyber systems. Many nations will be unprepared at this time to agree to limit their control of cyber activities they regard as essential to their national security interests. International agreements will also be impossible where irreconcilable differences in policies exist among nations, particularly regarding political uses of the Internet, privacy, and human rights (Sofaer et al., 2009). But, while these factors limit the potential scope and utility of international cyber-security agreements, they do allow for international cooperation on many issues that could prove beneficial.

While thinking of international cooperation as a means toward achieving cybersecurity, it is important to keep in mind that the potential for improving cybersecurity through international agreements can best be realized through a program that identifies: the activities likely to be

subjects of such agreements and those that are not. The measures include the following items. The measures likely to be used by parties to improve cybersecurity in each area of activity appropriate for international cooperation. The forms developed that any international body may utilize or establish for this purpose. The authority such a body would be assigned and also the basis upon which its activities would be governed. International agreements negotiated on the basis of these practical premises could help to create a more secure cyber environment through measures that go beyond conventional forms of deterrence.

Another implication has to do with ICT laws, i.e., the legal aspect of information technology use and deployment. Cybercriminals are already exploiting vulnerabilities and loopholes in national and regional legislation as they shift their operations to countries where appropriate and enforceable laws are not yet in place, and can, with almost total liberty, even launch attacks even on victims in countries that do have laws in place. When several hijacked computers and networks that have been compromised and are spread over many countries are used to launch cyber attacks using a decentralized model (based on peer-to-peer arrangements), no national or regional legal framework can adequately deal with such a problem. This challenge can only be addressed globally.

Many countries have adopted or are working on legislation to combat cybercrime and other misuses of information technology. These laws are drawn up to be enforceable in well-defined geographical boundaries that are either national or regional. But even if all countries had laws, a cybercriminal operating in Country A cannot be easily deported to Country B where the crime has been committed, unless these legal frameworks are inter-operable, and this is not the case today. Efforts to address this challenge have been made by establishing bilateral agreements and various “Memoranda of Understanding” between countries (ITU, 2008). However, this

model has its limitations because of the complexities in managing numerous bilateral agreements, especially when countries need to extend such agreements to many countries. In fact, a well-planned international agreement would be a better solution.

In addition to this, the results of the current study are also relevant to country leaders, government officials, strategists, and policy makers. First, the model can be used as an assessment tool for countries' policy makers and cybersecurity legislators by enabling them to compare themselves to similar countries in terms of income group, ICT development level, innovation diffusion level, cybersecurity initiatives, and growth competitiveness levels. Such an approach would allow a country's officials to compare specific ICT, innovation, and cybersecurity policies with those adopted by other similar countries or with countries demonstrating best practices within these areas of competitiveness.

The model could also be used by national level cybersecurity departments or units prescriptively to gauge their current cybersecurity effectiveness and the effectiveness of current countermeasures. Based on their analysis, they could then target specific types of countermeasures to obtain the prescribed degree of cybersecurity effectiveness. Such an approach would allow them to more judiciously plan and allocate resources (technological and human) to these countermeasures. The model will also provide the means with which policy makers can gauge policies in use by their country's organizations and governmental institutions and compare them to those of other countries in the region or internationally, enabling them to gain insight into how effectively they are managing their cyberspace.

Finally, the study has several policy implications. Policies related to ICT and innovation should take into consideration the means through which ICT can be not only made available, but also easily accessible and properly used. ICT training and education should be encouraged and

enhanced. Also, policies related to innovation as well as national and international level agreements to support innovation processes and projects should be set (Cherchye, 2001). These policies should motivate innovation efforts through encouraging experimentation and providing investment tax credit, for example (Chesbrough, 2003). Last but not least, indeed, is the need for cybersecurity policies that take into consideration the importance of the factor and its effect at the economic and national security levels. Such policies should enhance and be supportive of international cooperation and agreements (ITU, 2012), private-public partnerships, building community awareness, and empowering the human capital to identify cybersecurity problems, participate in designing solutions, and sharing with the other community entities the responsibility for having a safe and a resilient cyber space (CTO, 2010). What highlights the importance of this policy is the fact that a cyber attack usually achieves its objectives through the exploitation of one or more vulnerabilities in technology, process or human action. Cyber events can be the result of accidents, in many cases through the unwitting action of employees or business partners who lose storage media or otherwise expose data. Cyber vulnerability may also be the result of the exploitation of poor practices, such as inadequate patching of known vulnerabilities, or insecure data transmission and storage. Therefore, cyber threat education and awareness--particularly prevention--are crucial elements for improving cyber resilience (World Economic Forum, 2012).

Today there's a growing demand for cybersecurity professionals and the shortage of trained personnel should initiate a number of public-private initiatives to identify students with the proper interests and abilities in high school or even earlier, and to provide them with educational opportunities and career paths. This makes it necessary for policy makers and nation leaders to invest in cybersecurity education and training and to support curriculum initiatives and

developments in colleges and universities to provide well-planned curricula for cybersecurity education. Colleges and universities have offered computer science programs since the days of punch cards, but the integration of computer science with security, law, law enforcement, public policy and all things related to cybersecurity should be translated into a well-designed curriculum that will provide the community, its entities, and various sectors with cybersecurity professionals that are empowered to deal with today's cyberspace risks.

The above discussion related to the importance of human capacity is based on the argument that human resource performance has implications for organizational and national performance outcomes (Huselid, 1995, Raskin, 1997). Efforts to elicit discretionary performance from employees are likely to provide returns in excess of any relevant costs (Bailey, 1993). This effort is especially important during process transformations where the employees face a varied working environment. Introduction of ICT and cybersecurity measures into a country's organizations and institutions will inevitably require some form of transformation on the part of human resources. End-user education and training is a critical intervention to support successful use of new IT resources in nations, especially the developing nations (Compeau & Higgins, 1995, Galletta et al., 1995, Olfman & Pitsatorn, 2000). ICT, and along with it cybersecurity, training is an indispensable complement to investment in ICT resources and ICT-based innovations (Powell & Dent-Micallef, 1997).

Moreover, national efforts to combat cyber threats and attacks have to take into consideration the fact that the vulnerability of modern societies, caused by their dependence on a spectrum of highly interdependent information systems, has global origins and implications. Based on this, international cooperation, ICT law enforcement, along with a secure infrastructure are presented as important elements in all cybersecurity-related policies. The information

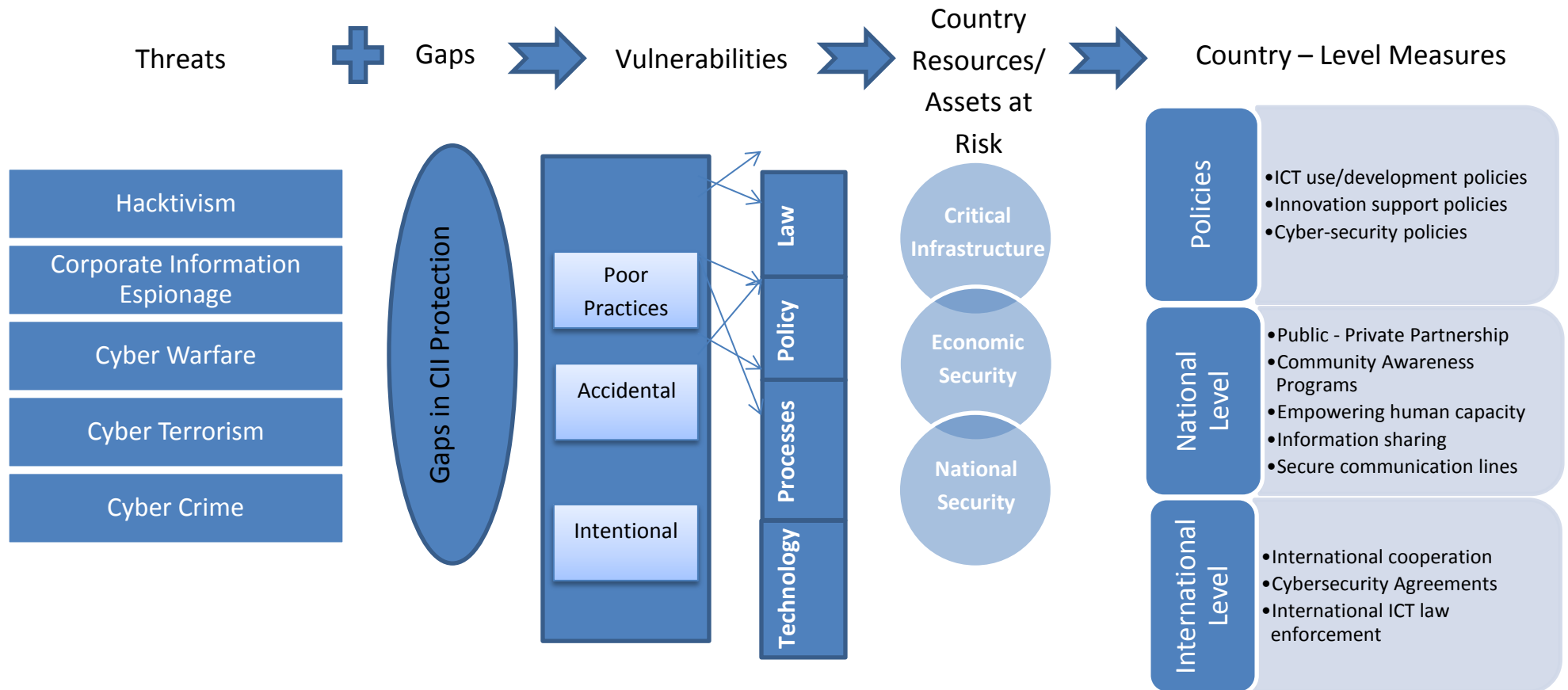
infrastructure transcends national boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside on the territory of other states. Additionally, cyberspace--a huge, tangled, diverse and almost ubiquitous web of electronic interchange--is present wherever there are telephone wires, cables, computers or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone (Cavelty, 2007). Any adequate protection policy that extends to strategically important parts of the information infrastructure will thus require global solutions: global cooperation and joint law enforcement. According to Cavelty (2008), activity at the international level should concentrate on challenges that cannot be mastered by a state or region on its own, such as global infrastructures like the Internet, or truly large-scale interdependencies. By taking such steps, international organizations can help to strengthen the complex and at times the overlapping web of national and regional initiatives in the realm of critical information infrastructure protection (CIIP), and can improve the security and dependability of systems, management practices and international policing efforts.

Because it is mainly infrastructure providers that are in the position to install technical safeguards for information technology security at the level of individual infrastructures, national governments depend on cooperation with the private sector to provide the public good of security to their citizens. But national protection measures only go so far: the securing of the global information infrastructure is a global task. Currently, divergences among national CIIP policies are a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors. However, in consideration of their economic and security interests, industrialized states are working to overcome these temporary obstacles in order to move resolutely toward robust

international conventions and mechanisms that protect the global information environment. As for the cybersecurity measure, this study is adopting the theoretical framework followed by Cavelti (2008); namely, approaching the concept from a national security perspective which is considered a sub-field of international relations.

To summarize, a number of initiatives related to cybersecurity and responses to cyber threats could be proposed among the international community participants. These could be envisaged within a model that can integrate the measures taken within an overall integrated and comprehensive framework. Provided that the implications mentioned above are taken into consideration, and a systemic approach that looks at the cyberspace problem in a holistic way is adopted, a country's strategists, economics and security analysts, and policy makers can start with an analytical framework that encompasses threat assessments, identifies gaps, determines vulnerabilities, and develops appropriate responses. The responses should take into consideration the results of the cyber threat impact analysis, as well as the criticality of the nation's assets in terms of critical infrastructures, economic security, and national security. These are visually depicted in Figure 18.

Figure 18 Country – Level Cyber Threat – Response Model



The first category of responses follows a traditional approach. This entails the adoption of policies and regulations to enhance ICT advancement processes, support innovation diffusion in the country, and respond to the current cyber paradigm.

The second category of responses promotes a nation-based approach. This entails, for instance, the sharing of information, mutual aid or coordinated action so that every stakeholder can mitigate cyber risk and contribute to a safer cyber environment. Several countries and international organizations are currently looking at the adoption of private-public partnerships that would apply in cyberspace. This also involves launching community awareness programs similar to that launched by the White House in November 2011. Other measures at the national level would involve cybersecurity education and providing support for universities and other educational institutions incorporating this specialization in their programs. Of course, the technology aspect cannot be ignored, and thus at the national level, efforts should be taken to ensure that the communications infrastructure is designed with sound security measures are well taken into consideration. In other words, the security measures should be within the first stages of the development life cycle, and should never be an afterthought measure. In other words, this includes a new model for insuring a nation's organizations, CIs, and CIIs against breaches on their data held within the cyberspace, as in cloud computing for example, indicating the possibility that cyber risks could be quantified for the development of scalable risk transfer markets (World Economic Forum, 2012). Other examples are the use of technology to ensure "security by design" and thus create embedded security, as well as proposals to deploy a new Internet architecture that incorporates online identification.

The third category is pertinent to international-level responses, which in corroboration with what Cavelti (2007, 2008) contended cannot be ignored, but rather should be well taken into consideration and properly done. Based on the international law theory, there should be serious efforts to have international cooperation agreements for cyberspace protection. ITU (2010) has developed a cybersecurity agenda including terms that entail international cooperation agreements and highlight their importance. The Internet and ICTs have enabled interconnection between countries that was not possible before. Countries cannot easily close their borders to incoming cyber threats and also cannot contain those coming from within their borders. Attempts to solve these challenges at national or regional levels are important, but they are undermined as they extend beyond these levels. Cybersecurity is as global and far-reaching as the Internet. Solutions, therefore, need to be harmonized across all borders. This necessarily entails international cooperation, not only at the governmental level, but also with industry, non-governmental and international organizations. Cybersecurity concerns all types of measures. For this reason, international organizations, such as the ITU, seek to harness the power of multi-stakeholder collaboration in order to arrive at global strategies to enhance cybersecurity. At the same time, ICT law enforcement should not be confined to the national level, but rather should be done with the international regulatory and legal system taken into consideration also. Such international measures have been suggested as equally, if not more, important than the national-level measures.

Limitations of the Study

As with all studies, this study is subject to limitations, which can potentially influence conclusions drawn from the dataset. First, because the data is country cross-sectional in nature, causal inferences should not be made regarding the effects of measured variables. For example,

rather than concluding that countries with higher ICT development and global innovation levels have more effective cyber security initiatives or measures, it is more appropriate to conclude that more technologically developed countries with higher innovation diffusion levels tend to have more effective cyber security measures. Thus, only correlational inferences can be drawn. However, the nature of the data set used in this study conforms well to its correlational research design and predictive model purposes.

Another possible limitation of the study could be the type of data used being secondary rather than primary. Of course, as with any other data source, secondary data have their advantages and disadvantages as elaborately discussed in Chapter III. One major disadvantage is inherent in the nature of the secondary data: the purpose of its collection, its scope, and its variables. For these reasons, the recommendations suggested by Boslaugh (2007) were followed, including careful screening and examination of the secondary data set to assess its relevance, proper definition, and relevance to the study purpose and research questions. In fact, given the nature of the study, with countries being the main unit of analysis, and with the need to answer questions involving country-level factors, the need for secondary comprehensive data was deemed necessary. This, along with the fact that the data used were generated by reputable international organizations with research experience recognized worldwide, makes the secondary data in this case more an advantage than a limitation. What adds to this advantage is the effort put forth by these international organizations--such as the World Bank, UNDP, World Economic Forum, and ITU--and the reviewing entities they use to provide extensive documentation and explanation of the procedures followed to collect data (Hox & Boeije, 2005) as well as the presentation of technical information in the form of documents or reports published on their websites.

Finally, another possible limitation is the way threats are treated using the current research design. For ease of analysis, threats were treated holistically meaning that all threats were lumped together and treated equally. This was probably not actually the case. More likely, some threats are more serious than others in terms of exploit, potential damage, costs, and so on. In other words, different types of threats may have different effects on the relationships presented in the model. In addition, one type of threat may have a different effect in various countries depending on the country, its resources, the skills available, and the cybersecurity measures taken, etc.

To elaborate on the last point, threats to cybersecurity can be roughly divided into two general categories: actions aimed at and intended to damage or destroy cyber systems (“cyber attacks”), and actions that seek to exploit the cyber infrastructure for unlawful or harmful purposes without damaging or compromising that infrastructure (“cyber exploitation”). Cyber attacks may target government or private assets. They include efforts by nations and non-nation actors to damage and degrade computer software, hardware, and other aspects of computer operations, as well as to compromise cyber systems by infiltrating them without proper authority to obtain information or to control them in a variety of ways. While some intrusions may not result in an immediate impact on the operation of a cyber system as, for example, when a “Trojan Horse” infiltrates and establishes itself in a computer, such intrusions are considered cyber attacks when they can thereafter permit actions that destroy or degrade the computer’s capacities.

Many forms of cyber attacks have been identified, and new forms are continuously being devised. Among the cyber attacks of greatest concern are those conducted or supported by nations and aimed at damaging or controlling cyber systems on which critical infrastructure

depend, including power grids, air traffic control, and financial systems. Many nation and non-nation actors seeking to attack or exploit a country's cyber systems mask their identities by initiating their efforts from foreign countries, or by routing them through foreign computers and servers. Frequently, transnational attacks (some serious) are attributed to "patriotic" hackers, encouraged or tolerated by their governments (Cavelty, 2008). Efforts to exploit cyber systems for the purpose of committing conventional crimes or for other purposes regarded by nations as harmful, are also common and have caused significant losses and other costs. Cyber exploitation includes using the Internet and other cyber systems to commit fraud, to steal, to recruit and train terrorists, to violate copyright and other rules limiting distribution of information, to convey controversial messages, and to sell child pornography or other banned materials (ITU, 2012). Cyber systems contain vast amounts of data which criminals have been able to seize and utilize, such as Social Security numbers; and they enable criminals efficiently to approach millions of potential victims in attempted frauds and other schemes.

Recommendations

Based on the limitations presented above, and in addition to the implications that were elaborated on the need for policy, training, education, and international agreements, to list a few, there are also certain recommendations for future research. First, longitudinal along with cross-sectional data are recommended. This is important for understanding economic, ICT, and innovation diffusion changes that resulted from or caused policy interventions. These studies provide an understanding of the dynamic processes that underlie a country's social and economic life. Their fundamental role in social science and policy research is the core rationale for the continued investment in longitudinal studies in the US and Western Europe.

ICT has brought forth a myriad of benefits at the individual, community, and national levels across all economic sectors and aspects of life. With all these positive contributions and bright aspects comes a dark and negative aspect--a destructive power usually enabled by advancements in information and telecommunication technologies. This taps into a research possibility to investigate the relationship between the level of ICT advancement and the degree to which a country gets exposed to this dark side if technology is a source of or a target of cyber threats and attacks. Moreover, this relationship may shed some light on the type of countermeasures adopted by the country, being majorly offensive, majorly defensive, or a relatively equal balance of both. Such relationships, along with the nations' history, culture, resources, and type of international relations policy it has with other countries, may help build certain measures or metrics to anticipate possible cyber terrorism, cyber warfare, and other cyber crime activities it may initiate or become subject to in the future.

Another recommendation is to examine the impact of cybersecurity curriculum, training, and awareness programs on cybersecurity levels in countries or states that have such education offered to individuals or organization seeking this kind of education. A comparative study involving countries with such educational programs offered and others without such programs integrated into the curriculum can shed some light on the important role that human capacity can play in the proper planning and implementation of cybersecurity initiatives.

Still another recommendation is to broaden and deepen the scope of the cybersecurity measure through introducing more dimensions to the construct; for example, human capacity (which conforms to the socio-technical nature of the ICT field), organizational initiatives, and the level of private-public partnerships in each nation.

Furthermore, future research is recommended to take country-level factors, such as a country's culture, regulatory environment, regional policies and agreements, economic freedom, propensity to risk, perceived corruption index, and intellectual property rights into consideration and use them as antecedents to a country's cybersecurity strategy, or as an assessment of its effectiveness. The same measures could be used to examine a country's ICT, innovation, and cybersecurity performance.

Finally, there is a recommendation that is not directly related to the scope of this research; namely, constructing an ICT human capital index that is more indicative than the one currently used (UNDP, 2011) of ICT, information security, and cyber security skills, training, and experience. Human capital as an index mainly represents the education level of people across nations. In fact, the common theme that flows through the majority of ICT indices is an understanding of affordability and access to ICTs, which does not consider in detail the crucial requirement of fundamental ICT skills. This limits the reliability of these reports as policy instruments, especially for developing countries. The most common measurement of ICT skills is educational attainment. In a study of Internet skills (using both observed capacity and self-reported skills) among US users, Hargittai (2012) finds that education is correlated with Internet skills. Furthermore, higher education levels imply more exposure to technology, which increases the ability to adapt more quickly to new technologies, and in many countries educational institutions are the first point of affordable access for many users (Kiiski & Pohjola, 2002). This, while important, cannot account for variances in computer skills and innovation abilities. Given the fact that most students worldwide are exposed to computer literacy courses in schools and universities--though at various degrees, the variance would be reduced, as far as the use of ICT is concerned. The same applies to innovation. It seems that at the country level, the ability to

innovate and put ICT into productive use might (1) already involve the innovative human capital element whether at the invention or the innovation level, and/or (2) outweigh the human capital represented mainly by education and other few social factors. The results reported by Brynjolfsson and Saunders (2010) suggested the importance of human capital as a moderator in the relationship of each of ICT and innovation to economic growth. Additional research at the firm level also reported a significant moderation effect of human capital in the relationship between a firm's innovation ability and ICT diffusion on one hand and organizational performance on the other. This is logical, and may prove pivotal to upgrade the country human capital index to include, in addition to education, a sense of equity, the involvement of women and others, an ICT skills pillar, as well as pillars related to human skills, abilities, and opportunities granted to the people of each country.

Future Research Directions

In addition to the recommendations for future research as discussed above, the researcher, based on life experiences and findings obtained in the current study, has developed an eye for some future research ideas. These include the following suggestions.

First, using the cyber threat data, a survival analysis could be done to analyze the anticipated strength and adverse impact of a cyber threat. Given the cybersecurity measures developed and upgraded in a country, the researcher can measure the duration length before a country goes down as well as the initiatives it should adopt to survive a particular attack. Survival analysis is a branch in statistics which includes a variety of “statistical methods designed to describe, explain or predict the occurrence of events” (Allison 2004, p. 369). Originated from biostatistics, survival analysis has become a widely used methodology in many fields of research. Depending on the field of research, survival analysis might therefore also be

called event history analysis, failure time, transition analysis, or duration analysis (in economics/econometrics). Survival analysis is used to answer questions such as:

1. Can certain cyber threats adversely affect the very existence and operations of a nation's CI?
2. Which initiatives increase the lifespan of a nation's CI and CII?
3. What makes some countries adopt certain cyber security policies earlier than others?

Second, taking the cybersecurity measure score for each country, a study involving a comparative analysis could be conducted to investigate information and cybersecurity measures adopted by various entities in the country. This can provide a rich framework within which cybersecurity, ICT, and innovation could be analyzed at the micro as well as the macro levels of a country.

Third, another future research direction is using cybersecurity and cyber threat data to examine their impact on organizational level initiatives to adopt new efficiency driving computing models, such as cloud computing, EHR/EMR systems, business intelligence in the cloud, and so on. Here, micro-level situations could be examined using micro as well as macro level data.

Finally, future research can move in the direction of cyber warfare. Here, cyber threat data, along with international relations policies, country-level characteristics (including historical, geographical, economic, political and economic agreements) can be used to examine the potential intention of certain nations to get involved in cyber warfare against other nations.

REFERENCES

- Abu-Nimeh, S., Foo, E., Fovino, I. N., Govindarasu, M., & Morris, T. (2013). Cyber security of networked critical infrastructures. *IEEE Network*, 27(1), 3-4.
- Acemoglu, D. & Dell, M. (2010). Productivity Differences between and within Countries. *American Economic Journal: Macroeconomics*, 2(1), 169–88.
- Acemoglu, D. (2012). Introduction to Economic Growth. *Journal of Economic Theory*, 147(2), 545-550.
- Acohido, B., & Swartz, J. (2008). *Zero day threat*. New York: Sterling Publishing Co., Inc.
- Adam, M.S. & Urquhart, C. (2009). No Man Is an Island: Social and Human Capital in IT Capacity Building in the Maldives. *Information & Organization*, 19(1), 1-21.
- Adams, R., Bessant, J., & Phelps, R. (2006). Innovation management measurement: A review. *International Journal of Management Reviews*, 8(1), 21-47.
- Afuah, A. (2001). Dynamic boundaries of the firm: are firms better off being vertically integrated in the face of technological change? *Academy of Management Review*, 44(6), 1211–1228.
- Agarwal, R. & Karahanna, E. (2000). Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, 24(4), 665-694.
- Agarwal, R. & Prasad, J. (1999). Are Individual Differences Germane to the Acceptance of Information Technologies? *Decision Science*, 30(2), 361-391.
- Aghion, P. & Howitt, P. (1998). *Endogenous Growth Theory*. MA: MIT Press.
- Ahn, J. (2002). Beyond Single Equation Regression Analysis: Path Analysis and Multi-Stage Regression Analysis. *American Journal of Pharmaceutical Education*, 66, 37-42.
- Aiman-Smith, L. & Green, S. G. (2002). Implementing new manufacturing technology: The related effects of technology characteristics and user learning activities. *Academy of Management Journal*, 45(2), 421-430.
- Alperovitch, D. (2011). *Revealed: operation shady RAT*. McAfee, retrieved from: <http://noramintel.com/wp-content/uploads/2011/08/McAfee-wp-operation-shady-rat.pdf>.

- Alter, S. (2003). 18 Reasons Why IT-Reliant Work Systems Should Replace 'the IT Artifact' as the Core Subject Matter of the IS Field. *Communications of the AIS*, 12(23), 366-395.
- Allison, P. (2004). Event History Analysis. In *Handbook of Data Analysis* (eds. Hardy, M. A. & Alan, B). London: Sage Publications Ltd., 369-386.
- Amato, M.P., Bartolozzi, M.L., Zipoli, V., Portaccio, E., Mortilla, M., Guidi, L., Siracusa, G., Sorbi, S., Federico, A., & De Stefano, N. (2004). Neocortical volume decrease in relapsing–remitting MS patients with mild cognitive impairment. *Neurology*, 63 (1), 89–93.
- Ammenwerth, E. Iller, C., & Mansmann, U. (2003). Can evaluation studies benefit from triangulation? A case study. *International Journal of Medical Informatics*, 70(2-3), 237-246.
- Anand, J., & Kogut, B. (1997). Technological capabilities of countries, firm rivalry and foreign direct investment. *Journal of International Business Studies*, 28(3), 445-465.
- Anderson, D.F., Cappelli, D.M., Gonzalez, J.J., Mojtahedzadeh, M., Moore, A.P., Rich, E., Sarriegui, J.M., Shimeall, T.J., Stanton, J.M., Weaver, E., & Zagonel, A. (2004). “Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem,” in *Proceedings of the 22nd International Conference of the System Dynamics Society*, Oxford, England, July 25-29.
- Anderson, R. & Fuloria, S. (2011). Security Economics and Critical Infrastructure. *University of Cambridge*.
- Andreev, P., Heart, T., Maoz, H., & Pliskin, N. (2009). Validating formative partial least squares (PLS) models: methodological review and empirical illustration. In *ICIS 2009 Proceedings*. Paper 193, retrieved from: <http://aisel.aisnet.org/icis2009/193>.
- Andrianaivo, M. & Kpodar, K. (2011). *ICT, Financial Inclusion, and Growth: Evidence from African Countries*. IMF Working Paper (WP/11/73), International Monetary Fund, Washington, DC.
- APCERT – Asia Pacific Computer Emergency Response Team (2011). *APCERT Annual Report 2011*, retrieved from: http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2011.pdf.
- Applegate, L.M., Austin, R.D., & Mcfarlain, F.W. (2003). *Corporate information strategy and management: text and cases* (6th ed.). New York: McGraw-Hill.
- Archibugi, D. & Michie, J. (1998). Technical change, growth, and trade: new departures in institutional economics. *Journal of Economic Survey*, 12(3), 247 – 332.

- Archibugi, D., Howells, J., & Michie, J. (1999). Innovation systems in a global economy. *Technology Analysis & Strategic Management*, 11(4), 527-539.
- Argyrous, G. (2001). Setterfield on Cumulative Causation and Interrelatedness: A Comment. *Cambridge Journal of Economics*, 25, 103-6.
- Arrow, K.J. (1962). The economic implications of learning by doing. *The Review of Economic Studies*, 29(3), 155 – 173.
- Arrow, K. J. (1964). Control in Large Organizations. *Management Science*, 10(3), 397-408.
- Ashford, W. (2013). Kaspersky calls for international cooperation on cyber security. *ComputerWeekly*, January 31, retrieved from: <http://www.computerweekly.com/news/2240177266/Kaspersky-calls-for-international-cooperation-on-cyber-security>.
- Assante, M. J. (2009). Infrastructure Protection in the Ancient World. In *Proceedings of the 42nd Hawaii International Conference on System Sciences, IEEE*, 1-10.
- Athey, S. & Stern, S. (1998). *An Empirical Framework for Testing Theories about Complementarity in Organizational Design*. Working Paper 6600, National Bureau of Economic Research.
- Atkinson, R.D. (2007). Deep Competitiveness. *Issues in Science and Technology*, Winter, 69-75.
- Attwood, A., Merabti, M., Fergus, P., & Abuelmaatti, O. (2011). SCCIR: Smart Cities Critical Infrastructure Response Framework. In *Developments in E-systems Engineering (DeSE), 2011*, IEEE, December, 460-464.
- Avgerou, C. (1998). How can IT enable economic growth in developing countries?. *Information Technology for Development*, 8(1), 15-28.
- Avgerou, C. & Walsham, G. (2000). *Information Technology in Context: Studies from the Perspective of Developing Countries*. London: Ashgate.
- Bagheri, E., & Ghorbani, A. A. (2007). On the collaborative development of para-consistent conceptual models. In *Seventh International Conference on Quality Software, 2007, QSIC'07, IEEE*, 336-341.
- Bagozzi, R. P. (Ed.). (1994). *Principles of marketing research*. Cambridge, Oxford, Mass: Blackwell.
- Bagozzi, R. P., Fornell, C., & Larcker, D. F. (1981). Canonical correlation analysis as a special case of a structural relations model. *Multivariate Behavioral Research*, 16(4), 437-454.

- Bailey, T. (1993). *Discretionary Effort and the Organization of Work: Employee Participation and Work Reform since Hawthorne*. New York: Institute on Education and the Economy.
- Bakos, Y. (1998). The Productivity Payoff of Computers: A review of the Computer Revolution: An Economic Perspective by Daniel E. Sichel. *Science*, 281(5373), 52.
- Banik, B., J. (1993). Applying triangulation in nursing research. *Applied Nursing Research*, 6(1), 47-52.
- Barbour, R.S. (1998). Mixing qualitative methods: Quality assurance or qualitative quagmire? *Qualitative Health Research*, 8(3), 352-361.
- Barclay, D., Higgins, C., & Thompson, R. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. *Technology Studies*, 2(2), 285-324.
- Barmin, Y., Jones, G., Moiseva, S., & Winkelman, Z., (2011). International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and information Security. *The SURF Journal*, 2(2010-2011), 69-82.
- Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, 51(6), 1173.
- Baroudi, J. J. & Orlikowski, W. J.(1989). The problem of statistical power in MIS research. *MIS Quarterly*, 13(1), 87-106.
- Barney, J.B. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99-120.
- Baroni de Carvalho, R., & Ferreira, M.A.T. (2001). Using Information Technology to Support Knowledge Conversion Process. *Information Research*, 7(1), retrieved from: <http://informationr.net/ir/7-1/paper118.html>.
- Bartel, A., Ichinowski, C., & Shaw, K. (2007). How Does Information Technology Really Affect Productivity? Plant-level Comparisons of Product Innovation, Process Improvement and Worker Skills. *Quarterly Journal of Economics*, 122(4), 1721-1758.
- Bathelt, H., Malmberg, A., & Maskell, P. (2004). Cluster and Knowledge: Local Buzz, Global Pipelines and the Process of Knowledge Creation. *Progress in Human Geography*, 28(1), 31-56.

- Batra, S. (2006). Impact of information technology on organizational effectiveness: a conceptual framework incorporating organizational flexibility. *Global Journal of Flexible Systems Management*, 7(1-2), 15-25.
- Bayo-Moriones, A. & Lera-López, F. (2007). A firm-level analysis of determinants of ICT adoption in Spain. *Technovation*, 27(6), 352-366.
- Beath C. (1991). Supporting the Information Technology Champion. *MIS Quarterly*, 15(3), 355-371.
- Becker, S. W. & Whisler, T. L. (1967). The innovative organization: A selective view of current theory and research. *The Journal of Business*, 40(4), 462-469.
- Beggs, P. (2010). *Securing the Nation's Critical Cyber Infrastructure*. US Department of Homeland Security, retrieved from:
http://www.ocio.ca.gov/OIS/Government/events/documents/Patrick_Beggs.pdf
- Belitz, H., Clemens, M., Von Hirschhausen, C., Schmidt-Ehmcke, J., Werwatz, A., & Zloczynski, P. (2011). *An indicator for national systems of innovation: Methodology and application to 17 industrialized countries*. DIW-Berlin Discussion Paper No.1129.
- Bell, M. & Pavitt, K. (1993). Technological Accumulation and Industrial Growth Contrasts between Developed and Developing Economies, *Industrial and Corporate Change*, 2(2), 157-210.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 369-386.
- Berkley, B. J. & Gupta, A. (1994). Improving service quality with information technology. *International Journal of Information Management*, 14(2), 109-121.
- Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010). On the analysis of the zeus botnet crimeware toolkit. In *2010 Eighth Annual International Conference on Privacy Security and Trust (PST), IEEE*, pp. 31-38.
- Blanke, J., Paua, F., & Sala-i-Martin, X. (2004). *The growth Competitiveness Index: Analyzing Key Underpinnings of Sustained Economic Growth*. Switzerland: World Economic Forum.
- Black S.E. & Lynch L.M. (2001). How to compete: the impact of workplace practices and information technology on productivity. *Review of Economics and Statistics*, 83(3), 434 - 445.

- Bocquet, R., Brossard, O., & Sabatier, M. (2007). Complementarities in organizational design and the diffusion of information technologies: An empirical analysis. *Research Policy*, 36(3), 367-386.
- Bollen, K. & Lennox, R. (1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological bulletin*, 110(2), 305.
- Boschma, R.A. (2005). Proximity and innovation: a critical assessment. *Regional Studies*, 39(1), 61–74.
- Boslaugh, S. (2007). *Secondary Data Sources for Public Health: A Practical Guide*. Washington DC: Cambridge University Press.
- Boudreau, M.C., Loch, K.D., Robey, D. & Straub, D. (1998). Going global: using information technology to advance the competitiveness of the virtual transnational organization. *The Academy of Management Executive*, 12(4), 120-128.
- Boyd, C.O. (2000). Combining qualitative and quantitative approaches. In *Nursing research: A qualitative perspective (2nd ed.)* (Eds. Munhall, P.L. and Boyd, C.O.). Boston: Jones & Bartlett, 454-475.
- Brammer, R.F. (2011). Cyber Security – The Vital Ingredient for Today’s and Tomorrow’s Infrastructure Needs. in the *Proceedings of Energy, Environment, Defense, and Security, Washington DC*, 1 – 10.
- Branscomb, L. (2004). Protecting civil society from terrorism: The search for a sustainable strategy. *Technology in Society*, 26(2-3), 271-285.
- Bresnahan, T., Brynjolfsson, E., & Hitt, L. (2002). Information Technology, Workplace Organization and the Demand for Skilled Labor: Firm-level Evidence. *Quarterly Journal of Economics*, 117(1), 339-376.
- Bresnahan, T. F. & Trajtenberg, M. (1995). General Purpose Technologies: ‘Engines of Growth’? *Journal of Econometrics*, 65(1), 83–108.
- Brock, J. K. U. (2003). The ‘power’ of international business research. *Journal of International Business Studies*, 34(1), 90-99.
- Brody, H. & Stabler, B. (1991). Great Expectations: Why Technology Predictions Go Awry. *MIT Technology Review*, 94(5), 38-45.
- Bruhn, M., Georgi, D., & Hadwich, K. (2008). Customer equity management as formative second-order construct. *Journal of Business Research*, 61(12), 1292-1301.

- Brunner, E.M. & Suter, M. (2008). *International CIIP Handbook 2008 – 2009*. Center for Security Studies (ETH Zurich), 4(1). Retrieved from:
<http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf> .
- Bryman A. (2004), *Triangulation and Measurement*, Department of Social Sciences, Loughborough University, Loughborough, Leicestershire, UK, retrieved from:
<http://www.referenceworld.com/sage/socialscience/triangulation.pdf>
- Brynjolfsson, E. & Hitt, L. M. (2003). *Computing productivity: Firm-level evidence*. MIT Working Paper 4210-01, National Bureau for Economic Research, 1-43.
- Brynjolfsson, E. & Saunders, A. (2010). *Wired for Innovation: How Information Technology is Reshaping the Economy*, Massachusetts: the MIT Press.
- Burnham, J. (2009). Economic Growth, Entrepreneurship, and the Deployment of Technology. In *Innovation Policies, Business Creation and Economic Development* (Ed. Aydogan, N.). New York: Springer Science and Business Media.
- Business Roundtable (2007). *Growing Business Dependence on the Internet*. Retrieved from:
http://businessroundtable.org/uploads/news-center/downloads/200709_Growing_Business_Dependence_on_the_Internet.pdf.
- Byres. E. (2011). “Son-of-Stuxnet” - Coming Soon to a SCADA or PLC System Near You, retrieved from: <http://www.tofinosecurity.com/blog/%E2%80%9Cson-stuxnet%E2%80%9D-coming-soon-scada-or-plc-system-near-you>.
- Campbell, D. T. & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait multimethod matrix. *Psychological Bulletin*, 56 (2), 81-105.
- Campbell, K., L.A. Gordon, M. P. Loeb & L. Zhou (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3), 431-448.
- Carlsson, B. (2006). Internationalization of innovation systems: A survey of the literature. *Research Policy*, 35(1), 56-67.
- Carter, L. & Belanger, F. (2005). The utilization of e-government services: citizen trust. innovation and acceptance factors. *Journal of Information Systems*, 15(1), 5-25.
- Cashell, B., Jackson, W.D., Jickling, M., & Webel, B. (2004). *The Economic Impact of Cyber-Attacks*, CRS Report for Congress. Congressional Research Service and the Library of Congress.
- Cass, D. (1965). Optimum growth in an aggregative model of accumulation. *Review of Economic Studies*, 32(8), 233 – 240.

- Cassel, C. M., Hackl, P., & Westlund, A. H. (1999). Robustness of partial least-squares method for estimating latent variable quality structures. *Journal of Applied Statistics*, 26(4), 435–446.
- Castoldi, N. & Bechini, L. (2010). Integrated sustainability assessment of cropping systems with agro-ecological and economic indicators in northern Italy. *European Journal of Agronomy*, 32(1), January, 59-72.
- Cavelty, M. D. (2007). *Critical information infrastructure: vulnerabilities, threats and responses*. UNIDIR Disarmament Forum, Issue 3, 15-22. United Nations Institute for Disarmament Research.
- Cavelty, M.D. (2008). *Cyber-Security and Threat Politics: US efforts to secure the information age*. NY: Routledge Taylor and Francis Group.
- CEPS (2010). *Protecting Critical Infrastructure in the EU*. Centre for European Policy Studies, Brussels.
- CERT: Software Engineering Institute – Carnegie Mellon (1997). Security of the Internet. *Frochlich / Kent Encyclopedia of Telecommunications*, 15, 231-255.
- Chamberlin, Thomas (1965). The Method of Multiple Hypotheses. *Science*, 148(3671), 754-759.
- Chandran, R., Phatak, A., & Sambharya, R. (1987). Transporter Data Flows: Implications for Multinational Corporations, *Business Horizons*, 30(6), 74-81.
- Chen, T. M. (2010). Stuxnet, the real start of cyber warfare? *IEEE Network*, 24(6), 2-3.
- Chen, J. S. J., & Tsou, H. T. (2006). Information technology adoption for service innovation practices and competitive advantage: the case of financial firms. *Information Research*, 12(3), 7.
- Charles, C. (1995). *Introduction to Educational Research*. New York: Longman.
- Cherchye, L. (2001). Using data envelopment analysis to assess macroeconomic policy performance. *Applied Economics*, 33(3), 407-416.
- Chesbrough, H.W. (2003). The Era of Open Innovation. *MIT, Sloan Management Review*, 44(3), 35.
- Chesbrough, H.W. (2002). *Open Innovation - The New Imperative for Creating and Profiting from Technology*. Boston, MA: Harvard Business School Press.
- Chin, W. W. (2010). How to write up and report PLS analyses. In *Handbook of Partial Least Squares* (eds. Esposito, V. et al.). New York: Springer-Verlag, 655-688.

- Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, 14(2), 189-217.
- Chin, W. W. & Newsted, P. R. (1999). Structural equation modelling analysis with small samples using partial least squares. In *Statistical strategies for small sample research* (Hoyle, R. H. Ed.), (pp. 307–341). Thousand Oaks, CA: Sage, 307-341.
- Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, 22(1), vii-xvi.
- Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In *Modern Methods for Business Research* (Ed. Marakas, G. E.), Mahwah: Lawrence Erlbaum Associates, 295-336.
- Christensen, S., Caelli, W. J., Duncan, W. D., & Georgiades, E. (2010). An Achilles heel: denial of service attacks on critical information infrastructures. *Information and Communications Technology Law*, 19(1), 61-85.
- Christensen, J.F. (1996). Analyzing the technology base of the firm: a multi-dimensional resource and competence perspective. In *Towards a Competence Theory of the Firm* (Ed. Foss, N.J. and Knudsen, C.). London: Routledge, 111–132.
- Christensen, J.F. (1995). Asset profiles for technological innovation. *Research Policy*, 24(5), 727–745.
- Clarke, R.A., & Knake, R.K. (2010). *Cyber War: the next threat to national security and what to do about it?* New York: Harper Collins.
- Clark, P.A. & Staunton, N., 1989. *Innovation in Technology and Organization*. London: Routledge.
- Cohen, J. (1968). Multiple regression as a general data analytic system. *Psychological Bulletin*, 70(6), 426-443.
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd Edition). New Jersey: Lawrence Erlbaum.
- Cohen, J. (1990). Things I have learned so far. *American Psychologist*, 45(12), 1304-1312.
- Colecchia, A. & Schreyer, P. (2002). ICT investment and economic growth in the 1990s: Is the U.S. a unique case? A comparative study of nine OECD countries. *Review of Economic Dynamics*, 5(2), 408-442.

- Collier, M. (2007) Estonia: Cyber Superpower. *BusinessWeek*, December 17, retrieved from: http://www.businessweek.com/globalbiz/content/dec2007/gb20071217_535635.htm.
- Compeau, D.R. & Higgins, C.A. (1995). Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research*, 6(2), 118-143.
- Conklin, A. & White, G. B. (2006). e-Government and Cyber Security: The Role of Cyber Security Exercises. In *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS)*.
- Conrad, S. H., LeClaire, R. J., O'Reilly, G. P., & Uzunalioglu, H. (2006). Critical national infrastructure reliability modeling and analysis. *Bell Labs Technical Journal*, 11(3), 57-71.
- Cornish, P. (2009). *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*. Brussels: European Parliament.
- Corso, M. & Paolucci, E. (2001). Fostering innovation and knowledge transfer in product development through information technology. *International Journal of Technology Management*, 22(1-3), 126-148.
- Cortright, J. (2001). *New Growth Theory, Technology and Learning: A Practitioner's Guide*. Reviews of Economic Development Literature and Practice: No. 4. U.S. economic Development Administration.
- Cox, D., Fitzpatrick, R., Fletcher, A., Gore, S., Spiegelhalter, D., & Jones, D. (1992). Quality-of-life assessment: can we keep it simple?, *Journal of the Royal Statistical Society*, 155(3), 353-393.
- Crian, D. A., Preda, A. M., Coculescu, C., & Altar-Samuel, A. N. (2010). Some Aspects Concerning the Correlation between ICT and Innovation in Europe. *The Journal of the Faculty of Economics – Economic*, 1(2), 1183 – 1189.
- Cronbach, L. J. (1957). The two disciplines of scientific psychology. *American Psychologist*, 12(11), 671-684.
- Croope, S. V. & McNeil, S. (2011). Improving Resilience of Critical Infrastructure Systems Postdisaster. *Transportation Research Record: Journal of the Transportation Research Board*, 2234(-1), 3-13.
- CTO (2010). *Cyber Security through international cooperation*. Cyber Security Forum 17–18 June 2010, London, Commonwealth Telecommunications Organization.

- Cukier, K.N., Mayer-Schonberger, V., & Branscomb, L.M. (2005). Ensuring (and Insuring?) Critical Information Infrastructure Protection. *Faculty research Working Paper Series RWP05-055*, John F. Kennedy School of Government, Harvard University. Retrieved from: http://belfercenter.ksg.harvard.edu/files/rwp_05_055_viktor_branscomb.pdf.
- Culnan, M. J. & Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choice Point and TJX Data Breaches. *MIS Quarterly*, 33(4), 673 – 687.
- D'Costa, A. P. (2006). *Exports, University-Industry Linkages, and Innovation Challenges in Bangalore, India*. World Bank Policy Research Working Paper 3887. Washington, DC: World Bank.
- Dalmini, M.T., Eloff, J.H.P., & Eloff, M.M. (2009). Information Security: The Moving Target. *Computer and Security*, 28(3-4), 189-198.
- Day, R.H. (2008). The technology evolving culture: character and consequence. *Journal of Evolutionary Economics*, 18(3), 313 – 322.
- De Haan, J. & Sturm, J. (2000). On the relationship between economic freedom and economic growth. *European Journal of Political Economy*, 16(2), 215-241.
- Dehning, B. & Richardson, V.J. (2002) Returns of Investment Technology: A Research Synthesis. *Journal of Information Systems*, 16(1), 7-30.
- Dehning, B., Richardson, V.J., & Zmud, R.W. (2007). The Financial Performance Effects of IT-Based Supply Chain Management Systems in Manufacturing Firms. *Journal of Operations Management*, 25, 806-824.
- Delone, W.H. & McLean, E.R. (2003). The Delone and McLean Model of Information Systems Success: A ten-year update. *Journal of Management Information Systems*, 19 (4), 9-30.
- Denning, D. E. (2000). Hacktivism: An emerging threat to diplomacy. *Foreign Service Journal*, 1(1), 10-17.
- Dennison, E. (1985). *Trends in American Economic Growth: 1929 – 1982*, Washington: Brookings Institution.
- Denzin, N. K. (1970). *The Research Act in Sociology*. Chicago: Aldine.
- Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods*. New York: McGraw-Hill.
- De Villiers, M. (2009). *Information Security Standards*. University of New South Wales, Faculty of Law, Research Series, Paper 34.

- Dewan, S. & Kraemer, K. (2000). Information Technology and Productivity: Evidence from Country Level Data. *Management Science*, 46(4), 548-562.
- Diamantopoulos, A. (2011). Incorporating formative measures into covariance-based structural equation models. *MIS Quarterly*, 35(2), 335-358.
- Diamantopoulos, A. (2006). The error term in formative measurement models: interpretation and modeling implications. *Journal of Modeling in Management*, 1(1), 7-17.
- Diamantopoulos, A., Riefler, P., & Roth, K. P. (2008). Advancing formative measurement models. *Journal of Business Research*, 61(12), 1203-1218.
- Diamantopoulos, A. & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, 17(4), 263-282.
- Diamantopoulos, A. & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, 38(2), 269-277.
- Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *ACM SIGMIS Database*, 35(4), 6-102.
- Dierickx, I. & Cool, K. (1989). Asset stock accumulation and the sustainability of competitive advantage. *Management Science*, 35(12), 1504–1511.
- Dijkstra, T. (1983). Some comments on maximum likelihood and partial least squares methods. *Journal of Econometrics*, 22(1-2), 67–90.
- Dondossola, G., Szanto, J., Masera, M., & Nai Fovino, I. (2008). Effects of intentional threats to power substation control systems. *International Journal of Critical Infrastructures*, 4(1), 129-143.
- Doran, J. & O'Leary, E. (2011). External interaction, innovation and productivity: an application of the innovation value chain to Ireland. *Spatial Economic Analysis*, 6(2), 199-222.
- Dosi, G. (1988). Sources, procedures, and microeconomics effects of innovation. *Journal of Economic Literature*, 26(3), 1120 – 1171.
- Dutta, S. (2011). The Global Innovation Index 2011: Accelerating Growth and Development. *INSEAD*.
- Dutta, S. & Mia, I. (2007). *Executive summary, the global information technology report, 2006–2007*. World Economic Forum.

- Downing, C.E., Gallagher, J. & Segers, A.H. (2003). Information Technology Choices in Dissimilar Cultures: Enhancing Empowerment. *Journal of Global Information Management*, 11(1), 20-39.
- Economou, P. (2008). *Harnessing ICT for FDI and Development*. Global Forum VII on International Investment, OECD, 27-28.
- Edgeworth, F.Y. (1881). *Mathematical psychics: an essay on the application of mathematics to the moral sciences*. London: Kegan Paul.
- Efron, B. (1979). Bootstrap methods: another look at the jackknife. *The annals of Statistics*, 7(1), 1-26.
- Ekstedt, M. & Sommestad, T. (2009). Enterprise Architecture Models for Cyber Security Analysis, in *proceedings of IEEE/PES Power Systems Conference & Exhibition (PSCE), 15-18 March 2009*, 1-6.
- Ellis, P. D. (2010). *The essential guide to effect sizes: Statistical power, meta-analysis, and the interpretation of research results*. New York: Cambridge University Press.
- Ernst & Young (2010). 13th *Global Information Security Survey 2010: Cloud computing: pros and cons*, retrieved from: <http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/13th-Global-Information-Security-Survey-2010---Cloud-computing--pros-and-cons>
- Ernst, D. (2006). *Innovation Offshoring – Asia’s Emerging Role in Global Innovation Networks*. East-West Center Special Report, Number 10, 1-48.
- Ernst & Young and the American Quality Foundation (1993). *International quality study: Best Practices report*. New York: Ernst & Young.
- Eslava, M., Haltiwanger, J., Kugler, A., & Kugler, M. (2004). The effects of structural reforms on productivity and profitability enhancing reallocation: evidence from Colombia. *Journal of Development Economics*, 75(2), 333-371.
- European Commission. (2010). *Europe 2020 – A European strategy for smart, sustainable, and inclusive growth*. Retrieved from: http://www.i4cense.org/sites/default/files/Europe_2020.pdf
- European Commission (2009). *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. Communication from the Commission on Critical Information Infrastructure Protection. Commission of the European Communities, Brussels.

- European Commission. (2004). Critical infrastructure protection in the fight against terrorism. *Communication COM*, 702. Commission Of The European Communities. Brussels, 20.10.2004.
- Ezell S. J. & Andes, S. M. (2010). ICT R&D Policies: An International Perspective. *IEEE Internet Computing*, 14(4), 76-80.
- Fallah, M. H. & Ibrahim, S. (2004). *Knowledge spillover and innovation in technological clusters*, International Association for Management of Technology (IAMOT), Washington, DC.
- Fare, R., Grosskopf, S., Norris, M., & Zhang, Z. (1994). Productivity growth, technical progress and efficiency change in industrialized countries. *American Economic Review*, 84(1), 66-83.
- Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39(2), 175-191.
- Federal Bureau of Investigation (1995). *Economic Espionage and Protection of Proprietary Economic Information Act of 1996*. Federal Bureau of Investigation Proposal, Washington, DC, 4 December.
- Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, ACM, 3-14.
- Fernandez-Ribas, A. & Shapira, P. (2009). The role of national and regional innovation programmes in stimulating international cooperation in innovation. *International Journal of Technology Management*, 48(4), 473-498.
- Field, A. (2009). Nonparametric tests. In *Discovering Statistics Using SPSS*. London: Sage Publications Limited, 539-583.
- Fisher, M. (2003). The New economy and networking. In *New economy handbook* (Ed. Jones D.C.). NY: Academic Press, 343-367.
- Fisher, R.A. (1925). *Statistical Methods for Research Workers*. Edinburgh: Oliver and Boyd.
- Fong, M. W. L. (2009). Digital divide: The case of developing countries. *Issues in Informing Science & Information Technology*, 6, 471-478.
- Fornell, C. & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 19(4), 440-452.

- Fornell, C. & Cha, J. (1994). Partial least squares. In *Advanced methods of marketing research* (ed. Bagozzi, R. P.), Oxford: Blackwell, 52-78.
- Fornell, C. & Robinson, W. T. (1983). Industrial organization and consumer satisfaction/dissatisfaction. *Journal of Consumer Research*, 9(4), 403-412.
- Fortin, C. (2005). The Digital Divide: ICT Development Indices 2004. *United Nations Conference on Trade and Development*. United Nations, New York and Geneva, retrieved from: http://unctad.org/en/Docs/iteipc20054_en.pdf.
- Foss, K & Foss, N.J. (2000). Economic organization in a process perspective. In *The Process of Competition*, (Ed. Krafft, J.). Cheltenham: Edward Elgar, 27-47.
- Fraenkel, J. R., & Wallen, N. E. (2006). How to design and evaluate research in education (sixth edition). New York: McGraw-Hill.
- Fratesi, U. & Senn, L. (2008). Regional Growth, Connections and Economic Modeling: An Introduction. In *Growth and Innovation of Competitive Regions* (Ed. Fratesi and Senn). Germany: Springer-Verlag Berlin Heidelberg, 3-27.
- Fraumann, E. (1997). Economic espionage: Security missions redefined. *Public Administration Review*, 57(4), 303-308.
- Freeman, C. (2002). Continental, national and sub-national innovation systems—complementarity and economic growth. *Research Policy*, 31(2), 191-211.
- Freudenberg, M. (2003). *Composite Indicators of Country Performance: A Critical Assessment*. OECD Science, Technology and Industry Working Papers, 2003/16, OECD Publishing.
- Fuhr, J.P. & Pociask, S.B. (2007). *Broadband services: economic and environmental benefits*. The American Consumer Institute.
- Gable, G.G., Sedera, D., & Chan, T. (2008). Re-conceptualizing information system success: the IS-Impact Measurement Model. *Journal of the Association for Information Systems*, 9(7), 377-408.
- GAO (U.S. Government Accountability Office) (2007). *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*. United States Government Accountability Office.
- Galletta, D.F., Ahuja, M.K., Hartman, A., Teo, T., & Peace, A.G. (1995). Social Influence and End-User Training. *Communications of the ACM*, 38(7), 70-79.

- Gallivan, M.J., Spitler, V.K. & Koufaris, M. (2005). Does Information Technology Training Really Matter? A Social Information Processing Analysis of Coworkers' Influence on IT Usage in the Workplace. *Journal of Management Information Systems*, 22(1), 153-192.
- Garcia-Muina, F. E., & Navas-Lopez, J. E. (2007). Explaining and measuring success in new business: the effect of technological capabilities on firm results. *Technovation*, 27(1), 30-46.
- Gassmann, O. (2006). Opening up the innovation process: towards an agenda. *R&D Management*, 36(3), 223-226.
- Gassmann, O. & Enkel, E. (2006). Towards a theory of open innovation: Three core process archetypes, *R&D Management*.
- Gassmann, O. & Enkel, E. (2004). Towards a Theory of Open Innovation: Three Core Process Archetypes. In *R&D Management Conference (RADMA) Lisbon, Portugal, July 6-9*.
- Gault, F. & Peterson, G. (2003). Measuring the diffusion of information and communication technology in society and its effects: Canadian experience. *International Statistical Review*, 71(1), 49-57.
- Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, 18(1), 1-7.
- Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, 35(2), III–XIV.
- Gefen, D., Straub, D. & Boudreau, M. (2000). Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, 7 (7), 1-78.
- Gefen, D. & Straub, D.W. (1997). Gender Differences in Perception and Adoption of E-Mail: An Extension to the Technology Acceptance Model. *MIS Quarterly*, 21(4), 389-400.
- Geisser, S. (1975). The predictive sample reuse method with applications. *Journal of the American Statistical Association*, 70(350), 320-328.
- Gibbs, J. L. & Kraemer, K. L. (2004). A Cross-Country Investigation of the Determinants of Scope of E-commerce Use: An Institutional Approach. *Electronic Markets*, 14(2), 124-137.
- Gibbs, J., Kraemer, K. L., & Dedrick, J. (2003). Environment and policy factors shaping global e-commerce diffusion: A cross-country comparison. *The Information Society*, 19(1), 5-18.

- Giovannini, E., Nardo, M., Saisana, M., Saltelli, A., Tarantola, A., & Hoffman, A. (2008). *Handbook on constructing composite indicators: methodology and user guide*. Paris: Organization for Economic Cooperation and Development (OECD).
- Goodhue, D.L. (1995). Understanding user evaluations of information systems. *Management Science*, 41(12), 1827-1844.
- Goodhue, D., Lewis, W., & Thompson, R. (2006). PLS, Small Sample Size and Statistical Power in MIS Research. In *Proceedings of the 39th Hawaii International Conference on System Sciences*, Kauai, Hawaii, January 4-7.
- Goodhue, D. L. & Straub, D. W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures. *Information & Management*, 20(1), 13-27.
- Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, Fall, 4(3), 102-135.
- Goodwin, L.D. & Goodwin, W.L. (1984). Qualitative vs. quantitative research or qualitative and quantitative research? *Nursing Research*, 33(6), pp. 378-380.
- Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.
- Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, 22(6), 461-485.
- Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C-Y, & Zhou, L. (2008). Cybersecurity, Capital Allocations and Management Control Systems. *European Accounting Review*, 17(2), 215-241.
- Gordon, L.A., Loeb, M.P., & Zhou, L. (2011). The Impact of Information Security Breaches: Has there been a Downward Shift? *Journal of Computer Security*, 19(1), 33-56.
- Gordon, M., Dakshinamoorthy, V., Wang, L., & Hammond, A. (2006). An Empirical Investigation of Innovation and Community Development through Information and Communication Technology. In *Proceedings of International Conference on Information and Communication Technologies and Development, ICTD '06, IEEE*, 218-222.
- Gordon, R. J. (1999). *Has the 'New Economy' rendered the productivity slowdown obsolete?* Northwestern University and NBER (National Bureau of Economic Research). Retrieved from: http://in3.dem.ist.utl.pt/master/03econ/lecture_8b.pdf.

- Gould, D. M., & Gruben, W. C. (1996). The role of intellectual property rights in economic growth. *Journal of development economics*, 48(2), 323-350.
- Grace-Martin, K. (2012). *Assessing the Fit of Regression Models*. StatNews #68, Cornell Statistical Consulting Unit, Cornell University, retrieved from: <http://www.cscu.cornell.edu/news/statnews/stnews68.pdf>.
- Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus*, December 18.
- Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, 17 (7), 109-122.
- Grazzi, M. & Vergara, S. (2011). *Determinants of ICT Access. ICT in Latin America: A Microdata Analysis* (Balboni et al. eds). Santiago de Chile: CEPAL.
- Greene, J.C. & Caracelli, V.J. (1997). *Advances in mixed-method evaluation: The challenges and benefits of integrating diverse paradigms*. San Francisco: Jossey-Bass.
- Greengard, S. (2012). The war against botnets. *Communications of the ACM*, 55(2), 16-18.
- Groh, A.P. & Wich, M. (2009). *A Composite Measure to Determine a Host Country's Attractiveness for Foreign Direct Investment*. IESE Business School University of Navarra Working Paper WP-833.
- Grossman, G. & Helman, E. (1991). *Innovations and growth in the global economy*. Cambridge, MA: MIT Press.
- Grupp, H. & Mogege, M. E. (2004). Indicators for National Science and Technology Policy. In *Handbook of Quantitative Science and Technology Research*. (Eds. Moed et al.). Netherlands: Kluwer Academic Publishers, 75-94.
- Gunasekaran, A., & Ngai, E. W. T. (2004). Virtual supply-chain management. *Production Planning & Control*, 15(6), 584-595.
- Guerard, J.B. (2001). A note on the forecasting effectiveness of the US leading economic indicators, *Indian Economic Review*, 36(1), 251-268.
- Haenlein, M. & Kaplan, A. M. (2004). A Beginner's Guide to Partial Least Squares Analysis. *Understanding Statistics*, 3(4), 283-297.
- Hair, J., Anderson, R., Tatham, R., & Black, W. (1998), *Multivariate Data Analysis*, Prentice Hall, Upper Saddle River, NJ.
- Hair, J. F., Black, W.C., Babin, B.J., Anderson, R.E., & Tatham, R.L. (2006). *Multivariate data analysis* (6th ed.). New Jersey: Pearson Prentice Hall.

- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice*, 19(2), 139-152.
- Hall, W. & Noursala, S. (2007). Facilitating emergence of an ICT industry cluster. In *ICE 2007 - 13th International Conference on Concurrent Enterprising - Concurrent (Collaborative) Innovation*, Sophia-Antipolis, France, June 4-6.
- Hansen, G. & Wernerfelt, B. (1989). Determinants of Firm Performance: The Relative Importance of Economic and Organizational Factors, *Strategic Management Journal*, 10(5), 399-411.
- Hargittai, E. & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review*, 30(1), 95-107.
- Harttgen, K. & Vollmer, S. (2011). *Inequality Decomposition without Income or Expenditure Data: Using an Asset Index to Simulate Household Income*. Human Development Research Paper. UNDP-HDRO, New York.
- Hayes, A.F. (2009). Beyond Baron and Kenny: Statistical mediation analysis in the new millennium. *Communication Monographs*, 76(4), 408-420.
- Hayes, B. C., Bartle, S. A., and Major, D. A. (2002). Climate for opportunity: A conceptual model. *Human Resource Management Review*, 12(3), 445-468.
- Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in international marketing*, 20(1), 277-319.
- Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy*, 1(4), 1-23.
- Heshmati, A. & Yang, W.S. (2006). *Contribution of ICT to the Chinese Economic Growth*. Techno-Economics and Policy Program Discussion Paper, Seoul National University.
- Higgins, C. A., Duxbury, L. E., & Irving, R. H. (1992). Work-family conflict in the dual-career family. *Organizational Behavior and Human Decision Processes*, 51(1), 51-75.
- Higgins, K. J. (2010). Security Incidents Rise in Industrial Control Systems. retrieved from: <http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/224400280/security-incidents-rise-in-industrial-control-systems.html>.
- Hollander, M. & Wolfe, D. A. (1999). *Nonparametric Statistical Methods* (2nd ed.). New York: Wiley-Interscience.
- Hollis, D. (2011). An e-SOS for Cyberspace. *Harvard International Law Journal*, 52(2), 374.

- Holmstrom, B. & Milgrom, P. (1994). The Firm as an Incentive System. *American Economic Review*, 84(4), 972-991.
- Homeland Security (DHS) & Department of Energy (DOE) (2007). *Energy: Critical Infrastructure and Key Resources Sector – Specific plan as Input to the National Infrastructure protection plan*. Department of Energy, Washington, DC.
- Homeland Security (DHS) & Department of Energy (DOE) (2010). *Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*, retrieved from: <http://www.hsdl.org/?view&did=7902>.
- Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual review of ecology and systematics*, 4(1973), 1-23.
- Howells, J. (1990). The internationalization of R & D and the development of global research networks. *Regional Studies*, 24(6), 495-512.
- Howells, J. R. (1995). Going global: the use of ICT networks in research and development. *Research Policy*, 24(2), 169-184.
- Hox, J. J. & Boeije, H. R. (2005). Data Collection, Primary vs. Secondary. *Encyclopedia of Social Measurement*, 1, 593-799.
- Huang, C. C. & Hsieh, C. C. (2010). Social relevance, then protection: A social-technical approach to CIIP. In *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, IEEE, 239-243.
- Huggins, R. (2003). Creating a UK competitive index: regional and local benchmarking. *Regional Studies*, 37(1), 89-96.
- Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic Management Journal*, 20(2), 195-204.
- Hunter, J. E. (1997). Needed: A ban on the significance test. *Psychological science*, 8(1), 3-7.
- Huselid, M.A. (1995). The Impact of Human Resource Management Practices on Turnover, Productivity, and Corporate Financial Performance. *Academy of Management Journal*, 38(3), 635-672.
- IDC (2001). *World Times Information Society Index*. International Data Corporation, Framlingham, MA.
- InfoDev- Information for Development Program (2007). *ICT, Innovation, and Economic Growth in Transition Economies*. The International Bank for Reconstruction and Development / The World Bank.

- Institute for Information Infrastructure Protection (I3P) (2009). *National Cyber Security: Research and Development Challenges*. Retrieved from: <http://www.cyber.st.dhs.gov/docs/i3pnationalcybersecurity.pdf>.
- ISTAG (Information Society Technologies Advisory Group) (2011). *Orientations for EU ICT R&D and Innovation beyond 2013*. European Commission- Information Systems and Media, Belgium.
- ITI (Information Technology Industry Council) (2011). *The IT Industry's Cybersecurity Principles for Industry and Government*. ITI, Washington, D.C. Retrieved from: <http://www.itic.org/clientuploads/ITI - Cybersecurity Principles for Industry and Government - Final1.31.11.pdf>.
- ITU- International Telecommunications Union (2012). *Measuring the Information Society*. Geneva: International Telecommunications Union, retrieved from: http://www.itu.int/en/ITUUD/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.
- ITU- International Telecommunications Union (2011). *Measuring the Information Society*. Geneva: International Telecommunications Union, retrieved from: <http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf>.
- ITU- International Telecommunications Union (2010). Creation of national computer incident response teams, particularly for developing countries and cooperation between them. Resolution 69 (Hyderabad, 2010). *World Telecommunications Development Conference*, retrieved from: http://www.itu.int/osg/csd/intgov/resolutions_2010/resolution69.pdf.
- ITU- International Telecommunications Union (2009). *Confronting the Crisis: its Impact on the ICT Industry*. International Telecommunication Union.
- ITU- International Telecommunications Union (2008). *Final Report of World Telecommunication/ICT Indicators Meeting (Document 016-Erev1)*. Geneva: International Telecommunication Union.
- ITU- International Telecommunications Union (2008). *Global Cybersecurity Agenda: A Framework for International Cooperation in Cybersecurity*. Geneva: International Telecommunication Union, Corporate Strategy Division, retrieved from: <http://www.itu.int/osg/csd/cybersecurity/gca/docs/brochure.pdf>.
- ITU- International Telecommunications Union (2007). *Measuring the Information Society – ICT Opportunity Index and World Telecommunication/ICT Indicators*. International Telecommunication Union.

- ITU- International Telecommunications Union (2006a). *World Telecommunication/ICT Development Report: Measuring ICT for social and economic development*. International Telecommunication Union.
- ITU- International Telecommunications Union (2006). *World Information Society Report*. International Telecommunication Union.
- ITU- International Telecommunications Union (2005). *A Comparative Analysis of Cyber security Initiatives Worldwide*. WSIS Thematic Meeting on Cyber security, Geneva, 28 June-1 July.
- ITU- International Telecommunications Union (2002). *Mobile/Internet index: Internet for a Mobile Generation*. International Telecommunication Union.
- Jablonsky, D. (2001). Army transformation: A tale of two doctrines. In *Transforming defense* (Crane, C. Ed.). Carlisle, PA: Strategic Studies Institute.
- Jalava, J., & Pohjola, M. (2007). ICT as a source of output and productivity growth in Finland. *Telecommunications Policy*, 31(8), 463-472.
- Jarvenpaa, S. L., & Ives, B. (1994). The global network organization of the future: Information management opportunities and challenges. *Journal of Management Information Systems*, 10 (4), 25-57.
- Jensen, M. & Mahan, A. K. (2007). Toward a Single ICT Index: Considerations for the Formulation of a Single ICT Index for the ITU. *International Telecommunication Union*.
- Jha-Thakur, U. (2011). Environmental Impact Assessment Follow-Up in India: Exploring Regional Variation. *Journal of Environmental Assessment Policy and Management*, 13(3), 435-458.
- Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, 24(4), 602-611.
- Johannessen, J-A., Olansen, J. & Olsen, B. (1999). Strategic Use of Information Technology for Increased Innovation and Performance. *Information Management & Computer Security*, 7(1), 5-22.
- Johnson, B., Lorenz, E., & Lundvall, B. A. (2002). Why all this fuss about codified and tacit knowledge? *Industrial and corporate change*, 11(2), 245-262.
- Johnston, R. (2003). *Clusters: A Review. Mapping Australia's Science and Innovation System Taskforce*. Department of Education, Science, and Training. Australian Center for Innovation Limited.

- Jonsson, E. (1998). An integrated framework for security and dependability. In *Proceedings of the 1998 workshop on new security paradigms*, ACM, January, 22-29.
- Jorgenson, D.W. (2001). Information Technology and the U.S. Economy. *American Economic Review*, 91(1), 1-32.
- Jorgenson, D. W., Ho, M. S., & Stiroh, K. J. (2002). Projecting Productivity Growth: Lessons from the U.S. Growth Resurgence. *Federal Reserve Bank of Atlanta Economic Review*, 87(3), 1-13.
- Kaarst-Brown, M. L. (2004). *How Organizations Keep Information Technology Out: The Interaction of Tri-Level Influences on Organizational and IT Culture*. Working Paper IST-MLKB: 2004-2, School of Information Studies, Syracuse University.
- Kanter, J. (2010). In Europe, Companies Work the Angles on the Carbon Trade. *New York Times*, October 10, retrieved from: http://www.nytimes.com/2010/10/11/business/energy-environment/11green.html?pagewanted=all&_r=0.
- Kaplan H. (2002). Event reporting, mindfulness and the high reliability organization: Is the glass half empty. *Vox Sanguinis*, 83(s1), 337-339.
- Karaev, A., Koh, S.L., & Szamosi, L.T. (2007). The cluster approach and SME competitiveness: a review. *Journal of Manufacturing Technology Management*, 18(7), 818-835.
- Karsten, H. (1995). It's like everyone working around the same desk: Organizational Readings of Lotus Notes. *Scandinavian Journal of Information Systems*, 7(1), 3-32.
- Kayworth, T. & Whitten, D. (2012). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, 9(3), 163-175.
- Keen, P.G.W. (1987). Telecommunications and Organizational Choice. *Communication Research*, 14(5), 588-606.
- Kelsey, J. T. (2008). Hacking into International Humanitarian Law: the principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review*, 106(7), 1427-1451.
- Kendall, M. & Gibbons, J. D. (1990). *Rank Correlation Methods* (5th ed.). New York: Oxford University Press, 1990.
- Kiiski, S. & Pohjola, M. (2002). Cross-country diffusion of the Internet. *Information Economics and Policy*, 14(2), 297-310.
- Kim, S. (2011). Testing a revised measure of public service motivation: Reflective versus formative specification. *Journal of Public Administration Research and Theory*, 21(3), 521-546.

- Kimchi, J., Polivka, B., & Stevenson, J. S. (1991). Triangulation: Operational definitions. *Nursing Research*, 40(6), 364-366.
- Klein, K. J. & Knight, A. P. (2005). Innovation implementation overcoming the challenge. *Current Directions in Psychological Science*, 14(5), 243-246.
- Klein, K. J., & Sorra, J. S. (1996). The challenge of innovation implementation. *Academy of management review*, 21(4), 1055-1080.
- Kleinbaum, D.G., Kupper, L.L., & Muller, K.E. (1988). *Applied regression analysis and other multivariable methods*. Boston: PWS-KENT.
- Kleinknecht, A., Van Montfort, K., & Brouwer, E. (2002). The non-trivial choice between innovation indicators. *Economic Innovation and New Technologies*, 11(2), 109-121.
- Knapp, T. R. (1978). Canonical correlation analysis: A general parametric significance testing system. *Psychological Bulletin*, 85(2), 410-416.
- Koellinger, P., 2008. The relationship between technology, innovation, and firm performance - empirical evidence from e-business in Europe. *Research Policy*, 37(8), 1317-1328.
- Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., & Savage, S. (2010). Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy (SP)*, IEEE, 447-462.
- Kotlarsky, J. & Oshri, I. (2005). Social ties, knowledge sharing and successful collaboration in globally distributed system development projects. *European Journal of Information Systems*, 14(1), 37-48.
- Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Berlin: Springer Verlag.
- Kuhn, A. (1974). *The Logic of Social Systems*. San Francisco: Jossey-Bass.
- Kumar, K. & van Dissel, H.G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems. *MIS Quarterly*, 20(3), 279-300.
- Kumar, N. (2003). Intellectual property rights, technology and economic development: Experiences of Asian countries. *Economic and Political Weekly*, 38(3), 209-226.
- Landes, D.S. (1998). *The Wealth and Poverty of Nations: Why are Some So Rich and Others So Poor?* New York: W.W. Norton.
- Landau, S. & Stytz, M. R. (2005). Overview of cyber security: a crisis of prioritization. *IEEE Security & Privacy*, 3(3), 9-11.

- Lanvin, B. & Passman, P., 2008, *Building e-skills for the Information Age*, in 'The Global Information Technology Report 2007-2008: Fostering Innovation through Networked Readiness,' S. Dutta and I. Mia (eds.), pp. 77-90, Palgrave Macmillan, April 2008.
- Lanyon, S. M. (1987). Jackknifing and Bootstrapping: Important "New" Statistical Techniques for Ornithologists. *The Auk*, 104(1), 144-146.
- Law, K. S. & Wong, C. S. (1999). Multidimensional constructs M structural equation analysis: An illustration using the job perception and job satisfaction constructs. *Journal of Management*, 25(2), 143-160.
- LeBel, P. (2008). The role of creative innovation in economic growth: Some international comparisons. *Journal of Asian Economics*, 19, 334 – 347.
- LeBel, P. (2005). Optimal Choices for risk management: The economic value of institutional reform in globalizing economies. *Global Business and Finance Review*, 10(3), 113 – 128.
- Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. *MIS Quarterly*, 33(2), 237-262.
- Lee, B. & Barua, A. (1999). An Integrated Assessment of Productivity and Efficiency Impacts of Information Technology Investments: Old Data, New Analysis and Evidence. *Journal of Productivity Analysis*, 12(1), 21–43.
- Lee, O.K.D., Banerjee, P., Lim, K. H., Kumar, K., Hillegersberg, J.V., & Wei, K. K. (2006). Aligning IT components to achieve agility in globally distributed system development. *Communications of the ACM*, 49(10), 48-54.
- Lee, Y. Lee, J. & Lee, Z. (2002). Integrating Software Lifecycle Process Standards with Security Engineering, *Computers and Security*, 21(4), 345-355.
- Lerner, E.J. (1984). International Data Wars are Brewing. *IEEE Spectrum*, 21(7), 45-49.
- Lesk, M. (2011). Cybersecurity and Economics. *IEEE Security & Privacy*, 9(6), 76-79.
- Lewin, A.Y., Massini, S., & Peeters, C. (2009). Why are companies offshoring innovation? The emerging global race for talent. *Journal of International Business Studies*, 40(6), 901–925.
- Lewis, J. A. (2010). *The cyber war has not Begun*. Center for Strategic and International Studies, retrieved from:
https://www.twq.com/files/publication/100311_TheCyberWarHasNotBegun.pdf.

- Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies, Washington, DC., 12.
- Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., & Zhang, P. (2010). Smart transmission grid: Vision and framework. *IEEE Transactions on Smart Grid*, 1(2), 168-177.
- Li, X. (2007). International actions against cybercrime: Networking legal systems in the networked crime scene. *Webology*, 4(3), 1-45.
- Liaw, S.S. (2002). Understanding user perceptions of world-wide web environments. *Journal of Computer Assisted Learning*, 18(2), 137-48.
- Linden, G., Kraemer, K. L., & Dedrick, J. (2009). Who captures value in a global innovation network?: the case of Apple's iPod. *Communications of the ACM*, 52(3), 140-144.
- Livari, J. (2005). An empirical test of the DeLone-McLean model of Information Systems success. *The Data Base for Advances in Information Systems*, 36(2), 8-27.
- Lohmoller, J. B. (1989). *Latent variable path modeling with partial least squares*. Heidelberg: Physica-Verlag.
- Lopez-Claros, A. & Mata, Y. N. (2010). The Innovation Capacity Index: Factors, Policies, and Institutions Driving Country Innovation. In *The Innovation for Developemnt Report 2009 – 2010*. European Business School, 3-57.
- Lopez, J., Alcaraz, C., & Roman, R. (2007). On the protection and technologies of critical information infrastructures. *Foundations of security analysis and design IV, Lecture Notes in Computer Science*, 4677, 160-182.
- Lovell, C.A.K., Pastor, J.T., & Turner, J.A. (1995). Measuring macroeconomic performance in the OECD: a comparison of European and non-European countries. *European Journal of Operational Research*, 87(3), 507-518.
- Lu, I. R., Kwan, E., Thomas, D. R., & Cedzynski, M. (2011). Two new methods for estimating structural equation models: An illustration and a comparison with two established methods. *International Journal of Research in Marketing*, 28(3), 258-268.
- Luallen, M. & Hamburg, S. (2010). RISI - The Repository of Security Incidents for process control. Industrial automation or SCADA. *Control Engineering*, retrieved from: <http://www.securityincidents.org/>.
- Lucas, H.C. (1991). *Information Technology and the Productivity Paradox: Assessing the value of Investing in IT*. New York: Oxford University Press, Inc.

- Lucas, R. E. (1988). On the mechanics of economic development. *Journal of monetary economics*, 22(1), 3-42.
- Lundvall, B. A. (1992). *National Systems of Innovation: Towards a Theory of Innovation and Interactive Learning*, London: Pinter Publishers.
- Lyytinen, K. & Damsgaard, J. (2001). What's wrong with the diffusion of innovation theory: The case of a complex and networked technology. In *Diffusing Software Product and Process Innovations* (Eds. Ardis, M. A. and Marcolin, B. L.). Norwell, MA: Kluwer Academic Publishers, 173–190.
- MacEachern, C. (Fall 2011). E-Canada and Cyber –attacks: Peril and Policy, *Dalhousie Journal of Interdisciplinary Management*, 7, 1-15.
- MacKenzie, D. I. & Royle, J. A. (2005). Designing occupancy studies: general advice and allocating survey effort. *Journal of Applied Ecology*, 42(6), 1105-1114.
- Malhotra, A., Majchrzak, A., Carman, R., & Lott, V. (2001). Radical innovation without collocation: a case study at Boeing-Rocketdyne. *MIS Quarterly*, 25(2), 229–249.
- Malmberg, A. & Maskell, P. (2006). Localized learning revisited. *Growth and Change*, 37(1), 1-18.
- Mansfield-Devine, S. (2011). Anonymous: serious threat or mere annoyance? *Network Security*, 2011(1), 4-10.
- Marcoulides, G. A. & Saunders, C. (2006). Editor's comments: PLS: a silver bullet? *MIS Quarterly*, 30(2), iii-ix.
- Mathison, S. (1988). Why triangulate? *Educational Researcher*, 77(2), 13-17.
- Mazen, A.M., Graf, L.A., Kellogg, C.E., & Hemmasi, M. (1987). Statistical power in contemporary management research. *Academy of Management Journal*, 8(4), 403-410.
- Mbatha, B. (2009). Web-based technologies as a double-edged sword in improving work productivity in government departments in South Africa: The case of Zululand district municipality, in *Proceedings of International Conference on Computers and Industrial Engineering*, (ICCIE, 25 August 2009), IEEE, 1914-1921.
- McAfee (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. McAfee, Inc., retrieved from: <http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf>.

- McAfee (2011). *Global Energy Cyberattacks: "Night Dragon"*. McAfee, Inc., retrieved from: <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.
- McArthur, J.W. & Sachs, J.D. (2002). The Growth Competitiveness Index: Measuring Technological Advancement and the Stages of Development. In *The Global Competitiveness Report 2001-2002* (Porter, M.E., Sachs, J.D., Cornelius, P.K., McArthur, J.W., & Schwab, K., Eds.). New York: Oxford University Press, 28-51.
- McCalman, P. (2002). National patents, innovation, and international agreements. *The Journal of International Trade & Economic Development*, 11(1), 1-14.
- McConnell, M. & Hamilton, B.A. (2002). Information Assurance in the Twenty-First Century, *Security and Privacy*, 35(4), 16-19.
- Merabti, M., Kennedy, M., & Hurst, W. (2011). Critical infrastructure protection: A 21st century challenge. In *2011 International Conference on Communications and Information Technology (ICCIT)*, IEEE, 1-6.
- Merriam-Webster, Inc (Ed.). (2003). *Merriam-Webster's collegiate dictionary*. Merriam-Webster.
- Metcalf J.S. & Andrew, J. (2005) Emergent innovation systems and the delivery of clinical services: the case of intra-ocular lenses. *Research Policy*, 43(9), 1283-1304.
- Milgrom, P. & Roberts, J. (1995). Complementarities and fit: strategy, structure, and organizational change in manufacturing. *Journal of Accounting and Economics*, 19(2-3), 179-208.
- Milgrom, P. & Roberts J. (1990). The economics of modern manufacturing: technology, strategy, and organization. *American Economic Review*, 80(3), 511-528.
- MIT & Harvard (2010). Understanding the Dynamics of Cyber International Relations. Harvard. The Minerva Initiative -Fostering a Community of Strategic ScholarshipFort Lesley J. McNair, September 16. Retrieved from: <http://web.mit.edu/ecir/pdf/ndu-slides-9-16.pdf>.
- Mitchell, E.S. (1986). Multiple triangulation: A methodology for nursing science. *Advances in Nursing Science*, 8(3), 18-26.
- Mook, D. G.(1983). In defense of external invalidity. *American Psychologist*, 38 (4), 379-387.
- Montgomery, D. B. & Morrison, D. G. (1973). A Note on Adjusting R^2 . *Journal of Finance*, 28(4), 1009-1013.

- Munda G. & Nardo M. (2003), *On the Methodological Foundations of Composite Indicators Used for Ranking Countries*. Universitat Autònoma de Barcelona, Spain.
- Murphy, K. R. & Myers, B. (2004). *Statistical power analysis: A simple and general model for traditional and modern hypothesis tests (2nd ed.)*. Mahwah, NJ: Lawrence Erlbaum Associates.
- Musa, P.F., Meso, P., & Mbarika, V.W.A. (2005). Toward Sustainable Adoption of Technologies for Human Development in Sub-Saharan Africa: Precursors, Diagnostics, and Prescriptions. *Communications of the AIS*, 15(1), 592-608.
- Mutula, S.M. & van Brakel, P. (2006). An Evaluation of E-Readiness Assessment Tools with Respect to Information Access: Towards an Integrated Information Rich Tool. *International Journal of Information Management*, 26(3), 212-223.
- Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, 21(2), 241–242.
- Nambisan, S. (2003). Information Systems as a Reference Discipline for New Product Development. *MIS Quarterly*, 27(1), 1-18.
- Nardo, M., Saisana, M., Saltelli, A., & Tarantola, S. (2005). *Tools for Composite Indicators Building*. European Commission JRC, EUR 21682.
- Nelson, R.R. & Winter, S.G. (2002). Evolutionary theorizing in economics. *Journal of Economic Perspectives*, 16(2), 23–46.
- Nemeth C. & Cook R. (2007). Reliability versus resilience: what does healthcare need? In *Proceedings of the Human Factors and Ergonomics Society 51st Annual Meeting*, Santa Monica, CA., 621-625.
- Neumann, P. G. (2007). Communication in industrial automation - what is going on? *Control Engineering Practice*, 15(11), 1332–1347.
- Neumann, P.G. (1999). Information is a Double-Edged Sword. *Communications of the ACM*, 42(7), 120.
- Newmann, W. W. (2002). Reorganizing for national security and homeland security. *Public Administration Review*, 62(s1), 126-137.
- Nickolov, E., (2005). Critical information infrastructure protection: analysis, evaluation and expectations. *Information and Security – An International Journal*, 17, 105–119.

- Niederman, F. (2005). International business and MIS approaches to multinational organizational research: the cases of knowledge transfer and IT workforce outsourcing. *Journal of International Management*, 11(2), 187-200.
- Nobel, R. & Birkinshaw, J. (1998). Innovation in Multinational Corporations: Control and Communication Patterns in International R&D Operations. *Strategic Management Journal*, 19(5), 479-496.
- Nordhaus, W. (1997). Do Real-Output and Real-Wage Measures Capture Reality? The History of Lighting Suggests Not. In *The Economic of New Goods* (Bresnahan & Gordon, Eds.). Chicago: University of Chicago Press for NBER, 29-66.
- North, D. (1990). *Institutions, Institutional change, and Economic Performance*. Cambridge: Cambridge University Press.
- Nunnally, J. C. & Bernstein (1994). *I. H. Psychometric theory*. New York: McGraw-Hill.
- OECD/JRC-European Commission. (2008). Handbook on Constructing Composite Indicators. *Methodology and User Guide*, Brussels: OECD, 148.
- OECD - The Organization for Economic Co-operation and Development - (2008). *Malicious Software (Malware): A Security threat to the Internet Economy*. OECD.
- OECD / Eurostat (2005). *OECD Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data* (3rd edition). OECD / Eurostat Joint Publication.
- OECD (2005). *Financing ICTs for Development: Efforts of DAC Members – Review of Recent Trends of ODA and its Contribution*. Development Assistance Committee (DAC), Paris.
- OECD (2004). *The OECD-JRC Handbook on Practices for Developing Composite Indicators*. Paper presented at the OECD Committee on Statistics, 7-8 June 2004, OECD, Paris.
- OECD (2003). *Composite indicators of country performance: a critical assessment*, DST/IND(2003)5, Paris.
- OECD (1999). *Boosting Innovation: The Cluster Approach*. OECD, Paris.
- O'Hara, J. (2010). Cyber-Espionage: A Growing Threat to the American Economy, *COMMLAW CONSPPECTUS*, 19, 241-275.
- Olfman, L. & Pitsatorn, P. (2000). End-User Training Research: Status and Models for the Future, in: *Framing the Domains of IT Management: Projecting the Future through the Past* (Ed. Zmud, R.W.,). Cincinnati, OH: Pinnaflex, 129-146.

- Oliner, S.D. & Sichel, D.E. (2002). Information Technology and Productivity: Where Are We Now and Where Are We Going? Federal Reserve Bank of Atlanta. *Economic Review*, 87(Fall), 15-44.
- Olivier, M. (2001). Towards a Configurable Security Architecture. *Data Engineering*, 38(2), 121-145.
- Ollo-Lopez, A. & Aramendia-Muenta, M. E. (2012). ICT impact on competitiveness, innovation, and environment. *Telematics and Informatics*, 29(2), 204-210.
- Olmstead, S. & Siraj, A. (2009). Cyber terrorism: The Threat of Virtual Warfare. *CROSSTALK: The Journal of Defense Software Engineering*, November-December, 16-18.
- Olsen, W. K. (2004). Triangulation in social research: qualitative and quantitative methods can really be mixed. In *Developments in Sociology: An Annual Review* (ed. Holborn, M.), Ormskirk, Lancs, UK: Causeway Press.
- Omay, T. & Baleanu, D. (2009). Solving Technological Change Model by Using Fractional Calculus. In *Innovation Policies, Business Creation, and Economic Development* (Ed. Aydogan, N.). New York: Springer Science and Business Media, LLC.
- Oppliger, R. (2007). IT Security: In Search of the Holy Grail, *Communications of the ACM*, 50(2), 96–98.
- Orlikowski, W. J. & Gash, D. C. (1993). *Technological Frames: Making Sense of Information Technology in Organizations*. Working Paper #3627-93, Alfred P. Sloan School of Management, MIT.
- Owen, R. S. (2008). Infrastructures of Cyber Warfare. In *Cyber warfare and cyber terrorism*. Hershey, PA: Information Science Reference – IGI Global.
- Pagallo, U. (2010). A new “Ring of Gyges” and the meaning of invisibility in the information revolution. *Journal of Information, Communication and Ethics in Society*, 8(4), 364-376.
- Palfrey, J. & Gasser, U. (2007). *Mashups Interoperability and eInnovation: Case Study*. Berkman Publication Series. Harvard University Research Center of Information Law and University of St. Gallen, St. Gallen.
- Palvia, P.C. (1997). Developing a Model of the Global and Strategic Impact of Information Technology. *Information & Management*, 32(5), 229-244.
- Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, 2012(1), 8-11.

- Parente, S. & Prescott, E. (1994). Barriers to Technology Adoption and Development. *Journal of Political Economy*, 102(2), 298 – 321.
- Parente, S. & Prescott, E. (1999). Monopoly Rights: A Barrier to Riches. *American Economic Review*, 89(5), 1216 – 1233.
- Parliament of Australia (2010). *Nature, Prevalence, and Economic Impact of Cybercrime, in Hackers, Fraudsters, and Botnets: Tackling the Problem of Cyber Crime*. House of Representatives, 9-42.
- Patel, P. & Paritt, K. (1994). The Nature and Economic Importance of National Innovation Systems. *STI Review OECD*, 3(14), 9-32.
- Patrakosol, B. & Olson, D. L. (2007). How interfirm collaboration benefits IT innovation. *Information & Management*, 44(1), 53–62.
- Patzer, G. L. (1995). *Using Secondary Data in Marketing Research: United States and Worldwide*. USA: Greenwood Publishing Group, Inc.
- Pavlou, P. A. & Chai, L. (2002). What drives electronic commerce across cultures? A cross-cultural empirical investigation of the theory of planned behavior. *Journal of Electronic Commerce Research*, 3(4), 240-253.
- Pedhazur, E. J. & Schmelkin, L. P. (1991). *Measurement, design, and analysis: An integrated approach*. Hillsdale, NJ: Erlbaum.
- Pedhazur, E.J. (1997). *Multiple Regression in Behavioral Research – Explanation and Prediction (3rd ed.)*. Orlando, FL: Holt, Harcourt Brace & Company.
- Pedhazur, E. J. (1982). *Multiple Regression in Behavioral Research*, New York: Holt, Rinehart, and Winston.
- Perry, G. & Lederman, D. (1999). *Adjustments after Speculative Attacks in Latin America and Asia: A Tale of Two Regions*. Washington: The International Bank for Reconstruction and Development/ The World Bank.
- Peters, M.A, Marginson, S., & Muphy, P. (2009). *Creativity and the Global Knowledge Economy*. New York: Peter Lang.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656.
- Pfeffer, J. & Sutton, R. I. (1999). *The knowing-doing gap: How smart companies turn knowledge into action*. Boston, MA: Harvard Business Press.

- Pfleeger, C. P. & Pfleeger, S. L. (2011). *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*. Westford, MA: Prentice Hall Professional.
- Pfleeger, S. L. & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, 25(1), 35-42.
- Phelps, E.S. (2009). Entrepreneurial Culture. *The Wall Street Journal*, February 12.
- Pilat, D. & Wolfl, A. (2004). ICT production and ICT use: what role in aggregate productivity growth? In *The Economic Impact of ICT: Measurement, Evidence, and Implications*. OECD, Paris: OECD Publications Service, 85-104.
- Pigman, G. A. (2007). *The World Economic Forum: A multi-stakeholder approach to global governance*. New York: Routledge.
- Plichta, S. B., Kelvin, E., & Munro, A. (2013). *Munro's Statistical Methods for Healthcare Research (6th ed.)*, New York: Wolters Kluwer, Lippincott, Williams & Wilkins.
- Poel, M. & Bodea, G. (2008). *The policy mix for e-Business use by SMEs: Inspiration from Denmark, Finland and other countries*. TNO Report 35569. Dutch Ministry of Economic Affairs.
- Pohjola, M. (2001). Information Technology and Economic Growth: A Cross-Country Analysis in *Information Technology, Productivity, and Economic Growth: International Evidence and Implications for Economic Development*, (Ed. Pohjola, M.). Oxford: Oxford University Press.
- Ponemon Institute (2010), *Cybersecurity Readiness Study: Benchmark Research of IT Security Leaders in the US and Europe*. Ponemon Institute.
- Porter, M. (1985). *Competitive Advantage, Creating and Sustaining Superior Performance*. New York: The Free Press.
- Porter, M.E. (1990). *The Competitive Advantage of Nations*. New York: Free Press.
- Powell, T.C. & Dent-Micallef, A. (1997) Information Technology as Competitive Advantage: The Role of Human, Business, and Technology Resources. *Strategic Management Journal*, 18(5), 375-405.
- Prahalad, C.K. & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review*, 66(3), 71-91.

- Prasad, A. (2011). Understanding It Business Value Creation and Evaluation in Least Developed Economies. *The Electronic Journal on Information Systems in Developing Countries*, 47(1), 1-18.
- Preacher, K. J. & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40(3), 879-891.
- Preacher, K. J. & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, Instruments, & Computers*, 36(4), 717-731.
- Prescott, M. B. & Van Slyke, C. (1996). The Internet as an innovation. In *Proceedings of the Association for Information System Americas Conference*, August.
- Pritcett, L. (1995). *Divergence, Big Time*. Background Paper for World Development Report 1995. The World Bank.
- PWC- PricewaterhouseCoopers (2011). *Cybercrime: protecting against the growing threat Global Economic Crime Survey*. PricewaterhouseCoopers, retrieved from: http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf
- Quenouille, M. H. (1956). Notes on bias in estimation. *Biometrika*, 43(3-4), 353-360.
- Quinn, J.B. (1996), The productivity paradox is false: information technology improves service performance. In *Advances in Service Marketing and Management* (Swartz et al. eds), 5, Connecticut: JAI Press Inc., Greenwich, 71-84.
- Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cybersecurity risk assessment for SCADA and DCS networks. *ISA transactions*, 46(4), 583-594.
- Ramsey, F. (1928). A mathematical theory of saving, *Economic Journal*, 38(11), 543 – 559.
- Raskin, J. (1997). Looking for a Humane Interface: Will Computers Ever Become Easy to Use? *Communications of the ACM*, 40(2), 98-101.
- Rebello, S. (1991). Long-run policy analysis and long-run growth. *Journal of Political Economy*, 99(3), 500-521.
- Reinartz, W. J., Haenlein, M., & Henseler, J. (2009). An Empirical Comparison of the Efficacy of Covariance-based and Variance-based SEM. A Faculty & Research Working Paper (Working Paper #: 2009/44/MKT). INSEAD, August 27.

- Reinartz, W., Krafft, M., & Hoyer, W. D. (2004). The customer relationship management process: Its measurement and impact on performance. *Journal of marketing research*, 41(3), 293-305.
- Reijswoud, V.E.V. (2009). Appropriate ICT as a Tool to Increase Effectiveness in Ict4D: Theoretical Considerations and Illustrating Cases. *Electronic Journal of Information Systems in Developing Countries*, 39(9), 1-18.
- Rigby, D., Woodhouse, P., Young, T., Burton, M., 2001. Constructing a farm level indicator of sustainable agricultural practice. *Ecol. Econ.* 39, 463–478.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11-25.
- Rivard, S., Raymond, L., & Verreault, D. (2006). Resource-Based View and Competitive Strategy: an Integrated Model of the Contribution of Information Technology to Firm Performance. *Journal of Strategic Information Systems*, 15(1), 29-50.
- Rivkin J. (2000). Imitation of complex strategies, *Management Science*, 46(6), 824–844.
- Roelandt, T.J.A. & den Hertog, P. (1999). Cluster analysis and cluster based policy making in OECD countries. An introduction to the theme. In: *Boosting Innovation: The Cluster Approach (OECD, Ed.)*. OECD, Paris, 9–23.
- Rogers, E.M. (1995). *Diffusion of Innovation (4th edition)*. New York: Free Press.
- Rogers, P. P., Ojha, D., & White, R. E. (2011). Conceptualizing complementarities in manufacturing flexibility: a comprehensive view. *International Journal of Production Research*, 49(12), 3767-3793.
- Romer, P. M. (1994). New goods, old theory and the welfare costs of trade restrictions, *Journal of Development Economics*, 43(5), 5-38.
- Romer, P.M. (1990). Endogenous technological change. *Journal of Political Economy*, 98(5), 71-102.
- Romer, P. M. (1986). Increasing returns and long-run growth. *Journal of Political Economy*, 94(5), 1002-1037.
- Romer H. & White W. (2006). *Security inside out*. Oracle security solutions. Retrieved from: <http://www.oracle.com/us/products/059502.pdf>
- Rosenberg, N. (2004). *Innovation and Economic Growth*. OECD. Retrieved from: <http://www.oecd.org/dataoecd/55/49/34267902.pdf>
- Rosenburg, N. & Birdzell, L.E., (1986). *How the West Grew Rich*. New York: Basic Books.

- Rosenkopf, L. & Nerkar, A. (2001). Beyond local search: Boundary-spanning, exploration, and impact in the optical disk industry. *Strategic Management Journal*, 22(4), 287-306.
- Rosenzweig, P. (2010). The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence. In *Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council. Washington, D.C.: National Academies Press, 245-270.
- Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing*, 19(4), 305-335.
- Saisana, M. & Tarantola, S. (2002). State-of-the-art report on current methodologies and practices for composite indicator development. EUR 20408 EN Report, European Commission, JRC, Italy.
- Saisana, M., Saltelli, A., & Tarantola, S. (2005). Uncertainty and Sensitivity analysis techniques as tools for the quality assessment of composite indicators. *Journal of the Royal Statistical Society Series A*, 168(2), 307-323.
- Sala-I-Martin, X., Bolbao-Osorio, B., Blanke, J., Hanouz, M. D., & Geiger, T. (2012). The Global Competitiveness Index 2011–2012: Setting the Foundations for Strong Productivity. In *The Global Competitiveness Report 2011-2012*. Geneva: World Economic Forum.
- Sambamurthy, V. & Chin, W. W. (1994). The Effects of Group Attitudes Toward Alternative GDSS Designs on the Decision-making Performance of Computer-Supported Groups. *Decision Sciences*, 25(2), 215-241.
- Samoilenko, S. & Osei-Bryson, K. M. (2008). An exploration of the effects of the interaction between ICT and labor force on economic growth in transition economies. *International Journal of Production Economics*, 115(2), 471-481.
- Saltelli, A. (2007). Composite Indicators between Analysis and Advocacy. *Social Indicators Research*, 81(1), 65-77.
- Sanidas, E. (2004). Technology, technical and organizational innovations, economic and societal growth. *Technology in Society*, 26(1), 67-84.
- Saunders, J. (2003). A Risk Management Methodology for Information Security: The Analytic Hierarchy Process, retrieved from: <http://www.johnsaunders.com/papers/risk-ahp/risk-ahp.htm>.
- Scarpetta, S., Bassanini, A., Pilat, D., & Schreyer, P. (2000). *Economic growth in the OECD area: recent trends at the aggregate and sectoral level*. Economics Department Working Papers No. 248, OECD, France, Paris.

- Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington: National Academies Press, 163.
- Schneider, C. M., Moreira, A. A., Andrade Jr, J. S., Havlin, S., & Herrmann, H. J. (2011). Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences*, 108(10), 3838-3841.
- Schneier, B. (2011). Advanced Persistent Threat (APT), retrieved from:
https://www.schneier.com/blog/archives/2011/11/advanced_persis.html
- Schneier, B. (2005). Cyberwar. Crypto-gram Newsletter, retrieved from:
<http://www.schneier.com/crypto-gram-0501.html>
- Schultz, E. (2007). Risks due to convergence of physical security systems and information technology environments. *Information Security Technical Report*, 12(2), 80-84.
- Schumpeter, J. (1934). *The Theory of Economic Development*. Cambridge, MA: Harvard University Press.
- Schutt, R.K.(2004). *Investigating the social world: The process and practice of research (4th ed)*. Thousand oaks, CA: Pine Forge.
- Sellin, N. (1995). Partial Least Squares Modeling in Research on Education Achievement, In *Reflections on Education Achievement (Eds. Bos, W & Lehmann, R.H.)*, Germany: Waxmann Verlag, pp. 256-267.
- Şener, S. & Saridogan, E. (2011). The Effects Of Science-Technology-Innovation On Competitiveness And Economic Growth. *Procedia-Social and Behavioral Sciences*, 24, 815-828.
- Sharma, R. & Yetton, P. (2007). The Contingent Effects of Training, Technical Complexity, and Task Interdependence on Successful Information Systems Implementation. *MIS Quarterly*, 31(2), 219-238.
- Sheskin, D. J. (1997). *Handbook of Parametric and Nonparametric Statistical Procedures*. United States: Chapman and Hall/CRC.
- Shih, E., Kraemer, K.L., & Dedrick, J. (2008). IT Diffusion in Developing Countries. *Communications of the ACM*, 51(2), 43-48.
- Shimeall, T. & Williams, P. (2002, August). Models of information security trend analysis. In *Proceedings of SPIE*, 4708, 43.

- Shue, C. A. & Lagesse, B. (2011). Embracing the cloud for better cyber security. In *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, IEEE, 245-250.
- Simmie, J. (2006). Do clusters or innovation systems drive competitiveness. In *Clusters and Regional Development*, New York: Routledge, 164-187.
- Simpson, T. W., Lin, D. K. J. & Chen, W. (2001). Sampling Strategies for Computer Experiments: Design and Analysis. *International Journal of Reliability and Applications*, 2(3), 209-240.
- Sinclair, N. (2009). *Resilience in critical infrastructures: the case of the Queensland electricity industry*. Queensland University of Technology.
- Singh, A. K. & Siddiqui, A. T. (2011). New Face of Terror: Cyber Threats, Emails Containing Viruses. *Asian Journal of Technology & Management*, 1(1), 1-16.
- Siqueira, A. C. O. & Fleury, M. T. L. (2011). Complementarities of human capital and information technology: small businesses, emerging economy context and the strategic role of firm resources. *Technology Analysis Strategic Management*, 23(6), 639-653.
- Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. In *Sociological methodology 1982 (ed. Leinhardt, S.)*. San Francisco: Jossey-Bass, 290-312.
- Sofaer, A. D., Clark, D., & Diffie, W. (2009). Cyber security and international agreements. In *National Research Council, Proceedings of a Workshop on Deterring Cyberattacks*. Washington DC: The National Academic Press, 179-206.
- Sofka, W. (2008). Globalizing Domestic Absorptive Capacities. *Management International Review*, 48(6), 769 – 792.
- Solow, Robert M. (1957). Technical Change and the Aggregate Production Function. *Review of Economics and Statistics*, 39(3), 312-20.
- Solow, R. (1956). A contribution to the theory of economic growth. *Quarterly Journal of Economics*, 1(2), 65 – 94.
- Soriano, C. R. R. (2007). Exploring the ICT and Rural Poverty Reduction Link: Community Telecenters and Rural Livelihoods in Wu'an, China. *The Electronic Journal of Information Systems in Developing Countries*, 32(1), 1-15.
- Starr, S. H. (2009). Towards an Evolving Theory of Cyberpower. In *The Virtual Battlefield: Perspectives on Cyber Warfare (Eds. Czosseck, C. and Geers, K.)*. Fairfax, VA: IOS Press, Inc. 18-52.

- Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: managing risk in the networked economy. *Strategy and Business*, 30(1), 70-79.
- Stieglitz, N. & Heine, K. (2007). Innovations and the Role of Complementarities in a Strategic Theory of the Firm. *Strategic Management Journal*, 28(1), 1-15.
- Stiglitz, J. E. (1998). *Towards a New Paradigm for Development: Strategies, Policies, and Processes*. Prebisch Lecture at UNCTAD, Geneva, retrieved from: <https://ceaemgmt.colorado.edu/ceae/images/File/mcedc/prebisch98.pdf>
- Stiglitz, J. E. (1998). Knowledge for development: Economic science, economic policy, and economic advice. In *Annual World Bank Conference on Development Economics*, 20, Washington: World Bank, 21.
- Stiglitz, J. (2009). Progress: What Progress? *The OECD Observer*, 272. Paris.
- Stiroh, K. J. (2001). What Drives Productivity Growth? *FRBNY Economic Policy Review*, March, 37-59.
- Stoll, C. (1990). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, New York: Simon & Schuster, Inc.
- Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society, Series B (Methodological)*, 36(2), 111-147.
- Straub, D. W. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, 13(2), 147-166.
- Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(24), 380-427.
- Straub, D.W. & Welke, R.J. (1998). Coping with System Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), 441-469.
- Sweeny, G. (1996). Learning efficiency, technological changes, and economic progress. *International Journal of Technology Management*, 11(1), 5-27.
- Tallon, P.P. (2008). Inside the Adaptive Enterprise: an Information Technology Capabilities Perspective on Business Process Agility. *Information Technology Management*, 9(1), 21-36.
- Tao, Y. & Grosky, W. I. (1999). Delaunay Triangulation for image object indexing: A novel method for shape representation. In *Proceedings of IS&T/SPIE Symposium Storage and Retrieval for Image and Video Databases VII*, San Jose, CA, Jan. 23-29, 631-642.

- Taylor, R. & Zhang, B. (2007). Measuring the Impact of ICT: Theories of Information and Development. in *Proceedings of Telecommunications Policy Research Conference, Washington, D.C.*, 1 – 39.
- Teece D.J, Pisano G, & Shuen A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.
- Teece, D.J. (1988). Technical change and the nature of the firm, in *Technical Change and Economic Theory*, (Eds. Dosi, G., Freeman, C., Nelson, R., and Soete, L). New York: Pinter, 256–281.
- Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. *Research policy*, 15(6), 285-305.
- Tegarden, L.F., Hatfield, D.E., & Echols, A.E. (1999). Doomed from the start: What is the value of selecting a future dominant design? *Strategic Management Journal*, 20(6), 495-518.
- Tenenhaus, M. (2008). Component-based structural equation modeling. *Total quality management*, 19(7-8), 871-886.
- Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, 48(1), 159-205.
- Tenenhaus, M., Amato, S., & Esposito Vinzi, V. (2004). A global goodness-of-fit index for PLS structural equation modelling. In *Proceedings of the XLII SIS scientific meeting*, 739-742.
- Thakur, R. Hsu, S.H.Y., & Fontenot G. (2012). Innovation in healthcare: Issues and future trends, *Journal of Business Research*, 65(4), 562-569.
- Tharakan, J. (2006). Education Engineers in Appropriate Technology for Development. *World Transactions on Engineering and Technology Education*, 5(1), 233-235.
- Thatchenkery, T., Kash, D., & Stough, R. (2004). Information technology and development: The Indian experience. *Technological Forecasting and Social Change*, 71(8), 771-879.
- The Economist (2013). Cybersecurity to the barricades: How America and Europe are trying to bolster their cyber-defenses. *The Economist*, February 16.
- The Guardian (2011). EU legal threat to UK benefits changes 'could result in £2bn bill'. The Guardian, September 30, retrieved from:
<http://www.guardian.co.uk/politics/2011/sep/30/eu-threat-uk-benefits-changes>
- The PRS Group (2013). International Country Risk Guide. Retrieved from:
<http://www.prsgroup.com/icrg.aspx>.

- The White House (May 2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. The White House.
- The White House (May 2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. The White House, iii, retrieved from: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
- The World Bank (2011). *Information and Communication Technologies*. 2011 Sector Strategy Approach Paper. The World Bank Group, Washington, DC.
- The World Bank (2013). *Country and Lending Groups*, retrieved from: <http://data.worldbank.org/about/country-classifications/country-and-lending-groups>.
- Thompson, B. (2000). Canonical correlation analysis. In *Reading and understanding more multivariate statistics* (Eds. Grimm, L. & yarnold, P.). Washington, DC: American Psychological Association, 285-316.
- Thompson, B., Diamond, K. E., McWilliam, R., Synder, P., & Sunder, S. W. (2005). Evaluating the Quality of Evidence from Correlational Research for Evidence-Based Practice. *Exceptional Children*, 71(2), 181-194.
- Thompson R., Barclay D., & Higgins C. (1995). The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. *Technology studies: special issue on Research Methodology*, 2(2), 1995, pp. 284-324.
- Thongrattana, P. T. (2010). Assessing reliability and validity of a measurement instrument for studying uncertain factors in Thai rice supply chain. In *SBS HDR Student Conference*, University of Wollongong, Research Online, retrieved from: <http://ro.uow.edu.au/sbshdr/2010/papers/4/>.
- Thurmond, A. V. (2001). The point of triangulation. *Journal of Nursing Scholarship*, 33(3), 253-258.
- Tidd , J . (2006). *A Review of Innovation Models*. Discussion paper, Imperial College, London.
- Tiirmaa-Klaar, H. (2011). *Cyber Security Threats and Responses at Global, Nation-State, Industry, and Individual Levels*. CERi SciencesPo., Ministry of Defense, Estonia. Retrieved from: <http://www.ceri-sciences-po.org/>.
- Tiwari, R., Buse, S., & Herstatt, C. (2007). Innovation via Global Route: Proposing a Reference Model for Chances and Challenges of Global Innovation Processes. *Technology and Innovation Management*, Working Paper, (49).
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation*. Lexington: Lexington Books.

- Trajtenberg, M. (2005). Innovation Policy for Development: an Overview. Paper prepared for the *LAEBBA 2005 second annual meeting, Buenos Aires, Argentina*.
- Trinchera, L. & Russolillo, G. (2010). *On the use of Structural Equation Models and PLS Path Modeling to build composite indicators*. Working Paper No. 30-2010, Università degli Studi di Macerata.
- Trustwave (2011). *Global Security Report*. Trustwave Spider Labs, retrieved from: www.trustwave.com/global-security-report
- Tucker, D. S. (1997). Federal Government's War on Economic Espionage. *The University of Pennsylvania Journal of International Economic Law*, 18(3), 1109-1152.
- Tulman, L. R. & Jacobsen, B. S. (1989). Goldilocks and variability. *Nursing Research*, 38(6), 377-379.
- Turner, P. & Turner, S. (2009). Triangulation in practice. *Virtual Reality*, 13(3), 171-181.
- Twomey, P. (2010). *Cyber security threats*. The Lowy Institute for International Policy, Sydney, retrieved from: http://lowyinstitute.richmediaserver.com/sound/Cyber_security_threats.ppt.
- UNCSTD – United Nations Commission on Science and Technology for Development (2007). *Information Economy Report 2007-2008: Science and Technology for Development – The New Paradigm of ICT*. UNCTAD Secretariat, Geneva: United Nations.
- UNCTAD- United Nations Conference on Trade and Development (2006). *The Digital Divide Report: ICT Diffusion Index 2005*. UNCTAD/ITE/IPC/2006/5. New York and Geneva: United Nations.
- UNCTAD- United Nations Conference on Trade and Development (2007). . *Information Economy Report 2007-2008. Science and Technology for Development: the new paradigm of ICT*. New York and Geneva: United Nations.
- UNDESA- United Nations Department of Economic and Social Affairs (2010). *World Urbanization Prospects: The 2009 Revision*. New York. Retrieved from: <http://esa.un.org/unpd/wup/index.htm/>.
- UNDP- United Nations Development Programme (2011). *The Human Development Index (HDI)*. Human Development Report Office, New York.
- UNDP- United Nations Development Program (2009). *Human Development Report 2009*, UNDP.

- UNDP- United Nations Development Program (2011). *Human Development Report 2011: Sustainability and Equity – A Better Future for All*, UNDP.
- UNESCO- United Nations Education, Scientific, and Cultural Organization (2005). *Information and Communication Technologies in Schools: How ICT can create New, Open Learning Environments*. France: UNESCO.
- United Nations (2000). *The Rule of Law in the Global Village*. Panel on “The Challenge of Borderless Cyber-Crime”. Palermo, Italy, retrieved from:
http://untreaty.un.org/ola/media/info_from_lc/cybercrime.pdf.
- United States Congress (2001). *U.S.A. Patriot Act*. Retrieved from:
<http://www.epic.org/privacy/terrorism/hr3162.html>.
- UNODC- United Nations Office on Drugs and Crime (2011). *How to prevent a disaster in cyberspace ?* Open-ended intergovernmental expert meeting on cybercrime. UNODC, Vienna, January 19, retrieved from:
http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Belgium_Cybercrime_EGMJan2011.pdf.
- Valente, T. W. (1993). Diffusion of innovations and policy decision-making. *Journal of Communication*, 43(1), 30-45.
- Vamosi, R. (2011). How Hactivism Affects Us All? *PCWorld*, Sep. 6, retrieved from:
http://www.pcworld.com/article/239594/how_hactivism_affects_us_all.html
- Van Akkeren, J. & Harker, D. (2003). The mobile Internet and small business: An exploratory study of needs, use and adoption with full-adopters of technology. *Journal of Research and Practice in Information Technology*, 35(3), 205-220.
- Van Ark, B., Inklaar, R., & McGuckin, R. H. (2003). ICT and productivity in Europe and the United States Where do the differences come from? *CESifo Economic Studies*, 49(3), 295-318.
- Van de Vrande, V., de Jong, J.P.J., Vanhaverbeke, W. & de Rochemont, M. (2009). Open innovation in SMEs: Trends, motives and management challenges. *Technovation*, 29(6-7), 423-437.
- Van Kessel, P. (2010). *Borderless Security*. Ernst & Young’s 2010 Global Information Security Survey, Ernst & Young.
- Vatis, M. (2006). The Next Battlefield: The Reality of Virtual Threats. *Harvard International Review*, 28(3), 56.

- Vinzi, V. E., Chin, W. W., & Henseler, J. (2010). *Handbook of Partial Least Squares: Concepts, Methods and Applications*. Heidelberg: Springer-Verlag.
- Von Bertalanffy, L. (1968). *General Systems Theory: Foundation, Development, Applications*. New York: George Braziller, Inc.
- Von Zedtwitz, M. (2004). Managing foreign R&D laboratories in China. *R&D Management*, 34(4), 439-452.
- Vu, K. M. (2011). ICT as a source of economic growth in the information age: Empirical evidence from the 1996–2005 period. *Telecommunications Policy*, 35(4), 357-372.
- Wade, M. & Hulland, J. (2004). Review: The Resource-Based View And Information Systems Research: Review, Extension, And Suggestions For Future Research. *MIS Quarterly* 28(1), 107-142.
- Wagner, C. S. & Leydesdorff, L. (2005). Network structure, self-organization, and the growth of international collaboration in science. *Research policy*, 34(10), 1608-1618.
- Walczak, S. (2012). Methodological Triangulation Using Neural Networks for Business Research. *Advances in Artificial Neural Systems*, 2012(1), 1-12.
- Walker, C. (2008). Governance of the critical national infrastructure. *Public law*, 2(Summer), 323-352.
- Walsham, G. (2010). ICTs for the Broader Development of India: An Analysis of the Literature. *Electronic Journal of Information Systems in Developing Countries*, 41(4), 1-20.
- Walsham, G., Robey, D. & Sahay, S. (2007). Foreword: Special Issue on Information Systems in Developing Countries. *MIS Quarterly*, 31(2), 317-326.
- Waltz, C.F., Strickland, O.L., & Lenz, E.R. (2010). *Measurement in Nursing and Health Research* (4th ed.). New York: Springer Publishing Company, LLC.
- Waltz, K. (1979). *Theory of International Relations*. New York: Random House.
- Wang, E. H. H. (1999). ICT and economic development in Taiwan: analysis of the evidence. *Telecommunications Policy*, 23(3), 235-243.
- Wasko, M. M. & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 29(1), 35-57.
- Webb, E. J., Campbell, D. T., Schwartz, R. D., & Sechrest, L. (1966). *Unobtrusive Measures: Nonreactive Measures in the Social Sciences*. Chicago: Rand McNally.

- Wejnert, B. (2002). Integrating models of diffusion of innovations: A conceptual framework. *Annual Review of Sociology*, 28, 297-326.
- Westrin, P. (2001). Critical Information Infrastructure Protection (CIIP) in *The Internet and the Changing Face of International Relations and Security*. ETH Zurich, Switzerland: Center for Security Studies, 67-79.
- Westrup, C., Al Jaghoub, S., El Sayaed, H., & Liu, W. (2003). Taking Culture Seriously: ICTs Culture and Development, in *The Digital Challenge: Information Technology in the Development Context*, (Eds. Krishna, S. & Madon, S.). London: Ashgate.
- White House (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, retrieved from: http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf.
- Wignaraja, G. (2008). Foreign Ownership, Technological Capabilities and Clothing Exports in Sri Lanka. *Journal of Asian Economics*, 19(1), 29-39.
- Wilson, C. (2008). *Botnets, Cybercrime, and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*. CRS Report for Congress. Congressional Research Service, January.
- Wilson, J. M., Jackson, B., Eisman, M., Steinberg, P., & Riley, K. (2007). *Securing America's Passenger-Rail Systems*. Santa Monica, CA: Rand Corporation.
- Wilson, J.W. & Jones, C.P. (2002). An analysis of the S&P 500 index and Cowles's extensions: price indexes and stock returns, 1870-1999. *Journal of Business*, 75(3), 505-533.
- Wold, H. (1985). Partial Least Squares. In *Encyclopedia of Statistical Sciences*, Vol. 6, (Ed. Kotz and Johnson). New York: Wiley, 581-591.
- Wold, H. (1982). Systems under Indirect Observation Using PLS. In *A Second Generation of Multivariate Analysis: Methods*, Vol. I, (Ed. C. Fornell). New York: Praeger, 325-347.
- Wold, H. (1975). Path models with latent variables: The NIPALS approach. In *Quantitative sociology: International perspectives on mathematical and statistical modeling* (Eds. Blalock et al.). New York: Academic Press, 307-357.
- Wolff, J. A. & Pett, T. L. (2006). Small-Firm Performance: Modeling the Role of Product and Process Improvements. *Journal of Small Business Management*, 44(2), 268-284.
- World Bank (2012). Knowledge for Development: KEI and KI Indexes (KAM 2012). Retrieved from: http://info.worldbank.org/etools/kam2/KAM_page5.asp.

- World Bank (2011). *World Bank List of Economies (January 2011)*. World Bank, retrieved from: <http://librarians.acm.org/sites/default/files/Jan%202011%20World%20bank%20list%20of%20Economies.PDF>.
- World Economic Forum (2012). *Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience*. June, retrieved from: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.
- World Economic Forum (2011). *The Global Competitiveness Report*, retrieved from: <http://www.weforum.org/pdf/gcr/2011/rankings.pdf>.
- World Economic Forum (2011). *Global Risks 2011 (6th edition): An initiative of the Risk Response Network*. Geneva: World Economic Forum.
- World Economic Forum (2010). *The Global Competitiveness Report 2010-2011*. World Economic Forum, Geneva, retrieved from: http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2010-11.pdf.
- World Economic Forum (2009). *The Global Competitiveness Report 2009-2010*. World Economic Forum, Geneva, retrieved from: <https://members.weforum.org/pdf/GCR09/GCR20092010fullreport.pdf>.
- World Economic Forum (2008). *Global Risks 2008: A Global Risk Report*. Geneva: World Economic Forum. Retrieved from: www.weforum.org/pdf/CSI/Global_Risks_2008.pdf.
- WSIS (World Summit on the Information Society) (Dec. 2003). *Building the Information Society: A Global Challenge in the New Millennium*. Declaration of Principles. Document WSIS-03 / Geneva/Doc/4-E.
- Xu, S., Zhu, K., & Gibbs, J. (2004). Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China. *Electronic Markets*, 14(1), 13-24.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys and Tutorials*, 15(1), 5-20.
- Yang, Q., Barria, J. A., & Green, T. C. (2011). Communication infrastructures for distributed control of power distribution networks. *IEEE Transactions on Industrial Informatics*, 7(2), 316-327.
- Yang, C. H. (2006). Is innovation the story of Taiwan's economic growth? *Journal of Asian Economics*, 17(5), 867-878.

- Yeniyurt, S., Cavusgil, S.T., & Hult, G.T.M. (2005). A Global Market Advantage Framework: the Role of Global Market Knowledge Competencies. *International Business Review*, 14(1), 1-19.
- Yetton, P., Sharma, R., & Southon, G. (1999). Successful Is Innovation: The Contingent Contributions of Innovation Characteristics and Implementation Process. *Journal of Information Technology*, 14(1), 53-68.
- Yu, C. & Xin-quan, G. (2011). The empirical study on the relationship between information technology capability and innovation performance: The moderating role of learning commitment. In *2011 International Conference on E-Business and E-Government (ICEE)*, May, IEEE, 1-4.
- Zack, M. H. (1999). Managing codified knowledge. *Sloan management review*, 40(4), 45-58.
- Zander, I. (1999). How do you mean ‘global’? An empirical investigation of innovation networks in the multinational corporation. *Research Policy*, 28(2-3): 195-213.
- Zhao, H., Kim, S., Suh, T., & Du, J. (2007). Social institutional explanations of global Internet diffusion: A cross-country analysis. *Journal of Global Information Management (JGIM)*, 15(2), 28-55.
- Zhou, P., Ang, B.W., & Poh, K.L. (2007). A mathematical programming approach to constructing composite indicators. *Ecological Economics*, 62(2), 291–297.
- Zhu K., Dong S., Xu S. X., & Kraemer K. L. (2006). Innovation diffusion in global contexts: Determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems*, 15(6), 601-616.
- Zhu, K., Kraemer, K.L., Xu, S., & Dedrick, J. (2004). Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry. *Journal of Management Information Systems*, 21(1), 17-54.
- Zmud, R. W. (1984). An examination of “push-pull” theory applied to process innovation in knowledge work. *Management Science*, 30(6), 727-738.

APPENDIX A

APPENDIX A

LIST OF COUNTRIES, REGION GROUPINGS, AND ECONOMY GROUP

	<i>Economy</i>	<i>Region</i>	<i>Income group</i>
1	Afghanistan	South Asia	Low income
2	Albania	Europe & Central Asia	Upper middle income
3	Algeria	Middle East & North Africa	Upper middle income
4	American Samoa	East Asia & Pacific	Upper middle income
5	Andorra	..	High income: non-OECD
6	Angola	Sub-Saharan Africa	Lower middle income
7	Antigua and Barbuda	Latin America & Caribbean	Upper middle income
8	Argentina	Latin America & Caribbean	Upper middle income
9	Armenia	Europe & Central Asia	Lower middle income
10	Aruba	..	High income: non-OECD
11	Australia	..	High income: OECD

12	Austria	..	High income: OECD
13	Azerbaijan	Europe & Central Asia	Upper middle income
14	Bahamas, The	..	High income: non-OECD
15	Bahrain	..	High income: non-OECD
16	Bangladesh	South Asia	Low income
17	Barbados	..	High income: non-OECD
18	Belarus	Europe & Central Asia	Upper middle income
19	Belgium	..	High income: OECD
20	Belize	Latin America & Caribbean	Lower middle income
21	Benin	Sub-Saharan Africa	Low income
22	Bermuda	..	High income: non-OECD
23	Bhutan	South Asia	Lower middle income
24	Bolivia	Latin America & Caribbean	Lower middle income
25	Bosnia and Herzegovina	Europe & Central Asia	Upper middle income
26	Botswana	Sub-Saharan Africa	Upper middle income
27	Brazil	Latin America & Caribbean	Upper middle income
28	Brunei Darussalam	..	High income: non-OECD

29	Bulgaria	Europe & Central Asia	Upper middle income
30	Burkina Faso	Sub-Saharan Africa	Low income
31	Burundi	Sub-Saharan Africa	Low income
32	Cambodia	East Asia & Pacific	Low income
33	Cameroon	Sub-Saharan Africa	Lower middle income
34	Canada	..	High income: OECD
35	Cape Verde	Sub-Saharan Africa	Lower middle income
36	Cayman Islands	..	High income: non-OECD
37	Central African Republic	Sub-Saharan Africa	Low income
38	Chad	Sub-Saharan Africa	Low income
39	Channel Islands	..	High income: non-OECD
40	Chile	Latin America & Caribbean	Upper middle income
41	China	East Asia & Pacific	Upper middle income
42	Colombia	Latin America & Caribbean	Upper middle income
43	Comoros	Sub-Saharan Africa	Low income
44	Congo, Dem. Rep.	Sub-Saharan Africa	Low income
45	Congo, Rep.	Sub-Saharan Africa	Lower middle income
46	Costa Rica	Latin America & Caribbean	Upper middle income

47	Côte d'Ivoire	Sub-Saharan Africa	Lower middle income
48	Croatia	..	High income: non-OECD
49	Cuba	Latin America & Caribbean	Upper middle income
50	Curaçao	..	High income: non-OECD
51	Cyprus	..	High income: non-OECD
52	Czech Republic	..	High income: OECD
53	Denmark	..	High income: OECD
54	Djibouti	Middle East & North Africa	Lower middle income
55	Dominica	Latin America & Caribbean	Upper middle income
56	Dominican Republic	Latin America & Caribbean	Upper middle income
57	Ecuador	Latin America & Caribbean	Upper middle income
58	Egypt, Arab Rep.	Middle East & North Africa	Lower middle income
59	El Salvador	Latin America & Caribbean	Lower middle income
60	Equatorial Guinea	..	High income: non-OECD
61	Eritrea	Sub-Saharan Africa	Low income
62	Estonia	..	High income: OECD
63	Ethiopia	Sub-Saharan Africa	Low income

64	Faeroe Islands	..	High income: non-OECD
65	Fiji	East Asia & Pacific	Lower middle income
66	Finland	..	High income: OECD
67	France	..	High income: OECD
68	French Polynesia	..	High income: non-OECD
69	Gabon	Sub-Saharan Africa	Upper middle income
70	Gambia, The	Sub-Saharan Africa	Low income
71	Georgia	Europe & Central Asia	Lower middle income
72	Germany	..	High income: OECD
73	Ghana	Sub-Saharan Africa	Lower middle income
74	Gibraltar	..	High income: non-OECD
75	Greece	..	High income: OECD
76	Greenland	..	High income: non-OECD
77	Grenada	Latin America & Caribbean	Upper middle income
78	Guam	..	High income: non-OECD
79	Guatemala	Latin America & Caribbean	Lower middle income
80	Guinea	Sub-Saharan Africa	Low income
81	Guinea-Bissau	Sub-Saharan Africa	Low income

82	Guyana	Latin America & Caribbean	Lower middle income
83	Haiti	Latin America & Caribbean	Low income
84	Honduras	Latin America & Caribbean	Lower middle income
85	Hong Kong SAR, China	..	High income: non-OECD
86	Hungary	..	High income: OECD
87	Iceland	..	High income: OECD
88	India	South Asia	Lower middle income
89	Indonesia	East Asia & Pacific	Lower middle income
90	Iran, Islamic Rep.	Middle East & North Africa	Upper middle income
91	Iraq	Middle East & North Africa	Lower middle income
92	Ireland	..	High income: OECD
93	Isle of Man	..	High income: non-OECD
94	Israel	..	High income: OECD
95	Italy	..	High income: OECD
96	Jamaica	Latin America & Caribbean	Upper middle income
97	Japan	..	High income: OECD
98	Jordan	Middle East & North Africa	Upper middle income

99	Kazakhstan	Europe & Central Asia	Upper middle income
100	Kenya	Sub-Saharan Africa	Low income
101	Kiribati	East Asia & Pacific	Lower middle income
102	Korea, Dem. Rep.	East Asia & Pacific	Low income
103	Korea, Rep.	..	High income: OECD
104	Kosovo	Europe & Central Asia	Lower middle income
105	Kuwait	..	High income: non-OECD
106	Kyrgyz Republic	Europe & Central Asia	Low income
107	Lao PDR	East Asia & Pacific	Lower middle income
108	Latvia	Europe & Central Asia	Upper middle income
109	Lebanon	Middle East & North Africa	Upper middle income
110	Lesotho	Sub-Saharan Africa	Lower middle income
111	Liberia	Sub-Saharan Africa	Low income
112	Libya	Middle East & North Africa	Upper middle income
113	Liechtenstein	..	High income: non-OECD
114	Lithuania	Europe & Central Asia	Upper middle income
115	Luxembourg	..	High income: OECD

116	Macao SAR, China	..	High income: non-OECD
117	Macedonia, FYR	Europe & Central Asia	Upper middle income
118	Madagascar	Sub-Saharan Africa	Low income
119	Malawi	Sub-Saharan Africa	Low income
120	Malaysia	East Asia & Pacific	Upper middle income
121	Maldives	South Asia	Upper middle income
122	Mali	Sub-Saharan Africa	Low income
123	Malta	..	High income: non-OECD
124	Marshall Islands	East Asia & Pacific	Lower middle income
125	Mauritania	Sub-Saharan Africa	Lower middle income
126	Mauritius	Sub-Saharan Africa	Upper middle income
127	Mayotte	Sub-Saharan Africa	Upper middle income
128	Mexico	Latin America & Caribbean	Upper middle income
129	Micronesia, Fed. Sts.	East Asia & Pacific	Lower middle income
130	Moldova	Europe & Central Asia	Lower middle income
131	Monaco	..	High income: non-OECD
132	Mongolia	East Asia & Pacific	Lower middle

			income
133	Montenegro	Europe & Central Asia	Upper middle income
134	Morocco	Middle East & North Africa	Lower middle income
135	Mozambique	Sub-Saharan Africa	Low income
136	Myanmar	East Asia & Pacific	Low income
137	Namibia	Sub-Saharan Africa	Upper middle income
138	Nepal	South Asia	Low income
139	Netherlands	..	High income: OECD
140	New Caledonia	..	High income: non-OECD
141	New Zealand	..	High income: OECD
142	Nicaragua	Latin America & Caribbean	Lower middle income
143	Niger	Sub-Saharan Africa	Low income
144	Nigeria	Sub-Saharan Africa	Lower middle income
145	Northern Mariana Islands	..	High income: non-OECD
146	Norway	..	High income: OECD
147	Oman	..	High income: non-OECD
148	Pakistan	South Asia	Lower middle income
149	Palau	East Asia & Pacific	Upper middle income

150	Panama	Latin America & Caribbean	Upper middle income
151	Papua New Guinea	East Asia & Pacific	Lower middle income
152	Paraguay	Latin America & Caribbean	Lower middle income
153	Peru	Latin America & Caribbean	Upper middle income
154	Philippines	East Asia & Pacific	Lower middle income
155	Poland	..	High income: OECD
156	Portugal	..	High income: OECD
157	Puerto Rico	..	High income: non-OECD
158	Qatar	..	High income: non-OECD
159	Romania	Europe & Central Asia	Upper middle income
160	Russian Federation	Europe & Central Asia	Upper middle income
161	Rwanda	Sub-Saharan Africa	Low income
162	Samoa	East Asia & Pacific	Lower middle income
163	San Marino	..	High income: non-OECD
164	São Tomé and Príncipe	Sub-Saharan Africa	Lower middle income
165	Saudi Arabia	..	High income: non-OECD
166	Senegal	Sub-Saharan Africa	Lower middle

			income
167	Serbia	Europe & Central Asia	Upper middle income
168	Seychelles	Sub-Saharan Africa	Upper middle income
169	Sierra Leone	Sub-Saharan Africa	Low income
170	Singapore	..	High income: non-OECD
171	Sint Maarten (Dutch part)	..	High income: non-OECD
172	Slovak Republic	..	High income: OECD
173	Slovenia	..	High income: OECD
174	Solomon Islands	East Asia & Pacific	Lower middle income
175	Somalia	Sub-Saharan Africa	Low income
176	South Africa	Sub-Saharan Africa	Upper middle income
177	South Sudan	Sub-Saharan Africa	Not classified
178	Spain	..	High income: OECD
179	Sri Lanka	South Asia	Lower middle income
180	St. Kitts and Nevis	Latin America & Caribbean	Upper middle income
181	St. Lucia	Latin America & Caribbean	Upper middle income
182	St. Martin (French part)	..	High income: non-OECD
183	St. Vincent and the Grenadines	Latin America &	Upper middle

		Caribbean	income
184	Sudan	Sub-Saharan Africa	Lower middle income
185	Suriname	Latin America & Caribbean	Upper middle income
186	Swaziland	Sub-Saharan Africa	Lower middle income
187	Sweden	..	High income: OECD
188	Switzerland	..	High income: OECD
189	Syrian Arab Republic	Middle East & North Africa	Lower middle income
190	Tajikistan	Europe & Central Asia	Low income
191	Tanzania	Sub-Saharan Africa	Low income
192	Thailand	East Asia & Pacific	Upper middle income
193	Timor-Leste	East Asia & Pacific	Lower middle income
194	Togo	Sub-Saharan Africa	Low income
195	Tonga	East Asia & Pacific	Lower middle income
196	Trinidad and Tobago	..	High income: non-OECD
197	Tunisia	Middle East & North Africa	Upper middle income
198	Turkey	Europe & Central Asia	Upper middle income
199	Turkmenistan	Europe & Central Asia	Lower middle income

200	Turks and Caicos Islands	..	High income: non-OECD
201	Tuvalu	East Asia & Pacific	Lower middle income
202	Uganda	Sub-Saharan Africa	Low income
203	Ukraine	Europe & Central Asia	Lower middle income
204	United Arab Emirates	..	High income: non-OECD
205	United Kingdom	..	High income: OECD
206	United States	..	High income: OECD
207	Uruguay	Latin America & Caribbean	Upper middle income
208	Uzbekistan	Europe & Central Asia	Lower middle income
209	Vanuatu	East Asia & Pacific	Lower middle income
210	Venezuela, RB	Latin America & Caribbean	Upper middle income
211	Vietnam	East Asia & Pacific	Lower middle income
212	Virgin Islands (U.S.)	..	High income: non-OECD
213	West Bank and Gaza	Middle East & North Africa	Lower middle income
214	Yemen, Rep.	Middle East & North Africa	Lower middle income
215	Zambia	Sub-Saharan Africa	Lower middle income
216	Zimbabwe	Sub-Saharan Africa	Low income

APPENDIX B

APPENDIX B

POWER ANALYSIS RESULTS

[1] – *Power analysis for the effect size of ICT: Estimating Sample Size*

t tests - Linear multiple regression: Fixed model, Single regression coefficient

Analysis: A priori: Compute required sample size

Input:	Tail(s)	=	One
	Effect size f^2	=	0.034483
	α err prob	=	0.05
	Power (1- β err prob)	=	0.80
	Number of predictors	=	3
Output:	Noncentrality parameter δ	=	2.4982840
	Critical t	=	1.6535080
	Df	=	177
	Total sample size	=	181
	Actual power	=	0.8006272

[2] -- *Power analysis for the effect size of Innovation: Estimating Sample Size*

t tests - Linear multiple regression: Fixed model, Single regression coefficient

Analysis: A priori: Compute required sample size

Input:	Tail(s)	=	One
	Effect size f^2	=	0.034483
	α err prob	=	0.05
	Power (1- β err prob)	=	0.75
	Number of predictors	=	3
Output:	Noncentrality parameter δ	=	2.3341624
	Critical t	=	1.6548084
	Df	=	154
	Total sample size	=	158
	Actual power	=	0.7514423

[3] -- *Power analysis for the effect size of Innovation after reducing the desired statistical power: Estimating Sample Size*

t tests - Linear multiple regression: Fixed model, Single regression coefficient

Analysis: A priori: Compute required sample size

Input:	Tail(s)	=	One
	Effect size f^2	=	0.034483
	α err prob	=	0.05

	Power (1- β err prob)	= 0.70
	Number of predictors	= 3
Output:	Noncentrality parameter δ	= 2.1814339
	Critical t	= 1.6563045
	Df	= 134
	Total sample size	= 138
	Actual power	= 0.7003982

[4] -- *Power analysis for the effect size of Cybersecurity: Estimating Sample Size*

t tests - Linear multiple regression: Fixed model, Single regression coefficient

Analysis: A priori: Compute required sample size

Input:	Tail(s)	= One
	Effect size f^2	= 0.095
	α err prob	= 0.05
	Power (1- β err prob)	= 0.80
	Number of predictors	= 3
Output:	Noncentrality parameter δ	= 2.5228952
	Critical t	= 1.6694022
	Df	= 63
	Total sample size	= 67
	Actual power	= 0.8025589

[5] -- *Power analysis for the effect size of Cybersecurity using the sample size derived from the secondary data used in the study: Computing Power*

t tests - Linear multiple regression: Fixed model, Single regression coefficient

Analysis: Post hoc: Compute achieved power

Input:	Tail(s)	= One
	Effect size f^2	= 0.095
	α err prob	= 0.05
	Total sample size	= 139
	Number of predictors	= 3
Output:	Noncentrality parameter δ	= 3.5142567
	Critical t	= 1.6570370
	Df	= 126
	Power (1- β err prob)	= 0.9678750

BIOGRAPHICAL SKETCH

Dr. Manal Yunis earned her doctor of philosophy degree in Computer Information systems from the College of Business Administration at UTPA. Before joining the PhD program at UTPA, Dr. Yunis worked for about 8 years as a faculty member of information systems and management courses in the School of Business at the Lebanese American University (LAU) in Beirut, where she also participated in the design and development of new courses, such as Technology management and ERP.

At UTPA, she's been an instructor of CIS and QUMT courses since 2010. Her teaching interests include IS in organizations, E-commerce, strategic IS, and global IT among others. Her research interests are within the area of information security, adoption and implementation of information systems and computing models in organizations, and global IT. Dr. Yunis participated and presented in national, regional, and international conferences, and has publications in several peer-refereed journals, such as IJSS, IJAIM, and IJQRM.