TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Institute of Informatics

Chair of Information Systems

IDU70LT

Risto Hansen, 143935IVGM

CYBER SECURITY CAPABILITY ASSESSMENT

Master's Thesis

Supervisor: Dr. Ingrid Pappel

Co-Supervisor: Prof. Robert Krimmer

Tallinn 2016

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else. I hereby declare that this thesis, which is the result of my work as an independent, are presented at the Tallinn University of Technology to apply for a Master's degree, and on that basis have not previously applied for an academic degree.

Author: Risto Hansen

11.05.2016

The work complies with the applicable requirements.

Supervisor: Dr. Ingrid Pappel

11.05.2016

Co-Supervisor: Prof. Robert Krimmer

11.05.2016

Abstract

Cyber security capability assessment

A secure e-government of a country with strategic e-services cannot exist without effective cyber security. This research is analyzing different available cyber security assessment models. This research is comparing different categories and indicators that are used in different assessment models and analyzing one widely spread assessment model in more detail.

This thesis is written in English and is eighty three pages long, including six chapters and one table.

Annotatsioon

Küberturvalisuse võimekuse hindamine

Turvaline e-riik mis kasutab strateegilisi e-teenuseid, ei saa eksisteerida ilma efektiivse küberturvalisuseta. Antud magistritöö analüüsib erinevaid küberturvalisuse võimekuse hindamise mudeleid. Antud magistritöö võrdleb erinevates küberturvalisuse võimekuse hindamise mudelites kasutatavaid kategooriaid ja indikaatoreid ning analüüsib detailsemalt ühte kõige laiemini levinud mudelit.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti kaheksakümne kolmel leheküljel, kuus peatükki ja üks tabel.

List of abbreviations and terms

ABI Research	Allied Business Intelligence, Inc.
APCERT	Asia Pacific Computer Emergency Response Teams
APEC	Asian Pacific Economic Cooperation
APT	Asia Pacific Telecommunity
ASEAN	the Association of South East Asian Nations
ASPI	Australian Strategic Policy Institute
AU	Africa Union
BDT	ITU's Telecommunication Development Bureau
CERT	Computer Emergency Response Team
CICTE	The Inter-American Committee against Terrorism
CIRT	Computer Incident Response Team
CoE	Council of Europe
CRI	Cyber Readiness Index
CSIRT	Computer Security Incident Response Team
CTU	Counter Threat Unit
CYB	ITU's Cybersecurity and ICT Applications Division
eGA	e-Governance Academy Foundation
EU	European Union
FIRST	Forum of Incident Response and Security Teams
G20	The Group of Twenty
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GDP	Gross Domestic Product
HLEG	High-Level Experts Group
ICANN	Internet Corporation for Assigned Names and Numbers
ICPC	ASPI International Cyber Policy Centre
ICT	Information and communications technology
IEC	The International Electrotechnical Commission
IMPACT	International Multilateral Partnership Against Cyber Threats
IoE	Internet of Everything
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU GCA	ITU Global Cybersecurity Agenda
ITU-D	Development Sector of the ITU
ITU-R	Radio Communication Sector of the ITU
ITU-T	Telecommunication Standardization Sector of the ITU
LAS	League of Arab States
LDCs	Least developed countries
M2M	Machine to machine
M3AAWG	Messaging, Malware and Mobile Anti-Abuse Working Group
MCA	Multi-Criteria Analysis

NATO	North Atlantic Treaty Organization
NATO CCD COE	NATO Cooperative Cyber Defense Centre of Excellence
NCSI	National Cyber Security Index
NOGs	Network Operations Groups
OAS	Organization of American States
OECD	Organization for Economic Cooperation and Development
PPP	Public Private Partnership
RFID	Radio-frequency identification
RIRs	Regional Internet Registries
SDA	The Security and Defense Agenda
SDOs	Standards-developing organizations
UN	United Nations
UNGA	United Nations General Assembly
UNICRI	UN Interregional Crime and Justice Research Institute
UNIDIR	United Nations Institute for Disarmament Research
UNODC	UN Organizations on Drug and Crime Problems
URL	Uniform Resource Locator
WEF	The World Economic Forum
WSIS	World Summit on the Information Society
WTDC	The World Telecommunication Development Conference

Table of Contents

List of tables

1. Introduction

Information and communication technologies (ICTs) are the driving energy behind the evolution of modern societies. ICT underpins the social, economic, and political growth of individuals, governments and organizations alike. (M. Wimmer, Traunmuller, & Lenk, 2001) ICTs have become essential for progress. Smart devices, cloud-based services, and M2M communications among many other technologies, are advancing the next generation of networked societies. Internet connectivity and digital technology are being systematically integrated into all verticals of the public and private sectors because they offer significant advantages: speed, flexibility, efficiency, productivity and cost reduction. (Scholl, 2013) ICTs are increasingly being deployed on new platforms, such as vehicular telematics and retail RFID systems. More significantly they are being used to upgrade critical infrastructures, including energy grids, transport networks, and healthcare systems.

Most countries have adopted ICT-enabled economic strategies and are working to provide affordable, reliable and fast communications to every household and business to move their information society into the digital age. (Ansip, 2015) Modernization initiatives like e-learning, e-health, e-banking and e-government, automating elements of the transportation infrastructure, next generation power grids and other essential services, are at the top of most countries economic agendas. (Grönlund, 2005)

Cyber security is major for sustaining a technologically sound model. The damage to financial systems or disruption of electricity through interference with ICT networks is a reality; these events constitute national cyber security threats. Malicious online agents are organized, numerous and of diverse persuasions: hacktivist, terrorist, criminal, political. The tools at their disposal become more complex and sophisticated over time and with experience the growing number of connected platforms only serves to offer new attack possibilities. There is no going back to simpler times. The society is adopting technological progress, and cyber security must form an integral and indivisible part of that process. (H. Zhao, 2015)

Unfortunately, cyber security is not yet at the core of many social and industrial technology strategies. Though cyber security efforts are numerous, they are dispersed and sometimes eclectic. Differences in technological development, internet penetration, government strategies and private sector dynamics mean that cyber security is emerging as a bottom-up approach, a natural occurrence when disparities exist among industries, private and public sectors, and nation states. A global culture of cyber security can be more successfully initiated from the top down. Information sharing and cooperation are key to tackling cross-border threats. Such elements

require a certain measure of the organization in a multitude of disciplines: legal, technical, educational. Though a particular sector or country may develop and adopt a highly efficient cyber security framework, the knowledge will rarely be shared outside of that circle.

The primary obstacle is that cyber security is a sensitive issue, whether from a private sector or a government perspective. Admission of vulnerabilities is usually seen as a weakness. This is a barrier to the discussion and sharing of threat information and best practices. Security through obscurity is not a viable defense model against modern cyber threats. The answer is to implement cyber security mechanisms at all layers of society. However, the incentive and the drive to do so are inadequate, either due to a simple lack of awareness or cost constraints. The first step toward to answer this question lies in comparing the cyber security capabilities of nation states and publishing an efficient ranking of their status. A ranking system motivates states to intensify their efforts and reveals shortcomings in cyber security. The real value of a nation's cyber security capability can truly be weighed only through comparison with others.

Problem statement

In November 2014, Estonian ICT companies visited Slovenia. The author of this thesis was the organizer of that business trip as the head of Estonian ICT cluster. During our five day trip, we visited twenty-three companies and associations. One particular topic was rising all the time:

- Please advise us how to create an effective cyber security strategy for our country?
- What is the list of categories we have to fulfill to have well-functioning cyber security?
- How to measure country's readiness in the field of cyber security?

These questions started to haunt the author ever since, and the author wanted to find out the answer to the question: how to assess the cyber security capability of a country?

A secure e-government of a country with strategic e-services cannot exist without effective cyber security. (Chen, Chong, & Zhang, 2004) The fast growth of ICT systems and networks has created new and undiscovered opportunities for cyber criminals to take advantage of online vulnerabilities and attack countries' critical infrastructure. Individuals, companies, and governments are increasingly reliant on the information stored and transmitted over advanced communication networks. (J. J. Zhao & Zhao, 2010) Most importantly, cyberspace is borderless: cyber-attacks can inflict immeasurable damage in different countries in a matter of minutes.

Unfortunately, cyber security is not yet at the core of many national technology strategies. We cannot say that the cyber security efforts are non-existent but sometimes they are eclectic and dispersed. (Lorents, Ottis, & Rikk, 2009)

Research objective

At the end of April 2015, the International Telecommunication Union (ITU) released a research project called the Global Cyber security Index (GCI) (ITU GCI, 2015). The aim of that project is to measure the commitment of countries to cyber security.

The author discussed that project with the author colleagues in the field of cyber security, and the author found out that quite many countries do not think ITU's research project gives accurate knowledge about the assessment of the cyber security capability of a state. After conducting an interview with Mr. Raul Rikk, Head of National Cyber Security Domain in Estonian e-Governance Academy, the author found out that Estonian e-Governance Academy is creating another version of cyber security index/methodology.

The main research questions is:

- How to assess the cyber-security capability of a country?

Following sub-questions help to determine the framework for assessment of cyber security capabilities:

- What methodologies are available to assess a Country's cyber security capability?
- What are the categories a Country needs to fulfill to assess its cyber security capability?

2. Methodology

With this research, the author wishes to analyze cyber security assessment of a country. The main reason is that the question how to assess the cyber security of a country rises continuously. To analyze the cyber security assessment of a country it is ideal to do a case study. The reason to do a case study is that case study is an empirical inquiry that investigates the case in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident. (Yin, 2014)

Case studies can either be explanatory, descriptive or exploratory. The author has selected the exploratory case study because by a preliminary literature research hardly any academic works could be identified that deal with a cyber security assessment. Therefore, it can be assumed that not much theory exists and that is why an explorative research approach is being used in this case study methodology. (Yin, 2014)

The author will analyze the Global Cybersecurity Index, which is most widely used and this index will be the author's unit of analysis.

In order to analyze the Global Cybersecurity Index the author will look for background material about other assessment models. Then the author will briefly analyze other assessment models to develop an understanding and then make comparison between the Global Cybersecurity Index and other assessment models.

3. Background of different indexes and assessment models

Cyber security development is a complex matter. Whether at the individual, enterprise or the nation-state level, various factors need to be examined and layered approach can provide more extensive coverage than single solutions. The application of cyber security is also a continuous process that needs to match ongoing cyber criminal threat and activities campaigns. The measurement of safety attitudes and progress over time are essential elements to strengthening policies, evaluating threats and foresee future cyber threat cases. (Geers, 2011)

During this research, the author has found seventeen different cyber security assessment models. Most of the cyber security indexes have published in the past few years, yet not all measure the same capabilities.

Allied Business Intelligence, Inc. is (also known as ABI Research) a technology market intelligence company, and they have proposed three main groups how different cyber security indexes can be broadly split. (ITU, 2015a)

These three major groups are:

1. indexes for assessing countries,
2. indexes for assessing organizations,
3. indexes for assessing threats.

Following the author will explain and describe each of them shortly. As the author's topic is about an assessment of the cyber security capability of a country, the author will focus more on the first group of indexes.

3.1 Indexes for assessing countries

Indexes for assessing countries have been developed by international organizations and think tanks, often in partnership with private sector entities (for example market research companies). At the highest level, these indexes look at policy and regulatory aspects, organizational measures, national strategies, and cooperative efforts among others. Some indexes provide an index scoring based on different indicators while others simply compare and contrast measures amongst countries. All indexes offer valuable information on cyber security practices and gaps at the nation-state level.

3.1.1 ASPI Cyber Maturity in the Asia-Pacific Region Index

Cyber Maturity in the Asia-Pacific Region is an index developed by the Australian Strategic Policy Institute (ASPI), which aims to provide information on a nation state's level of cyber maturity. A total of fourteen countries in the Asia-Pacific region has been analyzed. Into the index, there has also been added the UK and the US, as reference points for overall cyber maturity, so in whole sixteen countries. The Cyber Maturity in the Asia-Pacific Region index is mainly focused on the organizational aspects and policy of cyber security. The methodology proposed utilizes a "cyber maturity metric"(ASPI, 2014) to assess the various facets of countries cyber capabilities. A total of ten indicators have been produced within five categories, and each countries level of cyber maturity has been measured against the guidelines provided with each categories indicator. The Cyber Maturity in the Asia-Pacific Region includes an overall ranking of cyber maturity for each fourteen state within the region, as well as an individual score and short profile.

The publication is classified as an index since it has indicators, a scoring, and ranking mechanisms. Each country profiles are helpful and provide a snapshot of national activities. The five categories of the Cyber Maturity in the Asia-Pacific Region are:

1. organizational structures;
2. legislation;
3. international cooperation;
4. CERTs;
5. military capabilities.

Although it is only the Asia-Pacific regional index based on open source and publicly available information, the index could benefit from a survey-based data collection exercise. (ASPI, 2015)

3.1.2 Cyber Readiness Index 2.0

The Cyber Readiness Index 2.0 is developed by the Potomac Institute for Policy Studies. It is a further development of Cyber Readiness Index 1.0 (Hathaway, 2013). The Cyber Readiness Index is focused on evaluating nation state's cyber maturity as well as their

overall commitment to cyber issues. In Cyber Readiness Index 2.0 total of one hundred and twenty-five countries have been selected (in Cyber Readiness Index 1.0 there were thirty-five countries). The publication is mainly focused on policy and economic aspects of cyber security and includes fact-based assessments of country's cyber readiness. The index uses a set of seven categories:

1. national strategy;
2. incident response;
3. e-crime and law enforcement;
4. information sharing;
5. investment in research and development;
6. diplomacy and trade;
7. defense and crisis response

The Cyber Readiness Index 2.0 has a broad geographic range. However, the Cyber Readiness Index 2.0 does not offer any ranking, despite a scoring mechanism. (Hathaway, 2015)

3.1.3 Cyber Power Index

The Cyber Power Index is developed jointly by the Economist's Intelligence Unit and Booz Allen Hamilton Inc. The index is focused on policy, technical and organizational aspects of cyber security. The Cyber Power Index includes thirty-nine indicators, and sub-indicators grouped into four categories:

1. legal and regulatory framework;
2. economic and social context;
3. technology infrastructure;
4. industry application.

The aim of the Cyber Power Index is to provide a measurement tool for attributes of cyber security. The Cyber Power Index provides scoring and ranking for the cyber power of countries under analysis. The index examines the potential challenges and the benefits of reliance on digital infrastructure. However, the Cyber Power Index is not a global index. It covers nineteen countries of the G20, excluding G20 last member the EU. (Economist Intelligence Unit, 2011)

3.1.4 Cybersecurity: The Vexed Question of Global Rules

The report is developed by the Security and Defense Agenda (SDA) and McAfee (now Intel Security). The Cybersecurity: The Vexed Question of Global Rules offers an overview of the current issues relating to cyber security, threat trends and campaigns, cyber defense strategies, debates about rules and regulations to govern cyberspace, and stress tests of countries cyber capabilities. The stress tests include twenty-three country profiles as well as individual scoring developed by a set of ten indicators. The Cybersecurity: The Vexed Question of Global Rules methodology is based on a survey of two hundred fifty leading authorities in the field of cyber security. The scoring is based out of five stars. However, the Cybersecurity: The Vexed Question of Global Rules methodology it is limited in the geographic range of the twenty-three countries. (Grauman, 2012)

3.1.5 The Cyber Index

United Nations Institute for Disarmament Research (UNIDIR) developed a fact-based study of cyber security efforts at a national, regional and international level. The aim of the Cyber Index is to clarify different approaches connected to cyber security. The Cyber Index is mainly focused on the policy aspect of cyber security and includes fact-based assessments of policies or organizations addressing cyber security in one hundred fourteen countries. The Cyber Index also contains information on activities of international and regional organizations in this field. In the Cyber Index, there is a clear division between countries with a civilian versus a military approach to cyber security.

The Cyber Index has a broad geographic range, detailed country profiles and an excellent overview of military engagement. The Cyber Index uses only open source information and lacks reference to cybersecurity regulation, technical measures (standards, certification), capacity building. The Cyber Index does not score or rank countries. (UNIDIR, 2013)

3.1.6 Cybersecurity Policy Making at a Turning Point

The Cybersecurity Policy Making at a Turning Point publication has been developed by the Organization for Economic Cooperation and Development (OECD). The Cybersecurity Policy Making at a Turning Point analyzes cyber security strategies in ten countries and provide information on commonalities and differences between them. The Cybersecurity Policy Making at a Turning Point is based on a questionnaire. The questionnaire is then filled out by the volunteer countries and supplemented with relevant material. The Cybersecurity Policy Making at a Turning Point is mainly focused on policy and organizational aspects of cyber security. The Cybersecurity Policy Making at a Turning Point also provides an overview of initiatives undertaken by intergovernmental organizations.

The Cybersecurity Policy Making at a Turning Point research provides a broad overview of strategies and touches upon all International Telecommunication Union Global Cybersecurity Agenda (ITU GCA) pillars. The Cybersecurity Policy Making at a Turning Point further adds a useful overview of intergovernmental organization's initiatives. The Cybersecurity Policy Making at a Turning Point does not provide score or ranking and is limited in geographic range, with ten countries. (OECD, 2012)

3.1.7 Global Cybersecurity Index

An index developed by a cooperative effort between ABI Research and the International Telecommunication Union (ITU). The Global Cybersecurity Index provides insight into the cyber security engagement of sovereign nation states. The Global Cybersecurity Index is rooted in the ITU's Global Cybersecurity Agenda (GCA)(ITU, 2007).

The Global Cybersecurity Index focuses on five broad cyber security application areas with twenty-four indicators.The five areas are legal measures, organizational measures, technical measures, international cooperation and capacity building. The Global Cybersecurity Index gives a good understanding of the global ranking of cyber security readiness. A total number of one hundred and ninety-three countries have been analyzed, one hundred and four nations of which were a subject of both primary and secondary research and ninety countries only a subject of secondary research. The Global Cybersecurity Index includes an overall ranking, as well as six regional rankings and an individual score for each country.

The Global Cybersecurity Index is classed as an index since it has indicators, a scoring, and ranking mechanisms. The main the advantage of the Global Cybersecurity Index is its global character (the only research with such broad geographic range). The Global Cybersecurity Index is based on both survey among the ITU Member States and opens sourced material.

On the other hand, the Global Cybersecurity Index is only focused on policy and organizational aspects of cyber security and lacks thorough reference to technology. (ITU, 2014a)

3.1.8 EU Cybersecurity Dashboard

The EU Cybersecurity Dashboard is developed by BSA, The Software Alliance. The EU Cybersecurity Dashboard is focused on policy and organizational aspects of cyber security, with strong reference to legal foundations as well as cooperation between public and private sector. The EU Cybersecurity Dashboard includes twenty-five criteria across five themes: legal foundations for cyber security, education, operational entities, public-private partnership (PPP), and sector-specific cyber security plans. The EU Cybersecurity Dashboard covers the twenty-eight European Union Member States. The aim of the EU Cybersecurity Dashboard is to provide a reference base which allows the evaluation of country's policies regarding cyber security against twenty-five criteria and the cyber security stance compared to the other EU Member States.

The EU Cybersecurity Dashboard was developed based on publicly available information with no targeted interviews conducted. The EU Cybersecurity Dashboard does not offer scoring nor ranking mechanisms.

What is interesting about the EU Cybersecurity Dashboard is a graphic reference base which allows for a quick evaluation of countries' cyber security stance. The focus is primarily on policy, organizational and legal aspects of cyber security with strong reference to public-private-partnerships. On the other hand, it is limited in geographic range to EU countries and could strongly benefit from a survey-based data collection exercise. (BSA, 2015)

3.1.9 National Cyber Security Index

The National Cyber Security Index (NCSI) is developed by e-Governance Academy Foundation. The official publication date will be May 31, 2016, at the Tallinn e-Governance Conference. The National Cyber Security Index is a tool, which measures countries' capacity to ensure the proper functioning of its information society in cyberspace. The National Cyber Security Index describes strategic measures at the national level, which are necessary for securing public and private e-services, communication and information systems, and national databases. The National Cyber Security Index measures countries' capacity to prevent and manage strategic cyber threat scenarios. The National Cyber Security Index methodology is based on four categories: general cyber security, baseline cyber security, incident and crisis management and international influence. Additionally to mentioned four categories, it has twelve indicators and ninety-nine parameters. (Rikk, 2016)

3.2 Indexes for assessing organizations

Indexes for assessing organizations are slightly different from the indexes for assessing countries. Primarily, they seek to offer a benchmark or guidelines against which an organization can measure its level of cyber security development or capacity, without necessarily offering a comparative with other agencies. These types of indexes are also known as maturity models and are offering baselines for organizations, and states, to start the process of self-evaluation.

3.2.1 Information Risk Maturity Index 2014

The Information Risk Maturity Index has been developed jointly by PwC and Iron Mountain Inc. The scope of the Information Risk Maturity Index is to determine the maturity of information security by businesses. The Information Risk Maturity Index includes a set of thirty-four measures, grouped into four categories: strategy, security, people and communications. The measures have been developed for protection of a company's information assets and to foster the management. The aim of the Information Risk Maturity Index is to exhibit the extent to which the measures mentioned above are being implemented and monitored at the enterprise level. As such it is the Information Risk Maturity Index that enterprises can use to evaluate themselves. The Information Risk Maturity Index offers four levels of information risk maturity: unprepared for risk, risk

aware, equipped for risk and approaching maturity. The Information Risk Maturity Index is mainly focused on the organizational aspect of cyber security. The Information Risk Maturity Index offers some scoring results on information risk maturity and provides distribution of the results by region and size of the company. (PwC & Iron Mountain, 2012)

3.2.2 Risk and Responsibility in a Hyperconnected World

The Risk and Responsibility in a Hyper-Connected World were developed jointly by the World Economic Forum and McKinsey & Company. The aim of the Risk and Responsibility in a Hyperconnected World is to assess the potential impact of cyber attacks as well as readiness to response and present key areas where global leaders across the spectrum of public sectors, private and civil institutions can collectively explore to increase cyber resilience. The Risk and Responsibility in a Hyperconnected World also identify key action areas that should be studied regarding increasing cyber resilience. These areas are grouped into four categories: institutional readiness, community, systemic, public and international policy. The Risk and Responsibility in a Hyperconnected World are based on interviews with sector leaders as well as studies undertaken among multiple sector firms. (McKinsey & Company, 2014)

3.2.3 Cyber Operations Maturity Framework

The Cyber Operations Maturity Framework model was developed by Booz Allen Hamilton Inc. The Cyber Operations Maturity Framework presents the company's approach to cyber operations which include an Operational Model for organizations. This Cyber Operations Maturity Framework model integrates four functions: Anticipation, Awareness, Action, and After-Action. The Cyber Operations Maturity Framework provides five maturity levels in eleven key operational areas, and it is mainly focused on the operational aspect of cyber security. (Booz Allen Hamilton, 2011)

3.2.4 Cybersecurity Capability Maturity Model

The Cybersecurity Capability Maturity Model has been developed by the University of Oxford's Global Cyber Security Capacity Centre. The aim of the Cybersecurity Capability Maturity Model is the creation of a universally applicable cyber security maturity model.

The Cybersecurity Capability Maturity Model defines five capacity dimensions related to cyber security: cyber security policy and strategy; cyberculture and society; cyber security education, training, and skills; legal and regulatory framework; and organizations, technologies, and standards. The Cybersecurity Capability Maturity Model identifies set of forty-nine indicators depicting varying levels of cyber security capacity development. The Cybersecurity Capability Maturity Model is mainly focused on policy and organizational aspects of cyber security. (GCSCC, 2014)

3.3. Indexes for assessing threats

Indexes for assessing threats are the third group of indexes that evaluate the level of risk attributed to cyber attacks, incidents, security events, and vulnerabilities, among other threat scenarios. Indexes for assessing threats do not evaluate organizations or nation states, but merely provide an assessment of the threat landscape. That information can primarily be used for intelligence and awareness purposes. The indexes are often developed by individual academics and security practitioners, and private sector organizations.

3.3.1 Cybersecurity Intelligence Index

The Cybersecurity Intelligence Index was prepared by IBM's Managed Security Services. The Cybersecurity Intelligence Index includes an overview of cyber security threats based on cyber attack event data gathered by the company. The data was collected by monitoring client security devices and analysis from IBM's security operations centers. The Cybersecurity Intelligence Index provides a broad overview of technical challenges, case studies, and best cyber security practices in the private sector. The Cybersecurity Intelligence Index does not score or rank organizations or countries, nor does it include a formula for the calculation or any specific indicators for the calculation of an index. The Cybersecurity Intelligence Index provides the overall number of incidents, attacks, and security events, as well as distribution by industries, class of attackers and the category of incidents. (IBM X-Force Research, 2015)

3.3.2 Index of Cyber Security

The Index of Cyber Security was an individual effort developed by Mukul Pareek and Dan Geer Jr. and was focused on the technical aspect of cyber security. The Index of Cyber Security is an opinion-based measure of perceived risk to information infrastructures from a broad range of cyber security threats. A lower index value indicates a perception of increasing risk while a higher index value indicates the opposite. The Index of Cyber Security gathers the views of information security professionals on the most current and most interesting threats to industrial, corporate and governmental information infrastructure through a monthly survey. The Index of Cyber Security was based on a variation of the diffusion index methodology. Unfortunately, detailed statistics and individual sub-indices are shared only with respondents in a separate report. (Geer Jr & Pareek, 2012)

3.3.3 The CTU Cyber Security Index

The CTU Cyber Security Index was developed by Dell Secure Works. The aim of the CTU Cyber Security Index was to notify customers about threats and malicious activities which may require implementing protective measures. The CTU Cyber Security Index uses a four-level scoring system of overall network cyber security status which in a readable and straightforward manner informs customers about the current level of overall cyber security threat. The CTU Cyber Security Index is not numerical, but merely color coded based on the following four cyber security levels: Guarded, Elevated, High, and Critical. A panel of experts determined the cyber threats at the Dell SecureWorks Counter Threat Unit Research Team and based on data such as the release of security updates by companies such as Adobe Systems Incorporated and Microsoft Corporation. The CTU Cyber Security Index was focused on the technical aspect of cyber safety and was evaluated on a day-to-day basis.

3.3.4 The Gibson Index

The Gibson Index was an individual effort developed by Kevin Boyd. The Gibson Index was mainly focused on the technical aspect of cyber security. The Gibson Index offered a way to rank the level of severity of cyber attacks on a spectrum from zero to seven, zero being the least disruptive and seven the most disruptive. The levels are determined by

definitions and examples of events in each level. The Gibson Index was shut down by the author Kevin Boyd in June 2015.

3.4 Conclusion of overview

The cyber security indexes and assessment models mentioned above are just a summary of some of the more relevant cyber security assessment models. The author believes that there are likely to be much more ongoing research projects in cyber security assessment field. While this thesis does not provide a finite list of all, the point is to give a brief overview of some of the assessment models to continue to educate and inform on the value of indexes and assessment models.

4. Case study

The author has chosen to take a deeper study on the Global Cybersecurity Index 2014 (GCI 2014). The main reason is that the Global Cybersecurity Index the only index with such broad geographic range, a total number of one hundred and ninety-three countries.

4.1 Introduction

The Global Cybersecurity Index is a composite index combining twenty-four indicators into one assessment model to monitor and compare the level of ITU member states cyber security commitment concerning the five areas identified by the High-Level Experts Group (HLEG, 2008) and endorsed by the Global Cybersecurity Agenda (GCA) (ITU, 2007). These pillars form the five sub-indices of the Global Cybersecurity Index. First developed by the International Telecommunication Union in partnership with ABI Research in 2013, and with results presented in November 2014, the Global Cybersecurity Index was included under Resolution 130 (ITU, 2014c). The Global Cybersecurity Index is being enhanced in response to International Telecommunication Union member states request to develop a cyber security index and publish updates regularly.

The main objectives of the Global Cybersecurity Index are to measure:

- the type, level, and evolution of comparative cyber security commitment in countries over time;
- progress in cyber security engagement of all countries from a global perspective;
- advances in cyber security commitment from a regional perspective;
- the cyber security commitment divides, i.e. the difference between countries regarding their level of engagement in cyber security initiatives.

The objective of the Global Cybersecurity Index is to help countries identify areas for improvement in the cyber security field and to motivate them to take action to improve their relative Global Cybersecurity Index ranking, thus helping raise the overall level of cyber security worldwide. Through the information collected, the Global Cybersecurity Index aims to illustrate the practices of other countries so that International Telecommunication Union member states can comply selected aspects suitable to their public environments, with the added advantage of helping to spread best practices and foster a global culture of cyber security.

4.2 Background

The Global Cybersecurity Index was included in the Resolution 130 (ITU, 2014c) on strengthening the role of ITU in building confidence and safety in the use of ICT. Specifically, ITU member states are invited to support ITU initiatives on cyber security, including the Global Cybersecurity Index, to share information on efforts across sectors and to promote government.

A first iteration of the Global Cybersecurity Index was conducted in 2013-2014 in partnership with ABI Research. A total of one hundred and five countries out of one hundred and ninety-three International Telecommunication Union member states answered the questionnaire. For the rest of the eighty-eight non-respondents countries, the secondary research was used to build the index, and the research outcomes were sent to them for verification.

4.3 Conceptual Framework

The Global Cybersecurity Agenda (GCA) was initiated by the International Telecommunication Union Secretary-General as International Telecommunication Union's framework for international multi-stakeholder cooperation towards a secure and safer information society. The Global Cybersecurity Agenda focuses on the following five work areas:

- Legal Measures;
- Technical Measures;
- Organizational Measures;
- Capacity Building;
- Cooperation.

Legal measures authorize a nation state to set basic response mechanisms through investigation and prosecution of crimes and the imposition of sanctions for breach of law or non-compliance with the law. A legislative framework helps to establishing minimum standards of behavior across the board as well as to facilitate the growth of cyber security capabilities at the national level. A legislative frameworks objective is ensuring the presence of an adequate domestic framework to address cybercrime Therefor the Global Cybersecurity Index can be a tool to enable harmonization, facilitate international cooperation, promote good practices at the regional and international level. The legal environment is evaluated based on the presence or absence of legal frameworks dealing with cyber security and cyber crime.

Technical measures are playing a vital role in the defense against cyber threats. Without adequate technical capacities to detect and respond to cyber attacks, nation states remain vulnerable. Effective information and communications technology development and use can only truly prosper in a climate of trust and security. Therefore, governments need to establish capabilities and processes to use technology effectively as an enabler in addressing cyber threats. This would involve the creation of a national framework for tracking, warning and incident response, creating a responsible government agency or a national entity focused on dealing with cyber incidents. Clearly together with national standards bodies to incorporate international standards and industry best practices into domestic cyber security efforts. The technical measurement is evaluated based on the presence or absence of information technology-related measures, including standardization agencies, dealing with cyber security by the nation state.

Organizational measures are essential for the proper implementation of any national initiative. A wide strategic objective needs to be set by the nation-state, along with a large-scale plan for implementation, measurement and delivery. National bodies need to be present to evaluate the results and to implement the strategy. Without a national strategy, governance model and supervisory body, efforts in different sectors become disparate, thwarting efforts to attain national harmonization in cyber security capacity development. The organizational structures are assessed based on the existence or absence of institutions and strategies concerning cyber security development at the national level.

Capacity building is critical to the first three measures (legal, technical and organizational). Cyber security is most often tackled from a technological perspective even though there are numerous socio-economic and political implications. Human and institutional capacity building are necessary to raise knowledge and know-how across different sectors and branches, to formulate appropriate solutions, and promote the development of the competent specialists. Capacity building is assessed based on the number of research and development, education and training programs, together with relevant programs run by professionals and public sector agencies.

In cooperation measures, the cyber security and cyber crime are global issues and are blind to national borders or sectoral distinctions. Essentially, tackling cyber crime requires a multi-stakeholder approach with inputs from all sectors. Greater cooperation can enable the development of much stronger cyber security capabilities, helping to prevent repeated and persistent online threats and enable better apprehension, investigation and prosecution of malicious agents. International and national cooperation are evaluated based on the number, scope, and type of partnerships, cooperative frameworks, and information sharing networks. (ITU, 2014a)

These five measures form the basis of the indicators for the Global Cybersecurity Index. These five categories are critical to measuring national capabilities in cyber security because they form the essential building blocks of a national culture. Cyber security has a field of application that cuts across all sectors and industries, both vertically and horizontally. Enabling the development of national capabilities the political will and investments are needed. This can be done by justice and law enforcement departments, ministries and educational institutions, developers of technology and private sector operators, intra-state cooperation and public-private partnerships. (ITU, 2014a)

The long-term goal is to drive further efforts in the adoption and integration of cyber security on a global scale. A comparison of national cyber security strategies will reveal those states with high rankings in specific areas and consequently, expose lesser-known yet successful cyber security strategy. This can increase information sharing on deploying cyber security for these countries at different levels of development as well. By measuring the level of cyber security preparedness in various areas, the Global Cybersecurity Index will allow states to assess where the states are on a scale of development, where the states need to make more improvements and how far the states are from implementing an acceptable level of cyber security. All countries are moving towards a more connected and digitized environment, and adopting cyber security early on can enable the deployment of more resilient and secure infrastructure in the long term.

The Global Cybersecurity Index is a joint effort between the International Telecommunication Union's Telecommunication Development Bureau (BDT), to be more exact the Cybersecurity and ICT Applications Division (CYB) and ABI Research. The Cybersecurity and ICT Applications Division will act as an owner and a central point of the Global Cybersecurity Index, and ABI Research brings in its core skill sets in technology assessment, strategy development, competitive intelligence, business planning, and industry benchmarking for the realization of the Global Cybersecurity Index (ITU, 2014a). Under the arrangement, the International Telecommunication Union and ABI Research aim to:

- identify performance metrics;
- develop a global ranking mechanism;
- research and collect data on nation states' cyber security capabilities;
- contact and liaise with nation states and relevant organizations;
- identify and insert the relevant information in the index;
- publish a Global Cybersecurity Index.

4.4 Methodology

The statistical model used by the Global Cybersecurity Index is being based on a Multi-Criteria Analysis (MCA). The Multi-Criteria Analysis establishes preferences between options by reference to a specific set of identified goals for which there are set measurable criteria to assess the scope to which the objectives have been achieved. A simple linear additive evaluation model is being applied. The Multi-Criteria Analysis performance matrix defines the options, and each column defines the performance of the options against each measurement. The individual performance assessment is numeral.

The benchmark scoring is being based on the indicators. A group of experts in the field of cyber security has weighed each of five sub-indices.

The group of experts has fixed with the aim of providing a thorough and expert suggestions on the balance to be assigned to each question in the Global Cybersecurity Index questionnaire. The weight of issues that has been suggested by the group of experts reflects the importance of specific dimensions of the overall cyber security commitment of a nation state. Open-ended questions are included in the questionnaire to serve for additional requirements from International Telecommunication Union Telecommunication Development Sector Study Group 2 Question 3 (ITU, 2014c), which do not fit within the Global Cybersecurity Index computation.

The panel of experts consists of around ten to fifteen experts in the field of cyber security. Involvement in the panel of experts has been open to following:

- One appointee of each partner of the Global Cybersecurity Index (both strategic and contributing) is proposed. The partner will decide on participation.
- Volunteers participating in the International Telecommunication Union Telecommunication Development Sector Group 2 Question 3.
- Well-recognized and respected specialists in the field of cyber security not being in any of the above categories.

The membership of the panel of experts reflects regional diversity of expertise as well as the balance between different stakeholders, including governments, the private sector, and academia.

The evaluation process requires the experts to provide their suggestions regarding the balance for each question. Of course, inputs have been received by the International Telecommunication Union; weights have been averaged and submitted to the experts for discussion, with particular focus on outliers and any other pattern of disagreement;

Zero points are allocated where there are no activities; one point is assigned for action. The final scores per indicator will be reduced to total one hundred points.

4.5 Notation

x_{qc} value of the individual indicator q for country c, with q = 1,...,Q and c = 1,...,M.

I_{qc} normalized value of individual indicator q for country c

CI_c value of the composite indicator for country c.

The benchmark used will be the score of the hypothetical state that maximizes the overall commitment (GCI 2014 – 34; GCI 2016 – 100) points. The resulting composite index will range between zero (worst possible readiness) and one (the benchmark):

GCI 2014 – $CIc=Iqc/34$

GCI 2016 – $CIc=Iqc/100$

The normalization technique will be based on a ranking method:

$$I_{qc}=Rank\ (x_{qc})$$

(ITU, 2014a)

4.6 Categories and Performance Indicators

The Global Cybersecurity Index is a benchmark ranking measuring the cyber security development capacities of sovereign International Telecommunication Union member states. The Global Cybersecurity Index is essentially a composite indicator, focusing some individual indicators. The process of cyber security development can be analyzed within five essential categories. The following indicators and sub-indexes have been identified, and International Telecommunication Union member states are being ranked against the guidelines provided in each indicator. (ITU, 2014a)

4.6.1 Legal Measures

The legislation is a critical measure for providing a harmonized framework for entities to align themselves to a mutual regulatory basis, whether on the matter of minimum regulatory requirements or prohibition of specified criminal conduct. Legal measures allow a nation state to issue the basic response mechanisms to breaches, such as through investigation and prosecution of cyber crimes and the imposition of sanctions for violation of law or non-compliance of legislation. A legal framework sets the minimum standards of behavior across the board, applicable to all, and on which future cyber security capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place to harmonize practices to create consensus around cyber security norms and to facilitate international cooperation in combatting cyber crime. (ITU, 2014a)

The legal environment is being measured based on the number of existing legal frameworks and institutions dealing with cyber security and cyber crime. The sub-group is put together of the following indicators:

4.6.1.1 Cyber criminal legislation

Cyber criminal legislation determines laws on the unauthorized access, interception, interference of data, computers and information systems. It also includes procedural laws, as well as any precedents on cyber crime or computer misuse; a real-time collection of computer data and any existing articles on the expedited preservation of stored computer data; production orders, extradition of cyber perpetrators, confidentiality, limitation on use and mutual assistance. (ITU, 2015c)

4.6.1.2 Cyber security legislation

Cyber security regulation designates laws dealing with data protection, breach notification, cyber security certification/standardization requirements, implementation of cyber safeguards, cyber security audit requirements, child online protection, privacy protection, the liability of Internet service providers, digital signatures, and e-transactions. (ITU, 2015c)

4.6.1.3 Cyber security training

Cyber security training for law enforcement officers and other legal and judicial actors designates professional and technical, potentially recurring, training for enforcement agents, police officers, solicitors, barristers, judges, paralegals, lawyers, attorneys and other persons of the law enforcement and legal profession. Training targets are both public and private professionals. (ITU, 2015c)

4.6.2 Technical measures

The premier line of protection against cyber threats and malicious online agents is technology. Without adequate technical actions and the capabilities to detect and respond to cyberattacks, nation-states, and their respective entities remain vulnerable to cyber threats. The forthcoming and success of ICT can only really prosper in a climate of confidence and security. Therefore, nation states, need to be capable of developing strategies that promote the use of technology as a cyber threats enabler.

Addressing the cyber threats includes the establishing of a national agency focused on handling cyber incidents, a national framework set in place and a responsible public body for the watch, warning and cyber incident response, as well as industry best practices into domestic cyber security efforts and national standards bodies to incorporate international standards. (ITU, 2014a)

Technical measures can be assessed based on the existence of technical frameworks and institutions that deal with cyber security endorsed or created by the nation state. The sub-group has been put together of the following indicators:

4.6.2.1 National CERT/CIRT/CSIRT

The formation of a CIRT/CERT/CSIRT[1] with national responsibility provides the capabilities to identify, respond and defend cyber threats and increase cyberspace security in the nation state. Those abilities should be complemented with the gathering of the nation's intelligence from secondary reporting of security incidents whether from the Computer Incident Response Team's constituencies and/or other sources. (ITU, 2015c)

4.6.2.2 Government CERT/CIRT/CSIRT

A government CIRT/CERT/CSIRT is an agency that reacts to cyber security incidents which affect only governmental institutions. Separately from reactive services, it may also engage in proactive services such as security audits and vulnerability analysis. Unlike the national CERT, that services both the public and private sectors, the government CERT provides its services only to the components of the public sector. (ITU, 2015c)

4.6.2.3 Sectoral CERT/CIRT/CSIRT

A sectoral CERT/CIRT/CSIRT is an agency that responds to or cyber security incidents that affect a specific sector. Sectoral CERTs are established for critical sectors such as emergency services, healthcare, financial sector and public utilities. Unlike the government CERT, the sectoral CERT provides its services only to the constituents of a specific sector. (ITU, 2015c)

4.6.2.4 Cyber security standards implementation framework for organizations

This indicator measures the existence of a government-approved (or endorsed) framework(s) for the implementation of internationally recognized cyber security standards within the public sector (government agencies) and within critical infrastructure (even if operated by the private sector). (ITU, 2015c)

[1] A Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), or Computer Security Incident Response Team (CSIRT) is a team of IT security experts whose main business is to respond to computer security incidents.(ENISA, 2006) It provides the necessary services to handle them and support their constituents to recover from breaches.(Kruse II & Heiser, 2001)

4.6.2.5 Cyber security standards and certification for professionals

This indicator measures the existence of a government-approved (or endorsed) framework(s) for the certification and accreditation of professionals by internationally recognized cyber security standards. (ITU, 2015c)

4.6.2.6 Child online protection

Child online protection parameter assesses the existence of a national agency dedicated to child online protection, activities by non-government or government institutions to provide support and knowledge to stakeholders on how to protect children online. Also the accessibility of a state telephone number to report problems associated with the kids online, and any technical capabilities and mechanisms deployed to help protect children online. (ITU, 2015c)

4.6.3 Organizational measures

Procedural and organizational measures are essential for the correct implementation of any national initiative. A broad strategic objective to address cyber security needs to be set by the nation-state, with an extensive plan in implementation, measurement and delivery. Structures such as national agencies need to be established to put the strategy into effect and assess the success or failure of the plan. Without a state strategy, supervisory body and governance model, efforts in different industries and sectors become unconnected and disparate, preventing efforts to reach national harmonization regarding cyber security capability development.(ITU, 2014a)

The organizational structures can be assessed based on the existence of institutions and strategies organizing cyber security development at the national level. The creation of efficient organizational structures is necessary for promoting cyber security, combating cyber crime and promoting the role of the watch, warning and also an incident response to guarantee intra-agency, cross-border and cross-sector coordination between new and existing initiatives. The sub-section is composed of the following measurements:

4.6.3.1 Strategy

The development of policy to promote cyber security is recognized as a top priority. A national strategy for cyber security should maintain reliable, and resilient information infrastructure, and aim to ensure the safety of citizens. The National strategy should also minimize damage and recovery times from cyber-attacks, protect the material and

intellectual assets of citizens, organizations, the state and it should prevent cyber-attacks against critical infrastructures. Policies on national cyber security plans or strategies for the protection of information infrastructures are those officially endorsed and defined by a nation-state, and can include the following obligations: establishing clear liability for cyber security at all government levels, with clearly defined roles and responsibilities. Policies on national cyber security strategies should also make a clear commitment to cyber security, which is transparent and public; encouraging private sector involvement and partnership in government-led initiatives to promote cyber security; creating guidelines for governance that identifies key stakeholders. (ITU, 2015c)

4.6.3.2 Responsible agency

A responsible governmental agency for implementing a national cyber security policy and/or strategy can contain permanent committees or cross-disciplinary centers, official working groups and advisory councils. Most national institutions will be directly liable for watch and warning systems and incident response, and for the expansion of the organizational structures wanted for coordinating responses to cyber attacks. (ITU, 2014a)

4.6.3.3 Cyber security metrics

Cyber security metrics indicator measures the existence of any officially recognized sector-specific or national benchmarking exercises used to measure cyber security development, risk-assessment strategies, cyber security audits, and other activities and tools for assessing or evaluating resulting performance for future improvements. The objective is to measure the readiness of the country in assessing the risks posed by cyber threats as well as its capacity in evaluating the response, through periodic audits. The indicator does provide a qualitative analysis, but rather directs at emphasizing the importance on the continuous improvement of the efforts deployed. (ITU, 2015c)

4.6.4. Capacity building

Capacity building is internal to the first three measures (legal, technical and organizational). Understanding the implications, the risk, and the technology, and can help to develop better strategies, policies, legislation, and organization as to the various roles and responsibilities. Cyber security is a comparatively new area, not much older than the Internet itself. This field of study is most often tackled from a technological perspective, yet numerous political and socio-economic implications have applicability in this area. Human and institutional capacity building are necessary to increase knowledge and know-how across industries and sectors, to apply the most suitable solutions, and promote the development of the most proficient specialists.(ITU, 2014a)

A capacity-building framework for promoting cyber security should include the availability of resources and awareness-raising. Capacity building can be assessed based on the number and existence of development and research, training and education programs, and certified professionals and public sector agencies. Some information is collected through reliable secondary sources which provide certified training worldwide. The sub-section is composed of the following measurements:

4.6.4.1 Standardization bodies

Standardization is a good indicator of the level of maturity of the technology, and the emergence of new standards in main areas underlines the significant importance of standards. Although cyber security has always been an issue for national security and treated differently in different countries, there are common approaches how they are supported by usually recognized standards. This indicator measures the existence of a national cyber security standardization body and activities in the development and implementation of cyber security standards. (ITU, 2015c)

4.6.4.2 Cyber security good practices

Cyber security good practices measurement assesses the publication and research of best practices and guidelines on cyber security technology and its use, application to various scenarios and management. Best practices are procedures or methods which have a proven track record of success. Embracing best practices will not only reduce the probability of failure but also an increase of trust and efficiency. (ITU, 2015c)

4.6.4.3 Cyber security research and development programs

This indicator measures the investment into national cyber security research and development programs at institutions which could be private, public, academic, international or non-governmental. It also considers the presence of a nationally recognized institutional body overseeing the program. Cyber security research programs include, but are not limited to, malware analysis, security models and concepts cryptography research, and research into system vulnerabilities. Cyber security development programs refer to the development of software and hardware solutions that include, but are not limited to, firewalls, hardware security modules, honeypots and intrusion prevention systems. The presence of an overarching national body will increase coordination among the various institutions and sharing of resources. (ITU, 2015c)

4.6.4.4 Public awareness campaigns

Public consciousness includes efforts to promote widespread publicity campaigns to reach as many people as possible as well as making use of non-governmental organizations, institutions, internet service providers, organizations, libraries, local trade organizations, computer stores, community centers. Also, adult education programs and community colleges, parent-teacher organizations and schools to get the know-how across about safe cyber-behaviour online. Public awareness campaigns include actions such as setting up portals and websites to promote awareness, disseminating support material and adoption of those cyber security practices that would reduce exposure to the general public to cyber threats (e.g. Stop, Think, Connect campaign). The presence or absence of direct consultations will also be measured, such as incentives to develop cyber security clinics for underserved stakeholders potentially housed at educational institutions that would have the dual benefit of increasing the availability of applied cyber security training for the next generation of cyber security professionals. (ITU, 2015c)

4.6.4.5 Cyber security professional training courses

This indicator measures the existence of national or sector-specific educational and professional training programs. (ITU, 2015c)

4.6.4.6 National education programs and academic curricula

This indicator looks at the existence and the promotion of national education courses and programs to train the younger generation in cyber security-related skills and professions in schools, colleges, universities and other learning institutes. Cyber security-related skills include, but are not limited to, setting strong passwords and not revealing personal information online. Cyber security-related professions include, but are not limited to, cryptanalysis, digital forensics experts, incident responders, security architects and penetration testers. (ITU, 2015c)

4.6.4.7 Incentive mechanisms

Incentive mechanisms indicator looks at any incentive efforts by the government to encourage capacity building in the field of cyber security, whether through funding, grants, tax breaks, loans, disposal of facilities, and other economic and financial motivators. Incentives increase the demand for cyber security-related services and products, which improves defenses against cyber threats. (ITU, 2015c)

4.6.4.8 Home-grown cyber security industry

A favorable economic, political and social environment supporting cyber security development will incentivize the growth of a private sector around cyber security. The existence of manpower development, public awareness campaigns, capacity building and government incentives will drive a market for cyber security products and services. The existence of a home-grown cyber security industry is a testament to such a favorable environment and will drive the growth of cyber security start-ups and associated cyber-insurance markets. (ITU, 2015c)

4.6.5 Cooperation

Cyber security requires input from all industries and sectors, and for this reason needs to be tackled through a multi-stakeholder approach. Cooperation increases dialogue and coordination, enabling the creation of a more comprehensive cyber security field of application. Knowledge sharing is difficult at best between different disciplines, and within private sector operators. Information sharings becomes increasingly so at the international level. However, cyber threats are global in

nature and blind to sectoral distinctions or national borders. Cooperation enables distribution of threat information, attack scenarios, and best practices in response, mitigations, and defense. Greater cooperative initiatives can allow the development of much stronger cyber security capabilities, helping to deter persistent and repeated online threats, and enable better apprehension, investigation and prosecution of malicious agents. International and national cooperation can be measured based on the existence and number of partnerships, cooperative frameworks, and information sharing networks. (ITU, 2014a) The sub-group is composed of the following indicators:

4.6.5.1 Bilateral agreements

Bilateral agreements refer to any officially recognized or ratified national or sector-specific partnerships for sharing cyber security assets or information across borders by the government with one other regional entity, an international organization or foreign government (i.e. the cooperation or exchange of information, technology, expertise and other resources). The bilateral agreements indicator also measures whether the agreement is pending ratification or legally binding. Information sharing refers to the distribution of threat intelligence while assets designate the exchange of professionals (placements, secondments or other temporary assignments of employees), facilities, equipment and other tools and services. (ITU, 2015c)

4.6.5.2 Multilateral agreements

Multilateral agreements refer to any officially ratified or recognized sector-specific or national programs for sharing cyber security assets or information across borders by the government with multiple international organizations or foreign governments (i.e. exchange of information or cooperation, technology, expertise and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information-sharing indicates to the sharing of threat intelligence while assets designate the exchange of professionals (placements, secondments or other temporary assignments of employees), equipment, facilities and other tools and services. (ITU, 2015c)

4.6.5.3 Participation in international forums

As part of enhancing collaboration in Cyber security, the commitment of governments to participate in Cyber security events is at this moment measured. Such events include regional and international workshops, training and conferences. (ITU, 2015c)

4.6.5.4 Public-private partnerships

Public-private partnerships refer to ventures between the public and private sector. Public-private partnerships performance indicator can be assessed by the number of officially recognized sector-specific or national public-private partnerships for sharing assets (people, processes, tools) and cyber security information (threat intelligence). The sharing would be between the private and public sector (i.e. official partnerships for the exchange or cooperation of information, expertise, technology, and/or resources), whether nationally or internationally. (ITU, 2014a)

4.6.5.5 Interagency partnerships

The interagency partnerships performance indicator refers to any official partnerships between the various government agencies within the nation state. This can determine partnerships for asset or information sharing between programs, departments, ministries, and other public sector institutions. (ITU, 2015c)

4.7 Summary about ITU GCI 2014 case study

The Global Cybersecurity Index 2014 is a research project to rank the cyber security capabilities of nation states. Cyber security has a wide field of application that cuts across many industries and sectors.

After doing solid research about GCI 2014, everything above mentioned sounds nice, but there are also some other aspects that ITU should take into consideration in future. The author will give full summary after the following analysis chapter.

5. Analysis

The Global Cybersecurity Index 2014 was the first time by the ITU to evaluate the cyber security situation in countries globally. Today, ITU is gathering answers to their GCI 2016 questionnaire.

5.1 Data collection

Concerning the data collection the methodology is the same. First, they do primary research – they contact relevant national stakeholders and ask them to fulfill the questionnaire, and then they collect the data (i.e., answered questionnaire). The questionnaire will be answered online. Every respondent will be provided (via an official email from ITU) a unique URL for his/her safe keeping. The online questionnaire allows the respondents to upload relevant documents (and URLs) for each question as supporting information.

After the primary research they do secondary research – they use internal databases and publicly available resources. Secondary data was used to build the index for non-respondents, and the research outcomes were sent to them for verification/endorsement.

During the data collection for GCI 2014 one hundred and five countries out of one hundred and ninety-three member states responded the questionnaire.[2] Although the GCI 2016 is not ready yet the primary research deadline was in March 2016, and ITU got back one hundred and twenty-three filled questionnaires from their member states.[3]

After primary and secondary data collection there will be data extraction – organize and sort through collected data.

Final two steps are data input – assess the performance of each nation state and ratification – member state review of researched data.

There is also one risk concerning data collection. The success rate of this extensive data gathering (both primary and secondary research) effort depends heavily on the response rate to the questionnaire. So, ITU should actively promote the Global Cybersecurity Index to raise awareness to foster a global culture of cyber security.

[2] Information retrieved from ITU GCI 2014 webpage: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx
[3] Information retrieved from ITU GCI 2016 webpage: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx

5.2 Questionnaires

As the GCI 2016 is still in data collection phase and will be completed at the beginning of 2017, then it is not possible to compare the GCI 2014 and the GCI 2016.

Although, some major changes has been done with the questionnaire that has been sent out to all ITU member states.

In GCI 2014 questionnaire there were only seventeen questions (see Annex 1). In the GCI 2016 questionnaire there are one hundred and fifty-seven questions (see Annex 2). It is nine times more questions than in the GCI 2014 questionnaire. In each of the five pillars, some new questions have been added to refine the depth of research. The main difference between the GCI 2014 and the GCI 2016 questionnaires is that in the GCI 2014 questionnaire there were mostly open-ended questions, but in the GCI 2016 questionnaire there are more questions where the respondent will only confirm the presence or lack of certain pre-identified cyber security capabilities.

The rationale behind using pre-identified answer possibilities is the elimination of opinion-based evaluation and any possible bias towards certain types of answers. Moreover, the simple pre-identified answer concept will allow more direct and quicker evaluation as it will not require lengthy answers from countries. This will accelerate and streamline the process of providing answers and further evaluation. The pre-identified answer system evaluates the existence or absence of a specific activity, department, or measure.

Also, additional requirements from ITU-D Study Group 2 Question 3 the open-ended questions have been included in the questionnaire (see Annex 3), which do not fit within the GCI computation.

5.3 Indicators

The indicator part is the second biggest change between the GCI 2014 and the GCI 2016. When in the GCI 2014 there were seventeen indicators than in the GCI 2016 there are 24 indicators.

5.3.1 Legal measures category

In the GCI 2014 version in legal measures category, there were two indicators: criminal legislation and regulation & compliance. In the GCI 2016 version, there are three indicators: cyber criminal legislation, cyber security regulation, and cyber security training. The first two are same as in the GCI 2014 version, but the cyber security training indicator is new. It makes sense because having a legal structure is essential but to have educated

workforce is difficult if the country does not have a formal process for training legal actors about computer security. Also, the training for law personnel should be organized repeatedly and periodically. (ITU, 2015c)

5.3.2 Technical measures category

In the technical measures category, the first change is the indicator for CIRT/CERT/CSIRT[4]. In the GCI 2014 version there was one indicator for CIRT/CERT/CSIRT but in the GCI 2016 version, there are three indicators. The ITU experts have realized that each country's cyber security infrastructure might be different. So there might not be only one CIRT/CERT/CSIRT unit per country but there might be and some countries there are national CIRT/CERT/CSIRT, government CIRT/CERT/CSIRT and even sectoral CIRT/CERT/CSIRT. (ITU, 2015c)

A national CIRT/CERT/CSIRT refers to an entity which has been mandated with the national responsibility to monitor, handle and manage cyber security incidents with its local constituencies including academia, law enforcement, civil society, the private sector, critical information infrastructures and government. A national CIRT/CERT/CSIRT also interacts with national CIRTs of other countries as well as regional and international players for proper and efficient coordination in case of attacks. (ITU, 2015c)

A government CIRT/CERT/CSIRT is an entity that responds to computer security or cyber security incidents which affect solely governmental institutions. Apart from reactive services, a government CIRT/CERT/CSIRT may also engage in proactive services such as vulnerability analysis and security audits. A government CERT provides its services to constituents from the public sector only. (ITU, 2015c)

A sectoral CIRT/CERT/CSIRT is an entity that responds to computer security or cyber security incidents which affect a specific sector or industry. Sectoral CERTs are established for critical sectors such as emergency services, healthcare, public utilities and the financial sector. A sectoral CERT provides its services to constituents from a single sector only. (ITU, 2015c)

[4] A Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), or Computer Security Incident Response Team (CSIRT) is a team of IT security experts whose main business is to respond to computer security incidents.(ENISA, 2006)

The second change in the technical measures category is an entirely new indicator about child online protection. Concerning the legislation related to child online protection it will, in general, be needful to have the body of laws and regulations which make it clear that every and any crime or criminality that can be committed towards a child in the real world can also be committed on any electronic network and the Internet. It may also be necessary to adapt existing ones or develop new laws to outlaw certain types of behavior which can only take place on the Internet. (ITU, 2009)

5.3.3 Organizational measures category

In the organizational measures category in the GCI 2014, there was four and in the GCI 2016 version, there are three indicators. From the GCI 2014 version, the policy and roadmap for governance indicators have come together in the GCI 2016 under the strategy indicator. It is logical because national plans for the protection of information infrastructures or policies on national cyber security strategies are those officially defined and endorsed by a nation state. They can also include the following commitments: establishing clear responsibility for cyber security at all levels of government (local, regional and national or federal), with clearly defined responsibilities and roles. Also, making a clear commitment to cyber security, which is public and transparent; encouraging private sector involvement and partnership in government-led initiatives to promote cyber security. Finally a roadmap for governance that identifies key stakeholders. (ITU, 2015c)

The last indicator in the organizational category from the GCI 2014 has been renamed from national benchmarking to cyber security metrics in the GCI 2016 version.

5.3.4 Capacity building category

In the capacity building measure category, there were four indicators in the GCI 2014 version and the GCI 2016 there are eight indicators. The manpower development, professional certification, and agency certification indicators have been left behind and in the GCI 2016, there are new indicators.

One of the new indicators in the GCI 2016 is cyber security best practices indicator. Best practices are procedures or methods which have a proven track record of success. Adopting

best practices will not only reduce the probability of failure but also increase efficiency. (ITU, 2015c)

The second new indicator in the GCI 2016 version is cyber security research and development programs. For example, cyber security research programs include malware analysis, cryptography research, and research into system vulnerabilities and security models and concepts. Cyber security development programs refer to the development of software or hardware solutions that include for example firewalls, intrusion prevention systems, honey-pots and hardware security modules. The presence of national body will increase sharing of resources and coordination among the various institutions. (ITU, 2015c)

The third new indicator in the GCI 2016 version is public awareness campaigns. Public awareness includes efforts to promote widespread publicity campaigns to reach as many people as possible as well as making use of organizations, institutions and NGOs, ISPs, libraries, local trade organizations, community centers, computer stores, schools, adult education programs and parent-teacher organizations to get the message across about safe cyber-behaviour online. Public awareness also includes actions such as setting up portals and websites to promote awareness, disseminating support material and establishing cyber security adoption. (ITU, 2015c)

The fourth new indicator in the GCI 2016 version is cyber security professional training courses. It is meant that whether the government or some organizations develop, support or provide the development of any professional courses in cyber security. For example the promoting educational courses in the cyber security field. (ITU, 2015c)

The fifth new indicator in the GCI 2016 version is national education programs and academic curricula. It is meant that whether any educational institution provides programs to train the younger and also older generation in cyber security-related professions and skills in schools, colleges, universities and other learning institutes. Cyber security related professions include, for example, cryptoanalysts, digital forensics experts, incident responders, security architects and penetration testers.Cyber security related skills include, for instance, setting strong passwords and not revealing personal information online. (ITU, 2015c)

The sixth new indicator in the GCI 2016 version is incentive mechanisms indicator. It is meant by any incentive efforts by the government to encourage capacity building in the field of cyber security, whether through funding, loans, tax breaks, grants, disposal of

facilities, and other financial and economic motivators. The motivators can include dedicated and nationally recognized institutional body overseeing cyber security capacity building activities. Incentives increase the demand for cyber security related products and services, which improve defenses against cyber threats. Incentives increase the demand for cyber security related goods and services, which improves defenses against cyber threats. (ITU, 2015c)

The last new indicator in the GCI 2016 version is home-grown cyber security industry indicator. A favorable economic, political and social environment supporting cyber security development will incentivize the growth of a private sector around cyber security. This indicator looks at the existence of workforce development, public awareness campaigns, capacity building and government incentives that should drive a market for cyber security services and products. The presence a home-grown cyber security industry will drive the growth of cyber security start-ups and associated cyber-insurance markets. (ITU, 2015c)

5.3.5 Cooperation category

In the cooperation measures category in the GCI 2014 version, there were four indicators: intra-state cooperation, intra-agency cooperation, public-private partnerships and international cooperation. In the GCI 2016 version, there are five indicators: bilateral agreements, multilateral agreements, international fora participation, public-private partnerships and interagency partnerships. So only one indicator is the same, the public-private partnership indicator, and other indicators have changed. (ITU, 2015c)

The first new indicator in the GCI 2016 version is bilateral agreements indicator. The bilateral agreements seem to refer to any officially recognized sector-specific or national partnerships for sharing cyber security assets or information across borders by the government with one other regional entity, a foreign government or an international organization. For example the cooperation or exchange of technology, expertise, information, and other resources). (ITU, 2015c)

The second new indicator in the GCI 2016 version is multilateral agreements indicator. The multilateral agreements seem to refer to any officially recognized national or sector-specific programs for sharing cyber security assets or information across borders by the government with multiple international organizations or foreign governments. For example

the cooperation or exchange of technology, expertise, information, and other resources. (ITU, 2015c)

The third new indicator in the GCI 2016 version is international forums participation indicator. As part of enhancing collaboration in cyber security, the commitment of governments to participate in cyber security events is at this moment measured. Such events include regional and international workshops, training and conferences. (ITU, 2015c)

The fourth new indicator in the GCI 2016 version is interagency partnerships indicator. This performance indicator refers to any official partnerships between the various government agencies within the nation state. The interagency partnerships indicator does not refer to international collaboration. The interagency partnerships can designate partnerships for asset-sharing or information-sharing between departments, ministries, programs and other public sector institutions. (ITU, 2015c)

5.4 Notation.

The main difference in formulas is that in GCI 2014 version the benchmark used will be the score of the hypothetical country that maximizes the overall readiness points, which in GCI 2014 version was thirty-four points. In the GCI 2016 version, it was one hundred points. The resulting composite index will range between zero (worst possible readiness) and one (the benchmark):

GCI 2014 – $CIc = Iqc/34$

GCI 2016 – $CIc = Iqc/100$

Iqc normalized value of individual indicator q for country c.

CIc value of the composite indicator for country c.

(ITU, 2014a)

5.5 Summary about ITU GCI 2014 case study

The Global Cyber security Index 2014 is a research project to rank the cyber security capabilities of nation states. Cyber security has a wide field of application that cuts across many industries and sectors. Each country's level of development is analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation. The Index's goal was to determine how well countries are meeting their obligations in ensuring cyber security. The GCI aims to promote government strategies at a national level, drive implementation efforts across industries and sectors, integrate security into the core of technological progress and foster a global culture of cyber security.

After doing solid research about GCI 2014, everything above mentioned sounds nice, but there are also some other aspects that ITU should take into consideration in future. The GCI 2014 is the first attempt by the ITU to assess the cyber security situation in countries globally.

The current methodology of the GCI 2014 focuses on quantitative indicators rather than quality. In other words, it is measured whether certain documents, organizations and rules of procedure exist or not. The GCI 2014 does not assess the quality, content and impact of the measures. This has led to instances where a country whose formal paperwork is in order has been ranked higher than countries where cyber security measures are applied more efficiently. Therefore, the GCI 2014 does not measure the success of these safeguards and does not assess the effectiveness of the measures nor the level of risk to each country, merely the commitment, and efforts made by the countries in the rated areas of cyber security.

The current objective of the ITU is improving the global cyber security culture rather than providing an actual overview of the cyber security situation in countries. The GCI 2014 index aims to improve the cyber security awareness of decision-makers and draw attention to the need to improve cyber security on a systematic basis. So the purpose of GCI 2014 in the short term was to close security gaps, particularly in developing countries, while in the longer perspective it was to drive the efforts in the adoption of cyber security on a global scale.

In the GCI 2014, the share or the importance of the indicators was not defined. There seems to create an anomaly that in some category a country will get more points because in this category there are more questions to answer. There might be a situation where one country has many documents produced, for example with the help of international consultants, but realistically that country does not have nothing and nothing works. However, that country will get a very high place in the index as its share in that category is very high. The second example might be that having a

legal structure is essential but without an adequate CERT infrastructure or a trained workforce it is difficult to take effective action.

The GCI 2014 shows that the legal aspect of cyber security is the highest priority worldwide. Global concern over data protection and cyber crime mean that the focus on legal measures outranks all other categories. The legislation that member states implement allows them to regulate and monitor standards of behavior regarding cyber security across the board. However, without adequate technical measures and the capabilities to detect and respond to cyber attacks, countries and their respective entities remain vulnerable to cyber threats.

The GCI 2014 does provide a useful tool for identifying the nation's relative cyber security climate and potential risks. Another good finding in the GCI 2014 revealed was that, comparatively, developments were lacking in educating the public on cyber security measures, raising awareness and providing adequate training.

The Global Cybersecurity Index represents a significant step forward not only regarding public-private partnership and international cooperation but also in promoting the importance of cyber security at the global level. The Global Cybersecurity Index can only benefit from increased collaboration and it seems that the GCI 2016 will be much detailed and more adequate.

5.6 Summary of findings

As the author's topic is about an assessment of the cyber security capability of a country, the author has focused more on the first group of indexes.

Table 1. Indexes for assessing countries

	Name	Countries	Research Method*	Ranking	Score	Indicators	Index**
1.1	Cyber Maturity in the Asia-Pacific Region	16	Secondary	-	X	10	X
1.2	Cyber Readiness Index 2.0	125	Primary & Secondary	-	X	7	X
1.3	Cyber Power Index	19	Secondary	X	X	39	X
1.4	Cybersecurity: The Vexed Question of Global Rules	23	Primary	-	X	10	X
1.5	The Cyber Index	114	Secondary	-	-	-	-
1.6	Cybersecurity Policy Making at a Turning Point	10	Primary & Secondary	-	-	10	-
1.7	Global Cybersecurity Index	193	Primary & Secondary	X	X	24	X
1.8	EU Cybersecurity Dashboard	28	Secondary	-	-	25	X
1.9	National Cyber Security Index	n/a	Primary & Secondary	X	X	12	X

* Primary research method – model is based on a survey and/or a questionnaire, filled out by the volunteer countries. Secondary research method – model is based on open source and publicly available information. (Johnson, Onwuegbuzie, & Turner, 2007)

** As the model has indicators, a ranking, and/or scoring mechanisms it is classed as an index.

In Figure 1. all the indexes for assessing countries are listed. There is no specific order for listing. The newest assessment model in that list is National Cyber Security Index that is going to be launched May 31, 2016.

In that list, it is possible to distinguish two groups of indexes based on the number of countries. One group is up to one hundred countries, and the other group is from one hundred to one hundred and ninety-three countries. In future research, it might be interesting to compare these two groups. It is also possible to compare indexes based on region. For example indexes about European countries versus Asia-Pacific region or the World.

From that comparison, we can see that there are three research methods available: primary research, secondary research and primary-secondary research together. If a country would have to choose between indexes based on research method then using primary-secondary research together would be the best choice. If that is not possible then indexes with only primary research and then indexes with only secondary research method. However, there is a need to be aware that primary

research usually costs more and takes longer. On the other hand, there is also negative side on the secondary research, i.e. the data can be too old and/or not specific enough for country's needs.

If there would be a question that how should "perfect" methodology then look like. The author will bring out some outlines to consider.

The "perfect" assessment methodology should be compatible with practical problems. It should help the countries to increase the level of cyber security in their information society. If a methodology will only assess the indicator of the documentation the country has produced but does not evaluate has there been any effect after the document has been produced then there is no point to follow that assessment model.

Secondly, the "perfect" assessment model should give a very realistic evaluation. How big is the country's will to implement to a specific area, it is impossible to measure. However, as much as possible, then the index should evaluate does the capacity realistically exists. So in the index should have following questions: does a country have enough staff to fulfill the objectives; does the country have the people in place, does the country have sufficient resources which are needed for certain functions.

Thirdly, the "perfect" index should be a tool for developing the capability. The country can have simply see the "check-list," what has been done, what needs to be done and follow it. This tool would give the state a complete picture of what they should do at the national level.

Fourthly, the "perfect" index should provide the possibility to see the evidence about the facts that is presented for the country. The country should see links to documents and websites of some of the solutions. So the "perfect" index should be transparent and evidence-based. The evidence should not be confidential but available from public sources.

Of course, the "perfect" index could be a "living index", i.e. the index should not be publicized after every two years in a pdf document format, but it would be a "live" environment, constantly evolving.

Concerning the methodology structure, the author believes that it must be clear what is the starting point. So, the cyber security assessment model should be constructed in such way that the cyber security index is going to contribute to real cyber security needs. Thus, to build such index, the starting point should be the cyber threat scenarios. It is typical in the security planning process – the country understands what the risks are, and then will come to the correct measures. After that, the state can evaluate the importance of these measures.

The author believes that the “perfect” cyber security assessment models categories should be: implemented technologies; established institutions, regulations in force, knowledge development and international cooperation. These categories are very similar to the ones used in the Global Cybersecurity Index. Which are taken from Global Cybersecurity Agenda, that was launched in 2008. One peculiar thing is that similar categories are also mentioned in the Estonian Cyber Security Strategy (MKM, 2007) that was launched in 2007, after the series of cyber attacks on Estonia in spring 2007.(Ottis, 2008)

If a country should have to choose which index to take part and follow then the authors suggestion would be all of them. The main reason is that all listed indexes are different and therefore give a better understanding of country's situation in the cyber security field. If it is not possible to take part all of the indexes, then the author recommends choosing index(es) with ranking. It gives a country possibility to compare their country to others.

6. Conclusion

A secure e-government of a country with strategic e-services cannot exist without effective cyber security. The fast growth of ICT systems and networks has created new and undiscovered opportunities for cyber criminals to take advantage of online vulnerabilities and attack countries' critical infrastructure. Individuals, companies, and governments are increasingly reliant on the information stored and transmitted over advanced communication networks. Most importantly, cyberspace is borderless: cyber-attacks can inflict immeasurable damage in different countries in a matter of minutes.

Unfortunately, cyber security is not yet at the core of many national technology strategies. We cannot say that the cyber security efforts are non-existent but sometimes they are eclectic and dispersed.

The main research questions is: How to assess the cyber security capability of a country?

Following sub-questions help to determine the framework for assessment of cyber security capabilities:

- What methodologies are available to assess a country's cyber security capability?
- What are the categories a country needs to fulfill to assess its cyber security capability?

To answer the main research question, how to assess the cyber security capability of a country, the author gathered backround information and found out that for assessing the cyber security capability of a country, there are assessment models available. During this research, the author has found seventeen cyber security assessment methods. Nine of these methods assess the countries. After analyzing and comparing those nine assessment methods, the author has come to the conclusion that it is not possible to say that one specific model is better than others. The author would recommend using a combination of those models. Every assessment model measures different categories and is using different indicators. Therefore, the models are not easily comparable.

If a country has the possibility to fulfill all these models, it will be a greater benefit for the country. If a country does not have that possibility, then the author would recommend using models where there is also ranking part included. This gives the country an easily understandable check-list which shows where the country situates concerning cyber security capability and shows also

ranking comparing with other countries. From those country profiles, the country might easily find something new in the field of cyber security that the country might want to follow in future. Alternatively, to find advantages and disadvantages of the country's cyber security system. Secondly, comparison with other countries gives the country an opportunity to identify and correct cyber security loopholes. Thirdly, the country can compare cyber security by different categories with other countries. Fourthly, the country can discover cyber security categories the country did not know about before.

So how should a country assess the cyber security capability? The first step toward to answer this question lies in comparing the cyber security capabilities of nation states and publishing an efficient ranking of their status. A ranking system motivates states to intensify their efforts and reveals shortcomings in cyber security. The real value of a nation's cyber security capability can truly be weighed only through comparison with others.

To answer the first sub-question, what methodologies are available to assess a country's cyber security capability, the author has found nine cyber security assessment methods. The author analyzed all nine assessment methods and the author has come to the conclusion that it is not possible to say that one specific model is better than others.

To answer the second subquestion, what are the categories a country needs to fulfill to assess its cyber security capability, the author found out that with every assessment model measures different categories and is using different indicators. But the author has found out the five most important categories should be: implemented technologies; established institutions, regulations in force, knowledge development and international cooperation. The author has analysed them in previous chapter.

Future work

The author believes that there are likely to be much more ongoing research projects in cyber security assessment field in near future.

With many indexes and indicators, it is possible to go deeper and therefore the author believes that there might emerge so-called sub-indexes. For example, there might be an index in the future only where there are separately assesses only the legislation and regulations part. The smaller sub-index evaluates only what the legal regulations include.

It is possible that in the near future some of the indexes and assessment models will join. There might be that one organization has the resources, and another organization has the needed amount of specialists with knowledge.

References

Ansip, A. (2015). Why we need a Digital Single Market. European Commission. Retrieved from http://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf

ASPI. (2014). Cyber Maturity in the Asia-Pacific Region 2014. ASPI. Retrieved from https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf

ASPI. (2015). Cyber Maturity in the Asia-Pacific Region 2015. ASPI. Retrieved from https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf

Booz Allen Hamilton. (2011). Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity. Booz Allen Hamilton Inc.

BSA. (2015). EU Cybersecurity Dashboard. BSA, The Software Alliance. Retrieved from http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

Chen, Y.-S., Chong, P. P., & Zhang, B. (2004). Cyber security management and e-government. *Electronic Government, an International Journal*, *1*(3), 316–327. http://doi.org/10.1504/EG.2004.005555

Economist Intelligence Unit. (2011). Cyber Power Index: Findings and Methodology. Booz Allen Hamilton Inc. Retrieved from http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

ENISA. (2006). CSIRT Setting up Guide. ENISA. Retrieved from https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport

GCSCC. (2014). Cybersecurity Capability Maturity Model. The Global Cyber Security Capacity Centre (GCSCC). Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

Geer Jr, D. E., & Pareek, M. (2012). Index of Cyber Security. *Security & Privacy, IEEE, 10(3)*, 93–95.

Geers, K. (2011). *Strategic Cyber Security*. Kenneth Geers.

Grauman, B. (2012). Cyber-security: The vexed question of global rules. Security and Defense Agenda and McAfee. Retrieved from http://www.friendsofeurope.org/media/uploads/2015/06/SDA-Cyber-report-FINAL.pdf

Grönlund, Å. (2005). State of the Art in E-Gov Research: Surveying Conference Publications. *International Journal of Electronic Government Research*, *1*(4), 1–25. http://doi.org/10.4018/jegr.2005100101

Hathaway, M. (2013). Cyber Readiness Index 1.0. Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from http://belfercenter.hks.harvard.edu/publication/23607/cyber_readiness_index_10.html?breadcrumb=%2Fexperts%2F2132%2Fmelissa_hathaway

Hathaway, M. (2015). Cyber Readiness Index 2.0. Potomac Institute for Policy Studies. Retrieved from http://www.potomacinstitute.org/images/CRIndex2.0.pdf

HLEG. (2008). Report of the Chairman of High-Level Experts Group. High-Level Experts Group. Retrieved from http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

IBM X-Force Research. (2015). Cyber Security Intelligence Index. IBM Corporation. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

ITU. (2007). Global Cybersecurity Agenda (GCA). International Telecommunication Union. Retrieved from http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

ITU. (2009). Guidelines for Policy Makers on Child Online Protection. ITU. Retrieved from https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

ITU. (2013). Global Cybersecurity Index 2014 - Questionnaire. ITU. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Country_Questionnaire.docx

ITU. (2014a). Global Cybersecurity Index 2014. International Telecommunication Union. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

ITU. (2014b). ITU-D Study Group 2 Question 3/2: Securing information and communication networks: Best practices for developing a culture of cybersecurity. ITU. Retrieved from http://www.itu.int/net4/ITU-D/CDS/sg/doc/rgq/2014/D14-SG02-RGQ03.2-en.pdf

ITU. (2014c). Resolution 130 (Rev. Busan, 2014) - Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. The Plenipotentiary Conference of the International Telecommunication Union. Retrieved from https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf

ITU. (2015a). Cybersecurity Index of Indices. ITU. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdf

ITU. (2015b). Global Cybersecurity Index 2015/16 - Questionnaire Guide. ITU. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

ITU. (2015c). Global Cybersecurity Index 2015/2016 - Reference Model. ITU. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Reference%20Model_GCI-2016.pdf

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). *Toward a Definition of Mixed Methods Research* (Vol. 1). Journal of Mixed Methods Research.

Kruse II, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials*. Pearson Education.

Lorents, P., Ottis, R., & Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence. In N. Aykin (Ed.), *Internationalization, Design and Global Development* (pp. 180–186).

Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-02767-3_20

McKinsey & Company. (2014). Risk and responsibility in a hyperconnected world. World Economic Forum and McKinsey & Company. Retrieved from http://www.mckinsey.com/business-functions/business-technology/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises

MKM. (2007). Cyber Security Strategy 2008-2013 (Küberjulgeoleku strateegia 2008-2013). Ministry of Economic Affairs and Communications of Estonia. Retrieved from https://valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

OECD. (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD. Retrieved from https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ottis, R. (2008). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*. In Proceedings of the 7th European Conference on Information Warfare.

PwC & Iron Mountain. (2012). Beyond Cyber Threats: Europe's First Information Risk Maturity Index. PricewaterhouseCoopers LLP. Retrieved from http://www.continuitycentral.com/BeyondCyberThreats.pdf

Rikk, R. (2016). Interview with Mr. Raul Rikk from e-Governance Academy Foundation about development of National Cyber Security Index.

Scholl, H. J. (2013). Electronic Government Research: Topical Directions and Preferences. In M. A. Wimmer, M. Janssen, & H. J. Scholl (Eds.), *Electronic Government* (pp. 1–13). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-40358-3_1

UNIDIR. (2013). The Cyber Index: International Security Trends and Realities. United Nations Institute for Disarmament Research (UNIDIR). Retrieved from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Wimmer, M., Traunmuller, R., & Lenk, K. (2001). Electronic business invading the public sector: considerations on change and design. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001* (p. 10 pp.–). http://doi.org/10.1109/HICSS.2001.926520

Yin, R. K. (2014). *Case Study Research: Design and Methods* (Fifth edition). SAGE Publications, Inc.

Zhao, H. (2015, December 7). Meeting with ITU Secretary-General, Mr. Houlin Zhao in e-Estonia Showroom.

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49–56. http://doi.org/10.1016/j.giq.2009.07.004

Appendix 1 – Global Cybersecurity Index 2014 Questionnaire

The Global Cybersecurity Index (GCI) project aims effectively to measure each nation state's level of cyber security development. The definitive goal is to help foster a global culture of cyber security and its integration at the essence of information and communication technologies (ICT). The GCI project is based on the current mandate of the International Telecommunication Union (ITU) and the related activities and projects of the ITU's Telecommunication Development Bureau, the BDT. (ITU, 2013)

The ITU is the lead facilitator for World Summit on the Information Society (WSIS) Action Line C5 for assisting stakeholders in building security and confidence in the use of ICTs at regional, national and international levels. In this framework, the Global Cybersecurity Agenda (GCA) was launched by the ITU Secretary-General as ITU's framework for international multi-stakeholder cooperation towards a secure and safer information society and focuses on the following five work areas: Legal Measures, Technical, and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. These five pillars will form the basis of the indicators for the GCI.

The GCI project will be a joint effort between the BDT, specifically the Cybersecurity and ICT Applications Division (CYB) and ABI Research.

You are kindly invited to participate in a benchmarking exercise aimed at assessing the current situation of your Country against the Global Cybersecurity Index (GCI).

Your responses to this questionnaire are much appreciated. The ITU will prepare a compilation and comparative overview of responses to the benchmarking exercise once completed.

1. Legal Measures

A. Is there any criminal legislation regarding cyber activities? If so, please specify.
   Include URL, the title of laws/acts/articles, and/or wording.

B. Is there any regulation regarding cyber security and compliance requirements? If so, please specify.
   Include URL, the title of laws/acts/articles, and/or wording.

2. Technical and Procedural Measures

A. Is there one (or more) officially approved national or sector-specific CERT, CIRT or CSIRT team(s)? If so, please specify the names and number and whether they are legally mandated or not.

   Include URL, official name, and contact details.

B. Is there any officially-approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards? If so, please specify.

   Include URL, the official name of framework, responsible agency (and contact details) and a short description.

C. Is there any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of state agencies and public sector professionals? If so, please specify.

   Include URL, official name of framework, responsible agency (and contact details) and short description

3. Organizational Structures

A. Is there any officially recognized national or sector-specific cybersecurity strategy and/or policy? If so, please specify.

   Include URL, the official name of strategy/policy, responsible agency (and contact details) and a short description.

B. Is there any officially recognized national or sector-specific governance roadmap for cyber security? If so, please specify.

   Include URL, the official name of roadmap, responsible agency (and contact details) and a short description.

C. Is there any officially recognized national or sector-specific agency responsible for implementing a national cyber security strategy/policy/roadmap? If so, please specify.

   Include URL, the official name of responsible agency (and contact details) and a short description of responsibilities.

D. Is there any officially recognized political or sector-specific benchmarking exercises or referential used to measure cybersecurity development? If so, please specify.

   Include URL, the official name of benchmarking exercise, responsible agency (and contact details) and a short description.

4. Capacity Building

A. Is there any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector? If so, please specify.
   Include URL, official name(s) of programs/projects/best practices/guidelines, responsible agency(ies) (and contact details) and short description.
B. Is there any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector? If so, please specify.
   Include URL, official name(s) of programs/projects, responsible agency(ies) (and contact details) and short description.
C. Are there any public sector professionals certified under internationally recognized certification programs in cyber security? If so, please specify the number.
   Include type of certification and certificating agency.
D. Are there any certified government and public sector organizations certified under internationally recognized standards in cyber security? If so, please specify the number.
   Include type of certification and certificating agency.

5. International Cooperation

A. Are there any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states? If so, please specify.
   Include URL, the official name of partnership, responsible national agency (and contact details), participating countries, and a short description.
B. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector? If so, please specify.
   Include URL, the official name of program, responsible agency (and contact details), participating organizations, and a short description.
C. Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector? If so, please specify.
   Include URL, the official name of program, responsible national agency (and contact details), participating organizations, and a short description.
D. Are there any officially recognized participation in regional and/or international cyber security platforms and forums? If so, please specify.

Include URL, the official name of platform/forum, responsible national agency (and contact details), participating countries, and a short description.

(ITU, 2013)

Appendix 2 - Global Cybersecurity Index 2016 Questionnaire

The Global Cybersecurity Index (GCI) measures the commitment of countries to cyber security in the five pillars of the Global Cybersecurity Agenda: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation.

This questionnaire has merged questions adjusted for establishing the GCI 2016 score together with those required by ITU-D Study Group 2 Question 3 (see Annex 2). The questionnaire is composed of three separate sections, where questions in the first two sections have yes/no responses while the questions in the final section are open ended. The Global Cybersecurity Index questionnaire should be completed online. Every respondent will be provided (via an official email from ITU) a unique URL for his/her safe keeping. The online questionnaire allows the respondents to upload relevant documents (and URLs) for each question as supporting information.

The information being provided by respondents to this questionnaire is not expected to be of confidential nature.

SECTION 1

1 Is there any Cyber related legislation?

1.1 Is there any cyber criminal law?

1.1.1 Is there any substantive cybercriminal law?

1.1.1.1 Are there any articles on the unauthorized access of data, systems and computers?

1.1.1.2 Are there any articles on the unauthorized modification/interference of computers, systems and data?

1.1.1.3 Are there any articles on the unauthorized interception of data, systems and computers?

1.1.2 Is there any procedural cybercriminal law?

1.1.2.1 Are there any articles on the expedited preservation of stored computer data?

1.1.2.2 Are there any articles on production orders?

1.1.2.3 Are there any articles concerning search and seizure of stored computer data?

1.1.2.4 Are there any articles concerning the real-time collection of computer data?

1.1.2.5 Are there any articles related to extradition of cyber perpetrators?

1.1.2.6 Are there any articles relating to mutual assistance?

1.1.2.7 Are there any articles related to confidentiality and limitation of use?

1.1.3 Is there any case law on cybercrime or computer misuse?

1.2 Is there any cybersecurity legislation or regulation?

1.2.1 Is there any data protection regulation or legislation?

1.2.2 Is there any system and network protection legislation or regulation?

1.2.3 Is there any breach notification regulation or legislation?

1.2.3.1 For data?

1.2.3.2 For systems and networks?

1.2.4 Is there any cyber security certification/standardization legislation or regulation?

1.2.4.1 For public sector?

1.2.4.2 For private sector?

1.2.5 Does the regulation or legislation impose the implementation of cyber security measures?

1.2.5.1 On the public sector?

1.2.5.2 On the critical infrastructure operators?

1.2.5.3 On the private sector?

1.2.6 Does the legislation or regulation impose cyber security audits?

1.2.6.1 On the public sector?

1.2.6.2 On the critical infrastructure operators?

1.2.6.3 On the private sector?

1.2.7 Is there a regulation or legislation detailing the protection of privacy?

1.2.8 Is there a legislation or regulation related to digital signatures and e-transactions?

1.2.9 Is there a regulation or legislation related to the liability and responsibility of Internet Service Providers?

1.2.10 Is there a regulation or legislation related to the containment or curbing of spam?

1.3 Is there any cybersecurity training for law enforcement officers, judicial and other legal actors?

1.3.1 For law enforcement (enforcement agents and police officers)?

1.3.2 For judicial and other legal actors (judges, solicitors, barristers, attorneys, lawyers, paralegals, etc.)?

1.3.3 Is the training recurring?

2 Do you have any technical measures?

2.1 Is there a CERT, CIRT or CSIRT with national responsibility?

2.1.1 Does it have a government mandate?

2.1.2 Does the CERT, CIRT or CSIRT conduct recurring cyber security exercises?

2.1.3 Is the CERT, CIRT or CSIRT affiliated with FIRST?

2.1.4 Is the CERT, CIRT or CSIRT affiliated with any other CERT communities?

2.2 Is there a Government CERT?

2.3 Are there any sectoral CERTs?

2.4 Is there any framework for the implementation of cyber security standards?

2.4.1 In the public sector?

2.4.2 In the private sector?

2.5 Is there a framework for the certification and accreditation of cyber security professionals?

2.5.1 In the public sector?

2.5.2 In the public sector?

2.6 Are there any capabilities and technical mechanisms deployed to address spam?

2.7 Are there certain tools and technical measures related to providing cyber security, such as anti-spam software and/or anti-virus software, available to the persons with disabilities?

3 Do you have any organizational measures?

3.1 Is there a national strategy for cyber security?

3.1.1 Is your national strategy standalone?

3.1.1.1 Does it address the private sector?

3.1.1.2 Does it address the public sector?

3.1.1.3 Is there a section on the protection of critical information infrastructure?

3.1.1.4 Is there a roadmap for governance?

3.1.1.5 Is the strategy revised on a recurring basis?

3.1.1.6 Is the strategy open to public consultation?

3.1.1.7 Does the strategy include a national resiliency plan?

3.1.2 Is your national cyber security strategy included as part of another broader national strategy?

3.1.2.1 Is there a section on the protection of critical information infrastructure?

3.1.2.2 Is there a roadmap for governance of the cyber security section?

3.1.3 Does it define priorities for the public sector?

3.1.4 If there is not a cyber security strategy in place, is one currently in development?

3.1.5 Does the existing strategy or the one in development, include actions about persons with disabilities?

3.2 Is there a national agency/national body responsible for cyber security?

3.2.1 Is there an agency responsible for critical information infrastructure protection?

3.2.2 Is there a national agency/national body acting as focal point for Spam related issues?

3.3 Are there any metrics used to measure cyber security development at a national level?

3.3.1 Are cyber security risk assessments performed periodically?

3.3.1.1 Is there a cyber security benchmark for assessing risk?

3.3.1.2 Are the results rated or evaluated for future improvements?

3.3.2 Are recurring cyber security audits performed?

3.3.2.1 Are they mandatory?

4 Do you have any capacity building activities?

4.1 Is there a standardization body within the country?

4.1.1 Does it develop its cyber security standards?

4.1.2 Does it adopt existing international cyber security standards?

4.2 Is national or sectoral cyber security best practices collected or guidelines created?

4.3 Is there investment in cyber security research & development programs?

4.3.1 In the public sector?

4.3.2 In higher education institutions?

4.3.3 Is there a nationally recognized institutional agency/body overseeing cyber security R&D activity?

4.4 Are public awareness campaigns in cyber security developed and implemented?

4.4.1 For organizations?

4.4.2 For civil society?

4.4.2.1 For adults (>18 yrs)?

4.4.2.2 For youth (12-17 yrs)?

4.4.2.3 For children (<12yrs)?

4.4.3 As a part of public awareness campaigns, is the public informed about the benefits of using cyber security software, hardware or service-based solutions?

4.4.4 Are any such cyber security software, hardware or service-based solutions made available to the public?

4.5 Does your organization/government develop or support the development of any professional training courses in cyber security?

4.5.1 For organizations?

4.5.2 For the public sector?

4.5.3 For civil society?

4.6 Does your organization/government develop or support the development of any educational programs or academic curricula in cyber security?

4.6.1 In primary school?

4.6.2 In secondary school?

4.6.3 In higher education?

4.7 Are there any government incentive mechanisms to encourage capacity building in the field of cyber security?

4.7.1 Is there a nationally recognized institutional body overseeing cyber security capacity building activities?

4.8 Is there a homegrown cyber security industry?

4.8.1 Is there a cyber-insurance market?

4.8.2 Are there any incentives provided for the development of a cyber security industry?

4.8.2.1 Is there any support provided to cyber security startups?

5 Do you have any cooperative measures?

5.1 Are there any bilateral agreements for cyber security cooperation?

5.1.1 With nation states?

5.1.1.1 Is the agreement legally binding?

5.1.1.1.1 For information sharing?

5.1.1.1.2 For asset sharing?

5.1.1.2 Is the agreement informal, non-legally binding or pending ratification?

5.1.1.2.1 For information sharing?

5.1.1.2.2 For asset sharing?

5.1.2 With international organizations?

5.1.2.1 Is the agreement legally binding?

5.1.2.1.1 For information sharing?

5.1.2.1.2 For asset sharing?

5.1.2.2 Is the agreement informal, non-legally binding or pending ratification?

5.1.2.2.1 For information sharing?

5.1.2.2.2 For asset sharing?

5.2 Are there any multilateral or international agreements on cyber security cooperation?

5.2.1 Is the agreement legally binding?

5.2.1.1 For information sharing?

5.2.1.2 For asset sharing?

5.2.2 Is the agreement informal, non-legally binding or pending ratification?

5.2.2.1 For information sharing?

5.2.2.2 For asset sharing?

5.3 Does your organization/government participate international fora/associations dealing with cyber security?

5.4 Are there any public-private partnerships in place?

5.4.1 With local companies?

5.4.1.1 For information sharing?

5.4.1.2 For asset sharing?

5.4.2 With foreign companies?

5.4.2.1 For information sharing?

5.4.2.2 For asset sharing?

5.5 Are there any interagency partnerships in place?

5.5.1 For information sharing?

5.5.2 For asset sharing?

SECTION 2

1 Do you have measures for protecting Children Online?

1.1 Is there legislation related to child online protection?

1.2 Is there an entity/agency responsible for Child Online Protection?

1.2.1 Is there an established public mechanism for reporting issues associated with child online protection?

1.2.2 Are there any technical capabilities and mechanisms deployed to help protect children online?

1.2.3 Has there been any activity by the government or non-government institutions to provide support and knowledge to stakeholders on how to protect children online?

1.2.4 Is there any child online protection education programs?

1.2.4.1 For educators?

1.2.4.2 For parents?

1.2.4.3 For children?

1.3 Is there a national strategy for child online protection?

1.4 Are there public awareness campaigns on child online protection?

1.4.1 For adults (>18 yrs)?

1.4.2 For youth (12-17 yrs)?

1.4.3 For children (<12yrs)?

SECTION 3

Addendum: opinion based survey

1 In your opinion, how important is raising awareness on cyber security as a basic step to achieving security in cyberspace?

a) Not important
b) Somewhat important
c) Important
d) Very Important

2. Which groups are targeted by cyber security awareness campaigns in your country?

a) Children
b) Youth
c) Students
d) Elderly people
e) Persons with disabilities
f) Private institutions
g) Government agencies
h) Others

3. Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 for the highly targeted to the less targeted?

a) Children
b) Youth
c) Students
d) Elderly people
e) Persons with disabilities
f) Private institutions
g) Government agencies
h) Others

4. What are the cyber security issues that are addressed by existing awareness campaigns? (Replies to more than one item possible)

a) Internet safety
b) Privacy
c) Fraud
d) Phishing
e) Malware
f) Child Online Protection
g) Others

5. What is the degree of importance of each issue? Please arrange in order of the most important to the less important and give reasons for such order?
    a) Internet safety
    b) Privacy
    c) Fraud
    d) Phishing
    e) Malware
    f) Child Online Protection
    g) Others

6. Have you been collaborating with or receiving assistance from ITU in cyber security?
    a) If yes, please give details and your opinion on the effectiveness of this assistance/collaboration and tell us how us any specific cyber security areas to be looked into.
    b) If no, please inform us why and tell us how we can assist?

(ITU, 2015b)

Appendix 3 - ITU-D Study Group 2 Question 3/2

Securing information and communication networks:

Best practices for developing a culture of cyber security

1. Statement of the situation or problem

Securing information and communication networks and developing a culture of cyber security have become key in today's world for a number of reasons, including:

a) the explosive growth in the deployment and use of information and communication technology (ICT);
b) cyber security remains a concern of all and there is thus a need to assist countries, in particular developing countries, to protect their telecommunication/ICT networks against cyber attacks and threats;
c) the need to endeavor to ensure the security of these globally interconnected infrastructures if the potential of the information society is to be achieved;
d) the growing recognition at the national, regional and international levels of the need to develop and promote best practices, standards, technical guidelines and procedures to reduce vulnerabilities of and threats to ICT networks;
e) the need for national action and regional and international cooperation to build a global culture of cyber security that includes national coordination, appropriate national legal infrastructures, and watch, warning and recovery capabilities, government/industry partnerships, and outreach to civil society and consumers;
f) the requirement for a multistakeholder approach to effectively make use of the variety of tools available to build confidence in the use of ICT networks;
g) United Nations General Assembly (UNGA) Resolution 57/239, on creation of a global culture of cyber security, invites the Member States "to develop throughout their societies a culture of cyber security in the application and use of information technology";
h) UNGA Resolution 68/167, on the right to privacy in the digital age, affirms, among other things, "that the same rights that people have offline must also be protected online, including the right to privacy";
i) best practices in cyber security must protect and respect the rights of privacy and freedom of expression as outlined in the relevant parts of the Universal Declaration of Human

Rights, the Geneva Declaration of Principles adopted by the World Summit on the Information Society (WSIS) and other relevant international human rights instruments;

j) the Geneva Declaration of Principles indicates that "A global culture of cyber security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies", the Geneva Plan of Action encourages sharing best practices and taking appropriate action on spam at national and international levels, and the Tunis Agenda for the Information Society reaffirms the necessity for a global culture of cyber security, particularly under Action Line C5 (Building confidence and security in the use of ICTs);

k) ITU was requested by WSIS (Tunis, 2005), in its agenda for the implementation and follow-up, to be the lead facilitator/moderator for Action Line C5 (Building confidence and security in the use of ICTs), and ITU-T, ITU-R, ITU-D and the General Secretariat, based on such responsibility and in response to relevant resolutions adopted by the World Telecommunication Development Conference (WTDC) (Doha, 2006 and Hyderabad, 2010), by the Plenipotentiary Conference (Antalya, 2006 and Guadalajara, 2010), as well as by the World Telecommunication Standardization Assembly (Johannesburg, 2008 and Dubai, 2012), have carried out many studies in order to improve cyber security;

l) WSIS outputs(both phases: Geneva, 2003 and Tunis, 2005) called for building confidence and security in the use of ICTs;

m) WTDC Resolution 45 (Rev. Dubai, 2014) supported the enhancement of cyber security among interested Member States;

n) consistent with its mandate, ITU-D should play a role in bringing together Member States, Sector Members, and other experts to share experiences and expertise for securing ICT networks;

o) the results of Question 22-1/1 in the past study period, which include numerous reports, and contributions from across the globe;

p) there have been various efforts to facilitate the improvement of network security, including the work of the Member States and Sector Members in standards-setting activities in ITU-T and the development of best-practice reports in ITU-D; by the ITU secretariat in the Global Cybersecurity Agenda (GCA); and by ITU-D in its capacity-building activities in the relevant programme; and, in certain cases, by experts across the globe;

q) governments, service providers and end-users, particularly in the least developed countries (LDCs), face unique challenges in developing security policies and approaches appropriate to their circumstances;

r) The Member States and infrastructure operators would benefit from additional reports detailing the various resources, strategies and tools available to build confidence in the use of ICT networks and the role of international cooperation in this regard;

s) spam continues to be a serious concern;

t) evolving methodologies on common testing criteria for telecommunication networks;

u) the need for simplified test procedures at a basic level for security testing of telecommunication networks to promote a security culture.

2. Question or issues for study

a) Discuss approaches and best practices for evaluating the impact of spam within a network, and provide the necessary measures, including mitigation techniques, that developing countries can use, taking into account existing standards and available tools.

b) Provide information on current cyber security challenges that service providers, regulatory agencies, and other relevant parties are facing.

c) Continue to gather national experiences from the Member States relating to cyber security, and to identify and examine common themes within those experiences.

d) Continue to analyze results of the cyber security awareness survey carried out in the last study period, and issue an updated survey so as to measure progress over time.

e) Provide a compendium of relevant, ongoing cyber security activities being conducted by the Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above.

f) Examine specific needs of persons with disabilities, in coordination with other relevant Questions.

g) Examine ways and means to assist developing countries, with the focus on LDCs, regarding cyber security-related challenges.

h) Continue to gather national experiences and national requirements in the area of child online protection, in coordination with other relevant activities.

i) Hold ad hoc sessions, seminars, and workshops to share knowledge, information and best practices concerning effective, efficient and useful measures and activities to enhance cyber security, using outcomes of the study, to be collocated as far as possible with meetings of Study Group 1 or of the rapporteur group for the Question.

j) Gather national experience and requirements on common criteria and security testing that would facilitate the development of a framework and guidelines that could speed up the

security testing of telecommunication equipment, in collaboration with the relevant ITU-T study groups and other standards-developing organizations (SDOs), as appropriate, and taking into account available information and material in these entities.

3. Expected output

a) Reports to the membership on the issues identified in § two a) to j) above. The reports in question will reflect that secure information and communication networks are integral to the building of the information society and the economic and social development of all nations. Cyber security challenges include potential unauthorized access to, destruction of and modification of information transmitted on ICT networks, as well as countering and combating spam. However, the consequences of such challenges can be mitigated by increasing awareness of cyber security issues, establishing effective public-private partnerships and sharing successful best practices employed by policy-makers and businesses, and through collaborating with other stakeholders. Also, a culture of cyber security can promote trust and confidence in these networks, stimulate secure usage, ensure the protection of data and privacy while enhancing access and trade, and enable nations to better achieve the economic and social development benefits of the information society.

b) Educational materials for use in workshops, seminars, etc.

c) Accumulation of knowledge, information and best practices on effective, efficient and useful measures and activities to enhance cyber security in developing countries resulting from ad hoc sessions, seminars, and workshops.

4. Timing

This study is proposed to last four years, with preliminary status reports to be delivered on progress made after 12, 24 and 36 months.

5. Proposers/sponsors

ITU-D Study Group 1; Arab States; Inter-American proposal; Japan; Islamic Republic of Iran.

6. Sources of input

a) The Member States and Sector Members;

b) Relevant ITU-T and ITU-R study group work;

c) Relevant outputs of international and regional organizations;

d) Relevant non-governmental organizations concerned with the promotion of cyber security and a culture of security;
e) Surveys, online resources;
f) Experts in the field of cyber security;
g) Other sources, as appropriate.

7. Target audience

Target audience	Developed countries	Developing countries[5]
Telecom policy-makers	Yes	Yes
Telecom regulators	Yes	Yes
Service providers/operators	Yes	Yes
Manufacturers	Yes	Yes

a) Target audience

National policy-makers and Sector Members, and other stakeholders involved in or responsible for cyber security activities, especially those from developing countries.

b) Proposed methods for implementation of the results

The study program focuses on gathering information and best practices. It is intended to be informative in nature and can be used to raise awareness for the Member States and Sector Members of the issues of cyber security and to draw attention to the information, tools and best practices available, the results of which may be used in conjunction with BDT-organized ad hoc sessions, seminars, and workshops.

8. Proposed methods of handling the Question or issue

The Question will be addressed within a study group over a four-year study period (with the submission of interim results), and will be managed by a rapporteur and vice-rapporteurs. This will enable the Member States and Sector Members to contribute their experiences and lessons learned on cyber security.

[5] These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. (ITU, 2014b)

9. Coordination

Coordination with ITU-T, in particular, Study Group 17 or its successor, ITU-D Question 7/1 on persons with disabilities, as well as other relevant organizations, including FIRST, IMPACT, APCERT, OAS CICTE, OECD, RIRs, NOGs, M3AAWG, and others. Given the existing level of technical expertise on the issue in these groups, all documents (questionnaires, interim reports, draft final reports, etc.) should be sent to them for comment and input before being submitted to the full ITU-D study group for comment and approval.

10. BDT program link

The BDT program under Output 3.1 of Objective 3 shall facilitate the exchange of information and make use of the output, as appropriate, to satisfy program goals and the needs of Member States.

(ITU, 2014b)

Appendix 4 - List of GCI 2014 indicators

Nr	Indicator	Points
1.	**Legal measures**	
A.	Criminal Legislation	
B.	Regulation & Compliance	
2.	**Technical measures**	
A.	CERT/CIRT/CSIRT	
B.	Standards	
C.	Certification	
3.	**Organizational measures**	
A.	Policy	
B.	Roadmap for Governance	
C.	Responsible agency	
D.	National Benchmarking	
4.	**Capacity building**	
A.	Standardization Development	
B.	Manpower Development	
C.	Professional Certification	
D.	Agency Certification	
5.	**Cooperation**	
A.	Intra-state Cooperation	
B.	Intra-agency Cooperation	
C.	Public-Private Partnerships	
D.	International Cooperation	
	Total	**34**

(ITU, 2014a)

Appendix 5 - List of GCI 2016 indicators

Nr	Indicator	Points
1.	**Legal measures**	
1.1	Cyber criminal legislation	
1.2	Cyber security regulation	
1.3	Cyber security training	
2.	**Technical measures**	
2.1	National CERT/CIRT/CSIRT	
2.2	Government CERT/CIRT/CSIRT	
2.3	Sectoral CERT/CIRT/CSIRT	
2.4	Cyber security standards implementation framework for organizations	
2.5	Cyber security standards and certification for professionals	
2.6	Child online protection	
3.	**Organizational measures**	
3.1	Strategy	
3.2	Responsible agency	
3.3	Cybersecurity metrics	
4.	**Capacity building**	
4.1	Standardization bodies	
4.2	Cyber security best practices	
4.3	Cyber security research and development programs	
4.4	Public awareness campaigns	
4.5	Cyber security professional training courses	
4.6	National education programmes and academic curricula	
4.7	Incentive mechanisms	
4.8	Home-grown cyber security industry	
5.	**Cooperation**	
5.1	Bilateral agreements	
5.2	Multilateral agreements	
5.3	International fora participation	
5.4	Public-private partnerships	

5.5	Interagency partnerships	
	Total	**100**

(ITU, 2015c)