An approach of a maturity model for assessing offensive cyber warfare capability of countries

Name	**: S.M. Oedit**
Student number	**: 4035585**
Faculty	**: TPM**
First Supervisor	**: Mr. dr. ir. Semir Daskapan**
Second Supervisor	**: Dr. ir. Fardad Zand**
Chairman Graduation Commitee	**: Prof. dr. Y.H.Tan**
	Dr. ir. Jan van den Berg
Extern supervisor	**: Drs. Robbin te Velde**

Acknowledgement

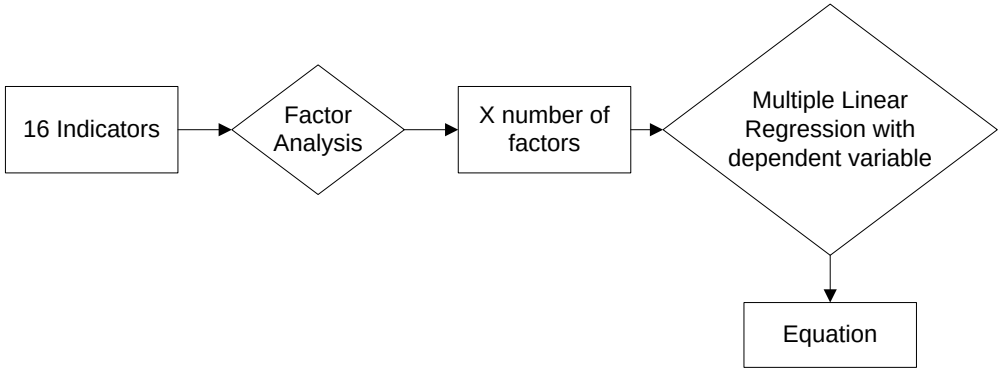
I would like to express my gratefulness to everyone, who supported me finishing my thesis. I am glad I was allowed to do my thesis at the department of Information and Communication Technology. I want to thank my supervisor Semir Daskapan for the opportunity to work on the project and for the guidance during the project. I am also thankful to my second en extern supervisor, Fardad Zand and Robbin te Velde respectively, for their suggestions and feedbacks to improve my research.
Further, I would like to express my gratitude to my great parents and to a special person in my life, Shailesh Kisoensingh, for all the love, patient, support and encouragement they have been giving me to complete my thesis.

Executive Summary

The number of cyber-attacks creates the realization that the vulnerability of critical infrastructures of a country are increasing. The numbers of cyber-attacks are so high that governments fear a cyber war. This makes it important for governments to prepare their nation for cyber war. To be able to make the right preparation and to design the right resilient systems it is necessary to know how dangerous other countries can be by measuring their offensive cyber warfare capabilities. This leads to the design of a model based on offensive cyber warfare attributes and public indicators for the assessment of offensive cyber warfare capabilities. The aim of this research is to provide an approach of a maturity model to assess offensive cyber warfare capabilities of countries based on public data, by which governments can make better decisions and policies to prepare themselves for cyber war.

The research has been started with an in depth desk research describing the process of cyber warfare, which resulted in a diagram with 6 categories. These categories have been defined based on some literature about traditional warfare and an analogy about individuals in war. The 6 categories describing the process are: Motivation, Channel, Target, Means, Method and Damage. This diagram shows the difference between traditional and cyber war. Only offensive cyber warfare attributes are specified in this diagram. This was necessary for finding the indicators for offensive cyber warfare capability. From these 6 categories only two have been used to define offensive cyber warfare capability. Motivation level does not contribute to capability level, but to the threat level. If one is motivated, it does not necessarily mean that one has the capability. The channel is the environment where the cyber attack is launched. Having access to the channel, having knowledge about it and skills for operating in this medium is necessary to launch a cyber attack. So channel is an important group to consider for assessing offensive cyber warfare capability. The Target actually does not decide on the capability of another. So this is not important for the design of the model. The Means are very important to assess the offensive capability level, because having the ability to create the means, having access to them and the ability to use them shows how capable one is. The Method is the way how the attack is performed for example from behind or from the front and thus is not contributing to the assessment of the capability level. Also Damage is not contributing to the capability of a country, because anyone can cause damage by hiring others. So based on this analysis Channel and Means are important for assessing the offensive cyber warfare capability level. Based on these 2 classification and their details in the diagram the indicators for offensive cyber warfare capability have been identified. This resulted in a theoretical model showing the relation between the indicators and the cyber warfare attributes. As data to direct indicators are limited, an approach of a model has been given based on proxy variable and indirect indicators for which data was available.

Finding data for indirect indicators has been difficult as well, but there are 16 indicators for which data has been found. The dataset for offensive cyber warfare capability was not available, so a proxy variable has been used. The closest proxy variable based on the categories Channel and Means is the ICT development index, which describes the access to, use of and skills in ICT. ICT development has been build from 11 indicators, from which 9 are the same for offensive cyber warfare capability. The assumption has been made that the ICT development index is a data collection method for offensive cyber warfare capability. Using the 16 indicators and the proxy variable the model has been designed following some analysis as is shown in the flowchart. The flowchart describes the statistical analysis in SPSS. On the 16 indicators factor analysis was done, which resulted in 4 factors that are the independent variables to explain offensive cyber warfare as the dependent variable. As there is no such dataset for the dependent variable the ICT development index is used in its place. Based on a linear regression the equation has been found; this is the model to assess offensive cyber warfare capability.



Due to limitation only an approach of a model for assessing offensive cyber warfare capability has been given, which is based on a proxy variable and indirect indicators:

$$y = 0.386\ factor\ 1 + 0.458\ factor\ 2 + 0.094\ factor\ 3 + 0.205\ factor\ 4 - 0.418$$

This equation is a first approach of a model assessing offensive cyber warfare capability, on which further research can be conducted.

The growth in capability level is described by maturity levels. There are 5 maturity levels defined for offensive cyber warfare capability based on the Channel and Means capability, which are: Beginners, Semi-intermediate, Intermediate, Semi-advanced and Advanced.

In chapter 1 an introduction has been given, describing the aim of this research, the research questions and the research methods. In chapter 2 the theoretical background has been built resulting in a diagram describing offensive warfare, maturity levels and a

theoretical model for assessing offensive cyber warfare capability. Chapter 3 gives an approach of a model and the statistical analysis to be performed. Chapter 4 has been devoted on reflection and the report ends with conclusions and research relevance.

Table of content

List of Figures

List of Tables

1. Introduction

The numbers of cyber attack and security vulnerability within the past years has been increasing (HP DVLabs; HP Teams, 2011). An increase in vulnerability gives opportunities for exploitations. Cyber attacks differ in sophistication level, the damage they can cause and the reason behind the attack. A cyber attack can be initiated from different information and communication networks. For example Malwares Sites can be opened on a computer, but also on a mobile phone. Figure 1.1 illustrates an increase in Mobile Malware Samples, which has been released in a MCAfee Threats Report (Third Quarter 2011). Figure 1.2 illustrates the pattern of increase in new malware sites per day, reported by MCAfee as well. (MCAfee Threats Report: Third Quarter 2011, 2011)

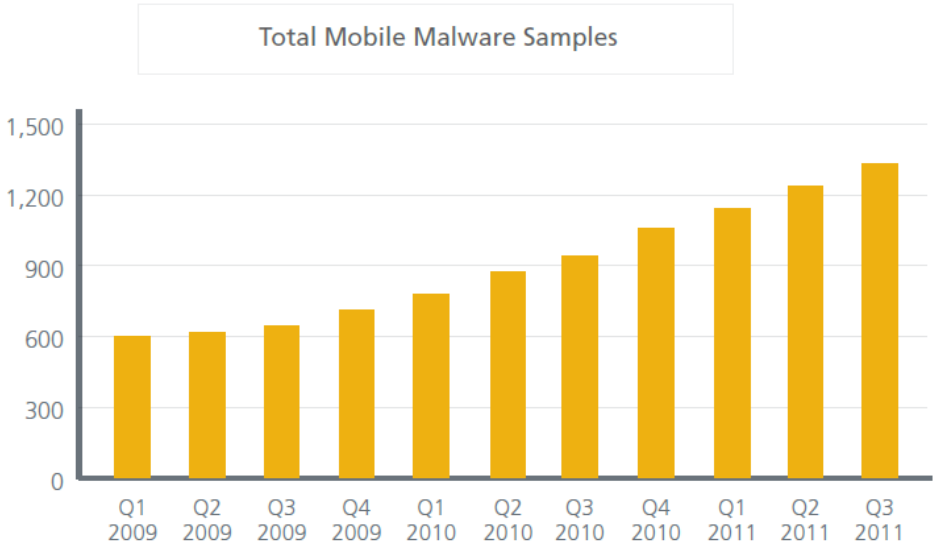


Figure 1.1 Total Mobile Malware Samples (McAfee Labs, 2011)

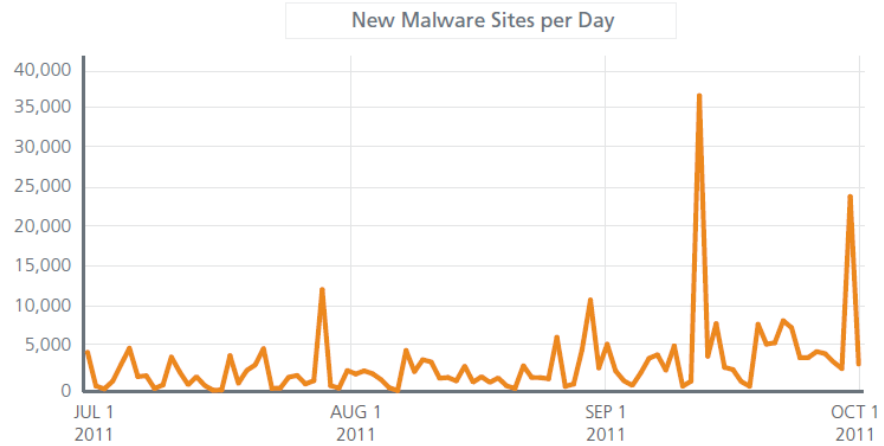


Figure 1.2 New Malware Sites per day (McAfee Labs, 2011)

Not only the number of attacks within the cyberspace over these years has been growing, but also the sophistication level of these cyber attacks. With the increasing sophistication nations are heading towards cyber war. McAfee even fears cyber war in 2012 (McAfee Labs, 2011) (Colin van Hoek, 2011). A very well-known example of a cyber attack is the Stuxnet worm that was used to interrupt operations at an Iranian Nuclear Plant (David Lee, 2012). Another example is Flame, which has been used to collect private data from countries like Iran and Israel. Researchers think that this is more a government supported attack. Also Duqu was a cyber attack that was used to steal data (David Lee, 2012). In cyber warfare the target of attacks are most likely to be critical infrastructures (Papa & Shanoi, 2008). Critical infrastructures are very important properties for keeping the society and economy functioning (Saalbach, 2011). *"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government* (Moteff & Parfomak, 2004)*."* As the sophistication level and number of cyber attacks are increasing countries must prepare their nation for war in cyberspace. Earlier, war was conducted in the domains land, sea, air and space, but now warfare has entered the fifth domain called cyberspace (C.Homan, 2010). This means that cyber war could be an additional domain to traditional warfare.

The dependency and use of internet has been growing, making the network systems more and more complex. The organization and security of these complex networks require intense analysis and attention, because the number of attacks within the cyberspace is growing day by day. The virtual dimension of network systems makes security more complex, because the internet has created systems that can go beyond its limits (Defense Information Systems Agency, 2010). According to research done by the International Telecommunication Union (ITU) the growth of internet users has the shape as has been shown in figure 1.3 (Free statistics, 2012). Not only access to internet makes it possible to launch a cyber attack, but also digital access devices that can be connected to a communication network make it possible to launch a cyber weapon.

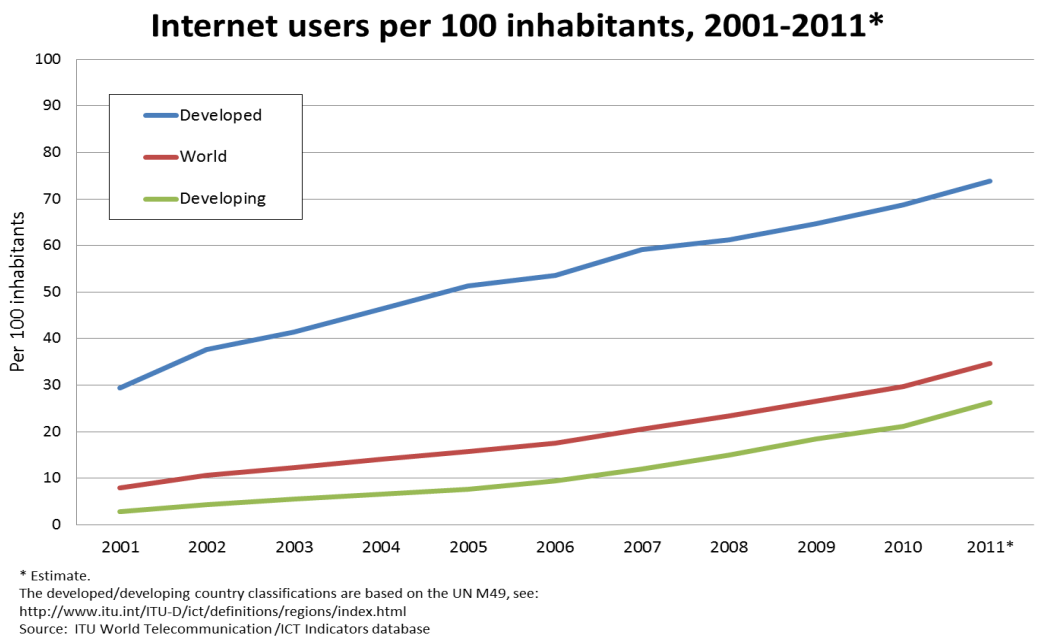


Figure 1.3 Internet users per 100 inhabitants

Many critical systems that control the modern nations are connected to the internet in some way. The networks of these systems are becoming more complex with time, leading to more vulnerability for attack. If any of these critical infrastructures would terminate operation for a long period, the consequences would have a rapid and harmful impact upon functioning of the society as a whole (G.Pye & M.J.Warren, 2009). Several countries like China, Russia, United States and others are preparing their country for cyber warfare (Fritz, 2008). The motives to conduct cyber warfare can be different for all countries. Governments have to prepare their country for cyber warfare, which makes assessing offensive cyber warfare capability of other countries important. You will know how to defend yourself and how to attack your opponent only if you know the strength and weaknesses of the opponent.

This research uses publicly available data (open source information) to estimate offensive cyber warfare capabilities, because access to a countries' secret data about its military capabilities is limited. There is the upcoming trend of Open Source Intelligence, where open source information is used to make useful interpretations about different situations. According to Intelligence Community Directive (July 11, 2006, number 301) open source information is information that is publicly available and everyone can lawfully access them by request, purchase or observation. Open Source Intelligence is the collection and analysis of publicly available sources to produce intelligent information/result/findings. (Intelligence Community Directive Number 301, 2006)

There is not much theory in the field about cyber warfare attributes and there is limited access to statistical data. This makes the research complex and causes restrictions, which leads the research to be based on assumptions.

1.1 Problem Description

In literature there are some descriptions about countries' cyber warfare capabilities, but the 'methods' used to assess their capabilities are different, non-standard and are not publicly available (Guitton, 2011) (G.Coleman, 2007). However, there is no standard model that can be used by any government to assess a countries' offensive cyber warfare capability (Guitton, 2011) (G.Coleman, 2007). Those methods are not assessing offensive cyber warfare capability but defensive. In order to be able to prepare ones' own nation, the government must be able to make assessments on other countries' offensive cyber warfare capability levels. This makes it important to design a model for the assessment of offensive cyber warfare capabilities based on offensive cyber warfare attributes and public indicators, which will help the government to assess other countries' offensive cyber warfare capability and make improved decisions and policies for its own nation. Any government must be able to assess other countries' offensive cyber warfare capability in order to be able to prepare their nation in the right way, but such a model does not exist yet. To see how a country can grow in capability level the maturity levels will be included in the model.

Goal: The aim of this research is to provide an approach of a maturity model to assess offensive cyber warfare capabilities of countries based on publicly available data, by which governments can make better decisions and policies to prepare themselves for cyber war.

Contribution: This research will contribute by providing the governments with a model by which other countries' offensive cyber warfare capabilities can be assessed based on publicly available data.

1.2 Research Objective and Research Question(s)

Research objective:
The aim of this research is to provide an approach of a maturity model to assess offensive cyber warfare capabilities of countries based on public data, by which governments can make better decisions and policies to prepare themselves for cyber war.

Main research question:
By which model can a countries' capability to perform offensive cyber war be assessed, based on publicly available data?

The following sub research questions are formulated:

1. What is offensive cyber warfare?

a. How can the process of offensive warfare be described?

b. What are the attributes of cyber warfare?

2. Which cyber warfare attributes can explain offensive cyber warfare capability?

a. Which public indicators can be chosen as independent variable to explain the offensive cyber warfare capability as the dependent variable?

b. Based on which direct or indirect indicators can an approach of a model for assessing offensive cyber warfare capability of countries be given?

3. How can the growth in capability level be described?

b. Based on which attributes can the maturity levels be described?

a. What are the different maturity levels for the offensive cyber warfare capability model?

4. How can an approach of the offensive cyber warfare assessment model be provided?

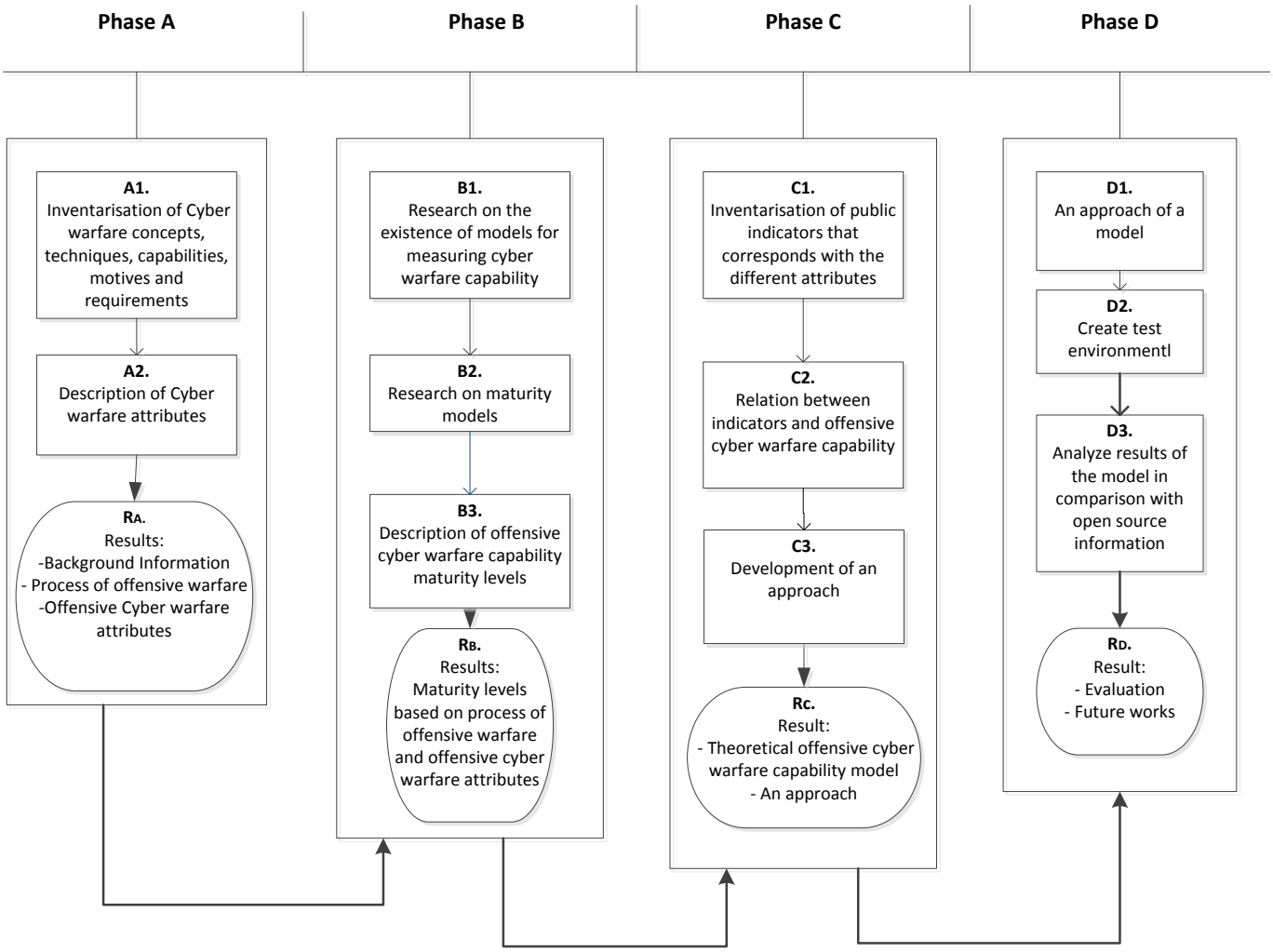


Figure 1.4 Roadmap

Description Roadmap:

The first step of this research includes an inventarisation on the different cyber warfare concepts. A description of all the important concepts are given, followed by a daigram describing the path/process of offensive warfare. In this diagram only the cyber warfare attributes are specified. It is important to understand the cyber warfare attributes, because they will help to find the right indicators for offensive cyber warfare capability. In the second phase a research is conducted on existing models for measuring cyber warfare capability of countries. After that a research on the development of maturity models has been done. Based on the diagram and the offensive cyber warfare attributes the maturity levels are described. The third phase is finding the indicators based on publicly available data . These indicators are chosen based on the cyber warfare attributes. These indicators are the independent variable to explain offensive cyber warfare capability as the dependent variable. The indicators are connected to the attibutes resulting in a theoretical model. Then an approach of a model for assessing offensive cyber warfare capability will be

given. This approach will be based on indirect indicators for which it is possible to find data. This model will be tested by creating a test environment and making assumptions. In the end the work will be evaluated and future work will be added.

1.3 Conceptual Framework

The research starts with an in-depth desk research on cyber warfare concepts, techniques, motives and attributes resulting in theoretical background for this research and a process describing offensive warfare attributes in which the offensive cyber warfare attributes only are specified. The second step is to find an analogy on measuring cyber warfare capabilities and describing the maturity levels for offensive cyber warfare capability. After this the research has been followed by finding the public indicators based on cyber warfare attributes and finding a relationship with offensive cyber warfare capability as the dependent variable. Then an approach of a model will be given containing the statistical analysis. Based on factor analysis and linear regression all these resulted in an approach of a model to assess offensive cyber warfare capability. The model has been tested and the results are compared to what has been found in literature. The conceptual framework in figure 1.5 outlines the courses of action.

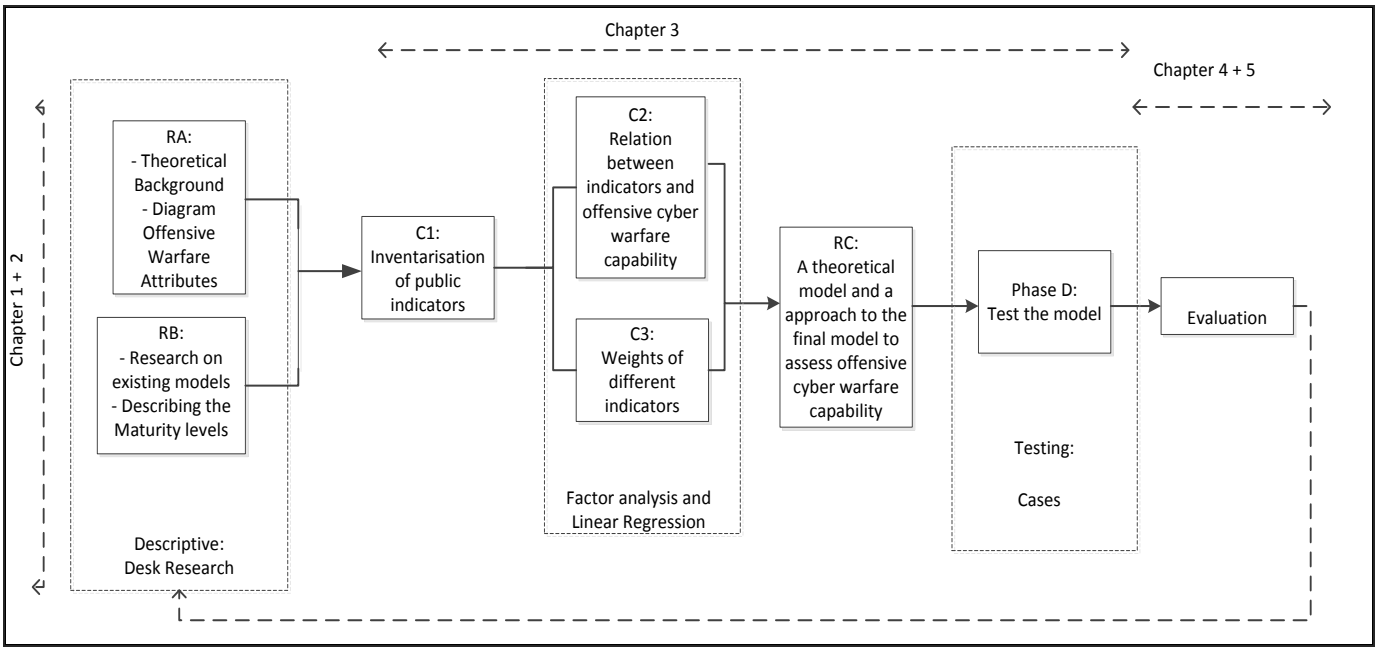


Figure 1.5 Conceptual Framework

1.4 Proposition(s)

Countries like United States, China and Russia are investing a lot of money in cyber warfare. Russia developed a cyber warfare doctrine and IT experts are working together with academic communities (G.Billo & W.Chang, 2004). Japan is also busy with preparation for cyber warfare and developed a cyber weapon as was published on the news. To attack in the cyberspace cyber weapons are used, which can be launched from anywhere and anytime. The targets of cyber warfare are critical infrastructures of a country. Developed countries have a lot of critical infrastructures on which the society depend. Least developed countries' critical infrastructures do not use developed cyber systems, because they cannot afford it. Their infrastructures are mostly broken; an example is Congo (nations encyclopedia, 2012). Based on literature some predictions about a countries capability can be made, which has been written as propositions.

Proposition 1:
Least developed countries are less mature than developed countries.

Proposition 2:
European countries are more mature than Middle East countries.

1.5 Limitations and assumptions

This research has some limitations:

- The research is based on public data (open source information), which means the research excludes secret data of countries. Not all statistical data is available, so some important indicators might have been excluded.

Because of limitations within this research some assumptions have to be made to be able to conduct the research. General assumptions for the research:

- The public data is reliable, because they have been collected from well known statistical organizations, which are the ITU and World data bank**.**
- The Cyber warfare attributes that show threat level instead of capability level will be excluded from the research. After all a threat does not imply capability. For example, if a country X has a conflict with another country Z than X will find a way to launch an attack on Z. This does not necessarily mean that X has the capabilities; it might be that he just hired others to do the work for him. Thus this example shows that the motivation behind the attack defines the threat level of a country and not the offensive cyber warfare capability. But if capability and threat level are combined, then the most dangerous countries can be found.

- For the dataset of offensive cyber warfare capability a proxy variable has been used, because a statistical dataset for offensive cyber warfare capability is not available.
- The United States is used as one of the reference point. In literature United States is said to be very capable in the field of cyber warfare (Carr, 2011) (He-suk, 2012). So our model must give results where the United States is high among the countries for which the assessment is done, at least in the top 10% of all countries included in the research analysis.
- The target of Cyber war is critical infrastructure. Because least developed countries have least developed critical infrastructures and they are least mature in cyber warfare capability, the reference point for least mature countries will be Congo. Congo must be at least in the 10% of least mature countries. Congo has no developed infrastructures (nations encyclopedia, 2012); some that existed were destroyed during the war or damaged during the wars in the period of the late 1990s.

1.6 Research Strategy

A detailed analysis of the research strategy has been included in figure 1.4 and 1.5:

- Desk Research: The first step of the research is collection and analysis of publicly available data. At the beginning of the research insight has been gained into concepts of cyber warfare through literature study, which is descriptive in nature and led to a theoretical background necessary for this research. Also through desk research an appropriate analogy for designing capability and maturity model has been identified. The desk research lead to description of process of cyber warfare attributes, based on which the indicators are identified. The offensive cyber warfare capability as the dependent variable has been explained in terms of the indicators as independent variable.
- Test Cases: In order to test the model a test environment has been created. To execute the test, datasets of indicators for countries for which there is data, are selected. Based on these datasets the assessment of offensive cyber warfare capabilities has been done using the new designed model. The results indicate how mature countries are in the field of cyber warfare.

2. Theoretical Background

Within this chapter a description of important cyber warfare attributes will be given. Attributes are qualities or characteristics assigned to an object. These attributes can be found in a diagram describing the process of offensive warfare, in which only the offensive cyber warfare attributes are specified. Further the growth in offensive cyber warfare capability level is described by maturity levels, which is based on the diagram.

2.1 Cyber Warfare Concepts

Based on a literature review it became clear that there are many definitions for cyberspace and cyber warfare. In this research the definition for cyberspace has been chosen from an USA military pamphlet, because this research focuses on nation supported cyber warfare and the model to be provided is aimed for the government. Another reason is that using a definition given by military sounds more reliable, than choosing one of the many different definitions given to cyberspace. The definition for cyberspace sounds as follows: *"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers* (U.S. Army Capabilities Integration Center, 2010)*."* From this definition the meaning of cyber warfare will be derived. Cyber Warfare consists of two words: Cyberspace and Warfare. In order to define cyber warfare and find its attributes it is important to look back at the definitions of those words separately. Definition of War: "*A state of open, armed, often prolonged conflict carried on between nations, states, or parties."* (The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company). The definition of war arise the question about what a conflict is. A conflict is *a state of disharmony between 2 or more entities* (The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company). A conflict occurs when 2 or more entities cannot go along together, so warfare means engage in war with an enemy. According to literature cyber warfare has been defined in different ways. Two of the definitions are given here:

1. "*Cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means"* (G.Billo & W.Chang, 2004).
2. *"Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"* (Clarke, 2010).

In the definitions by nation-state is meant a country that has defined borders and territory. The second definition does not emphasize the defensive part of cyber warfare. In none of

the definitions cyberspace has been mentioned, which has a broader meaning than just a computer network. That is why *in this research the meaning given to Cyber Warfare is nation supported warfare in cyberspace that can be both offensive and defensive as well.*

In this research a model has to be designed for the assessment of offensive cyber warfare capability of a country. In order to define cyber warfare capabilities a first expression of capability should be given. A definition of Capability: *"Capabilities are conceived as the efficiency with which a firm employs a given set of resources (inputs) at its disposal to achieve certain objectives (outputs)* (Dutta, Narasimhan, & Rajiv, 2004)." Cyber Warfare Capability can be divided into offensive and defensive capability. These capabilities can be achieved when a country combines the available resources efficiently. Cyber warfare capability of a country can be conceived as the ability of a country to attack or defend itself in cyber warfare. In this research the focus is on the ability of a country to attack another country. The maturity level of a country is determined by its capability level. To see a growth in capability level the maturity levels will be included in this research. A meaning of maturity: *"Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization* (Paulk, Curtis, Chrissis, & Weber, 1993)*."* The maturity level shows growth in capability level. In this research it is about maturity on country level in the field of cyber war. So the definition given to maturity of cyber warfare capability is a potential growth in cyber warfare capability, which indicates the ability to attack others and defend oneself within the cyberspace. Within this research the maturity levels focus on capability to offend other countries.

Cyber warfare can be divided into intelligence, defensive and offensive operation, but in this research intelligence is incorporated in offensive and defensive operations. Thus in this research we make the distinction between defensive and offensive cyber warfare capabilities (F.Erbacher, 2005) (G.Billo & W.Chang, 2004) (G.Pye & M.J.Warren, 2009). There is literature about enhancing cyber defensive capability on micro level, which can be lifted up to capabilities on macro level necessary for an operative response by a country to cyber warfare threats (NATO C3 Agency, 2011). There is unfortunately not such a comparable model for offensive cyber warfare capability, so in this research the focus will be on offensive cyber warfare capabilities of countries for which a model will be designed.
The protection of a communication and information system (CIS) infrastructure against cyber attack is called Cyber Defense, while Cyber Offense is launching a cyber attack on a CIS.

To design a model for assessing offensive cyber warfare capability the theoretical background about cyber warfare attributes will be explained. As there are many definitions given to cyber warfare and cyberspace as well, it becomes difficult to specify the offensive

cyber warfare attributes. To get a clear picture of the offensive cyber warfare attributes a diagram for the process of offensive warfare has been derived. Only details of the cyber warfare attributes are included in this diagram. The traditional offensive warfare attributes are not specified as it is not relevant for this research. This leads to the development of a diagram for the process of offensive warfare, with specified details for offensive cyber warfare attributes.

2.1.1 Deriving the Diagram for Offensive Warfare

To determine the cyber warfare attributes a diagram describing the process of offensive warfare will be used. This will clearly show the distinction between traditional warfare and cyber warfare. It makes it possible to clearly see the attributes of offensive cyber warfare, based on which the indicators are chosen to explain offensive cyber warfare capability of a country. Cyber warfare can be divided into cyber offense and cyber defense as has been mentioned before, where cyber offense and defense include computer and network attacks on a macro level (nation supported attack on another country). This means attack on critical infrastructures of a country initiated by another country.
Neither is there any literature describing the process of cyber warfare explicitly and nor cyber warfare attributes. That is why based on literatures about traditional warfare, a logical view and an analogy the process for cyber warfare has been described. Based on the definition of war in chapter 1 and according to J.Pike (2000-2012) a country has reasons for attacking an enemy. Every state has its own reason, which can be placed in a category named Motivation. In traditional warfare there is war between 2 countries X and Y. They are both each others' enemy. In warfare the enemy or a precious/vulnerable asset of the enemy is the target of attack. In cyber warfare there is also a target, which is the critical infrastructure of the enemy's country. So Target is also a category. As there are many war domains, a country is allowed to choose its own war domain. This war domain defines the Channel, the place where the war occurs. Based on the war domain a country should choose its Means, which are the weapons used to attack. In traditional warfare different methods are used to attack an enemy (Pike, 2000-2012). In cyber warfare there are different methods to attack, which give the next category within the process of cyber warfare and that is the Method. The purpose of war is to cause harm/damage to the enemy. Depending on the war domain, the means and the methods it is possible to describe the damage level. Damage is another category in the process. The process includes 6 categories which are **Motivation, Channel, Target, Means, Methods** and **Damage.** Looking at an analogy in daily life it also becomes possible to describe the categories for the process of offensive warfare. The analogy used here describes attack on individual level, in which person A wants to attack his enemy person B. Person A has a reason why he wants to attack another person B, which describes his Motivation level. The Target of attack is his enemy

(person B) and the place where he chooses to attack is the Channel. It can be a physical attack, like a punch in the face or it can be a non-physical attack, like sending virus to his pc or attacking psychologically. The weapon person A can use is a gun, a fist, teasing and others. The weapon is the category Means. Person A can attack from behind or from the front, which describes the Method of attack. The Damage that person A causes to person B depends on the means and methods person A has used. A country has reasons to enter into warfare with other countries. Their **motivation** behind such a decision is important. To attack they choose the medium where they will fight the war, which is the **channel**. In a war there is a **target**, which is the third category within the diagram. To attack during war a country needs **means**. These are launched in different ways, which is the **method**. Depending on the mean and the method of attack there will be certain amount of **damage**.

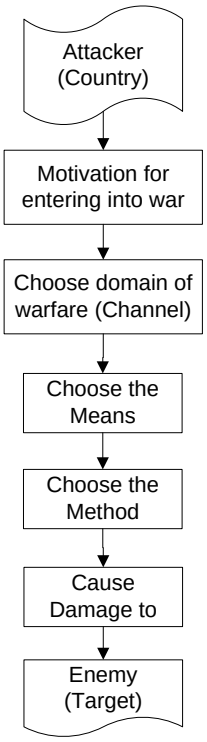


Figure 2.1 The path/ process of warfare

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke (2010) also published in their paper the most unique attributes of cyber warfare, which will also be used to develop the diagram for cyber warfare attributes. In a report "the national military strategy for cyberspace operations (2006)" the attributes of cyberspace and information warfare are published, which will support identifying the attributes of cyber warfare (The national military strategy for cyberspace operations , 2006). The attributes should differentiate cyber warfare from traditional warfare in a unique way. The diagram in which the process of offensive cyber warfare has been described shows the differences between offensive

warfare attributes and traditional warfare. In the diagram only the offensive cyber warfare attributes are specified. The attributes of cyber warfare make it unique and different when compared to other forms of warfare. In appendix 1 a picture of the diagram has been given, but as it is too small and not readable there has been zoomed in on the different criteria.

The interpretations of the different categories on first level follow here:

1. **Channel** of Offensive Warfare:

Channel can be defined as the transmission path for war weapons. This can be divided into physical and non-physical channels. By physical is meant things that can be perceived by the senses; they are detectable. By non-physical is meant things that cannot be detected by the senses. Physical channels are tangible and can be divided into land, water, air and space. Non-physical channels are intangible and can be divided into the subcategories digital, psychological and others.

Channel of Cyber Warfare:

When it comes to channel of cyber warfare, the following question will be asked: "what is the transmission path over which cyber weapons can be sent?" The definition that will be given to channel of cyber warfare is "the transmission path over which a cyber weapon is sent to initiate the attack and cause the damage". For example in traditional warfare when the channel is land, a tank (a fighting vehicle) can move over land and while moving it can cause damage by firing. Cyber attack occurs over a non-physical channel, where the use of digital technology within an electronic environment creates a digital space that cannot be detected by our senses. In a world with fast changing technologies and high level use of digital technology the channel of cyber warfare will be defined as digital. The digital category has been divided into other subcategories, which are Digital communication devices, Wireless Network, Wired Network. Further divisions can be found in the diagram.

2. **Target** of Offensive Warfare:

Target is the object of attack and can be divided into physical and non-physical targets. Physical targets are tangible things and non-physical are intangible things.

Physical targets are Buildings, Natural Resources, Critical infrastructures like for example the Electricity Network and others. Non-physical has the same subcategories as in channel to know digital, psychological and others.

Target of Cyber Warfare:

When it comes to target of cyber warfare the question that can be asked is: "What do you want to attack/destroy?" Physical target are critical infrastructures of countries, but the attack is actually initiated through a non-physical target to know the critical information infrastructures (CII). CII can be divided into supporting ICT platforms like SCADA (one that supports the different CI's by providing the ICT platform) and the independent CII, which is

needed by other CII's for optimal functioning. One independent CII is the internet (McDonogh, 2009). Critical infrastructures are very important properties for keeping the society and economy functioning (Saalbach, 2011). The digital part can be divided into more detailed divisions as has been shown in the appendix 1.

3. **Means** of Offensive Warfare

Means of warfare can be divided into launching means and damaging means. The launching means are tools that support the transmission of the damaging mean. For example a gun is a launching mean and the bullets are the damaging means. A launching tool supports the damaging tool. The main divisions under launching and damaging means are physical and non-physical means. Physical means are for example bomb, arms, tanks and other tangible weapons. Non-physical means can be divided into digital, psychological and other non-physical means.

Means of Cyber Warfare:

Means of cyber warfare answers two questions: "What is sent over the channel? With what is it sent over the channel?" The launching means for cyber warfare answer the question with what is it sent and these can be divided into the following software platforms: The Operating system, Middleware and Applications. Damaging means of cyber warfare are the cyber weapons that are transferred over the transmission path. With this the answer can be given to what is sent over the channel. Cyber weapon is a software program that has the potential to disturb the storage of data or logical processes of adversary's computer. Cyber Weapon can be divided into (Denning, 2000):

- Offensive attack tools such as bots and malware like virus, Trojan, worms. Botnet is very likely to be used in Cyber Warfare, as these can be initiated from networks of other countries for example. They are becoming larger and are spreading until it reaches its goal. Tracing back the starting point of the attack becomes more difficult when botnets are used.
- Dual use tools, for example scanners to assess port vulnerability and other network monitoring tools.
- Defensive tools, like Authentication, encryption, firewalls etc.

4. Offensive Warfare **Methods**:

Methods are the techniques used to accomplish a task, which involves certain moves/steps. The methods for offensive warfare operations can be divided into physical and non-physical methods. Physical method can be divided into *Direct and Indirect attack*: Sun Tzu wrote in his book "The Art of War" that attacks can be divided into direct and indirect attacks. He took this from the book of Wei Liao Tzu [4th cent. B.C.] , who said that 'Direct warfare favors frontal attacks, indirect warfare attacks from the rear.' (Tzu, 4th cent. B.C.) Direct and Indirect methods are the 2 main physical categories, which is also in the

diagram. These two main physical categories can be divided into different methods (Pike, 2000-2012):

1. Move to contact: This technique is used to gain in depth information about a target (T) when there is lack of information.
2. Attack on the single axis: This technique does not attack the target (T) directly. Instead it starts the attack from another object B and then the attack will go from B to C reaching the target (T).
3. Attack on multiple axes: This technique is used when the path to the target (T) cannot be approached immediately. So other objects around T for example B and C will be attacked first to distract the attention from T to B and C. In this way T gets isolated and there is space to initiate an attack on T.
4. Cordon and attack: Using this method forces the target to enter a more open area (exposure of T), where the attack on it becomes easier. The techniques works as follows: some important areas around T are surrounded by armies and then the attack on T is initiated.
5. Fix and Bypass: If one has to pass a certain enemy area before he can get to its destination (D), then a limited attack on D will be initiated to create space for bypass.
6. Multiple Nodal attacks: This technique gives the opportunity to attack more than one node simultaneously or sequentially until it reaches its target (T).

Cyber Warfare **Methods**:

The methods for cyber warfare belong to the category of non-physical methods. This category has been divided into digital, psychological and others just like for the other classifications. The methods for cyber warfare are digital as they take place in a digital environment. There are different cyber warfare techniques that can be used to attack a network. The two most basics are the passive and the active attacks. During passive attack there is no interaction with the involved parties. The main purpose is to gather information that is being transferred (Networkingmind, 2011). Active attack is interfering, breaking into a secured system and modifying information that is being transferred (Networkingmind, 2011). Some famous types of cyber attacks are: Distributed Denial of Service Attack, Website Defacement and Data Modification (Saalbach, 2011) (Toorani.M, 2009).

Distributed Denial of Service Attack tries to disable access to network resources. These types of attacks are initiated from multiple nodes targeting one main node, where the whole group of infected systems is controlled by one party.

Website Defacement is an attack on a website where the attacker exchanges the original website or web pages with his own.

Data Modification means changing original data without being authorized for it and sending false data to the receiver. The receiver thinks the message was sent by the actual sender. But the actual sender does not even know the message has been changed.

5. **Damage** by Offensive Warfare

Damage can be divided into the categories tangible and intangible damage. Tangible damage is materialized damage. Intangible damage is damage that is immaterialized damages. Tangible damages can be divided into fire damage, water damage and others. Intangible damage can be divided into psychological damage, reputation damage, social damage, financial loss, privacy damage, digital damage and others (Schade, 2010) (Damage, 2012) (Damages (disambiguation), 2010) (Damages, 2012) (Forbes, 2007).

Damage by cyber warfare:

Damage is the effect of an attack; effect of the cyber weapon after it has been executed. The damage caused by a cyber attack is intangible damage. Some sub digital damages can be found in the diagram. A simple example of damage is privacy violation caused by the virus Flame. Flame is used by attackers to steal information of others. It has the ability to infect a computer and spread to other computers.

6. **Motivation** for Offensive Warfare

Motivations are the reasons behind an attack. The reason for war can be different for every attacker. According to The Jewish Talmud there are three universal reasons for war: Economic, Religious and Power. The Dutch psychoanalyst Joost Meerloo wrote that people go in war because of anger to express their feelings. Based on this another category for war can be psychological. According to the evolution theory warfare can be a reason of complex social organizations, high population density and competition over resources (War, 2012). Other reasons for war can be financial and political gain (NATO PA - 173 DSCFC 09 E bis - NATO and Cyber Defence, 2009). Based on this information the following motivation categories are identified: Economic, Religious, Political and Psychological. Countries have varying motivations for cyber warfare, so it can be any of the mentioned reasons within the diagram (G.Billo & W.Chang, 2004). Examples for motivation to go into war can be found in history, like the Taliban's in Afghanistan.

2.1.2 The Offensive Cyber Warfare Attributes

The diagram describing the process of offensive warfare can be seen in appendix 1. In the diagram the main offensive cyber warfare attributes are detailed. The main offensive cyber warfare attributes can be derived based on the diagram:

- To get involved in cyber warfare a country needs access to the digital channel.
- In cyber warfare a country needs digital means to attack other countries.
- A country has a motivation to initiate a cyber attack.
- The targets of cyber warfare are information infrastructures of countries.
- The Damage caused during cyber warfare are digital, but can also be physical and psychological.
- The methods used during cyber warfare are digital.

The details of these attributes can be found in the diagram in appendix 1.

2.2 Maturity models

In this research the offensive cyber warfare assessment will result in maturity levels as has been said in the introduction. According to the authors Prof. Dr. Jörg Becker, Dr. Ralf Knackstedt Dipl.-Wirt. Inform. Jens Pöppelbuß, there are hundreds of maturity models and in their paper "Developing Maturity Models for IT Management – A Procedure Model and its Application" they give some guidelines for the development of a maturity model.
"A Maturity model consists of a sequence of maturity levels for a class of objects. It represents an anticipated, desired or typical evolution path of these objects shaped as discrete stages. Typically, these objects are organizations or processes (Becker, Knackstedt, & Pöppelbuß, 2009)". The maturity level shows growth in capability level. In this research it is about maturity on country level in the field of cyber war. The definition given to maturity of cyber warfare capability is a potential growth in cyber warfare capability, which indicates the ability to attack others and defend own nation within the cyberspace. In this research the focus is on maturity to offend. The maturity model has two extremes a lowest and a highest level. It is a measurement scale to assess the position of an object on the evolution path. This assessment is done based on criteria and attributes that must be met by an object in order to be ranged on a certain maturity level. (Becker, Knackstedt, & Pöppelbuß, 2009)
Based on the definition and attributes of a maturity model it is obvious that the domain is cyber warfare and a country the object of assessment. The assessment will be based on cyber warfare attributes that should be met by a country in order to be ranged on a certain maturity level. Based on cyber warfare attributes the indicators are identified to explain offensive cyber warfare as the dependent variable. The offensive warfare diagram has 6 major classifications: Motivation, Channel, Target, Means, Method and Damage. Motivation

level does not contribute to capability level, but to the threat level. If one is motivated, it does not necessarily mean that one has the capability. The channel is the environment where the cyber attack is launched. Having access to the channel, having knowledge about it and skills for operating in this medium is necessary to launch a cyber attack. So channel is an important group to consider for assessing offensive cyber warfare capability. The Target actually does not decide on the capability of another. So this is not important for the design of the model. The Means are very important to assess the offensive capability level, because having the ability to create the means, having access to them and the ability to use them shows how capable one is. The Method is the way how the attack is performed for example from behind or from the front and thus is not contributing to the assessment of the capability level. Damage is not contributing to the capability of a country, because anyone can cause damage by hiring others. Thus Channel and Means are important for measuring the offensive cyber warfare capability level. Based on these 2 classification and their details in the diagram (appendix 1) the indicators that are thought to be important have been identified.

2.3 The Offensive Cyber Warfare Capability Maturity Levels

The offensive cyber warfare capability is based on the two classifications Channels and Means, which emphasize the ICT development in a country. The focus is on how capable a country is in using the available Channel and Means for offensive cyber warfare. Based on the classifications Channel and Means a country can have low, medium or high capabilities in one or both of the classifications. Based on these low, medium and high levels table 2.1 has been developed to show the different maturity levels, which are Beginners, Semi-intermediate, Intermediate, Semi-advanced and Advanced. The divisions for these levels have been made based on an analogy with an object developing its capabilities. The Means capability can be medium only if Channel capability is medium, but when Channel is low then Mean cannot be medium. If Channel capability is medium it does not necessarily say that Means capability should be medium. The capability maturity level describes what a country can do in cyber war, based on whether they have low, high, medium Channel and Means Capability. Maturity of offensive cyber warfare capability is a potential growth in offensive cyber warfare capability. This growth has been described by the maturity levels as discrete stages.

Access to, use of and skills of Channel = Channel Capability (the ability to use the digital device, to access the digital systems and the skills to create these devices and systems)
Access to, use of and skills of Means = Means Capability (the ability to use the digital programs, to access the digital programs and the skills to create digital programs/software)

Table 2.1 Maturity Levels

	Channel Capability	**Means Capability**
Beginners	Low	Low
Semi –intermediate	Medium	Low
Intermediate	Medium	Medium
Semi – Advanced	High	Medium
Advanced	High	High

The five maturity levels are:
Level 1: Beginners
On the beginners level a country cannot attack critical infrastructures of another country, because they cannot create means by themselves.

Level 2: Semi-intermediate
On this level a country has some ability to access the cyber war medium and create non-sophisticated cyber weapons. These types of cyber weapons can be easily detected by virus-scanners and cannot cause any harm.

Level 3: Intermediate
On this level a country has the ability to create viruses and launch a lot of these types of attacks on smaller ICT networks. The viruses are not easily detected, but causes limited harm to the network systems. The damage can be covered, without big losses.

Level 4: Semi- Advanced
On this level a country can launch sophisticated cyber weapons on critical infrastructures, which can be detected and corrected before the whole system goes down and before it causes the society big harm. The damage is large, but does not effect the society yet.

Level 5: Advanced
On this level a country can create very sophisticated means, which cannot be detected by network administrators and virus-scanners. These sophisticated weapons causes harm to critical infrastructures and makes the network go down. This has a big negative effect on the society as a whole, because the critical infrastructures stop functioning.

2.4 The Theoretical Offensive Cyber Warfare Model

The theoretical model for assessing offensive cyber warfare capability of a country is described in this paragraph. As has been explained before only the categories Channel and Means are important for the assessment of cyber warfare capability. Looking at the analogy of an individual attacking another individual it becomes clear that the capability of the attacker is not determined by who the target is, but it is determined by the means (weapons) and channel (attack medium) he can access plus the ability to create and use these. The attacker's motivation level, the damage and method to attack do not determine his capability. When a person is motivated it does not mean that he is capable to attack. The damage the attacker can cause depends on the attack medium and weapons he uses, but also on the defense system of the target. So the damage is not a category that can explain offensive capability of the attacker. In the same way, only the categories Channel and Means are used to determine the offensive cyber warfare capability of a country. The direct indicators that can explain the offensive cyber warfare capability are included in figure 2.2. As this figure is too small there has been zoomed in and divided in two separate figures 2.2a and 2.2b. Within figure 2.2 not only indicators that explain ability to use and access, but also ability to create are included. The indicators showing ability to create are related to the digital knowledge base of a country, which is also important for the assessment of offensive cyber warfare capability of a country. As there is limited data for the direct indicators it was necessary to include indirect indicators in the model. As can be seen the red text in figures 2.2, 2.2a and 2.2b indicate the indirect indicators for which it was possible to find data. By going down to a lower level, first order and second order indicators, some indicators become macro level economic and social indicators like GDP and literacy rate. Based on the indirect indicators an approach for the model has been given in chapter 3.

For cyber warfare a country needs access to the digital channel and he must be able to use these as well. Further he must have access to the means, the ability to create the means and to use these. There are different methods to access the cyber warfare channel. These are:

- Use of digital communication devices
- Access to a wired network
- Access to a wireless network

All the indicators mentioned in figure 2.2 can contribute to the assessment of capability to access the channel of cyber warfare. Access to, use and creation of digital Channel can be assessed by the indicators in figure 2.2 a, which has been written in table 2.2 giving an explanation why these indicators can be used.

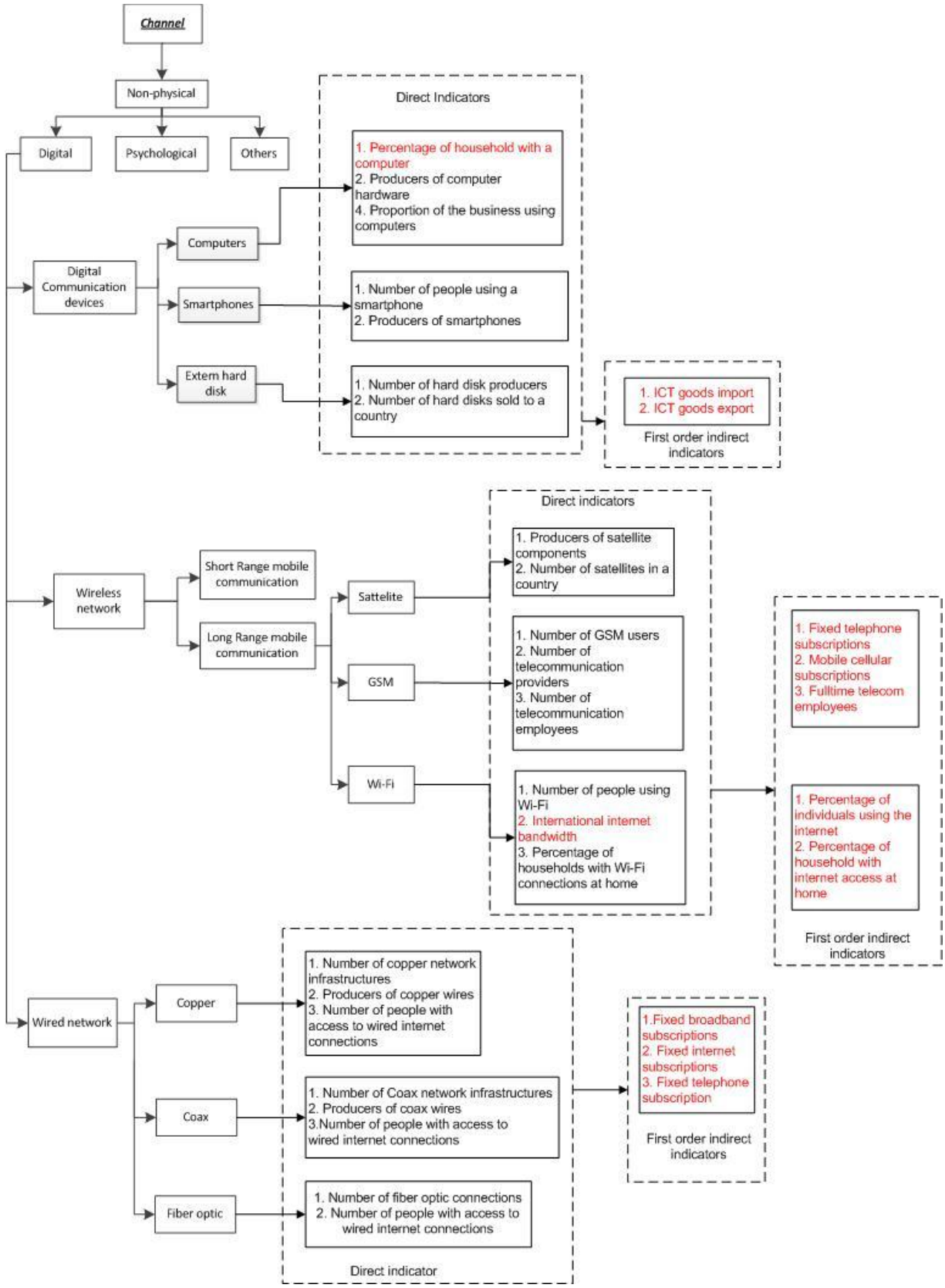


Figure 2.2 a Zoomed in on Channel (Theoretical model)

Table 2.2 Indicators Channel

Direct Indicators	**Explanation**
1. Percentage of household with a computer	A computer gives access to the digital channel. By knowing how many people uses a computer it becomes clear whether a country has a developed digital channel.
2. Producers of computer hardware	If there are producers of computer hardware, it is likely that the country has the knowledge to get involved in cyber exploitation.
3. Number of people using a computer	This indicator shows how many people can use a computer and thus how developed their digital channel is.
4. Proportion of the business using computers	If a large proportion of the business uses computers it is likely that this country has knowledge in house.
5. Number of people using a Smartphone	A Smartphone can give access to the internet creating opportunities for cyber attacks.
6. Producers of Smartphones	If a country has producers of Smartphones it means that they have knowledge in house.
7. Number of hard disk producers	A hard disk can be used to transfer a cyber weapon. Producers of these means digital knowledge in house.
8. Number of hard disk sold to a country	When more people uses extern hard disk, it means that the digital networks of that country are more developed.
9. Producers of satellite components	The country has digital knowledge, which can be used for cyber exploitation.
10. Number of satellites in a country	The higher the number of satellites the more developed the digital channel.
11. Number of GSM users	The higher the number the more developed the digital channel.
12. Number of telecommunication providers	This indicator indicates knowledge in house to create/ access/ use channel.
13. Number of telecommunication employees	This indicator indicates knowledge in house to create/ access/ use channel.
14. Number of people using Wi-Fi	This indicator tells something about the size and development of digital channel.
15. International internet bandwidth	Shows how developed the digital channel is.
16. Percentage of households with Wi-Fi connections at home	The indicator not only indicates the size and development of digital channel, but also higher chances for finding hackers.
17. Number of copper network infrastructures	When a country has copper infrastructures it is likely that they have access to the channel.
18. Producers of copper wires	When there are producers of copper wires, it is likely that such a country can afford copper infrastructures creating access t o the digital channel.
19. Number of Coax network infrastructures	The number of coax network infrastructures indicates how well developed the channel is.
20. Producers of coax wires	When there are producers of coax wires, it is likely that such a country can afford coax infrastructures creating access t o the digital channel.
21. Number of fiber optic connections	When a country has fiber optic connections it shows how developed their digital environment is.
22. Number of people with access to wired internet connections	This indicator shows how good the access to and use of the digital channel is.

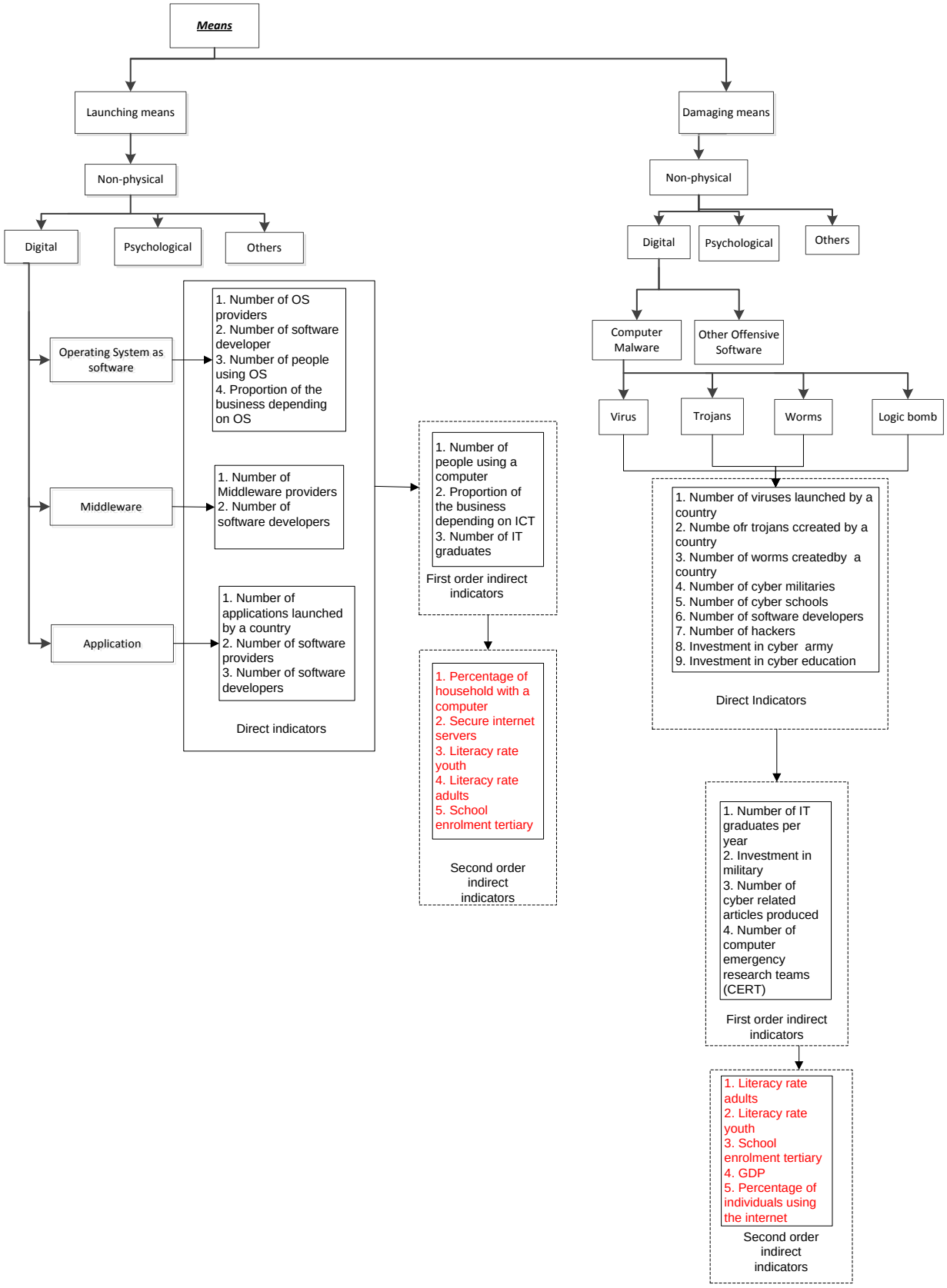


Figure 2.2 b Zoomed in on Means (Theoretical Model)

To attack in cyberspace a country needs cyber weapons, which can be found in the category of Means. The means can be divided into launching and damaging means, both of these means are digital for cyber weapons. By knowing whether a country has the means and whether they can create and use it, it becomes possible to determine its offensive cyber warfare capabilities. The indicators connected to the means shows whether a country can create, use and access the means by themselves. Looking at the past how many cyber attacks a country has executed, how many programmers a country have and the other indicators it becomes possible to assess the offensive cyber warfare capability.

Indicators that can explain the ability to access, use and create cyber warfare means are included in figure 2.2 and an explanation for why these can be indicators are included in table 2.3.

Table 2.3 Indicators Mean

	Direct Indicators	**Explanation**
1.	Number of OS providers	Indicates how many and how well developed the launching means are in a country.
2.	Number of programmers	Indicates whether there is knowledge to create cyber weapons
3.	Number of people using OS (operating system)	Indicates how many and how well developed the launching means are in a country.
4.	Proportion of the business depending on OS	Indicates how many and how well developed the launching means are in a country.
5.	Number of Middleware providers	Indicates how many and how well developed the launching means are in a country.
6.	Number of applications launched by a country	Indicates the ability to create cyber weapons.
7.	Number of software providers	Indicates ability to create cyber weapons
8.	Number of viruses, trojans, worms created by a country	This shows how capable a country is to initiate a cyber attack.
9.	Number of cyber attacks launched by a country	This shows the capability to initiate cyber attacks.
10.	Number of cyber militaries	This indicator also tells how well developed a county's army is in the field of cyber war.
11.	Number of cyber schools	This indicates the ability to create cyber warriors.
12.	Number of internet users	The total number of internet users shows how well developed the launching and damaging environment is.
13.	Number of hackers	Indicates how capable a country is to attack others in cyberspace.
14.	Investment in cyber army	The higher the investment the higher the opportunity to increase capability.
15.	Investment in cyber education	Higher investments give opportunity to create higher capabilities.

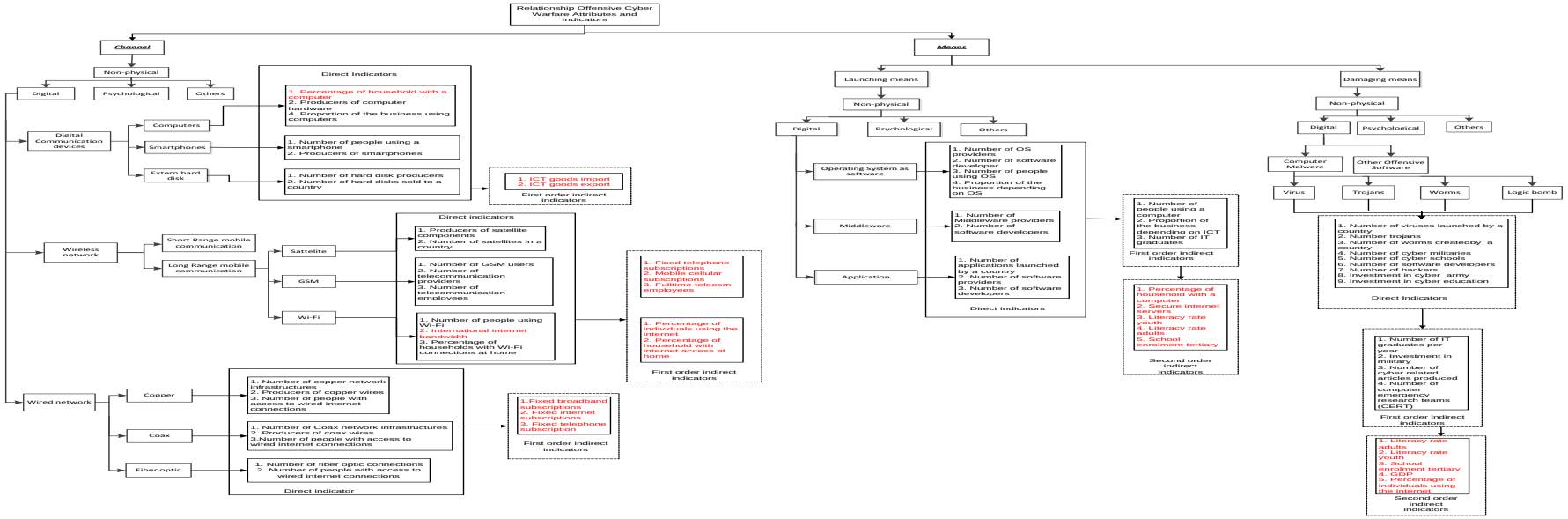


Figure 2.2 Relationship Offensive Cyber Warfare Attributes and Indicators

As access to data for the indicators mentioned in the theoretical model are limited it is not possible to execute a statistical analysis on the direct indictors to find the practical assessment model. The following chapter, chapter 3, gives an approach of a model involving the necessary statistical analysis to be performed.

2.5 Conclusions

Within literature there are many definitions given to cyberspace and cyber warfare. In this chapter the offensive cyber warfare attributes are described in a diagram showing the process of offensive warfare. This diagram has been defined based on an analogy of individuals in war and based on literature about traditional warfare. Within this diagram only offensive cyber warfare attributes are in details, because this is necessary for further research. Based on this diagram a distinction between offensive cyber warfare and traditional warfare can be made. The process of offensive cyber warfare has been explained by 6 categories, which are Motivation, Target, Channel, Means, Methods and Damage. These categories are defined based on analogy of an individual in war and some literatures about traditional warfare. Based on 2 of these categories the direct indicators for assessing offensive cyber warfare are identified, which can be seen in figure 2.2. The two categories that can explain capability are Channel and Means. In figure 2.2 the theoretical model for assessing offensive cyber warfare capability has been given.

The diagram showing the process of offensive warfare can be seen in appendix 1. The main offensive cyber warfare attributes based on the diagram are:

- To get involved in cyber warfare a country needs access to and knowledge about the digital channel.
- In cyber warfare a country needs digital means to attack others.
- A country has a motivation to initiate a cyber attack.
- The targets of cyber warfare are critical information infrastructures of countries.
- The damage caused during cyber warfare are digital, but can also be physical and psychological.
- The methods used during cyber warfare are digital.

To get a view in capability growth the maturity level for offensive cyber warfare are described, which consists of 5 levels: beginners, semi-intermediate, intermediate, semi-advanced and advanced. Due to limitation of data it is not possible to make a model based on direct indicators. In chapter 3 only an approach of the model has been given based on indirect indicators for which it was possible to find data.

3. An Approach of a model

In this chapter an approach of a model has been given based on statistical analysis. The software tool that has been used for the statistical analysis is SPSS. However it is also possible to use other statistical tools like SAS and others. In chapter 2 within the theoretical model the direct indicators are included. As access to data for these indicators are limited, the approach has been made based on the indirect indicators mentioned in figure 2.2. The data has been collected from different publicly available sources. The cut-off points for each maturity level have been described. Based on the results of the test some interpretations have been made about the offensive cyber warfare capability of countries as regions.

3.1 Methodological approach to statistics

The methodological approach for the analysis and design of the model involves the steps that have been followed to develop the model, which has been discussed here:

1. The first step is finding the publicly available indicators for offensive cyber warfare attributes, which has been done in chapter 2. As access to statistical data was limited indirect indicators are used. For each indicator the averages of the years 2005 until 2008 have been used for the analysis, because data for 2009 until now is not available. There are countries with at least one year reported and still the averages are used. Data older than 2005 would not be representative and too old to use, since cyber warfare is a new field in development.

2. The second step was to find a dataset for the offensive cyber warfare capability as the dependent variable. As there is no such data, a proxy variable has been used as the dependent variable. This data set is needed to do the statistical analysis and find a relationship between indicators as the independent variable and offensive cyber warfare as the dependent variable.

3. The third step was normalizing the dataset by converting the values into z-scores. On the standardized values of the proxy variable and the indicators a correlation analysis was performed to see the relation between the two variables.

   Standardizing a variable is done when the values of the variables are from different scales. So the observed values of a variable becomes a z-score (standard score) after it has been standardized, so the mean gets the value 0 and the standard deviation becomes 1. By standardizing each variable, their contribution to the mean becomes equal (Standardizing Variables). Z-Scores show the position of a particular score with respect to the mean, so this value can be the same as the mean or lower than the mean or higher than the mean of a group of scores. The **standard deviation** is a method to

find out how the observed values are bunched around the mean of the dataset. When the observed values are clustered highly the standard deviation is small, but when the observed values are spread the standard deviation is high (Standard Deviation Definition | Investopedia).

Correlation is a statistical method that can tell us how variables are related to each other. The correlation coefficient, which is the result of a correlation analysis, has a range from -1.0 to +1.0. When the coefficient is near to +1 or -1, the relationship between the variables are said to be very close. *"If r is close to 0, it means there is no relationship between the variables. If r is positive, it means that as one variable gets larger the other gets larger. If r is negative it means that as one gets larger, the other gets smaller (often called an "inverse" correlation)* (Correlation - Statistical Techniques, Rating Scales, Correlation Coefficients, and More - Creative Research Systems, 2010)*."*

4. The fourth step was a factor analysis on all the indicators that a have significant correlations among themselves. In order to use these indicators as the independent variable a factor analysis is performed to find factors that do not correlate with each other. The aim of factor analysis is to find a pattern in the relationships among the variables. "*It tries to find out if it is possible to explain the observed variables in terms of a much smaller set of variables called factors* (B.Darlington)*."* The reason for working with hypothetical variable or factor is to reduce the dimensionality, because if the dimension is reduced the structure in the data will become clear. The factors suggest that there is something underlying in the dataset, which is discovered. (Bartholomew & Knott, 1999) Factor analysis is executed by investigating the pattern of correlation between the observed variable. *"Measures that are highly correlated (either positively or negatively) are likely influenced by the same factors, while those that are relatively uncorrelated are likely influenced by different factors* (J.DeCoster, 1998)*."* To do the factor analysis (FA) Principal component analysis, one of the forms of FA, has been used.

   Cronbach's alpha is used to see whether there is internal consistency in the group, thus whether the variables are closely related. If the alpha is high these variables do measure an underlying variable. Usually alpha > 0.7 is used in social science research (UCLA Academic Technology Services). In this research also alpha > 0.7 has been used.

   The Bartlett's test of Sphericity is used to find out whether the correlation matrix is an identity matrix. In an identity matrix the values on the diagonals are all one's and off the diagonal they are all zeros. This means that the variables are not correlated and Bartlett's test of Sphericity will not be significant. This would mean that the factor analysis cannot be done, because the factors will not load properly as there is no correlation. So the Bartlett's test of Sphericity must be significant in order to the Factor

analysis. (Chapter 14; Factor Analysis, Path Analysis, and Structural Equations Modeling, 2009) The Kaiser-Meyer-Olkin (KMO) measure determines whether a factor analysis is allowed after looking at the correlation of the observed variables and the partial correlations. KMO can vary from 0 to 1 and when it is smaller than 0.5 factor analyses is not allowed.

5. The fifth step was a regression analysis between the factors and the proxy variable. Regression analysis involves various methods for modeling and examining variables to find a relationship between a dependent and one or more independent variable. Based on a multiple linear regression analysis it is possible to explain how the value of the dependent variable modifies when one independent variable varies, whereas the others are held constant (Joseph F. Hair; Rolph E. Anderson; Ronald L. Tatham; William C.Black, 1995) (D.Myers). In this research offensive cyber warfare capability is the dependent vaiable that needs to be explained in terms of independent variables. In order to find a relationship between offensive cyber warfare capability and the factors and to see how each factor effects the offensive capability, multiple linear regression has been used.

6. The sixth step was testing the equation that resulted from step five. For the test the datasets for 2009 have been used. This test is done in order to see how the countries can be ranked based on their offensive cyber warfare capability. This test should give results where the United States is at least in the 10% range of the countries with high capability and Congo in the least capable 10%, as has been stated in the assumptions in chapter 1. Some countries are mentioned frequently in cyber war literature, like Russia, China and Israel, but they do not say if they are speaking about dangerous countries or capable countries. That is why it was not possible to include other prospective countries as high capable. However, countries in similar situation as Congo are expected to have low capability as well.

7. The last step is to define the offensive cyber warfare capability ranges for the maturity levels based on the results from the test. Maturity level gives an indication how capable a country is. A country can be a beginner, semi-intermediate, intermediate, semi-advanced and advanced.

3.2 Cyber Warfare capability indicators

A distinction can be made between direct and indirect indicators. Within figure 2.2 the direct indicators and the indirect indicators are included. Unfortunately the direct indicators cannot be used for the development of the model, because access to such datasets is limited. That is why the assessment model is based on the indirect indicator of figure 2.2. These indicators as the independent variable will explain offensive cyber warfare capability as the dependent variable. As can be seen in table 3.1 the list of the indicators for offensive cyber warfare capability has been given. In appendix 5 the definitions for each indicator has been given including the sources of the statistical data. In table 3.2 an explanation has been given why these indicators can be used to assess offensive cyber warfare capability. The indicators should have a significant correlation with the proxy variable in order to be used for further analysis, because a relationship between them is sought. Indicators that do not have a significant correlation are excluded.

Table 3.1 Offensive cyber warfare capability indicators

Indicator
1. Fixed Broadband subscriptions per 100 inhabitants
2. Fixed internet subscriptions per 100 inhabitants
3. Fixed telephone subscriptions per 100 inhabitants
4. Mobile cellular subscriptions per 100 inhabitants
5. Percentage of individuals using the internet
6. Fulltime telecommunication employees
7. International internet bandwidth
8. Percentage of household with a computer
9. Percentage of household with internet access at home
10. Secure internet servers
11. GDP
12. ICT Good import
13. ICT Good export
14. Literacy rate adult
15. Literacy rate youth
16. School enrollment tertiary

Table 3.2 Offensive cyber warfare capability indicators and an explanation

Indicator	***Explanation why it is a indicator for Cyber warfare capability***
1. Fixed Broadband subscriptions per 100 inhabitants	This indicator is connected to the possibilities for launching an attack. It is also connected to hackers, because it is likely that they will use fast internet connections to initiate an attack.
2. Fixed internet subscriptions per 100 inhabitants	This indicator is connected to attacks and hackers, because access to internet gives opportunity to learn about cyber attacks.

3. Fixed telephone subscriptions per 100 inhabitants	Within the definition of this indicator it is said that VoIP subscribers are included. So this indicator also gives an indication whether or not a country has access to internet.
4. Mobile cellular subscriptions per 100 inhabitants	The actual indicator that should be here is mobile subscriptions with internet connections. As the access to such a dataset was limited, this indicator has been used. Because a mobile subscription gives the possibility to at least access internet, for example home Wi-Fi of a friend. It makes it possible to read more about hacking. At least a start towards cyber awareness.
5. Percentage of individuals using the internet	Internet is a must in cyber warfare. When a large percentage of individuals in a country use internet, it is more likely that this country can find experts for creating cyber weapons.
6. Fulltime telecommunication employees	Because it was not possible to find a dataset for number of programmers, this indicator is used to give an indication whether a country has the ability to attack. The higher the number of telecommunication employees, the higher the chance that at least one of them can create cyber weapons.
7. International internet bandwidth	The higher the international bandwidth used by country, the more developed the country is. This indicator shows the capacity of international connections between countries for transmitting Internet traffic, which is needed to launch a cyber weapon. The higher, the more ability a country has.
8. Percentage of household with a computer	To go into cyber war a country needs computers. If the number of computers in a country is high, it is likely that the country can find good programmers to create cyber means.
9. Percentage of household with internet access at home	Access to internet gives possibility to learn and read more about cyber attacks. It gives the country a possibility to educate its nation through it. Plus it gives the opportunity to create cyber warriors.
10. Secure internet servers	High number of secure internet servers shows that the country is more aware about cyber war.
11. GDP	This indicator is related to whether a country can invest in cyber education.
12. ICT Good import	Based on this indicator it is possible to see which countries have high imports and which low. High import means that a country has the money to buy ICT equipments, but they do not have the knowledge in house to create it.
13. ICT Good export	If a country exports ICT goods, it has high educated people creating the ICT services. The ICT knowledge, skills and access is very high in such a country. It is likely that they can create cyber weapons by themselves.
14. Literacy rate adult	When the adult literacy rate is high, it is more likely that they have the ability to read and learn about cyber war and creating cyber weapons.
15. Literacy rate youth	When the adult literacy rate is high, it is more likely that they have the ability to read and learn about cyber war and creating cyber weapon.
16. School enrollment tertiary	This indicator tells how many inhabitants have the potential

	to read, write and thus be able to learn about Cyber war.

The data for these indicators are selected from **International Telecommunication Union Information and Communication Technology** (ITU, ITU Information and Communication Technology, 2012) (ITU, The World Telecommunication / ICT indicators database, 2011) and from **The World Bank** (The World Bank Group, 2012).

3.3 Selecting the values for the dependent variable

In order to do a statistical analysis it is necessary to collect or find data from public sources for the dependent variable offensive cyber warfare capability. Such a dataset is not available thus a proxy variable has been used. Based on the 2 classifications Channel and Means it seems important to have *skills of/access to/use of channel* and *skills of/access to/use of means* in order to launch a cyber attack. Based on these two the indicators in figure 2.2 have been identified.

A proxy variable is a quantifiable variable which can be used as replacement for the theoretical variable that cannot be measured (Pedhazur & Schmelkin, 1991). Based on literature review and the derived diagram the most important attributes for defining offensive cyber warfare capability are *skills of/access to/use of* the channel (digital) and the means (digital). The most closely related variable that could be used as a proxy variable is the ICT development index as this is based on use of ICT, access to ICT and ICT skills.
As described previously in this chapter, there is a list of indicators that can explain offensive cyber warfare capability. ICT development index is also based on indicators and some of these are the same for offensive cyber warfare capability.

The ICT development index is a good proxy, because the offensive cyber warfare capability is strongly based on high level of ICT knowledge, ICT use and access to ICT tools/services. The ICT development index does tell how developed the ICT is within in a country. All these are needed for offensive cyber warfare, but there are more indicators that can explain offensive cyber warfare than what has been included in the ICT development index only.

What actually has been done in order to develop the model for offensive cyber warfare capability is making some assumptions regarding the ICT development index, which are:

- ICT development index is a good proxy variable
- The ICT development index is a data collection method for the dependent variable

The ICT development index of 2008 has been used since the average of 2005 until 2008 for each indicator has been taken for the analysis. Access to ICT development index of 2005 until 2007 was limited. The ICT development index has been designed based on 11

indicators from which 9 indicators are the same for offensive cyber warfare. For the assessment of offensive cyber warfare there are 16 indicators, so 7 of these are not used for the ICT development index. The ICT development index has a significant correlation with all the 16 indicators. The indicators from table 3.1 and the ICT development index will be used to find a model to assess offensive cyber warfare capability. Figure 3.1 gives the process of analysis to design the model, which result in an equation.

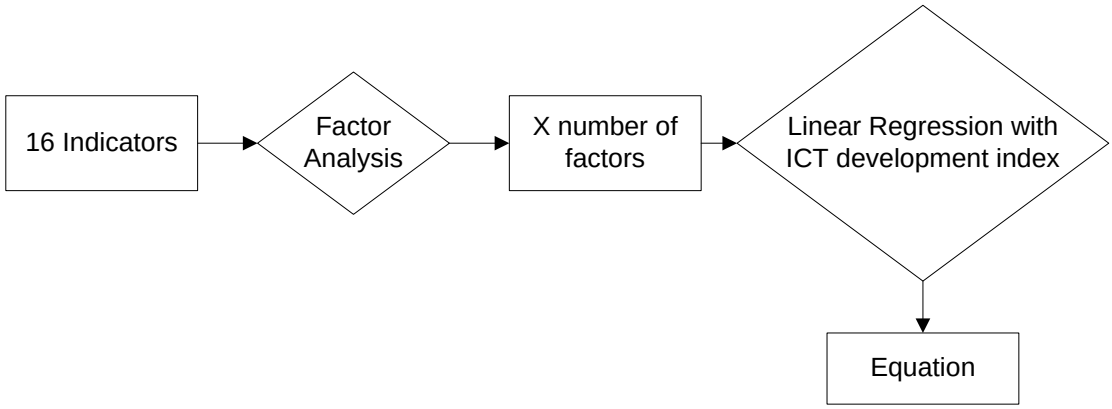


Figure 3.1 Process for model design

Using the 16 indicators from table 3.1 a factor analysis is done. From this analysis we get some factors. Using these factors as the independent variable, linear regression has been done with the ICT development index (proxy variable) as the dependent index.
From this we get an equation, which assess offensive cyber warfare capability.

3.4 Results

In this part of the chapter the results can be found that have been collected from the statistical analysis within SPSS.

3.4.1 Correlation

The data for the variables are gathered from the ITU and World Bank. For each variable the average for 4 years (2005-2008) are taken. The year 2009 is the test year. The ICT development index of the year 2008 has been used as the proxy variable. Before starting the statistical analysis the datasets (all the dependent and independent variable) were saved as normalized variables within SPSS.

The next step was finding significant correlation between the indicators and the ICT development index. The indicators that have a significant correlation with the ICT development index have been used. Based on a correlation analysis between indicators and ICT development index, the indicator annual investment and telecommunication services

were removed from the list. In the table below, the indicators in the yellow boxes are the same indicators used for the ICT development index. Only 2 indicators of the ICT development index are not in the list for offensive cyber warfare capability, which are: Active mobile broadband subscriptions per 100 inhabitants and Secondary gross enrollment ratio. The ICT development index is made from 11 indicators in total; 9 of these indicators are the same for offensive cyber warfare capability. There are also 7 other indicators for assessing offensive cyber warfare capability, which also have a significant correlation with ICT development index, which can be seen in the correlation table of ICT development index and the offensive cyber warfare capability indicators (see appendix 2). In table 3.3 the 9 indicators that are the same for the ICT development index are in yellow boxes.

Table 3.3 ICT development index's indicators in 9 yellow boxes

Indicator
1. Fixed Broadband subscriptions per 100 inhabitants
2. Fixed internet subscriptions per 100 inhabitants
3. Fixed telephone subscriptions per 100 inhabitants
4. Mobile cellular subscriptions per 100 inhabitants
5. Percentage of individuals using the internet
6. Fulltime telecommunication employees
7. International internet bandwidth
8. Percentage of household with a computer
9. Percentage of household with internet access at home
10. Secure internet servers
11. GDP
12. ICT Good import
13. ICT Good export
14. Literacy rate adult
15. Literacy rate youth
16. School enrollment tertiary

3.4.2 Factor Analysis: Principal component analysis

The indicators of table 3.1 have significant correlation with the proxy variable. To find the underlying variable (factor), which causes the strong correlation among the indicators, principal component analysis has been used. Before extracting the factors the correlation between the indicators, KMO and Alpha has been determined. In appendix 2 the correlation table has been included. All indicators have a significant correlation with the proxy variable. As can be seen in the table 3.4 the Bartlett's Test is significant, KMO is larger than 0.5 and Cronbach's Alpha is > 0.7, which means a factor analysis is allowed on these variables.

Table 3.4 KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.647
Bartlett's Test of Sphericity	Approx. Chi-Square	634.094
	df	120
	Sig.	.000

Table 3.5 Reliability Statistics

Cronbach's Alpha	N of Items
.874	16

After the factor analysis 4 components or factors are produced. These 4 are chosen based on the eigenvalue >1, KMO > 0.5 and indicators with factor loading > 0.5. For each factor the indicators' loadings are different. This can be seen in appendix 3, in the rotated component matrix. Rotation just rotates the plane, because the factors get more sense then. In this component matrix the component loadings can be observed, the higher the loadings, the higher the correlation of the indicator with that component.

3.4.3 Regression Analysis

The 4 factors that were produced during the factor analysis are used as independent variable for the regression analysis. During the analysis the following table has been found:

Table 3.6 Coefficients[a] (average from 2005 until 2008)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.418	.026		-16.038	.000
	REGR factor score 1 for analysis 1	.386	.026	.590	14.587	.000
	REGR factor score 2 for analysis 1	.458	.026	.700	17.304	.000
	REGR factor score 3 for analysis 1	.094	.026	.144	3.567	.001
	REGR factor score 4 for analysis 1	.205	.026	.314	7.751	.000

a. Dependent Variable: Zscore(ICT_Development_Index)

B in table 3.6 is the weight of each factor on the dependent variable. All the B values are significant as can be seen in the last column of table 3.6. From this table the equation for assessing offensive cyber warfare capability has been found:

$$y = 0.386\ factor\ 1 + 0.458\ factor\ 2 + 0.094\ factor\ 3 + 0.205\ factor\ 4 - 0.418$$

y = offensive cyber warfare capability
Factor 1, 2, 3 and 4 are the 4 components that has been found during the principal component analysis

One unit increase of factor 1 causes an increase of 0.386 in the offensive cyber warfare capability. One unit increase of factor 2 causes an increase of 0.458 in the offensive cyber warfare capability and so on. Beta shows how well the independent variables correlate with the dependent variable; in fact it is the correlation coefficient between both. Factors 1 and 2 have high correlations, while factors 3 and 4 not. This is caused by Beta, which shows the correlation coefficient of the factors (grouped indicators) with the dependent variable (ICT development index). The indicators in factor 1 and 2 have higher correlation with the ICT development index than factors 3 and 4.

The numbers of years included in the research analysis are now extended to see whether this will have an effect on the equation. Here the averages of 2005 until 2009 are used for the analysis. The same steps (from the methodology) are executed to find the equation. The factor analysis resulted in factor scores, which have been used as the independent variable during the regression analysis. These are the results that have been found:

Table 3.7 Coefficients[a] (average from 2005 until 2009)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.187	.021		-9.046	.000
	REGR factor score 1 for analysis 1	.572	.021	.755	27.428	.000
	REGR factor score 2 for analysis 1	.081	.021	.108	3.906	.000
	REGR factor score 3 for analysis 1	.449	.021	.597	21.673	.000
	REGR factor score 4 for analysis 1	.107	.021	.142	5.173	.000

a. Dependent Variable: Zscore (ICT_Development_Index)

As can be seen there is a change in value of B, which will have an influence on the results of offensive cyber warfare capability. This difference can be explained by the component score coefficient table. The weights of each indicator and their factor loadings are slightly different than when the analysis was done with the average from 2005 until 2008. This has influence on the end results of the model. Another reason for the differences can be explained by the fact that during this analysis there were 71 valid cases from 199 (these are the total number of countries). In the previous analysis (using averages from 2005-2008) there were only 31 valid cases. A case-wise deletion has been used and the averages have been calculated for countries with at least one year reported (see example in appendix 7). That's why extending the years gives less missing data.

As a test year was needed, it was necessary to work with the averages of 2005 until 2008 and use 2009 as the test year. For some indicators there is no data for 2010 that's why 2010 could not be used as a test year.

3.5 Test

To test the model the dataset for all indicators for the year 2009 has been used. In order to find the factor scores for 2009 the component coefficient matrix in appendix 4 has been used. The factor scores are a linear combination of the indicators and the component score coefficient (Gerda M. van den Berg). The component score coefficient gives the weight of every indicator on the factor scores.

Formula Factor Score:

$$FS = a1 * I1 + \cdots + aj * Ij$$

FS = Factor Score
a = component score coefficient (appendix 4)
I= indicator value

To obtain the factor scores for the test year 2009 the formula for factor scores has been used. These factor scores are the independent values and are substituted in the model equation of offensive cyber warfare capability. This gives the results for offensive cyber warfare capability. Based on the results from the equation, the ranking of the countries for 2009 have been found; this can be seen in appendix 6.

3.5.1 Cut-off points maturity levels

The maturity levels are already described in chapter two. In this chapter only the values have been given to each level. Based on normalization, the value range for offensive cyber warfare capability lies between -1.5 and 1.5.
Thus the range is -1.5 < offensive cyber warfare capability < 1.5. But as the minus sign might be confusing for interpretations the value range had been converted to positive by the following steps:

- First the range has been divided by 1.5 resulting in -1< offensive cyber warfare capability < 1.
- Secondly a value of 1 has been added to the results of the first step giving a range of 0 < offensive cyber warfare capability < 2.
- The highest OCW after the first two steps is 1.6 (Hong Kong). The normalized values should lie between 0 < OCW capability < 1, so all the values are divided by 1.6.

The final range used for making interpretation is 0 < offensive cyber warfare capability < 1. There is no such theory to explain the cut-off points for the maturity levels, so equal divisions for the ranges have been made. The cut-off points are given in percentages of the range 0 < offensive cyber warfare capability < 1. Each level gets 20%, which gives the following ranges for the different maturity levels:

Based on figure 3.2 the following ranges for the maturity levels can be found:
Level 1: Beginners (OCW ≤ 0.200)
Level 2: Semi-intermediate (0.200 < OCW ≤ 0.400)
Level 3: Intermediate (0.400 < OCW ≤ 0.600)
Level 4: Semi- Advanced (0.600 < OCW ≤ 0.800)
Level 5: Advanced (0.800 < OCW ≤ 1)

OCW stands for offensive cyber warfare capability and this abbreviation will be used further in this report. The final offensive cyber warfare capability model with maturity levels can be seen in figure 3.2.

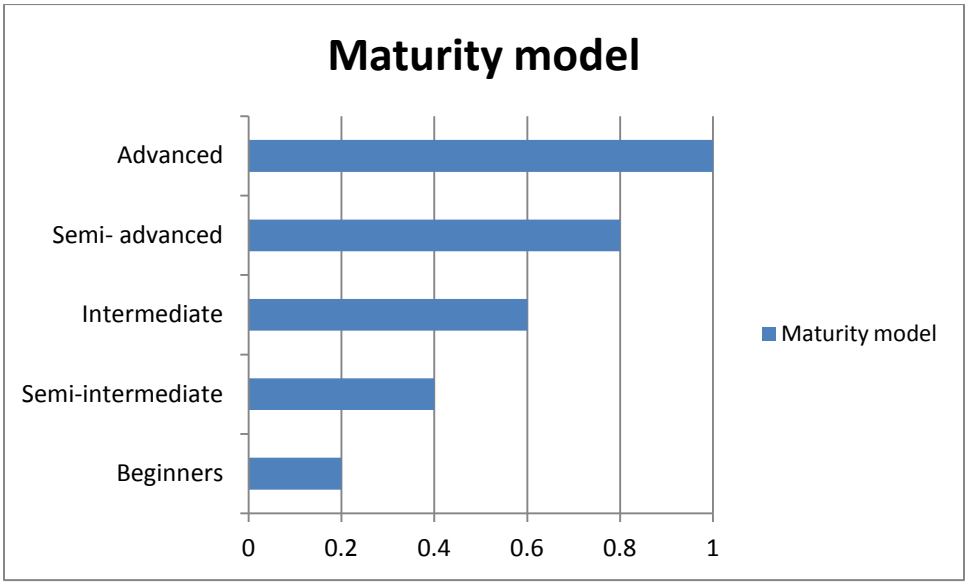


Figure 3.2 Offensive Cyber Warfare Capability Maturity model

3.5.2 Interpretations

In appendix 6 the Offensive Cyber Warfare Capability Ranking of countries can be seen. The appendix starts with the strongest and goes down to the weakest countries. The first country is the most offensive capable and the last one in the less offensive capable. This has also been placed in a chart in figure 3.3 starting with Hong Kong as the most capable and United States as the second strongest. As can be seen in appendix 6, most African countries have low scores, because a lot of countries in Africa belong to the category of developing or least developed countries (United Nations, 2012).

Making the assumption that the offensive cyber warfare capability was the same as the proxy variable in the year 2008, we can compare the results of 2009 with 2008. In 2008, United States was not even in the top 3 of offensive capable countries. When the model is

tested for the year 2009, United States is on the second place among all the countries for which it was possible to do the assessment. Within the threat intelligence report of McAfee USA has been reported frequently in the list of top intrusion attackers. According to the result of the test of this model USA is high in the list.

The result shows that Congo has the lowest score and countries that do not have developed infrastructures or whose infrastructures were destroyed and damaged during wars in late 1990s or even by earthquake, also have low scores e.g. Afghanistan, Haiti and others as can be seen in appendix 6. As can be seen in appendix 6, countries like Hungary and Slovenia are high on the list among the countries that are included in the assessment. This is caused by some indicators that have high values for these countries and also by the high B weight on the factors, in which these indicators are included. Slovenia has high capability, because of high literacy rate and tertiary school enrollment, which is incorporated in factor 2 having a high B weight. Hungary has high literacy rate, but also high percentage of individuals with internet access and ICT goods export which is incorporated in factor 1 and 2. The B's of these two factors are high, as can be seen in table 3.6.

The results in appendix 6 are influenced by the number of valid cases during the design of the equation. Furthermore, some of the indicators are general to explain offensive cyber warfare directly, but there is a link between them as can be seen in figure 2.2. Also the averages of at least one reported year are used, as has been shown in appendix 7 for the indicator 'fixed internet subscriptions per 100 inhabitants'. Averages give the most representative values when the observed values are very close and do not differ a lot from each other. The values over the years do differ and still the averages are used. However, it was necessary to execute the analysis with averages, because there are 16 indicators and finding countries with all the data was not possible. However, the equation gives valid results as can be seen in appendix 6 and as had been assumed (developed countries higher capability than least developed countries).

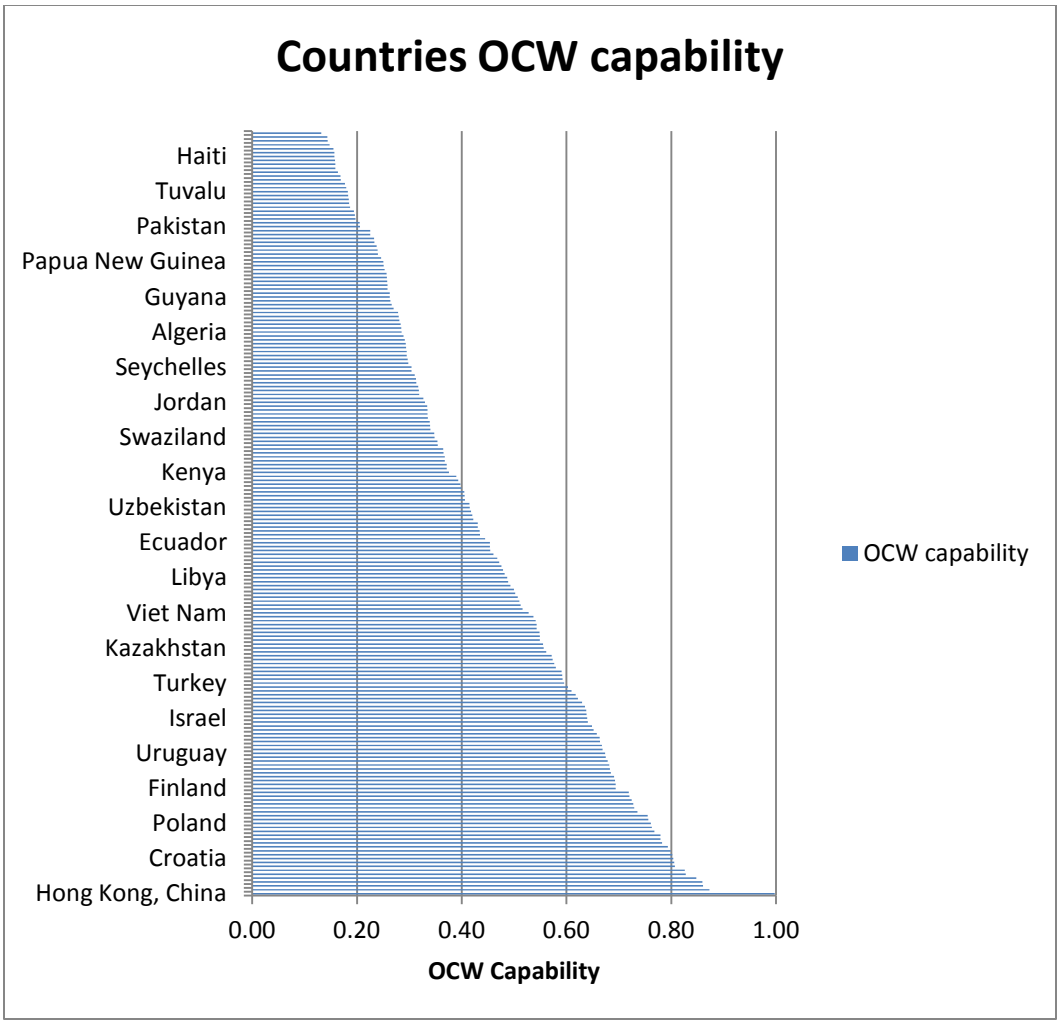


Figure 3.3 Offensive cyber warfare capabilities of countries in 2009

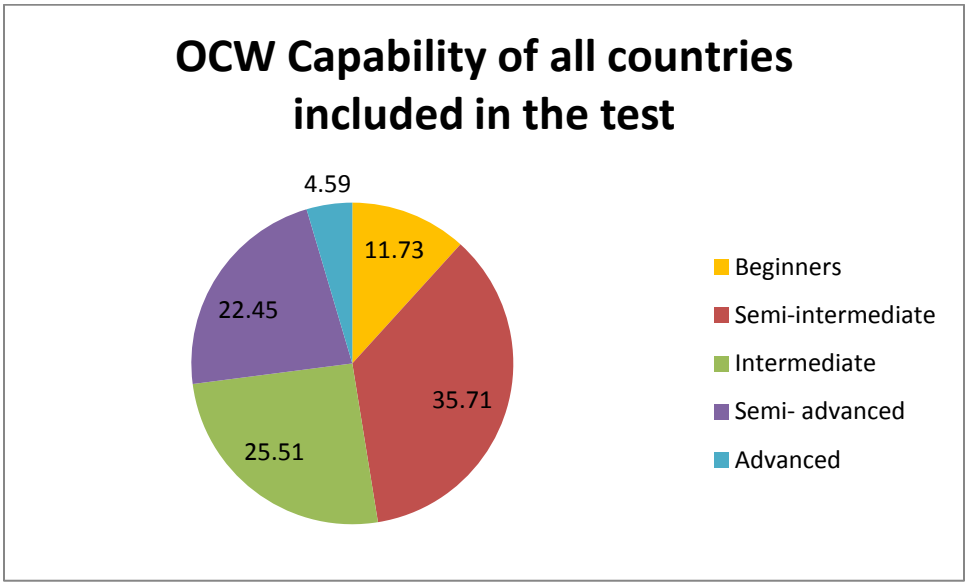


Figure 3.4 OCW Capability levels of all countries included in the test

There are 196 countries for which it was possible to assess their OCW capability using the model equation. There are not many countries in the advanced level compared to the other levels (see fig. 3.4). The countries in the advanced level are the countries with the highest capability. There are also not many in the beginners group. Largest group of countries belong to semi-intermediate. This can be explained by the fact that there are more developing countries than developed countries and also by increasing use of internet.

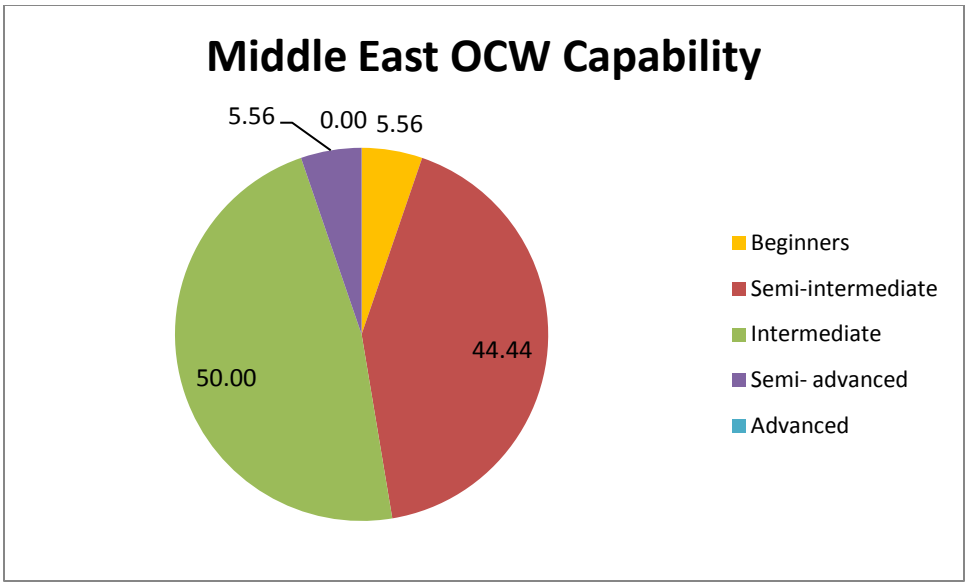


Figure 3.5 Middle East OCW Capability Levels

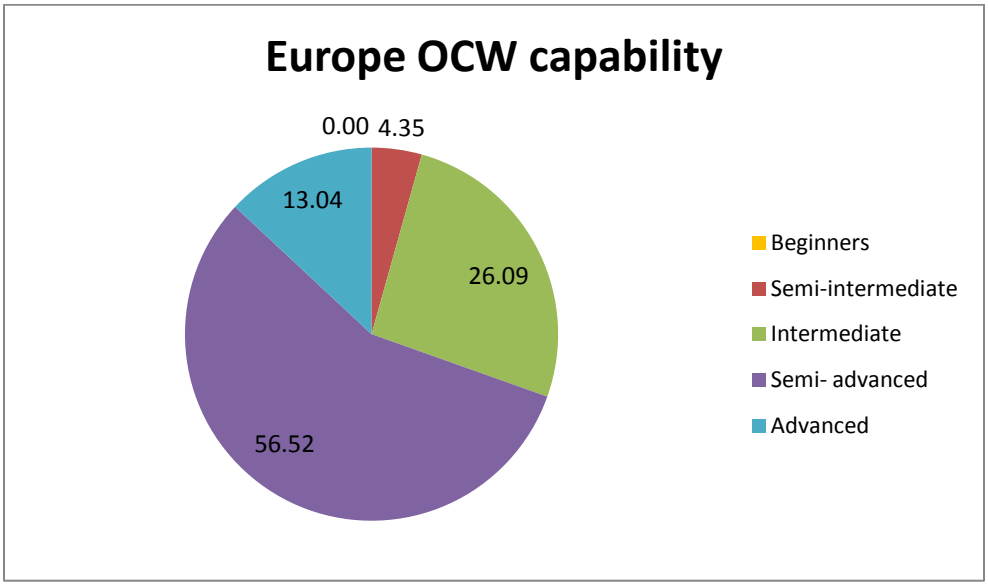


Figure 3.6 Europe OCW Capability Levels

As can be seen in figure 3.5 Middle East countries have no advanced countries and only one semi-advanced country, which is Israel (5.56%). This means that most of these countries' capabilities are lower than those of Europe (figure 3.6). Figure 3.6 shows that there are no countries in Europe that can be placed under the category of beginners. Some countries are semi intermediate, which are Azerbaijan and Albania as has been showed by the 4.35%. Most of them are semi-advanced. Most European countries are more capable than Middle East countries, because most European countries are more developed.

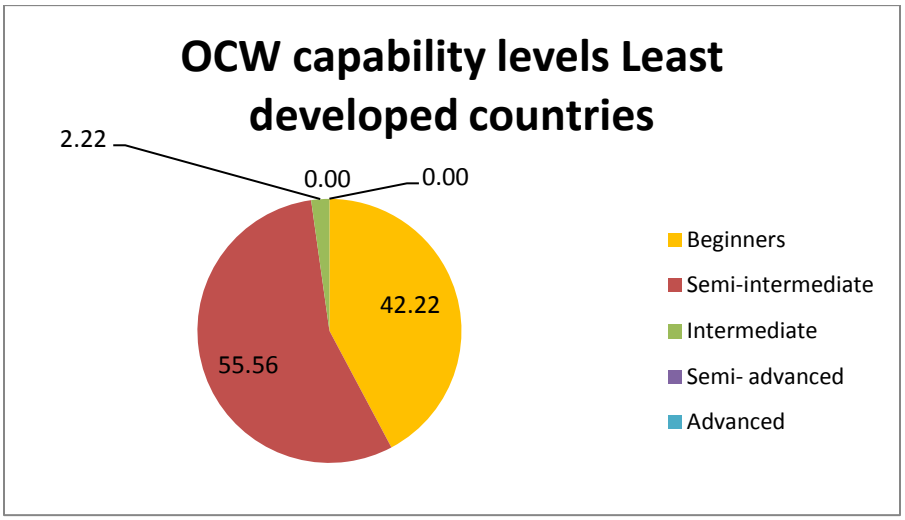


Figure 3.7 OCW Capability levels least developed countries

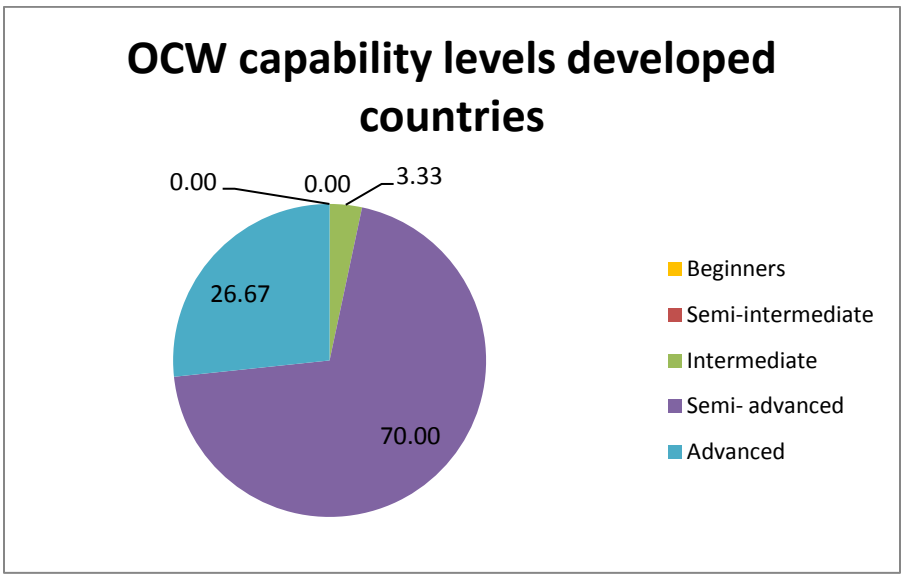


Figure 3.8 OCW Capability levels developed countries

As can be seen in figure 3.7 and 3.8, least developed countries are less mature in cyber warfare than developed countries.

3.6 Conclusion

In this chapter an approach of a model has been given for assessing offensive cyber warfare capability of a country. The steps that have been followed are added in figure 3.9. The model that has been found in this chapter is a first approach to the final model. The model is an equation based on a proxy variable and indirect indicators explaining ability to access, to use and skills to create channel and means, which assesses offensive cyber warfare capability:

$$y = 0.386\ factor\ 1 + 0.458\ factor\ 2 + 0.094\ factor\ 3 + 0.205\ factor\ 4 - 0.418$$

Finding data for indirect indicators has been difficult as well, but there are 16 indicators for which data has been found. The results of the test in appendix 6 are influenced by the number of valid cases during the design of the equation. Furthermore, some of the indicators are too general to explain offensive cyber warfare directly. However there is a link between them as can be seen in figure 2.2.

Developed countries have higher offensive cyber warfare capability according to this equation, which also had been expected because of the indicators that has been used like GDP. The approach of the model is influenced by macro level economic and social indicators like GDP and literacy rate. The research is based on 4 years (2005 until 2008) and the averages of these years are taken. The averages have been calculated for countries with even only one year reported. This might have affected the equation and thus so the results during the test, but the results are valid as they meet the assumptions made during the research. The equation fulfills its intended purpose as a first approach of a model assessing offensive cyber warfare capability of countries, which is based only on public data.

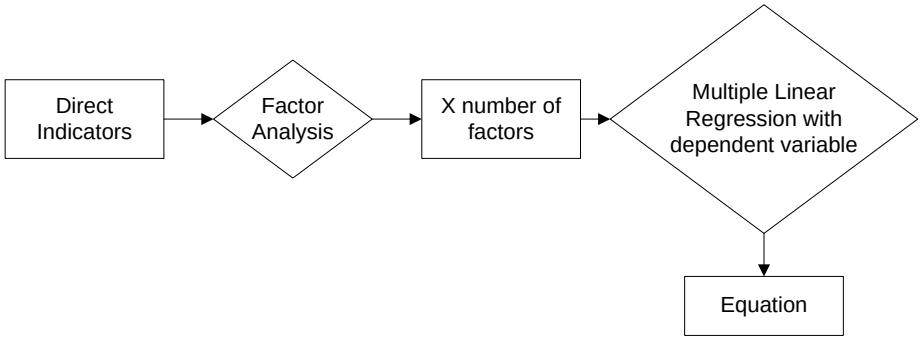


Figure 3.9 Steps for statistical analysis

Based on the equation and the results of the test the cut-off points for the maturity levels have been defined for which equal divisions of 20% are taken as there is no such theory describing these points.

4. Reflection

In this part a reflection on the research will be given. The aim of this research is to provide an approach of a maturity model to assess offensive cyber warfare capabilities of countries based on public data, by which governments can make better decisions and policies to prepare themselves for cyber war. Why public data, because access to a countries' secret data is limited and the upcoming trend of open source information stimulates use of public data for intelligent findings. As there is no literature describing the offensive cyber warfare attributes clearly and specifically, it was important to build the theory for cyber warfare attributes. During the research a diagram describing the process of offensive warfare has been developed, in which only offensive cyber warfare has been specified. The diagram clearly shows the difference between traditional and cyber warfare. The attributes of offensive cyber warfare are derived from the diagram, which has been used to provide a theoretical model for the assessment of offensive cyber warfare. The direct indicators that can explain the different cyber warfare attributes are put together in a model. In this theoretical model only the categories Channel and Means are included as these are the categories showing capability level. In further research motivation level can be included in the model, because then the model will predict the most dangerous or threatening countries.

As access to data is limited it is not possible to perform statistical analysis on the direct indicators of the theoretical model. Therefore, some indirect indicators are included based on which an approach of a model has been given involving the statistical steps that need to be performed. The result of this approach is based on limited data; the average of 2005 until 2008 has been used as there was not enough data for 2009 until 2011 and using data before 2005 is not representative as it is too "old". By old is meant that cyber warfare is a new developing field and thus data before 2005 might not be representative. Using the averages has influenced the approach, because for some countries averages of at least one reported year are used. Some of the indicators, like GDP, are too general and a proxy variable has been used for an approach of the model; this approach of the model for assessing offensive cyber warfare capability can be seen as a first set up for further research.

Further research can be conducted on the theoretical model by revising some indicators that evolve with time for example the number of hard disks sold to a country will change with time due to cloud computing. Also more prospective countries and more recent years can be added. Working with only publicly available data limits the research and makes it more complex. For future research, finding data for the indicators and the dependent variable might still be hard, but the researcher should take time to collect the data by himself or revise the indicators if necessary.

5. Conclusion

As there is limited data about cyber warfare and as there was no literature describing the cyber warfare attributes specifically it was necessary to do this first. In chapter 2 the offensive cyber warfare attributes are described in a diagram showing the process of offensive warfare (appendix 1). This diagram has been defined based on an analogy of individuals in war and based on literature about traditional warfare. Within this diagram there are different categories, which are Motivation, Target, Channel, Means, Methods and Damage describing the process of offensive warfare. Based on this diagram a distinction between offensive cyber warfare and traditional warfare can be made. Cyber warfare is digital war, while traditional war is more physical. Only 2 of the categories explain capability level; Channel and Means. The direct indicators for assessing offensive cyber warfare are identified, which resulted in a theoretical model for assessing offensive cyber warfare (figure 2.2). In this model the indirect indicators are included that have been used to give an approach of a model.

The diagram describing the process of offensive cyber warfare consists of 6 categories. Based on the diagram the main cyber warfare attributes are found:

- To get involved in cyber warfare a country needs access to and knowledge about the digital channel.
- In cyber warfare a country needs digital means to attack others.
- A country has a motivation to initiate a cyber attack.
- The targets of cyber warfare are critical information infrastructures of countries.
- The damage caused during cyber warfare are digital, but can also be physical and psychological.
- The methods used during cyber warfare are digital.

These attributes are more detailed as can be seen in appendix 1. To get a view in capability growth the maturity level for offensive cyber warfare are described, which consists of 5 levels: beginners, semi-intermediate, intermediate, semi-advanced and advanced. The cut-off points are determined based on the approach and have a range of 20% for each level, as there is no theory explaining these. Due to limitation only an approach of a model for assessing offensive cyber warfare capability has been given, based on a proxy variable and indirect indicators explaining access to, ability to use and skills of channel and means:

$$y = 0.386\ factor\ 1 + 0.458\ factor\ 2 + 0.094\ factor\ 3 + 0.205\ factor\ 4 - 0.418$$

The steps involved for the analysis can be seen in figure 3.9. The equation is a first approach of a model, on which further research can be conducted.

6. Research Relevance

The research adds theoretical knowledge to the field of cyber warfare. It also gives the government a tool to assess cyber warfare capability of other countries. However, this model is not yet practical, because of data. This model can create awareness and help governments to make more careful and thoughtful decisions. Also, the results of this research give a better understanding about assessing cyber warfare capability to others as well.

References

1. The World Bank Group. (2012). *Indicators | Data*. Retrieved 2012, from The World Bank: http://data.worldbank.org/indicator
2. U.S. Army Capabilities Integration Center. (2010). *TRADOC Pamphlet 525-7-8: Cyberspace Operations Concept Capability Plan 2016-2028.* Fort Monroe, Virginia 23651-1047: Department of the Army Headquarters, United States Army Training and Doctrine Command.
3. | A. M. Meerloo, M.D. (2009). The Rape of the Mind. In *The Rape of the Mind* (p. p.134). Progressive Press.
4. B.Darlington, R. (n.d.). *Factor Analysis*. Retrieved July 11, 2012, from www.psych.cornell.edu: http://www.psych.cornell.edu/darlington/factor.htm
5. Bartholomew, D. J., & Knott, M. (1999). *Latent Variable Models and Factor Analysis.* New York: Oxford University Press Inc.
6. Becker, P. D., Knackstedt, D. R., & Pöppelbuß, D.-W. I. (2009). *Developing Maturity Models for IT Management - A procedure model and its application.* Münster: BISE - Research Paper.
7. C.Homan. (2010). *Cyber space het domein van een nieuw soort totale oorlog.* Clingendeal.
8. Carr, J. (2011). *Inside Cyber Warfare.* United States of America.
9. Chapter 14; Factor Analysis, Path Analysis, and Structural Equations Modeling. (2009). Jones and Bartlett.
10. Clarke, R. (2010). *Cyber War: The next Threat to national security and what to do about it.* Harpin Collins.
11. Colin van Hoek. (2011, december). *MCAfee vreest echte cyberoorlog*. Retrieved december 2011, from www.nu.nl: http://www.nu.nl/internet/2703008/mcafee-vreest-echte-cyberoorlog.html
12. Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber War.*
13. *Correlation - Statistical Techniques, Rating Scales, Correlation Coefficients, and More - Creative Research Systems*. (2010). Retrieved July 09, 2012, from www.surveysystem.com: http://www.surveysystem.com/correlation.htm
14. D.Howard. (1997). *An analysis of security incidents on the internet 1989-1995.* Pittsburgh, Pennsylvania: Carnegie Mellon University.
15. D.Myers, M. (n.d.). *Quantitative Research in Information Systems - Section 7: Glossary*. Retrieved July 15, 2012, from dstraub.cis.gsu.edu: http://dstraub.cis.gsu.edu:88/quant/7glossary.asp

16. *Damage*. (2012). Retrieved March 28, 2012, from http://en.wikipedia.org: http://en.wikipedia.org/wiki/Damage

17. *Damages (disambiguation)*. (2010, March 21). Retrieved March 28, 2012, from http://en.wikipedia.org: http://en.wikipedia.org/wiki/Damages_(disambiguation)

18. *Damages*. (2012, Januray). Retrieved March 28, 2012, from http://en.wikipedia.org: http://en.wikipedia.org/wiki/Damages#Nominal_damages

19. David Lee. (2012, May 28). *Flame: Massive cyber-attack discovered, researchers say*. Retrieved July 21, 2012, from BBC News: http://www.bbc.co.uk/news/technology-18238326

20. *Defense Information Systems Agency*. (2010). Retrieved october 2011, from www.disa.mil: www.disa.mil

21. Denning, D. (2000). Reflections on Cyberweapons Controls. *Computer Security Journal, Vol. XVI, No. 4* , 43-53.

22. Dutta, S., Narasimhan, O., & Rajiv, S. (2004). Conceptualizing and measuring capabilities: Methodology and emperical application. *Strategic Management Journal* .

23. F.Erbacher, R. (2005). *Extending Command and Control Infrastructures to Cyber Warfare Assets.* Utah State University, Logan, UT 84322, USA.

24. Forbes, T. (2007, September 13). *quantifying losses, damage, expert, brand, intangibles, ip, intellectual property*. Retrieved April 3, 2012, from www.intangiblebusiness.com: http://www.intangiblebusiness.com/Brand-Services/Legal-services/Press-coverage/Quantifying-intangible-losses~960.html

25. *Free statistics*. (2012, february 28). Retrieved april 23, 2012, from ITU:Commited to connecting the world: http://www.itu.int/ITU-D/ict/statistics/

26. Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *The Bulletin of Centre for East-West Cultural and Economic Studies* .

27. G.Billo, & W.Chang. (2004). *CYBER WARFARE: An Analysis of the means and motivations of selected nation states.*

28. G.Coleman, K. (2007, October). World War III: A Cyber War has begun.

29. G.Pye, & M.J.Warren. (2009). An emergent security risk: Critical infrastructures and Information Warfare. *Journal of information warfare* .

30. Gerda M. van den Berg. (n.d.). PRINCALS for beginners. Leiden.

31. Graeme Hutcheson; Nick Sofroniou. (1999). *The multivariate social scientist: Introductory Statistics Using Generalized Linear Models.* London.

32. Guitton, C. (2011). Reconsidering State Military: Strategy for Strategic Cyberwarfare . Geneva.

33. Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computer & Security* , 31- 43.

34. He-suk, C. (2012). *N.K. Third for cyber war capabilities*. Retrieved August 5, 2012, from view.koreaherald.com: http://view.koreaherald.com/kh/view.php?ud=20120607001276

35. Horwitz, R. D. (2008, October 13). *YUTorah Online - Parashat Bereshit: The Conflict between Cain and Abel (Rabbi David Horwitz)*. Retrieved April 3, 2012, from www.yutorah.org: http://www.yutorah.org/lectures/lecture.cfm/728352/Rabbi_David_Horwitz/Parashat_Bereshit:_The_Conflict_between_Cain_and_Abel

36. HP DVLabs; HP Teams. (2011). *2011 top cyber security risks .* HP Enterprise Security.

37. Intelligence Community Directive Number 301. (2006, July 11). *National open source enterprise* .

38. ITU. (2012). *ITU Information and Communication Technology*. Retrieved March 2012, from www.itu.int: http://www.itu.int/ITU-D/ict/

39. ITU. (2011). The World Telecommunication / ICT indicators database.

40. J.Cooke-Davies, T. (2005). *The Executive Sponsor – The Hinge upon which Organisational Project Management Maturity Turns?* Edinburgh.

41. J.DeCoster. (1998). *Overview of Factor Analysis.*

42. Joseph F. Hair; Rolph E. Anderson; Ronald L. Tatham; William C.Black. (1995). *Multivariate Data Analysis.*

43. Lab, M. (2011). *MCAfee Threats Report: Third Quarter 2011.* MCAfee Lab.

44. McAfee Labs. (2011). *2012 Threat Predictions.* Santa Clara: McAfee.

45. McDonogh. (2009). *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Brussels: COMMISSION OF THE EUROPEAN COMMUNITIES .

46. Moteff, J., & Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* CRS Report for Congress.

47. nations encyclopedia. (2012). *Congo, Democratic Republic of The Infrastructure, power, and communications, Information about Infrastructure, power, and communications in Congo, Democratic Republic of The*. Retrieved August 7, 2012, from http://www.nationsencyclopedia.com: http://www.nationsencyclopedia.com/economies/Africa/Congo-Democratic-Republic-of-The-INFRASTRUCTURE-POWER-AND-COMMUNICATIONS.html

48. NATO C3 Agency. (2011, January). *Multinational cyber defence capability development (MN CD2) Initiative.* Retrieved March 3, 2012, from http://www.nc3a.nato.int/Pages/default.aspx: http://www.nc3a.nato.int/Opportunities/Documents/Multinational%20Cyber%20Defence%20Capability%20Development%20Initiative.pdf

49. *NATO PA - 173 DSCFC 09 E bis - NATO and Cyber Defence*. (2009). Retrieved March 21, 2012, from www.nato-pa.int: http://www.nato-pa.int/default.Asp?SHORTCUT=1782

50. Networkingmind. (2011). *What are the difference between passive and active attacks ? | Home of Computer Science Students, Develovers, Programmers, Hardware and Network Administrators*. Retrieved April 4, 2012, from www.networkingmind.com: http://networkingmind.com/what-are-difference-between-passive-and-active-attacks

51. Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and Implications.* Tallin, Estonia: www.ccdcoe.org.

52. Papa, M., & Shanoi, S. (2008). *Critical Infrastructure protection II.* Springer.

53. Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability Maturity Model for Software, Version 1.1.* Pennsylvania: Carnegie Mellon University Pittsburgh.

54. Pedhazur, E., & Schmelkin, L. P. (1991). *Measurement, Design and Analysis: an integrated approach.* New Yersey: Lawrence Erlbaum Associates Inc.

55. Pike, J. (2000-2012). *FM 3-06.11 Chapter 4*. Retrieved March 29, 2012, from www.GlobalSecurity.org: http://www.globalsecurity.org/military/library/policy/army/fm/3-06-11/ch4.htm#tab4-6

56. Prof.Dr.Jürg Schwarz juerg. (2011, March). Research Methodology: Tools Applied Data Analysis with SPSS, Lecture 03: Factor Analaysis.

57. *Proxy variable: Definition from Answers.com*. (n.d.). Retrieved July 07, 2012, from www.answers.com: http://www.answers.com/topic/proxy-variable

58. Saalbach, P. D. (2011, January 12). Cyber Warfare Methods and Practice version 3.0. *LV Internet Policy* .

59. *Schade*. (2010, November 9). Retrieved March 28, 2012, from http://nl.wikipedia.org: http://nl.wikipedia.org/wiki/Schade

60. *Standard Deviation Definition | Investopedia*. (n.d.). Retrieved July 15, 2012, from www.investopedia.com: http://www.investopedia.com/terms/s/standarddeviation.asp#axzz20hxDtMyW

61. *Standardizing Variables*. (n.d.). Retrieved July 15, 2012, from http://vault.hanover.edu: http://vault.hanover.edu/~altermattw/methods/stats/standardize.htm

62. The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. (n.d.). *Conflict-definition of conflict by the free online dictionary, Thesaurus and encyclopedia.* Retrieved feb 21, 2012, from Dictionary, Encyclopedia and Thesaurus - The Free Dictionary: http://www.thefreedictionary.com/conflict

63. The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. (n.d.). *War-definition of war by The Free Online Dictionary, Thesaurus and Encyclopedia.* Retrieved feb 21, 2012, from Dictionary, Encyclopedia and Thesaurus-The free dictionary: http://www.thefreedictionary.com/War

64. (2006). *The national military strategy for cyberspace operations .* Washington: Chairman of the Joint Chiefs of Staff Washington ,D.C. 20318.

65. Toorani.M. (2009). *SMEmail - A New Protocol for the Secure E-mail inMobile Environments.*

66. Tzu, S. (4th cent. B.C.). *The art of war.*

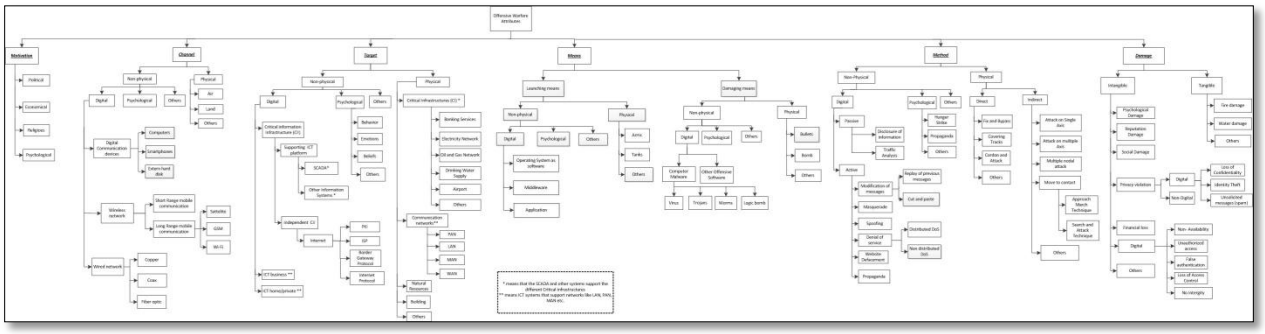
67. UCLA Academic Technology Services. (n.d.). *SPSS FAQ: What does Cronbach's alpha mean?* Retrieved July 14, 2012, from www.ats.ucla.edu: http://www.ats.ucla.edu/stat/spss/faq/alpha.html

68. United Nations. (2012). *United Nations Statistics Division- Standard Country and Area Codes Classifications*. Retrieved August 8, 2012, from United Nations Statistics: http://unstats.un.org/unsd/methods/m49/m49regin.htm

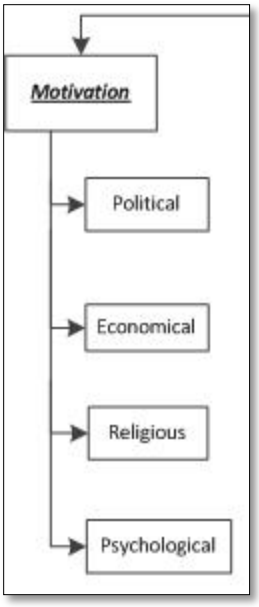
69. *War*. (2012, January). Retrieved March 27, 2012, from wikipedia.org: http://en.wikipedia.org/wiki/War#cite_note-79

70. *What are z-scores?* (2008). Retrieved July 15, 2012, from statistics-help-for-students.com: http://statistics-help-for-students.com/What_are_Z_scores.htm

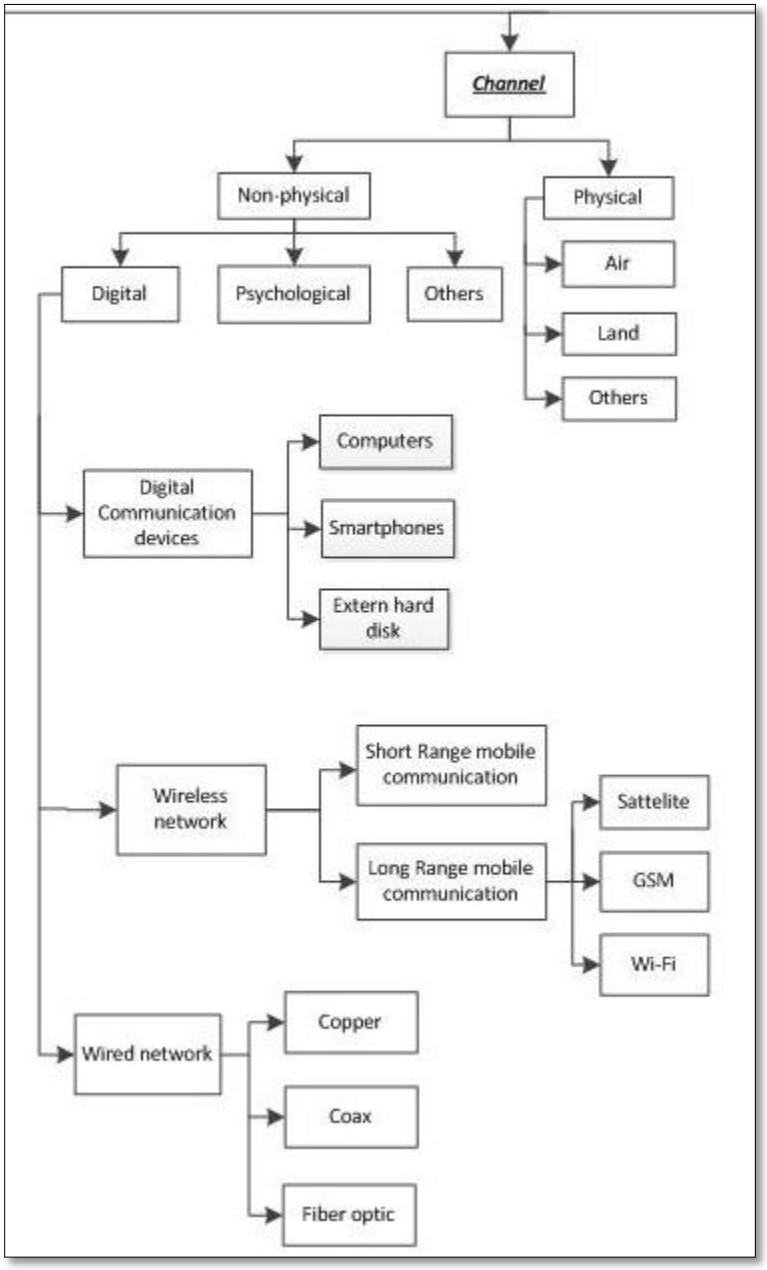
Appendix 1 Diagram for Offensive Warfare



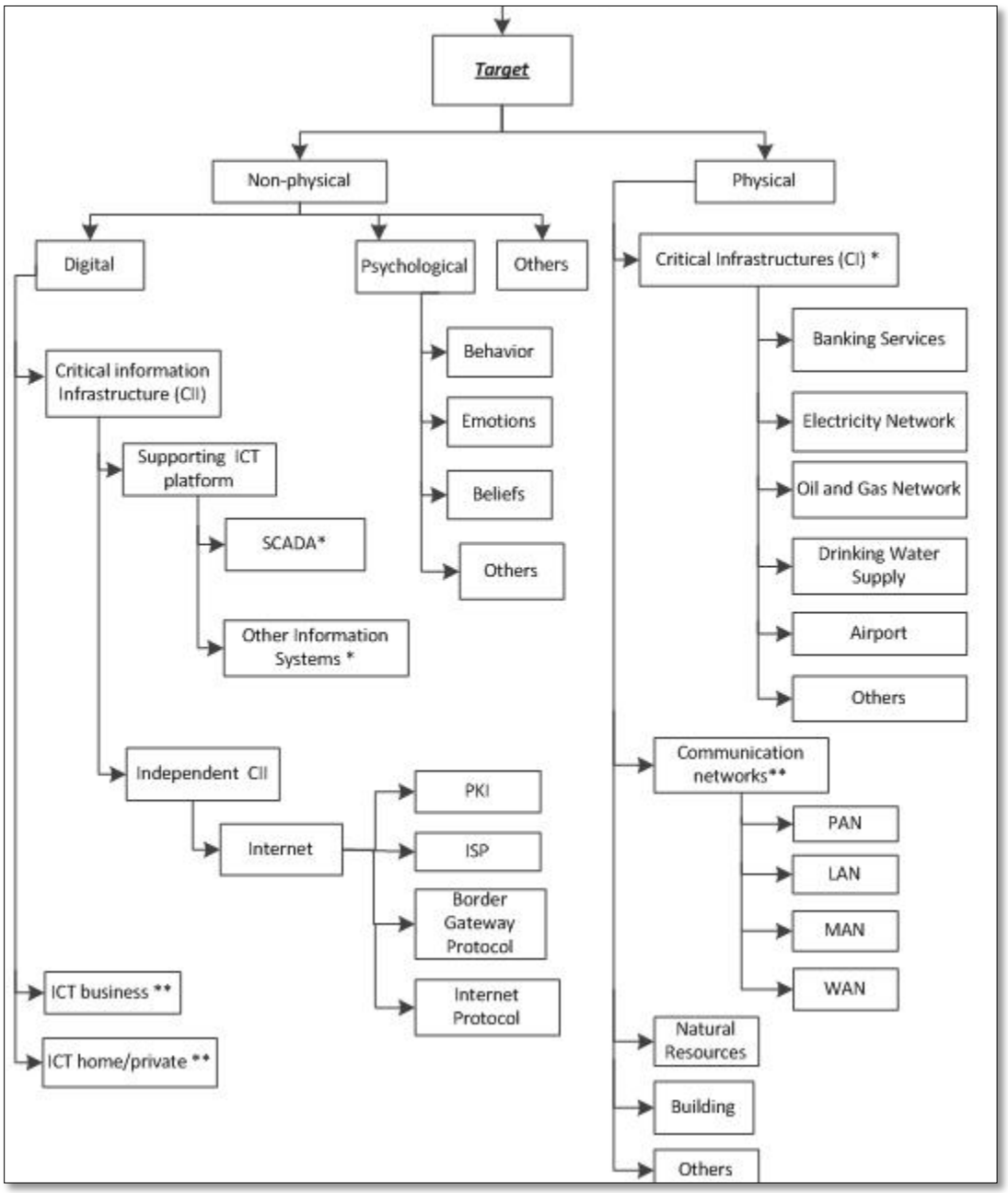
Motivation



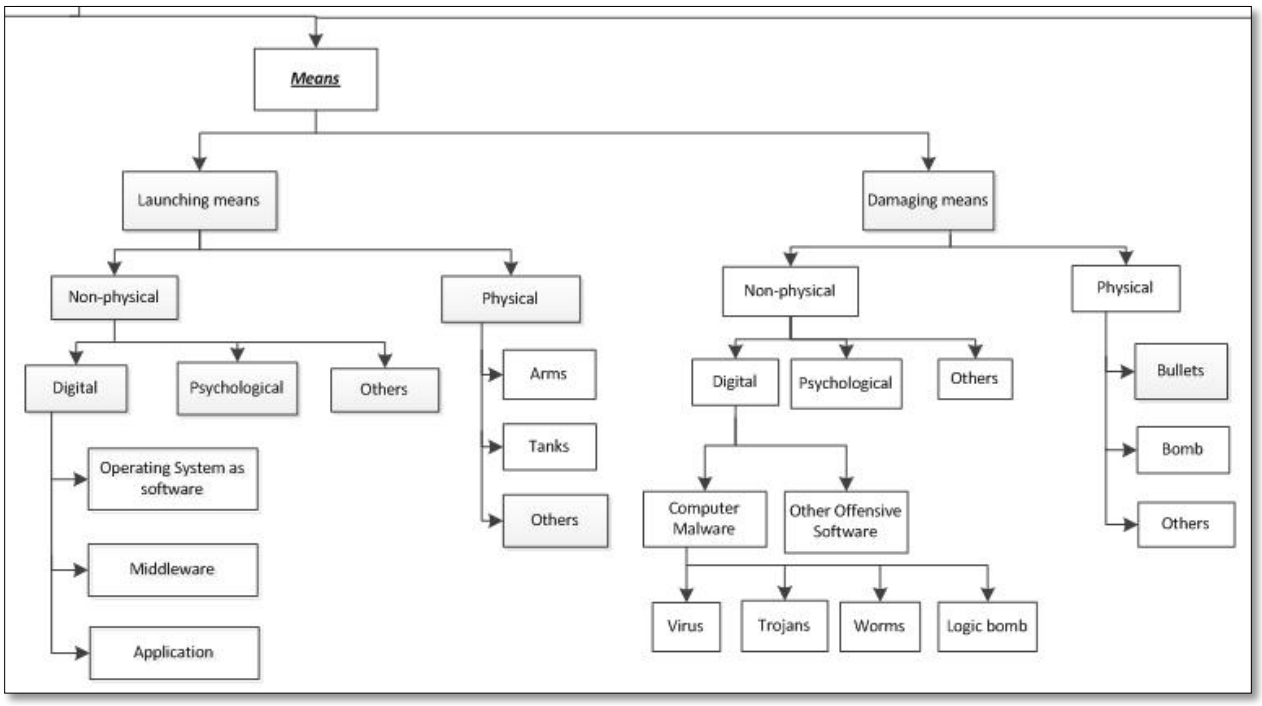
Channel


Channel
Non-physical
Physical
Digital
Psychological
Others
Air
Land
Others
Computers
Digital Communication devices
Smartphones
Extern hard disk
Short Range mobile communication
Wireless network
Sattelite
Long Range mobile communication
GSM
Wi-Fi
Wired network
Copper
Coax
Fiber optic

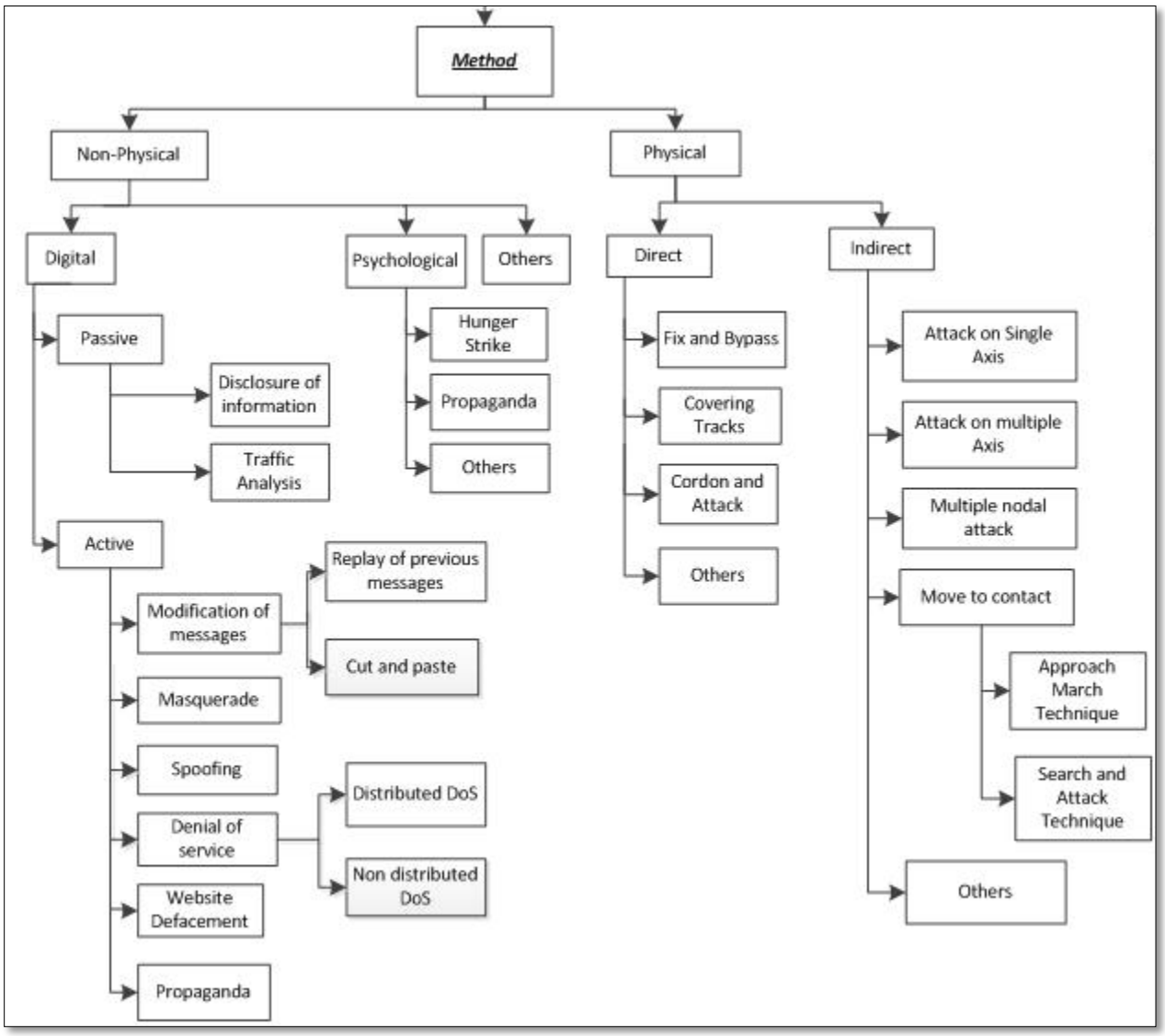
Target


Target
Non-physical
Physical
Digital
Psychological
Others
Critical Infrastructures (CI) *
Behavior
Emotions
Beliefs
Others
Banking Services
Electricity Network
Oil and Gas Network
Drinking Water Supply
Airport
Others
Critical information Infrastructure (CII)
Supporting ICT platform
SCADA*
Other Information Systems *
Independent CII
Internet
PKI
ISP
Border Gateway Protocol
Internet Protocol
Communication networks**
PAN
LAN
MAN
WAN
ICT business **
ICT home/private **
Natural Resources
Building
Others

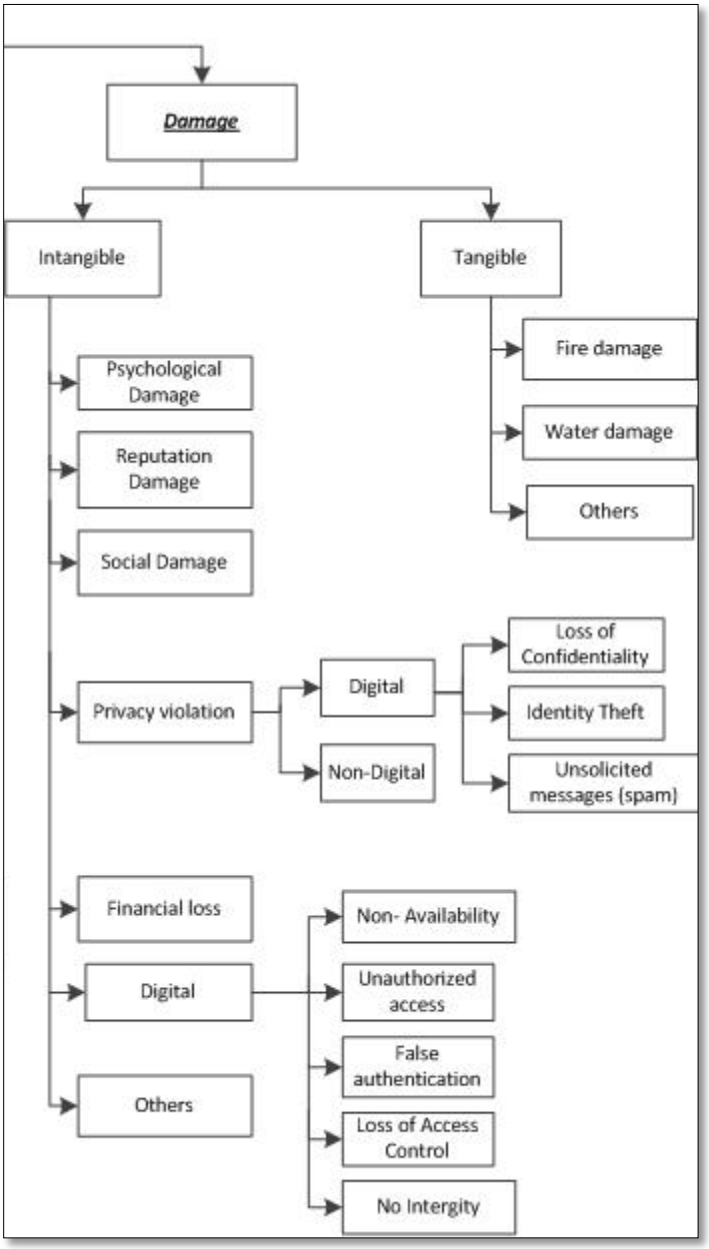
Means


Means
Launching means
Damaging means
Non-physical
Physical
Non-physical
Physical
Digital
Psychological
Others
Arms
Tanks
Others
Digital
Psychological
Others
Bullets
Bomb
Others
Operating System as software
Middleware
Application
Computer Malware
Other Offensive Software
Virus
Trojans
Worms
Logic bomb

Method


Method
Non-Physical
Physical
Digital
Psychological
Others
Direct
Indirect
Passive
Active
Disclosure of information
Traffic Analysis
Hunger Strike
Propaganda
Others
Fix and Bypass
Covering Tracks
Cordon and Attack
Others
Attack on Single Axis
Attack on multiple Axis
Multiple nodal attack
Move to contact
Approach March Technique
Search and Attack Technique
Others
Modification of messages
Replay of previous messages
Cut and paste
Masquerade
Spoofing
Denial of service
Distributed DoS
Non distributed DoS
Website Defacement
Propaganda

Damage


Damage
Intangible
Tangible
Psychological Damage
Reputation Damage
Social Damage
Privacy violation
Digital
Non-Digital
Loss of Confidentiality
Identity Theft
Unsolicited messages (spam)
Financial loss
Digital
Others
Non- Availability
Unauthorized access
False authentication
Loss of Access Control
No Intergity
Fire damage
Water damage
Others

Appendix 2 Correlation of ICT Development Index with the Indicators of Offensive Cyber Warfare Capability

Correlations

		Zscore(ICT_Development_Index)	Zscore(Fixed_broadband_subscriptions_per_100_inhabitant)	Zscore(Fixed_internet_subscriptions_per_100_inhabitants)	Zscore(Fixed_telephone_subscriptions_per_100_inhabitants)	Zscore(Mobile_cellular_subscriptions_per_100_inhabitants)	Zscore (Percentage_of_individuals_using_the_internet)	Zscore (Fulltime_telecom_employees)	Zscore (International_internet_bandwidth)	Zscore (Percentage_of_household_with_a_computer)	Zscore (Percentage_of_household_with_internet_access_at_home)	Zscore (Secure_internet_servers)	Zscore(ODP)	Zscore (ICT_Goods_Export)	Zscore (ICT_Goods_Import)	Zscore (Literacy_rate_adult)	Zscore (Literacy_rate_youth)	Zscore (School_enrollment_tertiary)
Zscore(ICT_Development_Index)	Pearson Correlation	1	.890**	.911**	.943**	.869**	.951**	.203*	.397**	.823**	.815**	.231**	.304**	.378**	.337**	.730**	.679**	.808**
	Sig. (1-tailed)		.000	.000	.000	.000	.000	.016	.000	.000	.000	.003	.000	.000	.000	.000	.000	.000
	N	151	150	142	151	151	151	113	149	141	141	146	151	136	140	52	53	127
Zscore(Fixed_broadband_subscriptions_per_100_inhabitant)	Pearson Correlation	.890**	1	.949**	.868**	.657**	.898**	.150*	.390**	.708**	.725**	.216**	.274**	.364**	.333**	.334**	.269*	.553**
	Sig. (1-tailed)	.000		.000	.000	.000	.000	.039	.000	.000	.000	.002	.000	.000	.000	.006	.022	.000
	N	150	194	176	194	194	194	140	191	169	167	184	189	158	165	56	56	147
Zscore(Fixed_internet_subscriptions_per_100_inhabitants)	Pearson Correlation	.911**	.949**	1	.893**	.692**	.911**	.158*	.353**	.713**	.733**	.190**	.231**	.386**	.398**	.441**	.382**	.557**
	Sig. (1-tailed)	.000	.000		.000	.000	.000	.036	.000	.000	.000	.006	.001	.000	.000	.000	.002	.000
	N	142	176	177	177	177	177	132	175	153	152	170	173	149	155	54	53	134
Zscore(Fixed_telephone_subscriptions_per_100_inhabitants)	Pearson Correlation	.943**	.868**	.893**	1	.730**	.866**	.216**	.368**	.700**	.688**	.210**	.278**	.336**	.305**	.571**	.499**	.653**
	Sig. (1-tailed)	.000	.000	.000		.000	.000	.005	.000	.000	.000	.002	.000	.000	.000	.000	.000	.000
	N	151	194	177	199	199	199	144	195	172	170	187	192	159	166	57	56	147
Zscore(Mobile_cellular_subscriptions_per_100_inhabitants)	Pearson Correlation	.869**	.657**	.692**	.730**	1	.779**	.103	.242**	.650**	.620**	.084	.147*	.272**	.313**	.673**	.605**	.638**
	Sig. (1-tailed)	.000	.000	.000	.000		.000	.109	.000	.000	.000	.127	.021	.000	.000	.000	.000	.000
	N	151	194	177	199	199	199	144	195	172	170	187	192	159	166	57	56	147
Zscore(Percentage_of_individuals_using_the_internet)	Pearson Correlation	.951**	.898**	.911**	.866**	.779**	1	.185*	.391**	.755**	.762**	.242**	.291**	.355**	.342**	.532**	.462**	.677**
	Sig. (1-tailed)	.000	.000	.000	.000	.000		.013	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	151	194	177	199	199	199	144	195	172	170	187	192	159	166	57	56	147
Zscore(Fulltime_telecom_employees)	Pearson Correlation	.203*	.150*	.158*	.216**	.103	.185*	1	.731**	.203*	.188*	.745**	.855**	.240**	.283**	.142	.162	.207*
	Sig. (1-tailed)	.016	.039	.036	.005	.109	.013		.000	.010	.016	.000	.000	.004	.001	.179	.147	.015
	N	113	140	132	144	144	144	144	144	131	131	136	141	118	122	44	44	110
Zscore (International_internet_bandwidth)	Pearson Correlation	.397**	.390**	.353**	.368**	.242**	.391**	.731**	1	.401**	.413**	.793**	.838**	.212**	.231**	.199	.191	.279**
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.004	.001	.073	.084	.000
	N	149	191	175	195	195	195	144	195	171	169	184	190	157	164	55	54	144
Zscore(Percentage_of_household_with_a_computer)	Pearson Correlation	.823**	.708**	.713**	.700**	.650**	.755**	.203*	.401**	1	.979**	.219**	.288**	.146*	.173*	.330**	.229	.584**
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.010	.000		.000	.003	.000	.043	.019	.009	.054	.000
	N	141	169	153	172	172	172	131	171	172	169	163	167	138	145	51	51	133
Zscore(Percentage_of_household_with_internet_access_at_home)	Pearson Correlation	.815**	.725**	.733**	.688**	.620**	.762**	.188*	.413**	.979**	1	.222**	.283**	.135	.171*	.294*	.202	.573**
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.016	.000	.000		.002	.000	.058	.020	.018	.077	.000
	N	141	167	152	170	170	170	131	169	169	170	161	165	137	144	51	51	133
Zscore(Secure_internet_servers)	Pearson Correlation	.231**	.216**	.190**	.210**	.084	.242**	.745**	.793**	.219**	.222**	1	.935**	.106	.107	.194	.171	.218**
	Sig. (1-tailed)	.003	.002	.006	.002	.127	.000	.000	.000	.003	.002		.000	.093	.089	.076	.106	.005
	N	146	184	170	187	187	187	136	184	163	161	187	181	156	161	56	55	142
Zscore(ODP)	Pearson Correlation	.304**	.274**	.231**	.278**	.147*	.291**	.855**	.838**	.288**	.283**	.935**	1	.166*	.178*	.178	.177	.267**
	Sig. (1-tailed)	.000	.000	.001	.000	.021	.000	.000	.000	.000	.000	.000		.019	.011	.094	.098	.001
	N	151	189	173	192	192	192	141	190	167	165	181	192	157	164	56	55	144
Zscore (ICT_Goods_Export)	Pearson Correlation	.378**	.364**	.386**	.336**	.272**	.355**	.240**	.212**	.146*	.135	.106	.166*	1	.850**	.190	.178	.176*
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.004	.004	.043	.059	.093	.019		.000	.089	.105	.023
	N	136	158	149	159	159	159	118	157	138	137	156	157	159	158	52	51	129
Zscore (ICT_Goods_Import)	Pearson Correlation	.337**	.333**	.398**	.305**	.313**	.342**	.283**	.231**	.173*	.171*	.107	.178*	.850**	1	.272*	.223	.222**
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.001	.001	.019	.020	.089	.011	.000		.023	.054	.005
	N	140	165	155	166	166	166	122	164	145	144	161	164	158	166	54	53	132
Zscore (Literacy_rate_adult)	Pearson Correlation	.730**	.334**	.441**	.571**	.673**	.532**	.142	.199	.330**	.294*	.194	.178	.190	.272*	1	.964**	.695**
	Sig. (1-tailed)	.000	.006	.000	.000	.000	.000	.179	.073	.009	.018	.076	.094	.089	.023		.000	.000
	N	52	56	54	57	57	57	44	55	51	51	56	56	52	54	57	55	43
Zscore (Literacy_rate_youth)	Pearson Correlation	.679**	.269*	.382**	.499**	.605**	.462**	.162	.191	.228	.202	.171	.177	.178	.223	.964**	1	.655**
	Sig. (1-tailed)	.000	.022	.002	.000	.000	.000	.147	.084	.054	.077	.106	.098	.105	.054	.000		.000
	N	53	56	53	56	56	56	44	54	51	51	55	55	51	53	55	56	43
Zscore (School_enrollment_tertiary)	Pearson Correlation	.808**	.553**	.557**	.653**	.638**	.677**	.207*	.279**	.584**	.573**	.218**	.267**	.176*	.222**	.695**	.655**	1
	Sig. (1-tailed)	.000	.000	.000	.000	.000	.000	.015	.000	.000	.000	.005	.001	.023	.005	.000	.000	
	N	127	147	134	147	147	147	110	144	133	133	142	144	129	132	43	43	147

**. Correlation is significant at the 0.01 level (1-tailed).
*. Correlation is significant at the 0.05 level (1-tailed).

Appendix 3 Rotated Component Matrix with 4 factors

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Zscore(Fixed_broadband_subscriptions_per_100_inhabitant)	.808	.243	.010	.464
Zscore(Fixed_internet_subscriptions_per_100_inhabitants)	.840	.273	.033	.403
Zscore(Fixed_telephone_subscriptions_per_100_inhabitants)	.753	.493	.145	.246
Zscore(Mobile_cellular_subsciptions_per_100_inhabitants)	.445	.695	.053	.342
Zscore(Percentage_of_individuals_using_the_internet)	.634	.519	.203	.395
Zscore(Fulltime_telecom_employees)	-.027	.022	.926	.010
Zscore(International_internet_bandwith)	.013	.132	.947	.084
Zscore(Percentage_of_household_with_a_computer)	.022	.178	.010	.931
Zscore(Percentage_of_household_with_internet_access_at_home)	.080	.127	.026	.942
Zscore(Secure_internet_servers)	.120	.102	.958	.009
Zscore(GDP)	.114	.110	.899	-.034
Zscore(ICT_Goods_Export)	.886	.023	.010	-.228
Zscore(ICT_Goods_Import)	.698	.248	.080	-.318
Zscore(Literacy_rate_adult)	.180	.930	.119	.081
Zscore(Literacy_rate_youth)	.151	.937	.119	.025
Zscore(School_enrollment_tertiary)	.216	.793	.072	.141

Appendix 4 Component Scores Coefficient Matrix

Component Score Coefficient Matrix

	Component			
	1	2	3	4
Zscore(Fixed_broadband_subscriptions_per_100_inhabitant)	.234	-.112	-.020	.138
Zscore(Fixed_internet_subscriptions_per_100_inhabitants)	.243	-.099	-.016	.105
Zscore(Fixed_telephone_subscriptions_per_100_inhabitants)	.172	.029	.003	.013
Zscore(Mobile_cellular_subsciptions_per_100_inhabitants)	.009	.177	-.033	.048
Zscore(Percentage_of_individuals_using_the_internet)	.113	.043	.021	.084
Zscore(Fulltime_telecom_employees)	-.028	-.047	.274	.010
Zscore(International_internet_bandwith)	-.039	-.015	.273	.028
Zscore(Percentage_of_household_with_a_computer)	-.077	-.037	-.002	.397
Zscore(Percentage_of_household_with_internet_access_at_home)	-.045	-.074	.005	.405
Zscore(Secure_internet_servers)	.012	-.042	.276	-.008
Zscore(GDP)	.011	-.029	.258	-.028
Zscore(ICT_Goods_Export)	.345	-.144	-.012	-.152
Zscore(ICT_Goods_Import)	.231	.002	-.004	-.209
Zscore(Literacy_rate_adult)	-.127	.363	-.027	-.084
Zscore(Literacy_rate_youth)	-.136	.379	-.028	-.108
Zscore(School_enrollment_tertiary)	-.088	.290	-.032	-.042

Appendix 5 Definition of the indicators

From ITU Information and Communication Technology (ITU, The World Telecommunication / ICT indicators database, 2011) (from http://www.itu.int/ITU-D/ict/)

- Fixed Broadband subscriptions per 100 inhabitants:
  "Refers to subscriptions to high-speed access to the public Internet (a TCP/IP connection), at downstream speeds equal to, or greater than, 256 kbit/s. This includes cable modem, DSL, fibre-to-the-home/building and other fixed (wired)- broadband subscriptions."
- Fixed internet subscriptions per 100 inhabitants:
  "Fixed (wired) Internet subscriptions refers to the number of active fixed (wired) Internet subscriptions at speeds less than 256 kbit/s (such as dial-up and other fixed non-broadband subscriptions)."
- Fixed telephone subscriptions per 100 inhabitants:
  "Fixed-telephone subscriptions refers to the sum of active number of analogue fixed-telephone lines, voice-over-IP (VoIP) subscriptions, fixed wireless local loop (WLL) subscriptions, ISDN voice-channel equivalents and fixed public payphones."
- Mobile cellular subscriptions per 100 inhabitants:
  "*Mobile cellular subscribers refer to users of portable telephones subscribing to an automatic public mobile telephone service using cellular technology, which provides access to the PSTN. Users of both post-paid subscriptions and pre-paid accounts are included."*
- Fulltime telecommunication employees:
  "Refers to the total number of persons, in full-time equivalent (FTE) units, employed by telecommunication operators in the country for the provision of telecommunication services, including fixed-telephone, mobile-cellular, Internet and data services."
- International internet bandwidth:
  "International Internet bandwidth refers to the total used capacity of international Internet bandwidth, in megabits per second (Mbit/s)."
- Percentage of household with a computer: *Percentage of countries households with a computer.*
- Percentage of individuals using the internet: *Percentage of a countries population using the internet.*
- Percentage of household with internet access at home*: Any member having the possibility to access internet from home has been included in the measurement.*

From The World Bank (The World Bank Group, 2012)from (http://data.worldbank.org/indicator):

- Secure internet servers: *"Secure servers are servers using encryption technology in Internet transactions."*
- GDP: "*GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used*."
- ICT goods exports (% of total goods exports): *"Information and communication technology goods exports include telecommunications, audio and video, computer and related equipment; electronic components; and other information and communication technology goods."*
- ICT good import: "*ICT goods imports (% total goods imports)*
- *Information and communication technology goods imports include telecommunications, audio and video, computer and related equipment; electronic components; and other information and communication technology goods*."
- Literacy rate, adult total (% of people ages 15 and above): "*Adult literacy rate is the percentage of people ages 15 and above who can, with understanding, read and write a short, simple statement on their everyday life."*
- Literacy rate, youth total (% of people ages 15-24): "*Youth literacy rate is the percentage of people ages 15-24 who can, with understanding, read and write a short, simple statement on their everyday life."*
- School enrollment, tertiary (% gross): *"Gross enrollment ratio is the ratio of total enrollment, regardless of age, to the population of the age group that officially corresponds to the level of education shown. Tertiary education, whether or not to an advanced research qualification, normally requires, as a minimum condition of admission, the successful completion of education at the secondary level."*
- International internet bandwidth: *""International Internet bandwidth is the contracted capacity of international connections between countries for transmitting Internet traffic."*

Appendix 6 Ranking Countries for 2009

Country	OCW capability	Normalized OCW
Hong Kong, China	0.89	1.00
United States	0.60	0.87
Hungary	0.57	0.86
Slovenia	0.56	0.86
Singapore	0.53	0.85
Netherlands	0.49	0.83
Estonia	0.48	0.83
Italy	0.44	0.81
Sweden	0.43	0.81
Croatia	0.43	0.80
Denmark	0.42	0.80
Russia	0.42	0.80
United Kingdom	0.40	0.79
Iceland	0.38	0.78
Korea (Rep.)	0.37	0.78
Portugal	0.37	0.78
Switzerland	0.34	0.77
Spain	0.33	0.76
Poland	0.33	0.76
Malaysia	0.31	0.76
Norway	0.31	0.75
Bermuda	0.27	0.74
Lithuania	0.25	0.73
Cyprus	0.25	0.73
Macao, China	0.24	0.72
New Zealand	0.23	0.72
France	0.23	0.72
Finland	0.16	0.69
Romania	0.16	0.69
Bulgaria	0.16	0.69
Australia	0.16	0.69
Ireland	0.14	0.68
Belarus	0.14	0.68
Belgium	0.14	0.68
Argentina	0.13	0.68
Austria	0.12	0.67
Uruguay	0.12	0.67

Malta	0.10	0.67
Greece	0.10	0.67
Latvia	0.09	0.66
Luxembourg	0.09	0.66
Barbados	0.08	0.66
Panama	0.06	0.65
Japan	0.06	0.65
Brunei Darussalam	0.04	0.64
Israel	0.04	0.64
Canada	0.03	0.64
Ukraine	0.03	0.64
Germany	0.02	0.63
China	0.01	0.63
Czech Republic	-0.01	0.62
Mexico	-0.02	0.62
Cayman Islands	-0.04	0.61
Bahrain	-0.05	0.60
Turkey	-0.07	0.60
Trinidad & Tobago	-0.08	0.59
Aruba	-0.08	0.59
Puerto Rico	-0.08	0.59
Gibraltar	-0.11	0.58
Saudi Arabia	-0.12	0.58
Liechtenstein	-0.12	0.57
Bosnia and Herzegovina	-0.13	0.57
Costa Rica	-0.15	0.56
Kazakhstan	-0.16	0.56
New Caledonia	-0.17	0.56
Antigua & Barbuda	-0.18	0.55
Qatar	-0.18	0.55
Faroe Islands	-0.18	0.55
Slovak Republic	-0.20	0.54
Moldova	-0.20	0.54
Colombia	-0.20	0.54
Monaco	-0.21	0.54
Viet Nam	-0.23	0.53
United Arab Emirates	-0.26	0.52
Serbia	-0.27	0.51
Andorra	-0.28	0.51
St. Kitts and Nevis	-0.28	0.51

Armenia	-0.30	0.50
Montenegro	-0.30	0.50
Jamaica	-0.32	0.49
El Salvador	-0.33	0.49
Libya	-0.33	0.49
Kyrgyzstan	-0.34	0.48
Mauritius	-0.35	0.48
Cuba	-0.36	0.48
Georgia	-0.37	0.47
Greenland	-0.38	0.47
Chile	-0.40	0.46
St. Vincent and the Grenadines	-0.41	0.45
Mongolia	-0.41	0.45
Ecuador	-0.41	0.45
Morocco	-0.43	0.44
Venezuela	-0.46	0.44
San Marino	-0.46	0.43
Brazil	-0.47	0.43
Cape Verde	-0.47	0.43
Samoa	-0.49	0.42
Guatemala	-0.49	0.42
Grenada	-0.50	0.42
Uzbekistan	-0.50	0.42
Syria	-0.51	0.41
Kuwait	-0.53	0.41
Philippines	-0.53	0.41
Thailand	-0.53	0.40
Tajikistan	-0.54	0.40
Oman	-0.55	0.40
Botswana	-0.56	0.39
Gabon	-0.56	0.39
Kenya	-0.60	0.38
Maldives	-0.61	0.37
Lebanon	-0.61	0.37
Bahamas	-0.62	0.37
Dominica	-0.62	0.37
St. Lucia	-0.62	0.37
Paraguay	-0.62	0.36
Tunisia	-0.65	0.35

Turkmenistan	-0.65	0.35
Swaziland	-0.66	0.35
Namibia	-0.67	0.35
French Polynesia	-0.68	0.34
Nigeria	-0.68	0.34
Suriname	-0.69	0.34
Ghana	-0.70	0.34
Albania	-0.70	0.33
Vanuatu	-0.70	0.33
Lesotho	-0.70	0.33
Jordan	-0.71	0.33
Azerbaijan	-0.72	0.33
Rwanda	-0.73	0.32
Iran (I.R.)	-0.74	0.32
Iraq	-0.74	0.32
Tanzania	-0.75	0.31
Equatorial Guinea	-0.75	0.31
Senegal	-0.76	0.31
Gambia	-0.77	0.30
Seychelles	-0.77	0.30
Côte d'Ivoire	-0.79	0.30
Angola	-0.79	0.30
Congo	-0.79	0.29
Peru	-0.79	0.29
Mauritania	-0.79	0.29
Comoros	-0.80	0.29
Malawi	-0.80	0.29
Burundi	-0.81	0.29
Algeria	-0.82	0.29
Myanmar	-0.82	0.28
Dominican Rep.	-0.82	0.28
Indonesia	-0.83	0.28
Bangladesh	-0.83	0.28
Nepal	-0.83	0.28
Egypt	-0.85	0.27
Honduras	-0.86	0.27
Fiji	-0.87	0.26
Guyana	-0.87	0.26
Mozambique	-0.87	0.26
Liberia	-0.88	0.26

Central African Rep.	-0.88	0.26
Guinea-Bissau	-0.88	0.26
Sierra Leone	-0.88	0.26
Eritrea	-0.88	0.26
Benin	-0.89	0.25
South Africa	-0.90	0.25
Papua New Guinea	-0.90	0.25
Sri Lanka	-0.91	0.25
Palau	-0.92	0.24
Belize	-0.93	0.24
Tonga	-0.93	0.24
Guinea	-0.94	0.23
Madagascar	-0.94	0.23
India	-0.96	0.23
Bolivia	-0.96	0.23
Pakistan	-1.01	0.21
Chad	-1.01	0.21
Marshall Islands	-1.03	0.20
Bhutan	-1.03	0.20
Nicaragua	-1.03	0.19
Uganda	-1.05	0.19
Somalia	-1.06	0.18
Solomon Islands	-1.06	0.18
Micronesia	-1.06	0.18
Tuvalu	-1.06	0.18
Cameroon	-1.07	0.18
Mali	-1.07	0.18
Cambodia	-1.09	0.17
Lao P.D.R.	-1.09	0.17
Djibouti	-1.11	0.16
Timor-Leste	-1.12	0.16
Kiribati	-1.12	0.16
Togo	-1.12	0.16
Haiti	-1.12	0.16
Sudan	-1.12	0.16
Afghanistan	-1.13	0.16
Ethiopia	-1.15	0.15
Burkina Faso	-1.15	0.14
Niger	-1.16	0.14
Congo (Dem. Rep.)	-1.18	0.13

Appendix 7 Example average of fixed internet subscriptions per 100 inhabitants

Country	2005	2006	2007	2008	Average
Bermuda	48.23	58.89	N/A	N/A	53.56
Bhutan	0.54	0.86	0.87	0.86	0.7825
Bolivia	0.79	1.25	2.1	1.29	1.3575
Bosnia and Herzegovina	4.8	6.29	7.24	8.91	6.81
Botswana	N/A	N/A	N/A	0.51	0.51
Brazil	2.35	3.15	4.59	14.37	6.115
Brunei Darussalam	4.95	4.75	15.39	21.95	11.76
Bulgaria	2.67	6.07	8.48	10.9	7.03
Burkina Faso	0.06	0.06	0.08	0.1	0.075
Burundi	N/A	N/A	N/A	0.06	0.06
Cambodia	0.06	0.08	0.11	0.14	0.0975
Cameroon	0.09	0.14	N/A	N/A	0.115
Canada	27.51	29.06	30.82	32.15	29.885