LEBANESE AMERICAN UNIVERSITY

Cyberstate Sovereignty

By

Zeina Badran

A thesis

Submitted in partial fulfillment of the requirements

for the Degree of the Master of Arts in International Affairs

School of Arts and Sciences

May 2016

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

LEBANESE AMERICAN UUNIVERRSITY

School of Arts and Sciences - Beirut Campus

Thesis Approval Form

Student Name: Zeina Budran I.D. #: 201400950

Thesis Title Cyberstate Sovereignty

Program: International Affairs

Department: Social Sciences

School: **School of Arts and Sciences**

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

Master's in Arts in the major of International Affairs

Thesis Advisor: Imad Salamey Signatu [redacted] /5/16

Member: Sami Baroudi Signatu [redacted] 11/05/2016

Member: Paul TABAR Signatu [redacted] 11/05/2016

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants to Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic format and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Zeina Badran

Signature: [redacted]

Date:

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

• I have read and understood LAU's Plagiarism Policy.

• I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.

• This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name:Zeina Badran

Signature: 

Date:

Dedication

This thesis is dedicated to my parents and in the memory of my beloved grandma

I am grateful for their endless love, support, and encouragement

ACKNOWLEDGMENT

I thank my parents for their sacrifices, love, encouragement and support throughout this journey.

I also thank my beloved grandma who continuously encouraged me to pursue my dreams despite all the challenges. I am grateful for all the lessons she taught me in my life and she will always be remembered.

I would like to extend my thanks to my friends who supported me through this challenging phase of my life.

I would like to thank Dr. Imad Salaemy, for guiding me throughout the process of this dissertation. I am thankful for his constructive supervision, support and encouragement during my master's degree.

I thank all my professors at LAU for their guidance and support.

CYBERSTATE SOVEREIGNITY

Zeina Badran

ABSTRACT

Globalization has played a pivotal role in the proliferation of cybercrime where the availability of modern technology has facilitated a wide access to information. The open border era has further expedited the procurement of information. Among the primary ramifications of cybercrimes is a serious breach in state's sovereignty within both economic and security contexts. This thesis examines the different types of cybercrimes and reveals their implications. It also explores states' responses through a comparative assessment of anti-cybercrime strategies utilized by UAE, USA, China, and EU. The thesis highlights differential challenges and rising requisites for interstate collaboration to help preserve cyberstate sovereignty.

Keywords: Cybercrime, Cybersecurity, Defense Strategy, Security models, Cybercrime Implications

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

ApCERT Asia Pacific Computer Emergency Response Team
Col CSD The Collaboration Teams of Cyber Security Division
CSTCB Cyber Security and Technology Crime Bureau
CIRT Computer Incident Response Team
CNCERT Computer Network Emergency Response Team
CERT Computer Emergency Response Team
C3 Cyber Crimes Center
CNI Critical National Infrastructure
CNCERT/CC China's National Computer Network Emergency Response Team Coordination Center
CCP Central Office Confidential Bureau and Central Cryptology Commission
CIIP Critical Information Infrastructure Protection
CSDP Common Security and Defense Policy
CSIRT Computer Security Incident Response Team
DOD Department of Defense
DHS Department of Homeland Security
EU European Union
EC3 European Cybercrime Center
ENISA European Union Agency for Network and Information Security
FBI Federal Bureau Investigation
GCC Gulf Cooperation Council
GDP Gross Domestic Product
IILG Internet Infrastructure Liaison Group
IR International Relations
IT Information Technology
ITU International Telecommunications Union
IP Internet Protocol
ICT Information and Communications Technology
ICS Industrial Control Systems
KPMG Klynveld Peat Marwick Goerdeler
NNISCSG National Network and Information Security Coordination Small Group
NESA National Electronic Security Authority
NIS Network and Information Security
NATO North Atlantic Treaty Organization
OGCIO Security Bureau Office and the Office of the Government Chief Information Officer
PITC Prevention of Information Technology Crimes
PWC Price Water Coopers
PPP Public-Private Partnership
SILG State Informatization Leading Small Group
SSA State Security Apparatus
SCO Shanghai Cooperation Organization

TRA	Telecommunications Regularity Authority
UAE	United Arab Emirates
USA	United States of America
UN GGE	United Nations Governmental Group of Expertise
UN	United Nations

Chapter 1

Introduction

Globalization participated in the spread of technology which facilitated the process of communication, business and education between people worldwide. Technology has become a part of a human's daily life in all activities. This leads to some interesting questions which are as follows: Is cybercrime the unforeseeable consequence of technology? To what extent does this new phenomena affect our world? How has cybercrime altered the concept of security and relations between nations?

It can be deduced that globalization played a role in creating cybercrime where the availability of modern technology has facilitated the access of information in all countries, and the lack of borders has simplified the capabilities of procuring information. On a security level it distinguished itself from traditional crimes that are concerned with human felonies and property offenses. (Hinduja, Sameer, 2007)

Cybercrime is considered to be one of the new arising threats that jeopardizes a state's economy and security it also affects the political dynamics of the state. It indirectly threatens the very foundations of the state's sovereignty and poses a great challenge for states to combat this new threat.

This study aims to assess cybercrimes' impact on states and their relations with each other. In order to do so it requires the examination of the different types of cybercrime in opposing views and in examining their costs and impacts on an economic, security and political level. This would clarify the distinction between the existing types of

cybercrime. Studying the impacts would highlight the magnitude of this threat and reveal the overlap between security and economic repercussions that threaten the state's survival.

A comparative study is to be done between four different security models (USA, UAE China, and EU). This would expose how nations and non-states actors, such as the EU can combat this problem with certain polices and strategies that would be tailored according to the types of threats which they would encounter. These security models were chosen based on their technological advancements and their level of security abilities. Both USA and China are competitive in technological matters, choosing China here was relevant to see what gaps are still missing to fight cybercrime. EU would represent the European countries' amount of cooperation and efforts on a regional level, whereas UAE would be a representative case of a Middle Eastern country that is semi-globalized. UAE has become a very vibrant economic country which attracts foreign investments and other projects, it would illustrate the difference in security levels in comparison to the other three defense models.

These four defense models would stress how cybercrime is transcending borders where security is no longer confined within state borders and the growing incapability of states to manage this issue on their own. This study would display the implications of cybercrime on the international community and in presenting how they are responding (e.g. international agreements). It would demonstrate the challenges of cybercrime and why the need for collaboration between states is imperative to manage this continuously

growing threat. The purpose of this approach seeks to provide a possible and suitable security model that could be adopted as a strategic defense method to combat cybercrime.

1.1 Definition and Types of Cybercrime

The definition of cybercrime is differently interpreted by many, however the most common one is: "an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It is only a cybercrime if a computer, or computers and the internet play a central role in the crime, and not an incidental one." (PWC, 2011)

To be able to understand cybercrime the term cyberspace is clarified, cyberspace: "is not a fixed, predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyber-world is a constructed world, a fabrication. Because it is a construct, cyberspace is mutable; much of it can be modified and transformed." The criminal actors exist in the real world, however their actions are not only reflected in cyberspace because their impacts are affecting the victims also in reality. (Finkela Kristin & Theohary A.Catherine, 2015)

It is intriguing how the definition of cyber-space presents a different perspective when attempting to define cybercrime and differentiating it from traditional crimes that are

carried out through physical means unlike in cybercrime where the crime is done through virtual techniques.

The purpose of showing the types of cybercrimes according to two opposing and diversified sources is to show and clarify the difference in types. Illustrating the different types is important to emphasize so that generalized categories of cybercrimes are not misinterpreted, along with the detailed types of cybercrimes. Since the detailed types offers us a much more concrete clarification of the types, whereby it helps in formulating better strategies and programs attempting to combat the complex and numerous types present. The different types of cybercrime are listed below:

Types of Cybercrime according to KPMG

- *Viruses and worms:* are computer programs that affect the storage device; it duplicates information without the person knowing.
- *Spam emails:* are unwanted emails or junk newsgroup postings. They are problematic if not filtered.
- *Trojan:* it is an illegal program that appears legal, once it is run it locates information related to passwords or it can weaken the system to forthcoming entries. It could destroy programs or data on the hard disk.
- *Denial-of-service (DoS):* this happens when criminals try to immobilize individual websites, computers or networks, by sending excessive messages.
- *Malware*: it is a software that takes control over the individual's computer and spreads a bug to others devices or social networking profiles. This software can be managed at a distance by hackers known as ' herders' they do so to spread

spams or viruses thereby creating a ‘botnet’ and so this enables them to control a network of computers.

- *Scareware*: it is a method that some cyber criminals rely on to force users to download specific software, which at first is provided as anti-virus software, but after a while they attack the user’s system, in this case the user ends up having to pay for the criminals to get rid of the viruses.
- *Phishing:* is a method where a person’s password and login information is stolen. In this case the cyber-criminal can use this to gain access to bank accounts or take over their social network.
- *Fiscal fraud:* in this method the official online payment channels are the target, the cyber-criminals can obstruct processes like tax collection and they can make falsified claims for benefits.
- *State cyber-attacks*: it is believed that some government agencies might be using cyber-attacks as a new means of warfare. As an example, there is one attack that happened in 2010, a computer virus called Stuxnet was utilized and aimed to perform an invisible attack on Iran’s secret nuclear program. The aim was to disable Iran’s uranium enrichment centrifuges.
- *Carders Stealing bank:* this is one of the most common and problematic cybercrimes because bank cards are being duplicated and this allows criminals to withdraw money in stores or at ATMs. (KPMG, 2011)

Table 1: Types of Cybercrime According to PWC

Types of Cybercrime
Economic crime – this type of crime is highly sophisticated, organized and funded it enables cyber-criminals to commit fraud.
Espionage – "organization's valuable intellectual property includes ('IP') includes electronic communications and files as well as traditional IP (Internet Protocol) like research and development ('R&D')." It would be possible for the victim to be unaware that IP theft has occurred, until fake products emerge on the market or another company registers a license based on their R&D.
Activism – attacks are carried out by supporters of an idealistic cause (e.g.) WikiLeaks.
Terrorism – attacks carried out by terrorist groups against state or private assets, this usually known as critical national infrastructure ('CNI') e.g. power, telecoms and financial systems.
Warfare – involves states attacking state or private sector organizations.

Source:(PWC, 2011)

The types of cybercrime mentioned by KMPG, tackle types of cyber- attacks that occur at an individual, organizational and state level unlike the ones that were generally described by PWC. PWC focuses on the types that mainly targets financial institutions and states. It is of significance to point-out the dissimilarities between activism, terrorism and warfare cyber-crimes. The first one is in support for a certain cause, terrorism is a type of

cyberspace attack based on political motives with the purpose of gravely damaging a country's economy or causing loss of life, based on PWC warfare attacks states or private organizations , they fail to clarify how. It may be interpreted as attacks that rely on the use of security, economic or political information to attack states; it could possibly be taken from private organizations that possess any type of this information.

1.2 Research Questions

The Questions are as follows:

1. What are the implications of cybercrime on states and their relations with each other?
2. Who are the actors involved in countering cybercrime in these 4 models?
3. What are the countermeasures that have been taken by the 4 models?
4. How do the 4 models differ in terms of Security?
5. How states are behaving towards cybercrime?
6. How cybercrime and security challenges world dynamics and international relations?
7. Are the suggested defense strategies in this thesis adoptable?

These research questions were chosen because many nations are encountering political, security and economic threats from cybercrime. Examining the types and impacts of cybercrime would help in showing the extent and magnitude of the threat. This would highlight the fact that cybercrimes threats on nations are not just based on directly targeting the security sectors on governmental levels. They are also aiming at other sectors and aspects which are undermining the states' sovereignty (e.g. financial institutions, firms etc...). Also, giving an overview about the actors (e.g. states

cooperating regionally or internationally) countering cybercrime would help in identifying the existing international agreements along with the states that are involved. The countermeasures taken by these four models would emphasize how security measures can no longer be restricted to states since the problem is spreading on a global level. Finally, it would be relevant to illustrate how cybercrime is challenging world dynamics and international relations.

1.3 Hypothesis and Significance

Hypothesis: Due to the increase in the necessity for cyber-security this obligates the nation state to transcend beyond geopolitics towards transnationalism in terms of preserving its sovereignty. There is a possible defense strategy model that could be adopted to minimize the impacts of cybercrime.

Significance: this paper is examining cybercrime since it poses a new threat to states, it is interesting to see the overlap between its economic and security implications especially that economic aspects become security issues when the target is aimed at governmental and financial institutions. The aim is to show the difference in the types and to emphasize the relevance of not misinterpreting generalized categories of cybercrimes along with the detailed types.

Cybercrime poses a threat to the infrastructure of states and to its sovereignty, showing how states respond to countermeasure this aspect is of importance since the world has become more globalized and the concept of security has been altered. Therefore, it

would be costly for states to neglect the threat because the absence of any cybersecurity measures would lead to the downfall of various states worldwide.

Many studies tried to explain the types of cybercrimes and challenges they pose to various nations, in some cases they choose specific countries to demonstrate the difference in the types of cybercrimes faced. They attempt to explain the causes and effects of this phenomenon. The explanations show that it is not easy to combat all the numerous types of cybercrimes, however they do conclude with some possible strategies that would help in decreasing the level of cybercrimes that take place.

This study attempts to explore whether cybercrime might hinder or enhance relations between states, it seeks to propose a security defense model that could be adopted on the international level to try and limit cybercrimes.

1.4 Methodology

The purpose of the study is to conduct a comparative country analysis by focusing on four distinct cyber-security models (USA, China, EU and UAE) to compare their different strategies and to examine their successes and failures. This would help reveal the capacities they have to preserve the state's security and sovereignty. The study is dependent on qualitative research where, the different types of cybercrimes and their impacts are presented based on two dissimilar sources that show these variances. The significance of presenting opposite views is to demonstrate a better understanding of the types of cybercrime countries are exposed to. An examination of the costs of cybercrimes throughout the study is beneficial to uncover the general economic, security and political impact it has on countries. It is noteworthy to know what aspects

are considered when estimating these costs. This also helps in elucidating the level of economic costs it has on a governmental level which includes security institutions. After analyzing the four models the paper seeks to propose a defense strategy that could be used against cybercrime.

1.5 Disposition of the Thesis

The disposition of the thesis consists of five chapters. The introductory chapter introduces the topic and outlines the definition as well as the types of cybercrime, the research questions, the hypothesis and significance of the research, the literature review and finally the methodology. Chapter two would include the literature review and a comparative country analysis on USA and EU cyber-security models which includes examining their different cybercrime divisions, their strategies and their cybersecurity approach on cybercrime. Chapter 3 is a comparative country analysis on UAE and China cyber-security models involved studying their cybercrime divisions, strategies and cybersecurity approaches. It includes an analysis of the costs and impacts of cybercrime, additionally it provides an analysis of factors that classifies states as either strong or weak states in terms of cybersecurity. Moreover, it entails studying the relations of the 4 cybersecurity models (USA, EU, China and UAE). Chapter 4 compares all of the 4 cybersecurity models, it assesses the effectiveness of these models and discusses the challenges and implications of cybercrime. It includes an analysis of international agreements concerning cybercrime. Chapter 5 discusses the conclusion and recommendations, the recommendations propose a cybersecurity defense strategy against cybercrime.

Chapter 2

Literature Review

The first part of this chapter includes the theoretical part concerning cybercrime and proceeds to present a comparative analysis on the first two cybersecurity models USA and EU. International affairs theories aims to study cybercrime in the context of state power. In this research two of the most significant are examined and discussed: the Neo-liberal - Constructivist and Securitization theories. Emphasis was given to cyberspace security in order to demonstrate the conceptual evolution of security in the digital age.

Neo-Liberal Theory:

Neo-liberals argue that both state and non-state actors have a role, even though states have better technological and financial resources but other non-state actors (such as: individuals, organizations etc...) have the capability to cause damage. Concerning the cyberspace realm, neoliberals argue that states cannot attack or defend themselves militarily in a virtual world to solve the security dilemma. Based on the neo-liberal perspective, the security dilemma could be resolved by establishing international institutions that would monitor and sustain cyber security. So on a theoretical level, it would be easier once an institution is established because each member would identify cyber activity and share their defensive strategies and capabilities. This would create transparency and the attack would be easily specified and the attacker would be punished. (Petallides, 2012)

Constructivist Theory:

Constructivists emphasize symbols, ideas and meanings according to Erkisson and Giocomello, they perceive symbolic politics to be significant in studying digital age security. The internet has developed a world of its own where it has developed a continuously evolving identity. From their perspective it involves interactions between states and non-state actors, they consider that the government is no longer able to offer the required security. Therefore, it is essential to maintain the engagement of private, local or individual actors in the networks security where they have the same significance as national and international attempts in protecting the digital environment. (Ionela Maria Ciolan, 2014) (Petallides J. Constantine, 2012)

Erkisson and Giacomello argue that constructivism stresses on how it is inevitable to interpret reality with respect to understanding of the social and political activities. Constructivism aims at studying certain mechanisms and patterns, they state that a material reality and a social reality exist and it is relevant to differentiate between them. Constructivists argue that social reality is prone to change since it is socially constructed, therefore social realities like interests and identities are not stagnant but continuously produced and reproduced. For constructivists, world politics begins at this basic level, where actors have a set of norms or beliefs concerning what is correct and incorrect. As for norms they shape identities, thus distinguishing the "we" from "them" and identities shape interests. According to constructivists, all these components are dynamic and if the interests are no longer the same this means that changes in identities and norms has occurred. (Eriksson Johan, Giacomello Giampiero, 2006)

Securitization theory:

Securitization is a move that carries politics beyond the existing rules of the game and places the issue as a unique type of politics or as an issue above politics. The aspect of politicizing an issue is called securitization. This means any public issue can be non-politicized so in this case the state does not deal with the issue and it is not transformed to an issue that requires the public's decision and debate. On the other hand, if the issue becomes politicized this means that it is of public policy significance to some extent. Moreover, the matter would need a government's decision as well as the government's resource provisions or it would require another form of governing the community. (Buzan Barry, Waever Ole, de Wilde Japp, 1998)

Technological advancements in the military field altered the perceptions and understanding of international relations and security. Traditional methods have been replaced by modern warfare which is based on internet and technology, so the military sector would utilize both public and private communication technologies. Therefore, cyber space and security have become highly significant on both a national and individual level. (Klingova Katarina, 2013)

The new non-military concepts of security are not only restricted to states. New actors have become involved in international security such as certain criminal organizations, groups and hackers that operate within and across state borders in attempts to break national security fields in cyber space. The issue of identifying the actors involved and what issues in security should be focused on constitute a controversial issue for experts

in the debate of cyber space security. Securitization theory became an alternate solution since it was suitable for "cyber space, its characteristics, threats or actors". (Klingova Katarina, 2013)

Securitization reveals how state actors cannot control the cyber space field since it is not restricted only to them, also the state actors lack direct access because the private companies control most of the networks and the providers. Therefore, maintaining security is difficult since military protection is inapplicable and no boundaries exist virtually. (Klingova Katarina, 2013)

The most important part of this theory is the securitizing process, Lene Hansen distinguishes between politicizing and securitization. To politicize an issue means that it is essential and its effects should be discussed and challenged politically. This refers to the public's decision-making process through debates and negotiations. On the other hand, securitization involves taking emergency actions with military actors managing the problem. A security issue comes first, since it threatens the whole existence of a state and its subjects rely on immediate and effective solutions to solve the situation.

Leaders and other actors have a choice in securitizing or not securitizing a certain issue. The decision and certain conceptualization as to how an issue is considered an existential threat is an issue of political choice. The Leaders speech would have to include facilitative conditions to successfully securitize an issue. There are two conditions: "the first is internal, linguistic-grammatical, to follow the rules or act and

the second is external contextual and societal to maintain a position from which the act can be made" (Austin 1975 (1962) in Buzan et al… 1998, p:32, (Klingova Katarina, 2013)) .So to acquire the audience's attention ,the securitizing actors should possess some authority. The second condition depends on competitive actors who continuously try to securitize an issue, because of the customary historical role of the state, it is presumed that state actors have the necessary and appropriate resources at their disposition to manage existential threats. (Klingova Katarina, 2013)

Copenhagen School:

Copenhagen School of security studies, argue that security is about survival and that a matter becomes a security issue, when it constitutes an existential threat to a certain object. This means that what is considered as a threat would require immediate or drastic measures to be resolved. They distinguish themselves from other scholars that provide a traditional military understanding to security. (Klingova Katarina, 2013) Copenhagen School argues that security should be considered as a speech act, where the main argument is not about debating if the threats are real or not, instead it is about the ways in which certain matters could be socially constructed as a threat.

The scholars argue that mentioning the word "security" could be seen as an act where all matters (military, political, economic and environmental) could become viewed as a threat. Not all matters of security could be securitized, a securitizing speech act should follow a certain structure that is taken from war and its meanings of "survival, urgency,

threat and defense." Copenhagen School defines securitization as a speech act that has to meet three criteria. The means of which an actor:

1. "Claims that a referent object is existentially threatened."
2. " Demands the right to take extraordinary measures to deal with that threat"
3. "Convinces the audience that rule-breaking behavior to counter the threat is justified." (Munster Van Rens, 2012)

So basically according to these three criteria, to securitize an issue the actor has to be able to show, that this matter poses an existential threat where the audience would be convinced and approve of it. It is only when the audience have approved to consider it as a security issue where it becomes politicized and so it would allow elites to stop following standard procedures and to directly take the necessary emergency measures. (Diskaya Ali, 2013)

The Copenhagen School acknowledged 5 sectors of security and considered the referent object as a collective of identities. They state five sectors in security: military, political, societal, economic and environmental. (Dani Dani, n.d.)

According to Barry Buzan a representative of the Copenhagen School, the security of a state reflects a combination of threats and liabilities in these five dimensions of national security that were previously stated. Hence, the process of categorizing threats under national security depends on the type of threat and how the receiver sees it. Buzan focused on examining the continuous change in the priority of security among these five

dimensions which are the main catalysts behind the change of one state's security. (Klingova Katarina, 2013)

Even though the Copenhagen School expanded the understanding of security, Buzan and his other colleagues announced societal security to be of great importance and they suggested a reconceptualization of the security field. (Klingova Katarina, 2013)

The constructivist and securitization theory seem to appropriately provide a suitable explanation for this phenomena especially because cybercrime continues to change in types, methods and the criminals involved in it. This study attempts to examine the four cyber-security models from an IR's theoretical perspective concerning the Information Revolution, Security and IR. The analysis includes the relevant actors that are involved in combating cybercrime, the countermeasures that have been taken and it would reveal the difference in terms of security among these models. Such analysis would contribute to understanding how states are behaving towards cybercrime. For this chapter the first two cyber-security models EU and USA are examined.

2.1 USA and EU Cybersecurity Models

USA Cybercrime Divisions:

USA has established a Cyber Crimes Center (known as C3) that investigates and fights cyber-crime on a domestic and international level and in cross-border crimes. There are three units in the C3: the Cyber Crimes Unit, Child Exploitation Investigations Unit and Computer Forensics Unit. These units are listed in table 2 along with their roles:

Table 2: 3 Units of Cyber Crimes Center

Cyber Crime Unit	**Child Exploitation Investigations Unit**	**Computer Forensics Unit**
○ Detect Identity and benefit document fraud as well as money laundering	○ Fight against Sexual exploitation of children	○ They examine digital storage devices that are captured (e.g. flash drives, mobiles etc.…)
○ Detect Financial Fraud and e-payment fraud), Commercial Fraud, Counter-proliferation investigations, Narcotics Trafficking and Illegal exports	○ Fight against the production, advertisement and distribution of child pornography and child sex tourism	○ They must manage digital devices that are volatile, mobile and prone to encryption by users.

Source:(U.S. Immigration and Customs Enforcement, n.d)

Table 3 below presents the existing USA cybercrime divisions.

Table 3: USA Cyber Divisions

USA Cyber Divisions	The Agencies' roles and other branches	Other Agencies
Department of Homeland Security	Ensures the security of federal civilian government networks and secures critical infrastructure National Cybersecurity and Communications Integration Center (NCCIC) oversees four branches: NCCIC operations and Integration (NO and I), US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and National Coordinating Center for Telecommunications (NCC)	United States Secret Service (USSS) investigates cybercrime cases and they are responsible for supervising the activities of the Cyber Crimes Center (EC3) of the ICE
Department of Justice	Federal Bureau of Investigations (FBI) supervises infraguard a platform used to share cyber-threat information with a wide community of industry stakeholders. They serve the state's domestic intelligence agency and the primary law enforcement agency. They maintain Computer Crime and Intellectual Property Section where computer crimes are investigated in cooperation with other governmental agencies, private sectors, academic institutions and foreign colleagues. They guide the National Cyber Investigative Joint Task Force (NCIJTF) that identifies, alters and interrupts cybersecurity threat with the assistance of intelligence alliance Five Eyes (FVEY)	
Department of Defense (DOD)	They protect the Department of Defense networks, systems and information. Defends US homeland and national interests against cyberattacks that have serious implications. They give cyber support to military operational and emergency plans as well as supervising the development of US military's Cyber Mission Force (CMF). Cybercom manages the operations as well as the defense of specified Department of Defense information networks. They ensure US/Allied freedom of action in cyberspace but they oppose this towards their opponents.	

Source:(Dr Van Der Meulen Nicole, Jo A Eun, Soesanto Stefan, 2015)

EU Cybercrime Divisions:

The European Commission developed the European Cybercrime Center (known as EC3) and it began to operate in January 2013.

The main role of EC3: it is a central point in fighting against cybercrime, they assemble all their European cybercrime expertise in order to help the state members in cybercrime investigations. They also have a unified and representative group of European cybercrime investigators across law enforcement and the judiciary. (European Commission Migration and Home Affairs, 2015)

The central role of ENISA: The European Union Agency for Network and Information Security (known as ENISA) is another EU cybersecurity agency, they work for EU institutions and EU member states. Their purpose is to make ENISA'S website a center for sharing information, expertise and best methods in information security. ENISA was created to handle certain technical and scientific responsibilities in information security. Table 4 shows the EU Agencies that are responsible to fight against cybercrime. (Dr Van Der Meulen Nicole, Jo A Eun, Soesanto Stefan, 2015)

Table 4: EU Agencies

	Agencies' Role Against Cybercrime	
European Union Agency for Network and Information (ENISA)	Carries out risk assessment and management. They ease the process of setting up national CERTs.	To improve cyber security and help the European Commission, EU members and business groups to approach, respond and inhibit network and information security problems
European Cyber Crime Center (EC3)	Raises public awareness, spear-heading technological research and development. Gives cyber-intelligence that connects law enforcement authorities, CERTs, industries and academic communities to develop intelligence on risks and from any threats that could arise.	Reduce cybercrime carried out by organized groups affecting sensitive information infrastructure or inflicting serious harm on the victim. **Joint Cybercrime Action Taskforce** they depend on the knowledge of different authorities within and past the EU to carry out prominent international investigations
Eurojust	Provides training for law enforcement authorities and prosecutors to synchronize their cybercrime investigations	Simplifies the process of cross-border cybercrime investigations by giving support to the employment of international mutual legal assistance (MLA) and extradition requests
National Computer Emergency Response Teams (CERTs)	Reacts to information security incidents and gives preliminary security services (e.g. warnings, training etc.…)	
European Union Computer Emergency Response Team (CERT EU)	Prepares for and reacts to cyberattacks on EU institutions and they simplify exchange of good practices	
European Union Cybercrime Task Force (EUCTF)	Serves as a stage for exchanging best practices	

	collaboration on armaments. Develops common crisis response platforms against cyberattacks.	

Source: (Dr Van Der Meulen Nicole, Jo A Eun, Soesanto Stefan, 2015)

2.2 USA and EU Cybersecurity Strategies

After examining the different cybercrime divisions both in EU and USA this section discusses the strategies they have adopted.

USA-strategies

USA focuses on the military part of cyber-security and they depend on international collaboration to improve cyber-security. In 2011, they have announced two strategies: "the Department of Defense Strategy for Operating in Cyberspace and the International Strategy for Cyberspace." The department of Defense has established a military command which is the cyber command; it is responsible for implementing the US's military strategy. The military strategy includes five initiatives: "treating cyberspace as an operational domain, adopt new defense operating notions, to cooperate with other US government departments and the private sector, establishing strong relationships with US allies as well as international partners, and lastly to leverage the US's ingenuity". (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

The international strategy includes seven aspects which the US intends to seek International cooperation on: "e-commerce, cyber-security, legal, military defense, internet governance, international development and internet freedom." Their approach

on these items is through diplomacy, international development and defensive collaboration. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

At a Legislative Level:

USA has developed certain criminal legislations on cybercrime which are as follows:

- 15 USC Chapter 103 - Controlling the Assault of Non-solicited Pornography and Marketing
- 18 USC, Chapter 47, § 1029 - Fraud and related activity in connection with access devices
- 18 USC, Chapter 47, § 1030 - Fraud and related activity in connection with computers
- 18 USC, Chapter 47, § 1037 - Fraud and related activity in connection with electronic mail
- 18 USC Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access

("Cyberwellness Profile United States," 2015)

USA established the following specific regulations and legislations concerning cybersecurity:

- 44 USC Chapter 35, Subchapter III - Information Security (§3541)

- Uniform Electronic Transactions Act - Electronic Signatures in Global and National Commerce Act
- Homeland Security Act - Cyber Security Research and Development Act
- Protecting Children in the 21st Century Act - Children's Internet Protection Act
- Adam Walsh Child Protection and Safety Act - Keeping the Internet Devoid of Sexual Predators Act
- Freedom of Information Act (5 USC § 552) - Privacy Act (5 U.S.C. § 552a)
- Federal Information Security Management Act of 2002

("Cyberwellness Profile United States," 2015)

These are only some of the legislations that have been established in USA, it is important to state that here are many other legislations relating to cybercrime and laws regarding the investigative procedure. USA has taken into account Fraud and related activity as well as the protection of children. Having legislation on cybersecurity research and development is one of the important aspects that USA has taken into consideration. Especially, since this helps USA build up the necessary cybersecurity expertise and skills to fight against cybercrime.

The Role of Public Sector Policy:

The White House Cyber-Security Coordinator who is recognized as the cyber-security Czar is the lead policy office in the US. Their role is to coordinate the work of various federal agencies that were created within individual departments and to manage

criticism which they might face. According to the 2011 international strategy these various agencies are to cooperate with similar international partners.

The US National Institute of Standards and Technology coordinates the National Initiative for Cyber-Security Education. There are four educational pathways: "increasing general cyber-security awareness for the public, formal cyber-security education in K12 (from elementary to high school levels), higher education and vocational programs, enhanced recruitment, growth and maintaining skilled public sector employees in cyber-security. In addition to cyber-security training and professional development needed for government civilian, military as well as contractor personnel". (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

Role of Public Sector Law:

USA is updating many legislations pertaining to cybercrime and the latest update is: a proposal to necessitate an annual report to Congress on foreign cybercrime against US government, industry and individuals along with the attempts to inhibit and prosecute cybercrime by foreign countries and multilateral organizations. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

Role of Private Sector for Profit:

In 2011 the Cyber Intelligence Sharing and Protection Act was presented as a means of enhancing communication between private sectors and the government. This Act enabled US Intelligence agencies to share confidential cyber-threat information with

accepted US companies, also it promotes sharing their information with the government or with other companies. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

FBI:

The FBI has formed partnerships in industries, academia and across all the government in order to combat cybercrime. The FBI's ability and expertise to combine efforts across the diverse programs facilitates their task in investigating, gathering and distributing information about and against cyber threats from criminals, nation-states and terrorists. The Cyber Division has executed Threat Focus Cells and this involves the presence of many experts from different agencies to cooperate and handle certain cyber threats. (Snow. M Gordon, 2011)

In 2015, the DOD developed a cyber-strategy to minimize the risks and to defend and ensure the security of USA's interests. The DOD placed five strategic goals:

1. "Build and Maintain Ready Forces and Capabilities to Conduct Cyberspace Operations."
2. "Defend the DOD Information Network, Secure DOD Data and Mitigate Risks to DOD Missions."
3. "Be Prepared to Defend the U.S Homeland and U.S Vital Interests from Disruptive or Destructive Cyberattacks of Significant Consequence."
4. "Build and Maintain Viable Cyber Options and Plan to Use Those Options to Control Conflict Escalation and to Shape the Conflict Environment at all Stages.

5. "Build and Maintain Robust International Alliances and Partnerships to Deter Shared Threats and Increase International Security and Stability. ("The Department of Defense CyberStrategy," 2015)

European Union- Strategies:

The EU's main strategic activities focus on dealing with Legislation, Reporting System, Internet Governance, Training and Cooperation with the private Sector. (Spiridon Virgil, n.d)

At a Legislative Level:

The strategy of the EU has five strategical objectives: accomplishing cyber resilience, decreasing the level of cybercrime, developing a cyberdefense policy and abilities pertaining to the Common Security and Defense Policy (CSDP), developing industrial and technological resources for cybersecurity and fifth one involves creating a clear international cyberspace policy for the EU as well as promoting EU's fundamental values. (Purser Steve, 2015)

Operational Cooperation and legislation:

When there is a serious request concerning a cyber-attack the EU member states have to respond within eight hours. Threat assessments and strategical analysis of cybercrime would be carried out by the designated EU agencies based on the information that is handed in by member states. They all have to abide by EU legislation on privacy and electronic communication and data protection this is an essential part of the process so

they could efficiently fight against cybercrime. (European Parliamentary Research Service, 2014)

The EU has applied the legislation and provided support in terms of operations, the legislative actions that were taken are seen below in table 5:

Table 5: The EU Legislative Actions

Framework Decision on Combating Fraud and Counterfeiting 2001	**E-Privacy Directive 2002**	**A Directive on Combating Sexual Exploitation of Children Online and Child Pornography 2011**	**A Directive on Attacks against information Systems 2013**
They determine fraud behaviors which EU states must consider as criminal offences that require punishment	Providers of electronic communications services should make sure that the services are secure and they should maintain client information	Their responsibility is to fight against sexual exploitation of children online by offenders trying to attract minors for sexual abuse	Handles large extensive cyber-attacks. Member states are required to fortify cyber-crime laws and to have harsher criminal punishments

Source:(European Commission Migration and Home Affairs, 2015)

At a Strategical Level: The 2009 Stockholm Programme has many measures to combat cybercrime. Europol's 2013 Serious and Organized Crime Threat Assessment sees cybercrime as a growing threat to the EU. The Justice and Home Affairs Council in June 2013, considers fighting organized cybercrime to be one of their main concerns between 2014 and 2017. (European Parliamentary Research Service, 2014)

The Role of Public-Private Sector:

EU established a public-private partnership (PPP) on cybersecurity in order to fortify their cybersecurity industry. The PPP aims at joining industrial and public resources to improve Europe's industrial policy on cybersecurity, it also focuses on a united strategic research and innovation guideline. This partnership assists in establishing trust among the member states and industrial actors and aims to balance the demand and supply for cybersecurity products and services. It would help increase the accessibility of industrial funds through efficient coordination and concentrating on the main technical aspects. The PPP assists in giving a better vision to the European research and innovation quality in cybersecurity and digital privacy.("Cybersecurity Industry," 2015)

2.3 USA and EU's Cybersecurity Approach

The section below seeks to analyze the EU and USA's cybersecurity models by examining the cybersecurity approach they used from a theoretical perspective. Before examining these models, this study discusses the realism and liberalism theory.

Realism:

Realists consider that the international system is anarchic and this obliges states to react based on their own national interests (survival). They focus on three main assumptions: "the state is the primary unit of analysis, states act in a rational way to satisfy their own national interests, power and security are the core values of the state". Realists exclude non-state actors, they consider that non-state actors should not be allowed to use any military power and they state that anarchic conditions result in the

"security dilemma" issue. Realists argue that power is to be measured in terms of military capabilities and the need to strive for security because they are the main forces in world politics. (Eriksson Johan, Giacomello Giampiero, 2006)

Structural realists state five assumptions to explain why states want power, these assumptions are as follows:

1. Great powers are the main actors and they operate in anarchic system
2. All states have some offensive military capabilities
3. States cannot be certain of the intentions of other states
4. The main aim of states is survival
5. States are rational actors and they have the capability to formulate strategies that will increase their chances of survival. (Mearsheimer J. John, n.d)

In brief, the realists place a lot of emphasis on the states' role and its power to protect itself by preserving its sovereignty and its military abilities. According to James Adams, from a realistic perspective the existing literature suggests that cyberspace tends to fall in the realism security model, because it is an anarchic system where states have to defend themselves.

Since there is no governing body to control the occurrences of cybercrime and to punish the actors each state is left to depend on itself in combating cybercrime. Realists argue that states are left with an option to either cooperate or defend themselves against allies who they can probably never trust. This would lead states to continuously try to upgrade and strengthen their defense systems out of fear that other states could build stronger

defense systems which would pose a threat to them. (Rueter C. Nicholas, 2011) (Petallides J. Constantine, 2012)

Offensive and Defensive Realism:

Defensive realists address the offence and defense balance and argue that it tends to be in the defender's favor and states that seek to acquire lots of additional power would end up fighting lost battles. So states would realize that it is better to focus on maintaining their status quo in the balance of power rather than seeking offensive mechanisms that have negative consequences. Offensive realists provide a counter-argument stating that it is inadequate to have balance specifically when balancing coalitions are established. This insufficiency would present a chance for an aggressor to take advantage of their opponents. Offensive realists argue that sometimes attacking could be of benefit but not always. (Mearsheimer J. John, n.d)

John Mearsheimer argues that the current international system is in constant conflict, strife and states will be driven by fear to maximize their power to reach the ultimate goal where they are hegemonic powers. So for states to achieve maximum power, they should have a stronger military system than others. Therefore, they would be relentlessly competing to develop their offensive and defensive capabilities. Hence, this would leave slim opportunities for states to cooperate with each other.

Defensive realists present a different argument by saying that military competition can be avoided if states communicated better and if they properly comprehended the intentions and interests of other states. Defensive realists argue that states only have the

interest to maintain security and do not attempt to acquire more power in the international arena because they are content with their current statuses. Based on this argument the defensive realists claim that since there is a mutual interest in survival, collaboration between states to improve mutual security should be possible. (Rueter C. Nicholas, 2011)(Petallides, 2012)

Liberalism:

The liberal theory focuses on the following aspects in IR: the liberals place emphasis on plurality of international actors, the significance of domestic political factors that determine the international behavior of states, the role of international institutions in creating the rules of behavior for state actors, expansion of the international studies agenda (specifically in the subfield of international political economy) and focusing on issues that are more than just survival methods in an anarchic world. (Eriksson Johan, Giacomello Giampiero, 2006)

Liberals argue that not only state actors have a vital role in international relations because new non-state international actors have surfaced (e.g. transnational corporation, political party networks, social movements etc.…). It is these globally complex and powerful transnational relations that challenge the state's sovereignty on a political, military, and economic level. (Eriksson Johan, Giacomello Giampiero, 2006)

After examining the EU and USA's divisions and strategies, this study deduced the following indicators in table 6 based on the observations noted in their cybersecurity models:

Table 6: Indicators of a realist and liberal approach

Indicators of a Realistic Approach	Indicators of a Liberal Approach
Presence of National Cybercrime Divisions operating only on a National Level	Presence of a National Cybercrime Divisions operating on a National and International Level
Presence of a National Cybercrime Division that collaborates internationally but in a limited manner	Intense international cooperation
The State is responsible for cybersecurity	A Non-State Actor is responsible for cybersecurity
Limited or no exchange of information concerning cybercrime threats and new cybersecurity measures	Presence and Vast exchange of information relating to arising cybercrime threats and new cybersecurity measures

After studying, USA's existing cybercrime divisions and cybersecurity strategies, their strategy seems to lie under the realism theory, more specifically the offensive-defensive theory. Their focus on creating so many cybercrime divisions on a national basis, further emphasizes the state's role and sovereignty in maintaining its cybersecurity. USA's constant evolvement and progression in establishing cybersecurity strategies continues to show the presence of fear from other states, or from the different types of cybercriminals that would attack their critical technological and informational infrastructure.

Part of their new cybersecurity strategy demonstrates a partially liberal approach since it involves collaboration on an international level. EU has a more liberal approach since it focuses on cooperation between member states, the difference between EU and USA strategies could be attributed to the fact that EU is a regional system. Hence, this makes

it difficult for the EU to try and adopt a realist approach. The table 7 below summarizes the dissimilarities that were found in these cybersecurity models:

Table 7: Dissimilarities of USA and EU Cybersecurity Models

USA	EU
Realist approach	Liberal Approach
The cyber-security strategy on a National level	The Cyber-security strategy is on a regional level
Hegemonic power	Presence of great powers and weak states
Focuses more on internal defense and less on international cooperation	Focuses more on international cooperation than internal defense
USA rules are extensive, lack harmony and not as compulsory as the EU	EU rules are stricter and more obligatory

In brief, despite USA's recent efforts to alter their cybersecurity defense strategy to a slightly more liberal approach it can be considered more as a realist ,since their strategies are heavily restricted to a state level with minimal external cooperation. Whereas, EU's strategy highlights the complexity of having a liberal yet strict approach in terms of cybersecurity. These variances between the two emphasize that these models have yet to prove if they would succeed or fail on a future level.

Chapter 3
UAE and China Cybersecurity Models

3.1 UAE and China Cybercrime Divisions

Cybercrime Divisions in UAE:

Over the years, UAE has witnessed a rise in economic activity and especially in the oil and gas industry, this evolvement has made it more vulnerable to cybercrime attacks. Not only is this due to the vast availability of internet in the region and its attractive economic wealth but also due to its fragile cybersecurity system.

There has been a rise in IT security attacks on governmental and industrial data this could be because of the bountiful presence of data in data centers. It is worthy to note that cyber criminals are being motivated by the political uprisings and variables (e.g. unemployment and corruption) in the Arab region.

In UAE cyber threats have been classified into two groups: problems arising from internet or traditional activities of crime and others from internet technology development (e.g. cyber terrorism and cyber theft of delicate data). The second is concerning the usual crime activities that have become sophisticated and advanced by computers (e.g. cases of stealing intellectual property and online sexual exploitation of the youth and others). (Neaimi Abdulla, Ranginya Tago, Lutaaya Philip, 2015)

Table 8 below sums up the existing cybercrime divisions:

Table 8: UAE Cybercrime Divisions

UAE Cybercrime Divisions
Computer Emergency Response Team (CERT)
Telecommunications Regulatory Authority(TRA)
Cyber-Police
National Department of Electronic Security

UAE initiated national security awareness campaigns in November 2007, it was launched by the Computer Emergency Response Team (aeCERT) to protect online information and to have an online identity platform. AeCERT sought to secure sensitive governmental information and blocked access to immoral websites within the region. The Telecommunications Regulatory Authority (TRA) was established in 2003, it is responsible for supervising UAE's telecommunications sector and information technology, as well as internet regulation and assembling a list of websites that should be censored. TRA has a role in informing the cabinet, which is UAE's chief executive body and it is responsible for the execution of a national cyberstrategy and policy. TRA managed to combat several cyber-attacks that aimed to access governmental websites.(Neaimi Abdulla, Ranginya Tago, Lutaaya Philip, 2015) (MoyenOrient3, 2014)

UAE relies on cyber-police and internet surveillance, the cyber-police force is responsible for monitoring the internet. Interestingly, the State Security Apparatus (known as SSA) of Abu- Dhabi has formed a special cybercrime unit to spy on the users and the internet and the SSA receives orders from the emirate's crowned prince. Within the Criminal Investigation Department of Dubai police, the Department of Anti-

Electronic Crimes was formed. This unit was criticized by journalists and others because the authorities had a very general view about cybercrime and its constituents. A National Department of Electronic Security was created by a UAE presidential decree in 2012, surprisingly there is limited information on this new division and its responsibilities. Moreover, it is unclear if it is an additional unit of Abu Dhabi's SSA. (MoyenOrient3, 2014)

UAE is still relatively new in terms of developing its cybersecurity defense system, but it shows potential if further commitment is shown to advance and acquire the necessary skills as well as the divisions needed to fight cybercrime to maintain the state's security.

China Cybercrime Divisions:

Hong Kong Police established a Cyber Security and Technology Crime Bureau to combat cybercrime (CSTCB). This Bureau is accountable for managing cyber security matters, investigating technology crimes, computer forensic examinations and preventing technological crimes.

The CSTCB attempts to improve cyber security and fight technological cybercrime in these three approaches:

1. Promote public awareness of computer and cyber security as well as the risks associated with social media through a multi-agency approach.
2. Improving collaboration with other law enforcement agencies.
3. Enhancing coordination and sharing of expertise when it comes to handling and investigating technological crimes. The Collaboration Teams of Cyber Security

> Division (Col CSD) under CSTCB is responsible for the preparation and application of crime prevention programs on technology crime. Their role is to raise the awareness of technology crime prevention amongst the general public. (Hong Kong Police Force, n.d)

For cybersecurity the National Network and Information Security Coordination Small Group (NNISCSG) was created in 2002 as a sub-group under State Informatization Leading Small Group (SILG) and they established China's National Computer Network Emergency Response Team Coordination Center (CNCERT/CC). The NNISCSG wrote a draft for China's national civilian cyber security strategy where crucial cybersecurity related polices and national strategies were accepted. The Ministry of Public Security is responsible for cybercrime and in protecting critical infrastructure, it also possess a network of research labs that is vastly spread on a national level.

Another division is the CCP (Central Office Confidential Bureau and Central Cryptology Commission also recognized as the State Encryption Bureau), which is accountable for "party, military and civilian encryption management excluding intelligence cryptology". (University of California, San Diego, 2012)

All confidential networks are managed by the CCP (also known as Secretariat Secrets Protection Office) they have been dynamic after the amendment of the state's secrets law in 2009. The Military is involved in the civilian sphere through the front end components of General Staff Department Units. It is noticeable that many divisions have been created for fighting against cybercrime. There are four major security

agencies that manage information security, but there is minimal oversight or managerial level review of these agencies available. The duties and credibility of the four divisions should be examined in order to avoid loopholes in the roles of agencies and in their credentials. (University of California, San Diego, 2012)

In brief table 9 shows the existing cybercrime divisions in China:

Table 9: China Cybercrime Divisions

China Cybercrime divisions
Cyber Security and Technology Crime Bureau (CSTCB)
National Network and Information Security Coordination Small Group (NNISCSG)
Ministry of Public Security
CCP (Central Office Confidential Bureau and Central Cryptology Commission

3.2 UAE and China Cybersecurity Strategies

UAE

UAE began to enhance its ability in terms of combating cybercrime, in 2012, they placed cybercrime legislation and formed a new national authority for cybercrime known as the National Electronic Security Authority (NESA). The independent NESA agency is linked to the UAE Supreme National Security Council. The purpose of NESA is to combat any attacks that target the military and infrastructure, it also supervises cybersecurity in all governmental agencies. The UAE shares a similar concern with

other GCC (Gulf Cooperation Council) states in battling cybersecurity, where their aim is to maintain domestic political control. UAE similarly, to the other GCC states are also worried in enclosing Iran's goals and in maintaining a competitive cooperative balance with its neighboring countries. It is important to mention that USA helped in strengthening UAE and other GCC countries' cyber defenses and provided them with technological assistance it specifically helped UAE through U.S contractors. (Dr Masadeh M.S. Anwar, n.d.)

The UAE established a law in 2006 which is called: the Prevention of Information Technology Crimes (PITC), the law states that Electronic Information refers to any information that is stored, processed, generated and transmitted by an information technology device in any form of signs and sounds. This law specified certain meanings such as Government Data, Information Program and other aspects in order to facilitate its implementation. (Dr Masadeh M.S. Anwar, n.d.)

The PITC Emirates' law (2-2006) has 29 articles the first article is under the title of definitions and the rest have no title. The reason they placed various definitions is to distinguish cybercrime from other crimes that it could be misinterpreted for. Irrespective of the number of articles, they are categorized to 3 types:

Group 1: the use of digital technologies in the commission of cybercrimes

This type includes offenses such as: illegal access to a website or information system (article No.2), forging official documents, hindering accessibility to services, systems,

programs or database (article No.5). Acquiring, modifying and destroying medical records (article No.7). Illegally intercepting, spying or receiving any communication that is transmitted (article No.8), utilizing the internet or other information technology device to illegally access credit card or other electronic card information (article No.11) offenses against individual privacy or family life (article No.16) as well as money laundering offenses (article No.19) (Dr Masadeh M.S. Anwar, n.d.)

Second group: Offenses against communications technologies themselves.

This group involves the use of Internet or information technology device to destroy, alter or deactivate programs, data or information on the Internet or on other information technology device (article No.6). Illegal access to an internet website to alter, destroy or seize control over the address (article No.14). In addition to illegally accessing websites or systems directly through the Internet or other information technology devices in order to obtain, destroy, disclose or manipulate Government data or information which is confidential or confidential pursuant to directives (article No.22) (Dr Masadeh M.S. Anwar, n.d.)

Third group: Traditional offenses supported by communications technologies

This type of offense includes the following: if others utilize the Internet or other information technology devices to threaten or blackmail others to act or omitting to act (article No.9), using the Internet and other devices to use other people's moveable property or forging deeds and using deception with the intention to defraud the victim (article No.10). Arranging, sending or storing information that opposes public morals

with the intent to disseminate it and to operate a venue for that purpose (article No.12). Luring males or females into committing acts of prostitution or fornication by using the Internet or other information technology devices (article No.13). Any offenses against Islam and Shari'a as well as other religions (article No.15).

Establishing a website or publishing information on the Internet and other technological devices in order to facilitate human trafficking (article No.17) or for selling and simplifying the process of trade narcotics and other mind altering substances (article No.18) or for a group involved in promoting programs and ideas that are contradictory to public order and morals (article No.20).

Or for terrorist groups using fictitious names to ease contact with their leaders, members and their ideas. Financial assistance to such groups or publishing knowledge pertaining to the manufacture or combustible, explosive and other devices used in terrorist activities (article No.21) (Dr Masadeh M.S. Anwar, n.d.)

UAE National Security Law:

UAE cyber law penalizes the offender who tries to gain illegal access to acquire information that would affect national security or national economy. Even if the offender failed to obtain the information, they would be implicated because of their intention to get the data and this would be a crime. In this law confidential government data involves: Electronic data and information on banks and financial institutions. (Aldurra Abad Fawaz, 2013)

Role of the Public Sector:

After examining the literature, no data was found on any official national or sector program to share cybersecurity resources within the public and private sector in UAE. ("Cyberwellness Profile United Arab Emirates," 2015)

China

China is concerned with three main things when it comes to security: preserving the regime's stability, fighting against third party threats, and the last one is about the implementation of laws and encouraging novelty in cyberspace. In Hong Kong the Security Bureau Office and the Office of the Government Chief Information Officer (OGCIO) work together in maintaining security from any cyber security threats.

They examine and deal with cyber security issues in order to take the necessary measures to strengthen their cyber security level. In order to protect the local internet infrastructure the (OGCIO) developed an Internet Infrastructure Liaison Group (IILG) in 2005. This was done to offer a platform where communication and exchange of information on issues of stability, security, accessibility and pliability of the local Internet Infrastructure takes place. (Digital 21 Strategy Advisory Committee, 2011) (Adelson Ian, Ahmerd Z. Mellissa, Coyne Vivian, Lim Han, Jia Zhifan, Paisley L.C., Truong Kim, 2014)

Hong Kong was one of the first Asian countries to develop a data privacy regulation in 1996, they have further employed more regulations in 2013, and they placed a very

severe regulation on direct marketing in the world. Hong Kong has legislation against computer crime and it is the Computer Crimes Ordinance. Throughout the recent years, they altered the Telecommunications Ordinance, Crimes Ordinance and Theft Ordinance, new violations have been labelled as crimes and the extent to which they cover offences has expanded. Some changes were made to some of the ordinances as mentioned below:

- Having unauthorized access to computers has been added to the Telecommunications Ordinance
- Property has been extended to entail any program or data in a computer or in a computer storage medium which has been included under Crimes Ordinance.
- Criminal damage to property has been modified and the misuse of a computer program or data has been added to the Under Crimes Ordinance. (Marsh and Mclennan Companies, 2014)

Role of the Public Sector Policy:

There is no official strategy that has been made public in China, their concern in information security is the context. The Governmental departments that are responsible in dealing with cybercrime are as follows: the Ministry of Public Security, the Ministry of Industry, the Ministry of State Security and the Military. In 2006 the National Defense White paper highlighted the "informationization of the military", this included improvement of cyber-warfare abilities and revolutionizing the military network infrastructure.

In 2007, the Ministry of Public Security presented the Multi-Level Protection Scheme, where banks, government and infrastructure companies have to use security technology that was being given by Chinese technology firms, since 2010 its implementation increased. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

Role of the Public Sector Law:

Public Security Bureau is responsible for internal cyber-security as stated in the Computer Information Network and Internet Security, Protection and Management Regulations (1997). In 2011, China's Supreme People's Court and Supreme People's Procuratorate cooperatively issued a legal interpretation which serves the purpose of fighting against internet crimes and hacking in a more hostile manner. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

Role of the Private Sector -for- Profit:

The Ministry of Industry and Information Technology collaborated with ten domestic Chinese search engines to prevent Phishing attacks on online users. In general, the private sector has taken protective measures against cybercrimes. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

Role of the Private Sector Not for-Profit:

The non-profit sector does not have a considerable formal role in China's cybercrime strategy. (Avner Levin, Paul Goodrick & Daria Ilkina, 2015)

3.3 UAE and China's Cybersecurity Approach

Both the realism and liberal theory have been discussed in Chapter 2, so this section includes an analysis of UAE and China's cybersecurity models where their cybersecurity approaches are examined from a theoretical perspective.

After examining China and UAE's divisions and strategies, the following indicators in table 10 were formulated based on the observations noted in their cybersecurity models:

Table 10: Indicators of a Realistic and Liberal Approach (China-UAE)

Indicators of a Realistic Approach in China	**Indicators of possibly adopting a Liberal Approach in UAE**
Presence of National Cybercrime Divisions operating only on a National Level	Planning to have National Cybercrime Divisions operating on a National and International Level
Presence of a National Cybercrime Division that collaborates internationally but in a limited manner	Enhancing international cooperation
The State is responsible for cybersecurity	Promoting intra and interstate cooperation
Limited or no exchange of information concerning cybercrime threats and new cybersecurity measures	Trying to improve the exchange of information relating to arising cybercrime threats and new cybersecurity measures

Based on these indicators China has adopted a realistic approach to fight cybercrime, they emphasize the state's role and they have limited cooperation on an international level. It is probable that they strongly believe it is the state that withholds the country. It is likely they fear accepting other states' assistance, because this would mean they

would have to share information on their security systems and mechanisms when fighting against cybercrime. Hence, they would be concerned that the state would lose its role in protecting and preserving the nation's security.

As for UAE, it is still in the process of developing its cybersecurity mechanisms and strategies but from these indicators it appears to be taking on a liberal approach. This could indicate that there is a correlation between the existence or absence of cybersecurity capabilities and strategies in a state and its approach to adopting a realistic, liberal or semi-liberal approach.

It is evident that UAE's resort to international collaboration is due to the absence of various cybersecurity strategies and issues (e.g. strategy, capability, etc.…) Table 11 summarizes the dissimilarities that were found in these cybersecurity models.

Table 11: Dissimilarities of China and UAE cybersecurity models

China	UAE
Realist approach	Adopting a liberal approach
The presence of an official cybersecurity policy	No national governance roadmap for cybersecurity
Focuses more on internal defense and has limited international cooperation	No internal defense system and there is minimal international cooperation
No dependence on International cooperation to formulate a national cybersecurity strategy	Cooperated with US contractors to assist them in cybersecurity
There is cooperation on the public sector level	Public Sector is not involved
There is no Intra-state cooperation but there is Intra-agency cooperation	No Intra-state and Intra-agency cooperation
No official cyberstrategy is present for the role of the Public Sector	There are policies that have been recognized as the national cybersecurity strategy
Higher level of expertise in cybersecurity	Lack of expertise in cybersecurity
The private sector has taken preventive measures	No apparent Private sector involvement

Source:("Cyberwellness Profile United Arab Emirates," 2015) ("Cyberwellness Profile China," 2015)

These differences highlight the following essential issues discussed below:

China has a cybersecurity strategy but it would need further improvements to minimize the problem and avoid extensive economic damages. As an additional benefit, international cooperation would help them in closing any cybersecurity gaps which they have. China has no official cyberstrategy for the role of the public sector even though they are working together, so this stresses the need of formulating a coherent and official cyberstrategy for this sector. China has taken preventive measures in the private

sector probably because it is usually more targeted than the public sector especially since it has a lot of financial and business institutions.

China has no Intra-state cooperation, which means there is no national or specified sector partnerships that are officially recognized to share cybersecurity resources across borders in China. There is Intra-Agency cooperation and it involves the Annual Chinese Conference on Computer and Network Security which is officially acknowledged as a national or sector-specific program for sharing cybersecurity assets within the public sector. This includes a Central Internet Security and Information Leading Group that improves the level of synchronization between different government department sectors.

As for UAE, it has started to work on cybersecurity, but it lacks a national cybersecurity strategy with a clearer idea of which units should be responsible. This aspect would show if they might need more units to fight cybercrime. UAE has insufficient cybersecurity expertise so capacity- building could help in enhancing their cybersecurity abilities. For UAE at the Intra-State Cooperation level, there is no data available on the existence of any framework for sharing cybersecurity assets across borders with other nation states. On an Intra-Agency level there is no information relating to a framework for sharing cybersecurity resources within the public sector in UAE.(“Cyberwellness Profile United Arab Emirates,” 2015) (“Cyberwellness Profile China,” 2015)

UAE has no cyberstrategy for the public sector and they are not collaborating together so there is a necessity to work on both matters. Involving the public sector would help UAE in clearly delegating responsibilities to the assigned cybersecurity units once they know which sectors are being attacked. It is not apparent that UAE is cooperating with the private sector, hence efforts to cooperate with them could provide them with an opportunity to decrease the level of cybercrime especially since they are more prone to cybercrime attacks.

China's approach would continue to be considered as a realist if it does not alter its cybersecurity strategies and open up to external cooperation rather than limiting it to the state's control. Whereas, UAE illustrates how the absence of cybersecurity strategies is leading it to adopt a more liberal approach in terms of cybersecurity. The absence of cybersecurity strategies would in the long run show if it is a successful catalyst that could drive states to adopt a liberal approach in cybersecurity similarly to UAE's case. It can only be witnessed in the future if China or UAE's model would be more successful to adopt.

3.4 Analysis of the Costs and Impacts of Cybercrime

Costs of Cybercrime:

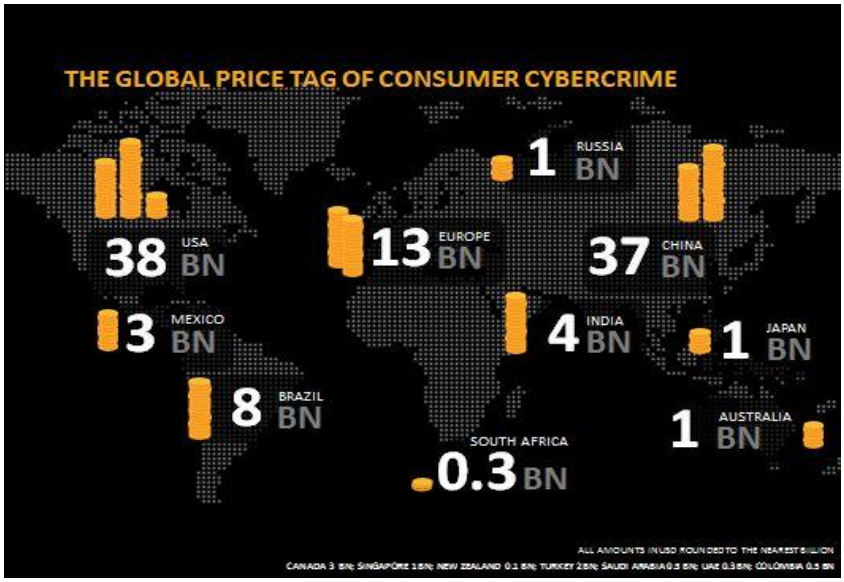
This part of this study examines the costs of cybercrime in these models chosen, it is critical to discuss this aspect since it would show the magnitude of the problem. The existing literature on the costs of cybercrime is limited, no clear set of costs are available only general information is found especially because estimates of cybercrime

are hard to calculate. There are many reasons that make it difficult such as the underreporting of cybercrime incidents and the complexity of getting the exact total cost of the loss. A general overview would be given concerning cybercrime's economic and political impact.

On a global level, the number of individuals experiencing cybercrimes has diminished. However, the average cost per victim has risen, the global price tag of consumer cybercrime is 113$ Billion annually, cost per cyber victim has increased up to 50%. (Paganini Pierluigi, 2013)

According to the data provided in Norton's report (October 9, 2013), the largest number of cybercrime victims seen below in figure 1 is heavily found in Russia (85%), China (77%), and South Africa (73%). The yearly number of victims has been estimated in 378 Million constituting the major price tag of consumer cybercrime in USA ($38 BN), Europe ($13 BN) and China ($37BN). This chart does not include UAE. Intriguingly, the number of cybercrime victims is mostly present in China and not in USA or Europe. Also, the price tag of consumer cybercrime is more prominent in USA and Europe. (Paganini Pierluigi, 2013)

Figure 1: The Global Price Tag of Consumer Cybercrime

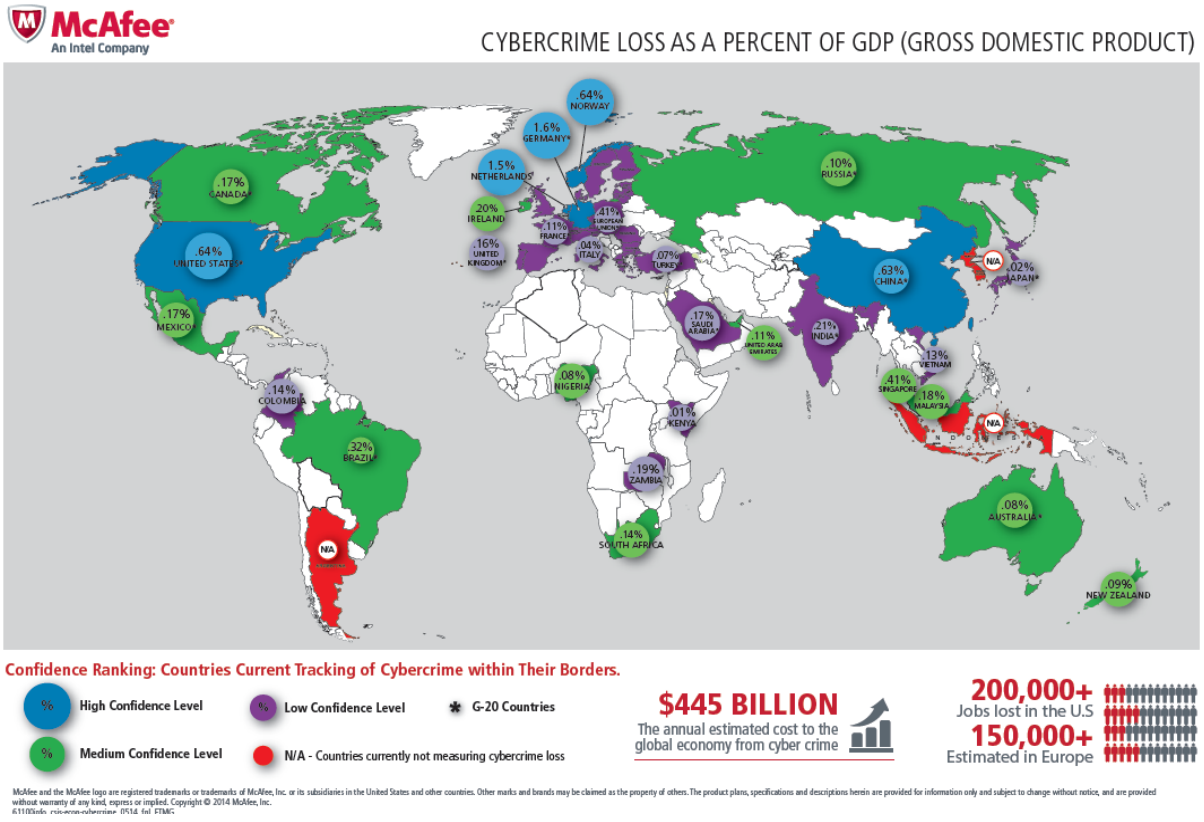


Source:(Paganini Pierluigi, 2013)

Both in China and USA the number of yearly victims is relatively close, this means they are highly attacked.

Figure 2 below measures the cybercrime loss as a percent of GDP in 2014 (Gross Domestic Product). According to the chart, the cybercrime loss for USA is 0.64%, as for China it is 0.63% which is relatively close to USA. The European Union has a loss of 0.41% and UAE's loss is 0.11%, this demonstrates that cybercrime losses are occurring mostly in USA and China. This data shows that UAE seems to be less of a target of cybercrime attacks than the other three but this does not mean that they could be targeted more or less in the future. Even though EU and UAE have a lower percentage loss than USA and China, there is a probability that it could be higher particularly because cybercrime's loss is difficult to calculate.

Figure 2: Cybercrime loss as a percent of GDP



Source:("Cybercrime Loss as a Percent of GDP," 2014)

There are many aspects to consider when assessing the costs of cybercrime and it is significant to reveal an insight to the points that are taken into account. The cost of cybercrime is seen in the amount of losses that are happening on an economic level in countries. General points are provided as a means to demonstrate these costs. Based on Mcafee's report, when estimating costs of cybercrimes and espionage these aspects are relevant to be looked upon:

- The loss of intellectual property is the loss of business –confidential information
- Direct financial loss
- Loss of sensitive business information (negotiating information)

- Opportunity costs includes reduced online trust, the interruption of services
- Additional costs of securing networks and expenditure to recover from cybercrimes
- Reputational damage to the hacked company this affects the reputation of the companies and organizations. (Center for Strategic and International Studies, 2013)

There are other economic costs such as the three kinds of opportunity costs and it is these three types which define the losses from cybercrime: decreased investment in Research and Development, risk averse behavior by businesses and consumers which limits internet usage and the rise of expenditure on network defense. (Center for Strategic and International Studies, 2014)

Economic and Political Impacts of Cybercrime

- **Economic impact**: cybercrimes can affect the economy of countries on an organizational and state level, where it affects markets, consumers and the trust that consumers have. Governments and organizations have to invest in strategies, programs and expensive consultations to repair the damages that cybercrime has. The attempts to calculate the costs is a heavy economic burden on states. Even individuals who are victims of cybercrimes, especially people whose bank accounts have been stolen, would have to start all over to regain their losses. (Center for Strategic and International Studies, 2014)

Cybercrime affects the international financial markets especially that any cyberattack in one country would have negative repercussions on markets worldwide, since they have become interconnected. Consumers' lack of trust would negatively affect E-commerce and lead to loss of revenues. Businesses and insurance companies would have to consider their security budgets, especially the insurance because they would have to reimburse for businesses that have been attacked. (Saini Hemraj, Rao Shankar Yerra, Panda.T.C, 2012)

Too much attention has been given to non-information warfare which leaves the country's national security vulnerable. This makes cyberattacks on information warfare easier for cybercriminals since they find gaps in the system, because no or limited efforts of protection were taken. Also, Cybercrime has impacts on private industries where various industrial sectors especially the big industries are being affected. (Das Sumanjit,Nayak Tapaswini, 2013) (Saini Hemraj, Rao Shankar Yerra,Panda.T.C, 2012)

- **Political impact**: cybercrime has an influence on the relations between nations, because states have become interconnected politically, so how they deal with one another in relevance to cybercrimes would be crucial. The relationships between nations is negatively affected on a national security level, especially when states might be in suspicion of another state's potential use of cybercrimes as a means of war. This creates political instability amongst nations where trust levels decrease. Thus, seriously affecting endeavors of collaboration to combat cybercrimes on a

global level. Furthermore, the willingness of states to share relevant information with others in order to protect their security is a sensitive matter. This issue could be a potential predicament between nations, and it might lead to failure of efforts to achieve global protection measures against cybercrimes.

Another political impact of cybercrimes would be on the military, where attempts are being used to sell governmental and military email addresses this poses a threat to the security of countries. It allows cybercriminals to gain personal and financial data about the representatives. Moreover, this does not stop cybercriminals from trying to access information relating to military operations. (Paganini Pierluigi, 2012)

There are other cybercrime impacts such as the following:

Impact on a Socio- Economic and Political Level:

The level of traditional crimes has increased and is no longer being given the same level of attention, this is because more emphasis has been placed to fight cybercrime. The rise in cybercrime is correlated with other factors such as: the level of urbanization, migration of population from surrounding areas, the level of unemployment, income disparities. So the economic structure and difficulties that people face economically is a contributing factor that makes people more prone to engage in cybercrime. The political system also has a role because they set the norms, rules, preventive measures and methods of controlling crime. The socio-economic aspect could lead to the formation of cybercriminals that try to rebel against the state's system. This presents a different side

of cybercrime, especially if nations intend to punish such groups and based on what evidence. In this case it would be a power struggle between nations trying to preserve their governing systems and between groups that are protesting in the name of people. Moreover, if there are no cybercrime laws existing the offenders would not be punished, hence the political structure and system have an influence when it comes to decreasing the level of cybercrime. (Das Sumanjit,Nayak Tapaswini, 2013)

Impacts on the Youth:

The use of social media and internet has opened a different window of opportunity for cybercriminals to perform cyberattacks. The youth are prone to cybercrime incidents through different social media outlets where they are sexually exploited especially females. Cybercrime incidents specifically sexual exploitation would later on negatively affect the youth's life decisions and self-esteem. It is significant to remember that cybercrime's major impacts are economic and political. Only two other types of impacts were discussed to highlight the existence of other cybercrime impacts, however this does not mean that there are no other impacts. (Das Sumanjit,Nayak Tapaswini, 2013)

3.5 Strong or Weak states in terms of Cybersecurity

This section considers some indicators that lead to the classification of states as strong or weak in terms of cybersecurity. These indicators are based on the analysis of the countries' capabilities that were discussed in Chapter 2 and in this chapter. Table 12 represents these indicators:

Table 12: Indicators of a Strong versus Weak state

Indicators of a Strong State	Indicators of a Weak State
High level of expertise in cybersecurity	No expertise in cybersecurity
Presence of national, regional or international cybercrime divisions	No national, regional or international cybercrime divisions
Presence of cybercrime legislation	Absence of cybercrime legislation
Presence of a high level cybersecurity strategy	No or weak level of cybersecurity strategy
Involved in international cooperation against cybercrime	Not involved in international cooperation against cybercrime
High technological advancement in security tools and systems	No technological advancement in security tools and systems
Presence of experts on cybersecurity	No experts on cybersecurity
High level of education in security studies and in the field of cybersecurity at universities	Security studies and cybersecurity is not taught at universities
High or medium level of public awareness on cybersecurity issues	Absence of public awareness on cybersecurity issues
High or medium level security programs for organizations, institutions and the government	No security programs for organizations, institutions and the government

These indicators could assist in being a guideline to check the strengths and weaknesses of the state's cybersecurity capabilities and it could help distinguish between the indicators that categorizes states as strong or weak. These indicators would contribute to formulating a strong basis for formulating a cybersecurity strategy since it would indicate the gaps that are present.

3.6 Examining the Relations of Cybersecurity Models

The EU is cooperating with other countries by using a cyber diplomacy approach where they focus on five key aspects of cyber diplomacy: supporting and protecting human rights in cyberspace, norms of behavior and applying the existing international law in the area of international security, internet governance, improving competition and prosperity in addition to capacity building and development.

EU-China Relations: in February 2012, the EU-China cybertask force was established at the bilateral summit in Beijing. China has been accused of carrying out cyberattacks on other governments and companies. Despite China's attempt to cooperate internationally on issues of cybercrime, they still place high emphasis on the government's role in managing cybercrimes. EU is careful of the regulatory requirements of China which would lead to an increase in costs and hinder trade as well as innovation. Due to China's violation of human rights and privacy, the EU is not seeking cooperation on cybercrime information-sharing and cybercrime cases. China's continuous efforts to control their cyberspace hinders ongoing EU and China discussions concerning the employment of international law in cyberspace. (Pawlak Patryk, Dietrich, 2015)

EU-USA Relations: The EU-US cyber dialogue was established after the EU-US summit on 26 March 2014. The dialogue involved cooperation within the EU-US Cybersecurity and Cybercrime Working Group that was created in 2011, international and strategic dimensions were added to their cyber relations. The EU-US Working

Group supported the Global Alliance to fight child sexual abuse online thus making it a fruitful collaboration. The working group works on public-private partnerships and incident management.

There is cooperation on an operational level. The aim of the EU- US dialogue is to achieve more stability in cyberspace and to support any efforts concerning this aspect. EU and USA both agree to the UN's GGE (United Nations Governmental Group of Expertise) perspective in 2013, which states that existing international law could be applied to cyberspace. Even though both EU and USA agree on most of the issues, there are some matters that require further discussion such as the collaboration of law enforcement and methods of investigation. (Pawlak Patryk, Dietrich, 2015)

U.S and China relations:

USA and China have cooperated in certain areas (e.g. network intrusions), the FBI has previously assisted the law enforcement units in China. An incident in 2012 led to a cooperation between the Chinese authorities and the U.S when the Chinese were attempting to investigate a fake bank scheme. The APCERT (Asia Pacific Computer Emergency Response Team) has been carrying out exercise drills to be prepared for international collaboration following potential cyber incidents. China takes part in these drills on an annual basis, these drills assist countries in improving their communication protocols, technical abilities and incident reaction.

Since USA prefers a multilateral joint approach for cybersecurity exercises and APCERT allows CERT participations from non-Asia Pacific countries, USA and China could do the drills together. (Adelson Ian, Ahmerd Z. Mellissa, Coyne Vivian, Lim Han, Jia Zhifan, Paisley L.C., Truong Kim, 2014)

U.S and UAE Relations:

USA supports American companies taking part in UAE's cybersecurity market and it is promoting a bilateral defense cooperation. USA is helping UAE deal with cybersecurity threats from Iran and they assisted GCC states by providing advice, technology and services of U.S contractors. USA could have a role in encouraging cooperation among the Gulf States concerning cybersecurity. (George Mason University (School of Public Policy), Virginia Economic Development Partnership's (VEDP), 2014) (Lewis Andrew James, 2014)

Analysis of the EU, China, USA and UAE Relations:

Upon the examination of the EU's relations with China and USA, it can be seen that cybercrime is affecting states behavior towards one another and it is influencing their relations. In this case it seems that China's attitude and willingness to continue to govern their own cyberspace complicates their relations with EU. There are many reasons that would cause a state to close opportunities of cooperation.

Based on the existing literature, it was found that EU has relations with China and USA but none with UAE. On the other hand, UAE has relations only with USA, but neither with EU and China. Only USA has a relation with all three EU, China and UAE. There

is insufficient or hardly any information stating the reasons why there is no UAE- EU and UAE- China relations. This study suggests certain factors that promote or hinder cooperation between states and it is possible that some of these factors play a role in encouraging cooperation between states. The factors are discussed below in table 13:

Table 13: Contributing versus Hindering Factors of Cooperation

Factors contributing to cooperation	Factors hindering cooperation
State's sovereignty is maintained	Loss of the state's sovereignty
Security does not become vulnerable	State's security becomes vulnerable
State's role is not undermined	Undermining the State's role
Presence of trust	Absence of trust
Conditions on security cooperation issues in aspects of the state's security is minimal	Medium to extensive cooperation conditions in aspects of the state's security
Trainings that promote trust between states	No trainings that promote trust between states
The states are of relatively equal technological capabilities	The level of technological capabilities between states highly varies
High or medium level of cybersecurity abilities	Low or non-existent level of cybersecurity abilities
Presence of cybersecurity strategies	Absence of cybersecurity strategies
The presence of positive mutual gains from cooperation	No positive or limited mutual gains from cooperation

Amongst the factors that were listed, the most influential factors would be trust, cybersecurity capabilities, presence of cybersecurity strategies, presence of mutual gains, state's role, security and sovereignty, as well as the equal levels of technology. The remaining factors are highly significant, but they do not have as much of an effect like the other factors when it comes to considering cooperation. Even though a weak

state may place conditions on security cooperation and have no cybersecurity trainings with other states, they have the potential to negotiate these factors and reach an agreement with the strong states.

Whether states have strategies or not it could affect their willingness to cooperate. This could have a very high or relatively low role in cooperation. Some strong states would want to assist weaker ones who have no strategies, and help them achieve the ability and expertise to formulate their own cybersecurity strategies and establish their cybersecurity defense systems. However, certain strong states that are advanced could fear cooperation with weak states especially those with no strategies, because they are concerned that their strategies and techniques would probably be copied or become more advanced.

In cases where some weak states that have strategies, cooperation could prove to be difficult from either the strong or weaker states, because one of them would reject working with the other. Some could oppose any attempts of assistance, because they might consider that they are less likely to be targeted from cybercrime.

Chapter 4

Comparison of the Four Cybersecurity Models

4.1 Assessment of the Effectiveness of the Four Cybersecurity Models

After analyzing USA, EU, China and UAE cybersecurity models, this chapter includes an assessment of the effectiveness of the four cybersecurity strategies in terms of differences and the present gaps in their strategies seen in table 14.

Table 14: Assessment of the four cybersecurity models

USA	EU	China	UAE
Creating many documents, initiatives and agencies makes the system complicated which affects their efficiency. The DHS (Department of Homeland Security) priorities includes resilience building in the cyber domain to secure federal civilian government networks and to protect the infrastructure and to respond to cyber-threats	Fragmentation exists within the EU in terms of coordination between agencies. This is also found in determining and managing the capability gaps among member states. Challenges in execution of plans and facing obstacles	Absence of a unified and coordinated policy method towards cybersecurity China's governance is divided regionally and on a practical level	Lacks a group of strong researchers in the field of cybersecurity. No cooperation between all the stakeholders in UAE region and there is insufficient support from the government
There is no single federal agency. They delegate responsibilities to many federal	There is uncertainty about adopting a formal or informal method for ensuring the	Disorganization of an unmanageable military network, intelligence and other state units	The top management in many government agencies need to be very cautious in the planning

departments and agencies. The new cyberdefense strategy focuses on offensive abilities and USA's will to mention the opponents	participation of the main actors in cybersecurity. There are dissimilar opinions and explanations being given	who have a role in cyber policy, activity and who are responsible with international as well as domestic security.	process for the organizations. Organizations should adopt cybersecurity in their strategies.
Despite many proposals and ramifications, passage into law is still an obstacle because of technical and legal hindrances. The absence of a central and cohesive plan that assigns the distinct roles and responsibilities for the main agencies in the field of cybersecurity.	No clarity concerning to whom the Network and Information Security (NIS) directive applies. There are difficulties in the definition it covers and the sources of its contentions		At a legislation level it is still relatively weak

Source:(Dr Van Der Meulen Nicole, Jo A Eun, Soesanto Stefan, 2015) (University of California, San Diego, 2012) (Neaimi Abdulla, Ranginya Tago, Lutaaya Philip, 2015)

Despite China's technological advancement it is not as capable as USA to handle cybercrime, they have many steps that are needed in order to constrain the problem from escalating. A very intriguing case was the UAE, even though it is a Middle Eastern country that is prosperous, they are lacking in terms of the essential expertise and measures needed to deal with cybercrime. On the other hand, it is a step forward because they have issued laws pertaining to the matter.

It appears that USA and the EU are at a more advanced level in cybersecurity systems than China and UAE. UAE has yet to enhance its ability against cybercrime and have all the necessary stakeholders involved in formulating a cohesive and clear strategy. As for USA, it reveals the complications of having many departments, this should help China, UAE and EU recognize that opening up several branches would only complicate the system and it would hinder their efficiency in responding to cybercrime threats. They could benefit from USA's mistakes by realizing that such a problem hinders effective cooperation and productivity.

USA's different cybercrime divisions constitute a challenge in dealing with cybercrime since it increases the complexity of the process and results in overlapping responsibilities between the designated agencies. This also results in a lack of effective implementation of the cybercrime practices. EU's cybersecurity system still has weaknesses that need to be improved, the EU should focus on strengthening the existing agencies and avoid creating more agencies like USA.

Establishing new cybercrime divisions should only be considered if there is a need or if an obviously huge gap should be covered, so it would be in the best interest of the EU to create new divisions only under certain circumstances. The EU members disagree about the role of law enforcement in cybersecurity, many disapprove of involving the law enforcement to help fight against cybercrime. The EU should try to have better coordination capabilities among the existing agencies and efforts are further needed to agree on the main actors that should be involved in cybersecurity. The Network and

Information Security (NIS) directive requires all states to have the minimal level of national cyber capabilities. Despite its purpose, the EU lacks clarity when it comes to considering who the NIS directive applies to.

The EU's approach towards cybersecurity is distinguished from the rest of the cybersecurity models. The EU's approach is divide into 4 aspects that include the Network and Information Security measures, Critical Information Infrastructure Protection (CIIP), fighting cybercrime and in having a framework for electronic communications where both data protection and privacy issues are included. (Di Camillio Federica, Miranda Valérie, 2016)

The EU faces difficulty in having common standards and equivalent levels of cybersecurity competence among member states. The distinctions in cybersecurity capabilities and the dissimilar priorities among EU members remains an impediment and it affects their level of efficiency. Whereas, China has censorship and they focus on ideological threats rather than technical. This means they would prevent any information that might lead the Chinese citizens to revolt against the regime, because this would result in political and economic instability.

China is focusing on information security from a political aspect and this has not led to effectiveness on the technical level concerning network security. Unbalanced law enforcement measures, disjointed bureaucracy and fragmented security measures are driving factors that led Chinese cybercriminals to target on a domestic level. This

flawed system generates an open online economy that is secretively operative and so cybercriminals target more victims domestically since it is less likely that the police would react. (Lindsay R. Jon, 2014)

This open online economy is called the "Chinese Underground Hacking Economy", the inefficient response of the law enforcement has led the cybercriminals to thrive. The hackers' businesses revolves around 5 categories: theft of real assets, theft of virtual assets online, cyber theft of IP (Internet Protocol) as well as sensitive information, abuse of internet resources and services for profit and the final category that includes creating and distributing internet crime tools and techniques. Moreover, China does not involve small or medium sized privately owned businesses in the development of security standards that are supported by the state. (Chen Jong De Jing, 2014)

China's case illustrates the negative consequences of having weak domestic laws to prosecute cybercriminals and in effectively implementing the laws. It is essential for China to develop a coordinated approach towards cybersecurity and their governance should be more domestic oriented than regional. Their focus on regional governance would result in differences of cybersecurity governance on a regional and domestic level, this would affect their ability to cooperate with neighboring countries and in handling cybercrime on a domestic level.

UAE's legislation is still weak compared to the other 3 models, the public and private sector are not involved. Censorship is another element which affects their ability in formulating cybersecurity strategies that take into consideration the negative implications of censorship on the country as a whole. More consideration needs to be given to the

planning process by high levels of management in organizations. For instance, incorporating cybersecurity measures in the organizations would help against cybercrime. At a legislative level, UAE needs to determine the stakeholders involved along with their responsibilities. The establishment of a clear coordination policy between agencies is needed, in order to evade any overlap in responsibilities and to ensure effective response measures against cybercrime.

Overall, the 4 cyber-security models have flaws in their systems, neither of the models could be chosen as the best model, because based on this assessment each of the systems has vulnerabilities that need to be further advanced. However, it could be mentioned that the USA and EU model represent a better standing in cybersecurity, but they set the example of how even industrialized countries still have more work to do in creating a suitable and effective cybersecurity defense system. USA and EU could learn from the mistakes found in their systems and China has to work on cooperating internationally and in fortifying its domestic cybersecurity system. USA's system demonstrates the ineffectiveness of having many agencies, because this would lead to an overlap in cybersecurity responsibilities amongst the agencies and it would make cooperation between them more difficult.

The lesson here is for states to examine and assess the different weaknesses in their cybersecurity systems because this would contribute to the development of better strategies and precautionary measures. Countries like UAE have a better chance in building a strong cybersecurity system by learning from the mistakes of other states in this case from USA, EU and China.

This issue would be to UAE's advantage because they would be able to avoid the same errors that the others have done and this would equip them with the essential components that need to be considered when developing cybersecurity strategies, policies and measures against cybercrime. Table 15 demonstrates the dissimilarities between the 4 cybersecurity models:

Table 15: Dissimilarities between the four cybersecurity models

	USA	**EU**	**China**	**UAE**
APPROACH	Realist	Liberal	Realist	Adopting liberal
STRATEGY	National level	Regional level	Official cybersecurity policy	Officially recognition of two policies as national strategy
POWER	Hegemonic	Great powers and weak states	Rising	Not Rising
COOPERATION	More Internal defense than international cooperation	More International cooperation than internal defense	Focuses more on Internal defense than international cooperation	No internal defense and minimal international cooperation
DEPENDENCY	Independent	Independent	Independent	Cooperated with US contractors
REGULATION	Extensive, lack harmony, and not as compulsory as the EU	Strict and obligatory	Not so strict and lack harmony	Does not have many
COOPERATE WITH PUBLIC SECTOR	Present	Partnership established	Present	Present

USA and China both appear to have realist approaches towards cybercrime unlike the EU which has a more liberal approach. In the case of UAE it is still relatively new in

establishing a cybersecurity strategy, but the existing literature suggests that it is adopting a liberal approach. When it comes to cybersecurity strategies the USA, China and EU have cybersecurity strategies as for UAE they announced two policies (the General Policy for the Telecommunications Sector and the Cabinet Resolution No.21 of 2013 concerning Information Security Regulation in Government Entities) as their official national cybersecurity strategy. ("Cyberwellness Profile United Arab Emirates," 2015).The different level of cybersecurity strategies between the three countries and UAE, indicates that UAE needs to reflect on several missing cybersecurity issues in their strategy to have better cybersecurity capabilities.

The USA is a hegemonic power compared to China and UAE, whereas, EU is a regional power that has strong and weak member states and China is a rising power as opposed to UAE. The power levels in these cybersecurity defense models varies, there could be a relation between the state's level of power and its need to constantly upgrade its cybersecurity defense system and the type of approach it adopts. Based on the analysis, USA has a stronger economic, political and technological stance than the remaining 3 countries and so to maintain its stand in the international arena it appears to have adopted a more of an offensive than a defensive cybersecurity strategy. It is a country that is not dependent on other regional states like the EU.

The presence of other weaker EU states makes their regional cybersecurity system vulnerable because they would have to continuously monitor and invest in increasing the cybersecurity of others in order to build a solid regional cybersecurity system.

Even though there are other EU countries that are strong in their own cybersecurity systems, economically they are dependent on others hence their ability to frequently upgrade their systems is not an easy task. The dependence of EU states on their unity is also an aspect of their weakness in terms of economy and cybersecurity, possessing advanced cybersecurity systems as well as investing in agencies, policies, technologies is a costly budget. So EU should consider a mechanism that would enable it to strengthen their cybersecurity abilities and to have a certain budget for cybersecurity.

It is imperative to highlight that EU has a regional cybersecurity strategy devised and it is only evident that some EU countries have national cybersecurity strategies and not all. The absence of cybersecurity strategies among certain EU states increases the gap in decreasing the level of cybercrime regionally. It also causes disparities when attempting to follow regional legislations and regulations pertaining to cybersecurity.

Despite the differences between China and USA they share the same concern in concentrating on their internal cybersecurity defense systems and they have limited cooperation in the international arena. As opposed to EU, where they have less focus on their internal cybersecurity defense system and more involvement in international cooperation. However, this does not signify that EU has not placed the necessary foundations at the legislative, operative and strategical level. USA, EU and China established their own cybersecurity strategies independently of any international cooperation. Even though USA, EU, and China created their own strategies it was important to show this difference that both on a state and regional level these

cybersecurity models were independent. It is only UAE who sought international assistance with U.S contractors to create their cybersecurity strategies.

This would be due to the lack of expertise that UAE has in the field of cybersecurity. The UAE has yet to build its cybersecurity defense system and they have minimal international cooperation. In terms of rules and regulations USA has many but they lack harmony, unlike EU where the rules are very strict and more mandatory.
On the other hand, UAE does not have many rules that reveal if there is harmony or if the rules are strict. USA, EU and China are cooperating with the public sector but UAE has no cybersecurity strategy that has involved the public sector. The EU has worked on involving the public and private sectors in their cybersecurity strategy. However, despite the EU's efforts there remains more challenges to close the gap between EU states and to be able to effectively fight against cybercrime.

In UAE's case it is essential for them to include the public sector because it involves many institutions (e.g. financial, Ministries and so forth) that could be negatively affected by cybercrime. Table 16 compares the differences among the existing strategies through the following aspects: Legal, Technical, Organizational, Capacity Building, Cooperation and Child Online Protection.

Table 16: Comparison of the four cybersecurity models' existing strategies

	USA	EU	China	UAE
Legal Measures				
Criminal Legislation on Cybercrime	Present	Present	Present	Present
Legislations and regulations relating to cybersecurity	Present	Present	Present	Present
Technical Measures				
Types of CERTs	Presence of CIRT: US CERT and an Industrial Control Systems (ICS-CERT)	Presence of CERTs	Presence of a CIRT:CNCERT	Presence of CIRT: aCERT
Presence of Standards and Certification	Present	Present initiatives to incorporate Standards and Certification	Presence of Standards No Certification	No Standards No Certification
Organizational Measures				
Policy	Present	Present	Present	Present
Roadmap for Governance	Present	Present	Not Present	Not Present
Responsible Agency	Present	Present	Present	Present
National Benchmarking	Present	No but they established Guidelines	Not Present	Not Present
Capacity Building				
Standardization Development	Present	Presence of initiatives to incorporate Standards and Certification	Present	Present *(aCERT)
Manpower Development	Present	Present	Present	Present
Professional Certification	No data available	No data available	Not present	Present
Agency	No data	No data	Not Present	No data

Certification	available	available		available
Cooperation				
Intrastate	Present	Present	No official recognition of intra-state cooperation	No data available
Interstate	Present	Present	Present	No data available
Public Sector	Present	Present	Present	No data available
International	Present	Present	Present	Present
Child Online Protection				
Legislation	Present	Present	Present	Present

*ACERT provides necessary standards, guidelines, and cybersecurity practices that can be implemented in public or private sectors.

Sources:("Cyberwellness Profile China," 2015)
("Cyberwellness Profile United Arab Emirates," 2015)
("Cyberwellness Profile United States," 2015)
(Wennerström Erik, 2004)
(Council of the European Union, 2015)
(European Commission Migration and Home Affairs, 2015)
(Purser Steve, 2014)

Based on this table, there are differences between these countries in the levels of technical measures, capacity building, organizational and cooperation. It is noteworthy to state that in the technical measures the standards that are examined are related to technical standards concerning cybersecurity. On the technical level China has standards but no certification whereas UAE has neither. As for the cooperative level, the cooperation was examined at an intra-state level (across borders or with other nations) level and at an intra-state agency level (national or sector-specific programs for sharing cybersecurity assets). Both USA and EU have intra-state and intra-state agency cooperation, in comparison to China's absence of official intra-state cooperation. China

only has intra-agency cooperation, as for UAE no available information is present on intra-state or intra-state agency level cooperation.

All the 3 countries have international and public sector cooperation except UAE, they have international cooperation. In capacity buildings the standards that are examined relates to cybersecurity standards and practices that could be implemented in specific sectors (public or private). Finally, there is a slight dissimilarity in the organizational measures where both China and UAE have no roadmap governance as opposed to USA and EU. Even though USA and EU have better measures than the others, it is still noted throughout the research that more improvements would be needed. The existing gaps in the systems of all the cybersecurity models is attributed to the numerous challenges that affect their ability in dealing with cybercrime. UAE's cybersecurity model is weaker compared to the rest, but it is a good start that they have begun to take some measures and so the reasons behind their vulnerable system lies in challenges and their lack of expertise in matters of cybersecurity. The ongoing problems these countries face internally is coordination and awareness between governments, agencies and organizations, whereas at the inter-state level they lack coordination, information sharing on the security and economic level.

4.2 Challenges and Implications of Cybercrime on States

Certain cybercrime challenges are discussed in this section some of which are as follows: Responsibility, Legislative, Technical, Organizational, Educational, Economic,

Political and cybersecurity challenges. There are other general sets of cybercrime challenges that exist, these tend to be more common since some states have yet to develop the necessary cybersecurity measures on various levels.

Responsibility: there should be clearly defined roles for the assigned agencies that are responsible for handling cybersecurity issues. The lack of harmony, consistency and efficiency of the designated agencies would lead to the deterioration of cooperation amongst agencies and such a flawed system would make a country's cybersecurity abilities vulnerable and more susceptible to cybercrime. (El-Guindy N. Mohamed, 2016)

Legislative: the absence or lack of sufficient legislations concerning cybercrime would make it difficult to distinguish between the types of punishment needed according to the type of cybercrime committed. Attempts to adopt regular jurisdictional measures when dealing with cybercrime is a wrong approach, since most of the cybercrime cases are carried out through the internet. However, this could probably work in some cases but overall regular measures would not apply. (El-Guindy N. Mohamed, 2016)

Detecting cybercrime and identifying the attacker is challenging and so taking the necessary prosecution measures would be difficult in this case. Determining the type and amount of costs lost through cybercrime attacks is another factor that obstructs the investigative process and in taking the appropriate punishment measures. Law enforcement agencies need to have the essential and modern instruments to be able to investigate cybercrime incidents especially because there is an increase in the use of

ICTs (Information and Communications Technology) by the offenders. (ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector, 2009) (El-Guindy N. Mohamed, 2016)

Many countries have dissimilar national cybercrime laws because they have various factors such as legal and constitutional differences. Legal jurisdiction is one of the elements that complicates the prosecution of cybercriminals especially if the cybercrime attacks are carried out on an international level or across borders. (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)

Technical Challenges:

Depending on ICT: Globally there is a high level of dependence on Information and Communications Technology (ICT), this makes the countries' critical infrastructure more vulnerable to cybercrime attacks especially because the current technical infrastructure is weak since there is a standardized operating system. Moreover, this reliance on ICTs jeopardizes military communication. (Gercke Marco, 2012)

Number of Internet Users: the number of internet users has increased worldwide and this number continues to increase, so the task of detecting the cybercriminals and tracking the source of the attack is a continuously evolving challenge for governments. This would force governments to regularly seek various and new methods to be able to

enhance their cybersecurity abilities and skills in detecting and tracking cybercrime attacks and the offenders. (Gercke Marco, 2012)

Devises and Access: Irrespective if the country is developed or developing, computer devices and access have become easily obtainable for anyone. Technologies are being sold at cheaper prices in black markets, even second- hand technologies so it would not matter if the device is old or new. Despite the high costs of internet in developing countries than developed countries, offenders would not use an internet service, but instead they would utilize services that do not require registration. Hence, this method that is used by offenders would decrease their chances of being identified and getting caught. (Gercke Marco, 2012)

Accessible Information: there are many webpages available on the internet and information is constantly being updated. The use of complex search engines and the availability of illegal internet sites that are exclusive for internet hackers and cybercrime offenders is problematic. The offenders use the complex search engines to screen out many results that are related to information on computer security issues. (Gercke Marco, 2012)

Missing Mechanisms of Control: there are no laws governing the internet, only some law makers and law enforcement agencies began to establish legal standards that require a degree of central control to some extent. Initially, the internet was designed as a military network with a basis of a decentralized network where the structure of the network was supposed to maintain its functionality as a whole. The internet's network infrastructure was created in a way to resist external efforts of control and it was not

designed to simplify investigative processes or to hinder attacks from within the network. (Gercke Marco, 2012)

Speed of Data Exchange Process: The fast transference of information in a short period of time minimizes the chance for law enforcement agencies to gather evidence that would help their investigation. Transferring information no longer requires the need for a person to be physically present in order to deliver a message to others. The short and rapid amount of time taken for the process of data exchange, limits the law enforcement's ability to estimate the amount of damage that has been done and in discovering how much information has been lost. (ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector, 2009)

Organizational Challenges:

Absence of developing the necessary organizational structure required to handle cybercrime and the lack of competent professionals would make organizations easy cybercrime targets. Any non-existent or insufficient cooperation between organizations and the designated actors responsible to deal with cybercrime matters makes it harder to prevent cybercrime attacks. Another factor would be the absence or presence of primitive precautionary measures against cybercrime. Moreover, increasing budgets for cybersecurity defense systems, investing in professionals, reporting mechanisms are other costs that an organization would need to consider.

Educational Challenges:

Many countries lack the necessary expertise, education and awareness about cybercrime. Inexperienced states would benefit from others that are well advanced in

cybersecurity issues, however improvements in this area would require some cooperation between states which is still a complex process due to the lack of trust present among many states. (El-Guindy N. Mohamed, 2016)

Economic Challenges:

Governments would have to invest in enhancing their cybersecurity defense systems to keep up with the level of modern technologies and techniques used by cybercriminals. Organizations would have to incorporate cybersecurity technology programs within their systems to obstruct extensive economic damages to their businesses.

Political Challenges:

Convincing nations to share their security attacks, cybersecurity expertise and skills with one another is an obstacle, since there is mistrust among nations and fear of exposing technical weaknesses in their systems. On the other hand, nations fear that others might take and build on their cybersecurity knowledge for offensive purposes that would serve their interests rather than using them for defensive aims against cybercriminals that are putting at stake the state's economy and national security.

Cybersecurity Challenges:

Cybercrime distinguishes itself from traditional crimes, cybercrime differs in terms of proximity, restricted scale, the physical constrictions and patterns. In cybercrime it is difficult to locate the offender and to prosecute them especially if the attack has been done in several countries. In such cases the obstruction of justice is due to the type of

cybercrime committed which is a transborder and transnational cybercrime. Secondly, the scale of cybercrime occurs on a wider extent targeting more victims and critical infrastructure. Thirdly, cybercrime offenders rely on this type of crime because they would be inconspicuousness to the law, they evade leaving any trace of evidence behind. The offenders commit the crime quickly, especially since it can be done in a more obscured manner. It would be hard to find patterns since there is no substantial accurate statistics and there are no standard definitions of offenses. Moreover, classifying cybercrime as an offence is not simple. (Brenner Susan, n.d.)

General Challenges of Cybercrime:

Cybercrime also has more general challenges that appear to be common among most countries, these challenges are:

- Absence or inadequate presence of awareness about cybersecurity issues
- Lack of trained and qualified manpower to conduct the necessary counter measures.
- No particular email account policy especially for the defense forces, police and security agency personnel.
- Cyber-attacks are being carried out from terrorists and from other countries
- There is no requirement that obligates a person who is joining the police force, to have the minimal and necessary knowledge about computer sectors. So they have no information about cybercrime and this makes them ineligible to handle any cybercrime issues.

- Cyber technology changes rapidly and it is constantly ahead of the advancement and evolvement of governmental sectors, thus the government becomes unable to track the source of cybercrime incidents.
- There is no encouragement or progression of the Research and Development in ICTs so they are not up to the required standards.
- Security forces and law enforcement personnel are unarmed and unprepared to handle sophisticated high- tech crimes.
- Current protocols and legislations are insufficient especially in terms of identifying and clarifying the investigative responsibility for crimes that occur on an international level.
- Scales of the crime (e.g. targets more victims)
- Jurisdictional Issues (e.g. borders,)

  (Poonia Singh Ajeet, 2014)(Police Executive Research Forum, 2014)

Cybercrime Classification Challenges:

There are several types of cybercrime and this constitutes a challenge for governments when they create a cybersecurity strategy, this issue would affect their ability to create suitable measures that are efficient in fighting against cybercrime. It would be easier if cybercrimes were classified into categories. According to Dr Poonia, there are 4 suggested categories of classification of cybercrime: cybercrime against individuals, property, organization and society. Even though this study suggests 4 classifications more can be added to the list such as cybercrime against a state's national security, economy and multiple states. (Poonia Singh Ajeet, 2014)

These challenges have negative implications because they are obstacles that many states face and in certain cases it could affect the relations between states. Cybercrime can affect the economic trade between states as well as political relations in cases where cybercrime is being carried out by a state against another state. The states are at a disadvantage because they have to frequently upgrade their cybersecurity systems and to heavily invest in taking the necessary precautionary measures that would assist them in limiting the level of cybercrime.

4.3 Analysis of International Agreements

This section discusses some of the international cooperation agreements that have been created to fight against cybercrime. The purpose of discussing the existing international agreements is to highlight the efforts that have been done and to indicate the factors that have been considered in the agreements. These agreements give us a general overview of the states that have participated in and the responsibilities they have agreed upon. The distinction between these agreements unfolds the different aims each of them serves against cybercrime. It provides some perspective on how states are behaving towards cybercrime by taking into account the challenges and weaknesses in their systems as well as placing efforts to remove the existing loopholes. These agreements would show if they succeeded or failed to serve their purpose.

Convention of Cybercrime:

The 2004 Budapest Convention on Cybercrime of the Council of Europe is currently the only treaty on cybercrime which is internationally binding. This convention which is also known as the Budapest Convention, is supposed to be a guide that states can benefit from.

It would help states establish their national legislation on cybercrime and it sets the structural basis for international cooperation. A principle concerning internet service providers and law enforcement agencies was placed among the principles that were placed for international cooperation. This convention includes the types of cybercrime and considers cyberattacks to be illegal irrespective of the intentions of the attacker. (United Nations Institute for Disarmament Research, 2013)

Group of Eight:

This agreement includes the following eight governments: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States. The agreement included principles concerning "freedom, privacy, and respect, protection of intellectual property, multi-stakeholder governance, cybersecurity and prosecution of crime". All the stakeholders involved would help provide information to the government and assist them in developing the standards of behavior and common methods in the use of cyberspace. The purpose of this group was to create a sharing mechanism among the industrial nations in order to prevent, investigate and prosecute cybercrimes. (United Nations Institute for Disarmament Research, 2013)

Shanghai Cooperation Organization (SCO):

This organization was created in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan. They meet annually and collaborated on issues of "security, economics and culture, they also worked on matters concerning energy, communication and transport". In 2011, they agreed on cooperating in the realm of Information Security.

It clarified that any release of information that had negative repercussions on the state's security would be considered as threats (e.g. threat to the socio-political or socio-economic system).The SCO has a written proposal that was founded on their agreement for the establishment of an "International Code of Conduct for Information Security." (United Nations Institute for Disarmament Research, 2013)

United Nations:

The United Nations General Assembly agreed on a set of resolutions relating to ICTs and cybersecurity, the purpose of these resolutions was to obtain the responsiveness of the UN member states' to the future cyber challenges. There are many UN agencies that are responsible in handling diverse levels of cybersecurity. Telecommunication and information security became a resolution in 1999, later on the General Assembly placed two new resolutions in 2003 and 2004, the first resolution is the formation of a " Global Culture of Cybersecurity and the Protection of Critical Infrastructures." The first resolution requires capable states to act and collaborate in order to inhibit, detect and react to security incidences. The second resolution requests the cooperation of all the pertinent international organizations and member states to share their expertise and necessary measures that would be beneficial for other member states to learn from while they attempt to have good cybersecurity systems. (United Nations Institute for Disarmament Research, 2013)

International Telecommunications Union (ITU):

The United Nations has a specialized ITU agency that is responsible for regulating telecommunications and the usage of the radio frequency spectrum. ITU has a crucial part in setting telecommunication security standards. The ITU is attempting to include cybersecurity but there are disputes among the member states about what limits are to be put concerning the ITUs involvement.

They are working to provide standards and technical assistance and they are trying to create technical guidelines that help defend and preserve the critical infrastructure. Their activities include training development for developing countries. In 2007, they released the Global Cybersecurity Agenda which aimed at giving a specific structure where all stakeholders could collaborate and come up with an international reaction towards the continuously arising challenges in cybersecurity. One of its other goals is getting the stakeholders to increase confidence and security in the information society. ITU cooperates with the International Multilateral Partnership against Cyber Threats and a forum for Incident Response and Security Teams. It is worth mentioning that the forum gives accreditation to computer emergency response teams (CERTs) worldwide. (United Nations Institute for Disarmament Research, 2013)

European Union:

Since the 2008 report on Implementation of the European Security Strategy, cyber threats have been considered a new threat to European Security. The EU focused on taking measures to fight cyberattacks and cybercrime, as well as ensuring the protection of the

critical infrastructure and network security. Their efforts regarding the protection of network and information have been existent since 2005. In October 2010, the EU has formulated a new EU Internal Security Strategy. The purpose of the new strategy is to enhance the level of cybersecurity for the EU citizens and businesses. In 2012 they had a CERT network which entailed all EU institutions and in 2013 they created the EU Cybercrime Centre. There is an information-sharing platform for EU since 2009, despite that they introduced the European Information Sharing and Alert System in 2013.

They considered having cybersecurity exercises and creating operative CERTS in all the EU states by the end of 2012, the purpose of this was to defend Europe from massive and extensive cyberattacks. (United Nations Institute for Disarmament Research, 2013) Currently, EU is seeking to establish a clear understanding of Cyber warfare, improving its cyber abilities worldwide, working on strengthening cyber defense in the EU and working on NATO's cyber defense policy. (Cîrlig-Cristina Carmen, 2014)
The agreements were analyzed according to their types and aims in table 17.

Table 17: Analysis of the International Agreements

Convention Of Cybercrime	**Group of Eight**	**Shanghai Cooperation Organization**	**UN**	**EU**	**ITU**
Internationally Binding	An agreement between industrial countries	A regional Cooperation	It is an International Agency	A regional cooperation	It is a UN agency
Addresses Legislative Issues	Addresses freedom, privacy, respect, protection of intellectual property, multi-stakeholder governance, cybersecurity and prosecution of crime	Works on issues of Security (e.g. cooperation in information security)	Established 2 resolutions: global culture of cybersecurity and protecting critical infrastructure	Has measures to fight cybercrime attacks and protect critical infrastructure	Sets Telecommunication standards and develops technical guidelines that help defend and preserve Critical infrastructure. Trains developing countries
Distinguishes the different types of Cybercrime	Holds all stakeholders responsible in sharing information with the government. Aims to establish norms and common approaches in the use of cyberspace.	They established an international code of conduct for Information Security	Requires states to cooperate	Requires EU member states cooperation	
	Aims to become a mechanism that is used among the industrial countries to prevent, investigate and prosecute cybercrimes		Sharing expertise and measures against cybersecurity includes: international organizations and states	Taking into account the role of the Business sector. Information Sharing includes: EU states	

Source:(United Nations Institute for Disarmament Research, 2013)

Upon examination of these agreements the following results were found:

- The agreements have different purposes
- The agreements involve only certain states and excludes others
- Each agreement addressed a different aspect to fight cybercrime
- No standard aspects of cybercrime were mentioned (e.g. types, legal measures and so forth)
- No other sectors were considered in the planning process of cybersecurity measures

EU and the Shanghai agreement are the only agreements that considered other sectors, but the involvement and cooperation of other sectors remains limited. The Convention of Cybercrime is the single exception where the standard aspects of cybercrime were mentioned.

These agreements were foundations for further efforts between countries, hence they cannot be classified as successful or failed agreements since the countries continued to eliminate or reduce any errors that were previously made. They accounted for the essential aspects that were previously neglected or overlooked. This shows how these agreements helped set the framework which states could build on and it is noted in the cases of the following agreements:

In 2015, the Shanghai Cooperation Organization members wrote an updated draft of the international code of conduct for information security. The UN has updated a clearer version of the norms and principles. It included certain norms that are

internationally expected from states and specific principles that should serve the international security. (United Nations, 2015)

There was a development of a new EU strategy. As an example to show what has been changed in the agreement the New EU Strategy is discussed below:

New EU strategy:

The EU has developed a new strategy which illustrates their persistence in trying to improve their efforts on cybersecurity and in achieving better coordination between the member states. The new strategy includes empowering criminal justice authorities to participate in international cooperation on cybercrime and electronic evidence depending on the foundations of the Budapest Convention on cybercrime. The objective of this project is to increase the number of states partaking in international cooperation by utilizing the Budapest Convention as their conjoint basis.

This project also seeks to increase and improve the legislation and criminal justice capabilities to fight against cybercrime and electronic evidence. The project includes the expansion and promotion of the international police and judicial cooperation on cybercrime and electronic evidence. Another goal is to have the public and private sector share information in accordance to the data protection necessities. The EU would evaluate any advancements and outcomes that occur on cybercrime in order to take them into account when developing future policies and strategies. (Council of Europe, n.d.)

They have included standardization in their new strategy, since this would help advance the private and public sector information security's approaches in identifying and reacting towards any arising threats and technological changes. The EU has also formed a Cyber

Security Coordination Group in order to give advice on a strategical level in IT security, Network and Information Security and Cybersecurity. (Purser Steve, 2014)
In this new strategy they were able to improve on the legislative level and in international cooperation because they added aspects that were previously not given the sufficient attention (e.g. international police, judicial cooperation). One of the benefits of their new strategy revolves around their incorporation of standards and further involvement of the public and private sector.

This shows further advancement in cybersecurity measures. Despite these efforts, assessment and monitoring would be continuously needed, since this would be an effective mechanism in detecting the failures, successes or gaps in previous policies and strategies. This would allow further progress and in increasing cooperation and cybersecurity defense systems among EU countries.

The aim of having examined these agreements is to expose the flaws and difficulties that are faced when international cooperation takes places, these aspects would be considered in the process of developing the proposed cybersecurity defense strategy that is to be discussed in the next chapter.

Chapter 5

Conclusion and Recommendations

5.1 Conclusion

Cybercrime is a rising threat where many governments fear that information could be accessed by different cybercriminals and transnational organizations that have the intention of causing political, economic and security instabilities in their countries. The world is intensively integrated so the fall of one country's economy could affect the others' investments, banks and trade. This problem needs global cooperation from all nations, also certain strategies and techniques need improvement. This research revealed the distinctions between USA, EU, China and UAE cybersecurity models. The research examined the various implications of cybercrime on states and their relations with each other, it also highlighted the different actors involved in handling cybercrime in these countries.

These 4 cybersecurity models utilized dissimilar countermeasures and their difference in security was seen through the analysis of the strategies, agencies and legislations which they have. Cybercrime has many challenges that affect the world dynamics and these 4 models illustrate how it is difficult to contain cybercrime irrespective of their capability levels. This shows how the states are behaving towards cybercrime, the analysis of their approaches ended in an interesting result. The outcome revealed that the presence or absence of existing cyber strategies in a country has an influential role in contributing or hindering possible cooperation with other states. Also, the presence of positive mutual gains (e.g. a state's economy) has an impact on cooperation.

So these two interesting results could lead the state to adopt a realistic or liberal approach towards cybersecurity. China is an example of how advanced states have a realistic approach towards cybersecurity, this aspect demonstrates how other similar states fear the loss of their sovereignty and control over their country's political situation. Such states would continue to fall short in their cybersecurity systems, since they have a limited level of cooperation with others and their political priorities seem to come first. In general, all of the 4 cybersecurity models are affected by cybercrime, however the magnitude of damage occurring in each country varies.

The Prisoner's Dilemma helps in understanding how cybercrime has altered world dynamics, because states are faced with a new arising threat where they have to make decisions concerning their cybersecurity. According to Jervis, the Prisoner's Dilemma theory states that the actors have no solution that lies in the participants' best interest. There are offensive and defensive incentives that would cause them to defect from their alliance with others. Defecting would be the only rational option if the game is to be played only once, but if it is repeated this aspect no longer applies. To prevent the others from having the power to defect, each of the participants would give up this ability if others were controlled in a similar manner. If the others are not restrained, then it is in the actor's interest to keep the power of defecting. Figure 3 below demonstrates the two circumstances with the numbers representing the order of the actors' preferences.

Figure 3: The Prisoner's Dilemma Chart

	Cooperate	Defect
Cooperate	2 2	1 4
Defect	4 1	3 3

Source: (Jervis Robert, 1978)

So in Cybersecurity states have these options either to cooperate or not, cybercrime is a phenomena in which states would play the prisoner's dilemma constantly since this situation raises a significant question which is: what makes cooperation more or less likely between states? The chances of states cooperating and reaching CC could increase by the following: 1) anything that increases and stimulates the actor's interest to cooperate by increasing the gains of mutual cooperation (CC) and/ or decreasing the price that the actor will pay if he cooperates and the other does not (CD). 2) Anything that decreases the incentives for defecting by decreasing the gains of exploiting the other (DC), 3) anything that increases the expectation of both sides that the other will cooperate. (Jervis Robert, 1978)

The prisoner's theory contributes to perceiving cybercrime from another perspective, for instance, states would be more likely to cooperate when their national security is being threatened or in cases where both countries would mutually benefit. On the other hand, they might chose to cooperate to know the vulnerabilities of other states and

utilize it for their advantage. However, it would be inevitable for all states not to cooperate at all since the world has become more interdependent and it is more likely that any high level threat of cybercrime in one state would negatively affect others especially in terms of economic and security aspects. EU is an example of how the states could be affected. This leads to one more issue concerning the states that have no cybersecurity strategies or have just begun like UAE, these states would be driven by either economic reasons or by fear. When such states become more economically wealthy, they would begin to feel the need to develop or improve the cybersecurity gaps in their systems.

This could especially occur if foreign partners fear placing their investments in states that lack cybersecurity in a modern world which is heavily dependent on technology and economic databases could be breached.

The discrepancies are not just perceived in these 4 cybersecurity models, they are also witnessed between many others. The on-growing problem emphasizes the need of collaboration between countries, so they would avoid a rapid downfall where the issue spills from one country to another. Countries would have a better chance in facing cybercrime and its challenges through unified efforts. The current security differences merely add to the complexity and continuity of the crisis which could possibly lead to worse situations that result in more economic losses and security threats. Cybercrimes cannot be eradicated since technological advancement is constantly arming the hackers and the attackers with new means to target countries' economies as well as their

securities. The spread of awareness and transference of expertise do have an extensive role in shaping the global security of nations, especially because they are interdependent. After studying these issues and carefully analyzing the differences and errors done in international agreements, this study proposes a cybersecurity defense strategy against cybercrime. This raises the following question: could this proposed defense strategy against cybercrime be adopted?

5.2 Recommendations

5.2.1 Proposed Cybersecurity Defense Strategy on a National Level:

As a recommendation this paper proposes a cybersecurity defense strategy against cybercrime. This strategy would provide a framework for countries that have no cybersecurity strategies and it would help other countries that are advanced in cybersecurity to check or include some aspects that have been left out.

Before introducing the proposed strategy, states should distinguish between three aspects: Cybercrime, Cyber-attacks and Cyberwarfare.

There are important characteristics below that distinguish between cybercrime, cyber-attack and cyber-warfare:

- Only non-state actors are involved
- Violation of criminal law done through the usage of a computer system
- Aims to challenge the functionality of a computer network
- The presence of political or national security goals
- The impact is equal to an armed attack or the act takes place in the situation of an armed conflict

Based on these characteristics, cybercrime involves only non-state actors and they violate criminal law since the act has been done through a computer. Both cyber-attack and cyber-warfare aim to undermine the functionality of a computer network and both have political and national security goals, but only cyber-warfare can result in an impact similar to an armed conflict or it takes place in the setting of an armed conflict. (Hathaway A.Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, 2011)

It is important to recall that there is no universal agreement concerning the definition of cybercrime, as previously discussed cybercrime involves economic crimes using computers and the internet. Cyber-attacks include attacks that are done by state actors, excluding the involvement of an armed conflict and by not allowing the attack to reach an armed attack. A cyber-attack could be also done by non-state actors that do not permit the attack to become an armed attack.

This type of attack is not considered as cybercrime since the criminals have not been incriminated by law on a national or international level. There is an overlap between cybercrime and cyber-attacks this is when non-state actors commit illegal crimes by utilizing computer networks in order to undermine this network and the crime has political or national security purposes. This case does not include the escalation of the act to an armed attack otherwise it would be viewed as cyber-warfare. (Hathaway A.Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, 2011)

Cyber-warfare differs from the two but it would also involve a cyber-attack. Cyber warfare includes actions that are done by nation- states or international organizations with the intention of attacking and harming other nation's computers or information networks. (Rand Corporation, n.d)

There is a commonality between the two, in the first case, cyber-warfare includes attacks that any actor takes on in the framework of an armed conflict. However, this act does not classify as a cyber-crime since there is a possibility that it is not viewed as war crimes or because the technique did not involve the usage of computers. So it could not be classified as a cyber-crime due to both these reasons. In the second case, the attacks done by the state actor could result in outcomes equally similar to traditional armed attacks. This attack could be considered legal or illegal since the act is being done by a state actor. (Hathaway A.Oona, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia, 2011)

It has been found throughout the research that differentiating between cybercrime, cyber-attacks and cyberwarfare is controversial. These characteristics are debatable because it would be difficult to find out who the attacker is without considering the crime as a violation of criminal law and with excluding the use of the computer as a tool. So irrespective if cyber-attacks and cyberwarfare are considered as separate categories or certain types of cybercrime,states should account for these issues during the planning of their cybersecurity strategies.

The proposed strategy includes two phases, the first part is the foundational basis and the second part of the strategy is a detailed one that includes several levels that need to be considered throughout the planning process.

Proposed Cybersecurity Defense Strategy Phase 1:

It is significant that all national strategies reach the following objectives: identify, protect, detect and respond.

Identify: to identify cybercrime threats states need to have a comprehensive understanding of their systems, resources, data and abilities.

Protect: necessary establishment and implementation of precautionary measures would be required to preserve and protect the critical infrastructure.

Detect: certain measures should be created and applied to detect the occurrence of any cybersecurity incidences.

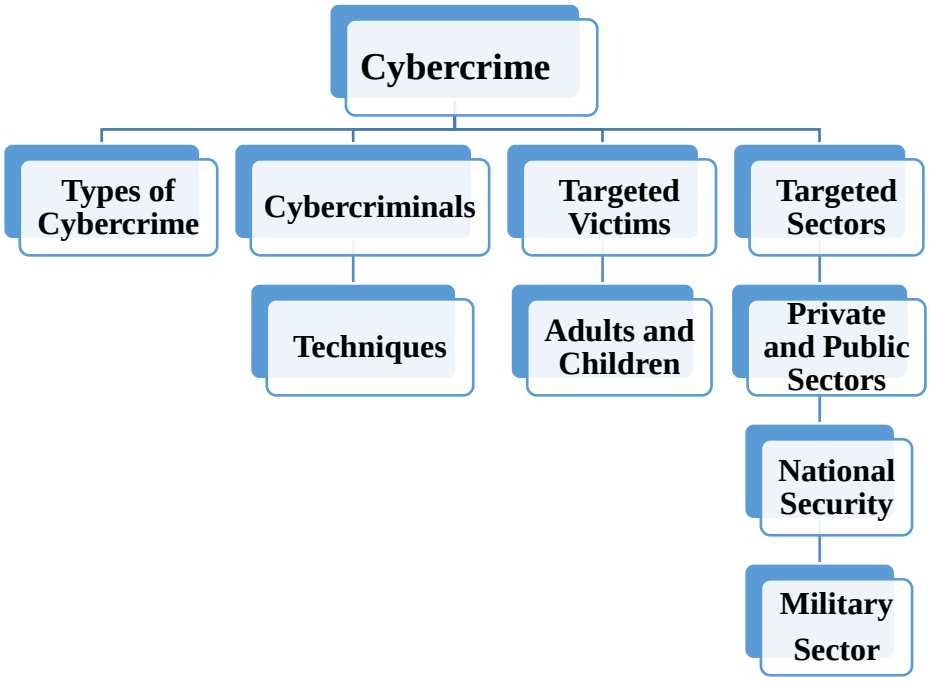
Respond: creating and employing the suitable processes needed to react towards cybersecurity incidents. (National Institute of Standards and Technology, 2014)

The proposed strategy contributes in providing the essential cybersecurity framework for countries, since it includes the basic elements that are needed in order to create and develop their own cybersecurity strategies. When states begin to formulate a national cybersecurity defense strategy it is imperative for them to include the following aspects listed below:

- A clear definition of cybercrime

- Define, list and distinguish the types of cybercrime (especially distinguish between cybercrime, cyber-attacks and cyberwarfare)
- Define and state the categories of cybercriminals
- State known cybercrime techniques used by cybercriminals
- Prepare precautionary measures for targeted victims (e.g. Adults and Children) and targeted sectors

Figure 4: Proposed Cybersecurity Defense Strategy Phase 1



It would be helpful to examine which sectors are mostly targeted and the most common cybercrime threats that the state is facing. This is a general checklist of some of the most common cybercrime attacks:

- Illegal data interference or system damage
- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data

- Computer-related copyright and trademark offences
- Sending or controlling sending of SPAM
- Computer-related fraud and forgery
- Computer-related acts involving racism and xenophobia
- Computer-related acts in support of terrorism offences
- Breach of privacy or data protection measures
- Computer-related identity offences
- Computer-related solicitation or ‘grooming’ of children
- Computer-related acts causing personal harm
- Computer-related production, distribution or possession of child pornography (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)

When devising countermeasures against cybercrime, it would be useful to see which sectors are mostly attacked by cybercrime. The following sectors that should be examined are: Defense, Energy, Transportation, Communication, Technology, Financial Services, Manufacturing, Banking/Insurance, Health Care, Retail, Public Sector, Services, Industrial, Hospitality as well as the Education and Research sector.
If the states do not have the sufficient expertise to devise the plan, it is recommended that they seek cooperation with other states and try to improve the awareness level.

Moreover, increasing the education level in cybersecurity fields would assist them in the long-run. In the case where there are no education programs in this field, research

and development is an aspect which would assist them in developing the required programs needed in the field of security. Creating these programs alongside external cooperation would be more helpful for states, since they could learn from other state's experiences concerning the necessary elements that the education program needs to include.

Proposed Cybersecurity Defense Strategy Phase Two:

The development of phase two of the strategy involves these levels:

Legal (including Child Online Protection Measures), Technical, Organizational, Capacity Building and Cooperation.

Legal Measures:

On a legal level states should account for issues such as:

- **Criminalization:** there are some acts considered to be cyber-specific acts under certain laws and other acts that are categorized as a general offense. So it is important that states clearly define which acts are considered as criminal offenses. (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)
- **Investigative Process:** there should be certain cyber-specific laws because using general laws and traditional investigative methods would not be sufficient to face the challenges of investigating a cybercrime incident. Traditional laws do not include imperceptible data, so the investigative laws should be able to handle the nature of electronic evidence and the masking methods used by offenders (e.g. Encryption, multiple internet routing connection.). Investigating

cybercrime should include: a clarified range of applying investigative powers to ensure legal confidence in its use and it requires adequate legal authority for actions which protect and maintain computer data and the collected stored data.(Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)

- **Jurisdiction and International Cooperation:** Transnational acts should be prosecuted at two jurisdictional levels the "substantive and investigative". At the substantive level some cybercrime cases are transnational and so states should be knowledgeable if their national criminal law applies to an offense that has partially occurred in its jurisdictions. On the investigative level, the state would need to proceed with the investigative process that concerns the other state's territory. In such cases formal and informal consent would be needed, but having international treaty laws at a both multilateral and bilateral level allows states to investigate without violating the sovereignty of other states.(Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)
- **Usage of Military for Cybersecurity:** states should carefully consider when the interference of the military is needed for cybersecurity. Any stolen governmental information , especially regarding defense systems poses a threat to national security.(Wallace Ian, 2016)

- **Computer Crime Laws:** Criminal and legal preventive measures should be developed against attacks that compromise the discretion, veracity and security of

computer systems. (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013) (Organization of American States, n.d)

- **Procedure Laws for Gathering Electronic Evidence:** states should have clear procedural measures that are according to international standards which enables governmental access to communications and stored data when required during investigative purposes. (Organization of American States, n.d)
- **Prevention:** this includes having the necessary principles that are: leadership, cooperation as well as the rule of law and having organizational skills which include preventive plans and this plan should have clear objectives. Application techniques, approaches and the development of national cybercrime strategies would assist in decreasing the possibility of crime. (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)
- **Reporting Mechanism:** there should be a reporting mechanism developed to provide the victim with right to file a cybercrime complaint. It is highly essential to clarify the role of designated agencies and the law enforcement officers when it comes to handling any cybersecurity complaints. It would be helpful for states to devise a reporting mechanism that includes the victim's personal details (e.g. name, age, address, contact details and so forth), the type and date of incident, the types of damages, the amount of damages and information that would help capture the suspect. (Akhgar Babak, Brewster Benjamin (CENTRIC), Politopoulou Vicky, Kavallieros Dimitrios, Drogkaris Prokopios (KEMEA), 2013)

In case of any financial damages information concerning the account numbers and the way in which the finances were lost need to be collected. It would be helpful if states created reporting mechanisms on 5 levels: personal, financial, organizational, Intellectual property and online child exploitation activities. The purpose of having these categories would serve as a guideline.

- **Public-Private cooperation:** most of the internet providers are from the private sector which means cyberspace is mostly owned and operated by them, so it is essential that policies include public-private partnerships. For instance it would include businesses, academia, the civil society and so forth. (BIAC, CSISAC and ITAC, 2012)

It is significant for states to know the 7 main constituents that need to be included in a national cybersecurity strategy in order to have an efficient cyber legislation and they are as follows:

- Information Sharing
- Cyber Insurance
- Cyber Supply Chain Security
- Cyber Self Defense
- Awareness, Education and Training
- Cyber Workforce
- Cybersecurity and Borders (Bucci Steven, Rosenzweig Paul, Inserra David, 2013)

Overall these constituents are crucial, but two of them raise certain aspects cyber insurance and cyber supply chain security. There is no accountability held by the private sector actors that are responsible for cybersecurity when third parties bear the costs caused by cybersecurity breaches. In other words the consumer would have to deal with the costs. Hence, establishing a liability system which obligates the providers of goods and services to pay for the damages that resulted from their failure in taking some protective measures is a vital step. Concerning the cyber supply chain security issue, hardware and major infrastructure constituents are important because it is a matter that is not been accounted for.

Any weaknesses in softwares could be mended by companies but hardware security problems would need to be replaced, so making sure that these electronic appliances are highly secure is important. Creating or assigning a certain organization that assesses, evaluates and accredits the technology companies' for their supply chain security is a helpful step. This would hold these companies responsible in ensuring a high standard level of security in their technical equipment and softwares.(Bucci Steven, Rosenzweig Paul, Inserra David, 2013)

Technical Measures:

Technical measures should include the establishment of cybersecurity standards, it is important that the standards are identified and assessed. There are certain technical components that count such as: building trust, information sharing and communication,

statistics, digital forensics, protection of critical information infrastructures and reporting mechanisms.

Building Trust:

Establishing trust between all members of the team or agencies is important, certain trust building activities are needed to ensure the collaboration and efficiency among the teams or agencies.(De Muynck (ENISA) Jo, Belasovs Agris, Dufkova Andrea, Portesi Silvia, 2012)

Information Sharing and Communication:

Communication should be present between the designated divisions that are responsible in handling cybercrime issues. A common approach should be used when classifying and encrypting information when communicating. (De Muynck (ENISA) Jo, Belasovs Agris, Dufkova Andrea, Portesi Silvia, 2012)

Statistics:

Statistical data should be collected on the level of cybercrime incidents taking into consideration the scale and damages that has been done. Collecting statistics would help the cybercrime centers or designated divisions in finding out certain cybercrime patterns and emerging cybercrime trends. It would be a beneficial decision making instrument since it would also reveal existing gaps in a state's cybersecurity system. (De Muynck (ENISA) Jo, Belasovs Agris, Dufkova Andrea, Portesi Silvia, 2012)

Digital Forensics:

There should be a digital forensic division that is responsible for recovering and investigating material that is present in digital and computer systems. This would enable the experts to trace and find out the offender's actions. It is essential for the experts to make sure that no modifications could occur to the original data by using a unique device called "write blocker". Especially, since the write blocker are devices that permit the procurement of information on a drive without creating a chance for it to coincidentally damage the drive contents. (Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva, 2013)

Protection of Critical Information Infrastructures:

This term is used to describe governmental assets that society needs in order to function. Protecting critical infrastructure means preserving it irrespective if it is physical or virtual because any attempts to damage or destroy would have a negative impact on the nation's security. The public and private owners and operators have a role in protecting the state's infrastructure. To be able to manage cybersecurity risks it is important to establish a clear understanding of the owners' systems. (National Institute of Standards and Technology, 2014)

Detection of cybercrimes:

Detection of cybercrimes is normally carried out by forensic experts due to its complexity; there are diverse types of detection methods that include: intrusion detection, fraud detection and suspicious content detection. Detection of cybercrimes can also occur on technical levels which might include certain softwares or programs that can do so,

despite these detection methods, cybercrimes might still occur because of the high level technological techniques that are being used by cyber criminals.

There was no abundant information found in this research while attempting to find the exact main detection methods of cybercrime on a general level, moreover even the very technical detection methods that were found were limited in numbers. Hence, this reveals the need for further efforts to be taken by countries by investing in ways to detect and combat cybercrimes. (Lallement Patrick, n.d)

Network Protection Strategy Principles:

There are main elements to bear in mind when working on the technical level, these elements include the following: network protection strategy principles which include protecting their Uniform access management, secure communications, ensure the security of the IT system, staff training and having security baselines. Protecting the uniform access management includes authentication and authorization of services so as to control the usage of a resource. It is essential that the IT develops the security baselines where the devices only give the needed services for the business. (Dr Wamala Frederick, 2012)

Organization Skills and Measures:

These measures include accounting for policies, a roadmap for governance, a responsible agency and a national benchmark. The roadmap would serve as a guide concerning the governance of cybersecurity. Assigning a responsible agency or agencies to be the primary cybersecurity actors is important, so they would be able to monitor, coordinate and ensure the implementation of cybersecurity strategies, policies and the roadmap. The

national benchmark would be a checklist that would provide a detailed and basic level of guidance on setting the needed security measures for operating systems and applications. (“Cyberwellness Profile United States,” 2015)

On another level overall coordination between all the designated agencies is needed to minimize any overlaps that could occur and to ensure better efficiency in the implementation process of the cybersecurity measures.

Organizational Measures:

The 5 essential functions that an organization should be doing in order to have good cybersecurity includes the following: identify, protect, detect, respond and recover. This means, it is imperative for organizations to comprehend how they should manage cybersecurity risks that could affect their systems, assets, data and capabilities. They should be able to take control and carry out the proper procedures in order to protect themselves from any possible security threats. Continuous supervision would be needed so that they can have a proper alert system of certain cybersecurity incidents. Organizations should have the essential policies and activities that are crucial in promptly responding to cybersecurity threats. Finally, they should continue to combat cybercrime and regain their abilities after the occurrence of any cyber intrusion. The 5 elements and their role in empowering organizations against cybercrime could help in diminishing the damages and repercussions of cybercrime. (Mickelberg Kevin, Pollard Neal, Schive Laurie, 2014)

There are many protection measures that the organization can take to decrease the level of cybercrimes, some of the measures are:

- Involving the CEO
- Ensuring that the organization is well prepared against cybercrimes
- Being aware about any new cybercrime issues
- Setting a team that can act and adapt to any cyber incident
- Recruit people with the necessary skills and expertise
- Take legal actions against cybercriminals once found
- Improve legal protection (Non-disclosure agreements, patents and so forth) (Gilhawley Damian, 2012)

Last but not least, a Cybersecurity Control Checklist would help organizations assess their cybersecurity systems. The elements that need to be considered are: personal security, physical security, technical security (e.g. account and password management and confidentiality of sensitive data) contingency and recovery plan, cybersecurity awareness and education in addition to compliance and audit. Despite the suggested measures that organizations could use, it is important for them to consider these 8 cybersecurity issues that should be of a concern. The 8 cybersecurity issues are:

1. Spending and having an inefficient strategy is unwise

Strategies should be linked to business objectives, with allocation of resources tied to risks.

2. Business partners fly under the security radar

Partners might infiltrate systems by relying on third parties but many organizations overlook third-party security.

3. A missing link in the supply chain

Flow of data to supply chain partners continues and they are not required to adhere to privacy and security policies.

4. Slow moves in mobile security

Mobile technologies and risks are proliferating but security efforts are not keeping up.

5. Failing to assess for threats is risky

Organizations usually include cyber risks in enterprise risk-management programs but they do not assess threats regularly.

6. It takes a team to beat the offender

External collaboration is essential to identify the threats and in improving cybersecurity but many organizations are not collaborating with one another

7. Presence of suspicious employee behavior

Cybersecurity incidents carried out by employees have bad impacts, but they are not dealt with in the same manner as external threats (e.g. Hackers)

8. Untrained employees affects profits

Employee vulnerabilities are well known, businesses are not training their employees to take good cybersecurity measures. (Mickelberg Kevin, Pollard Neal, Schive Laurie, 2014)

Capacity Building Measures:

Programs that provide cybersecurity standards, good practices and guidelines should be developed and this would help in applying these elements in private or public sectors. Creating awareness programs, workshops and trainings in cybersecurity for both public

and private sectors would equip people with the necessary knowledge and measures needed to fight against cybercrime. To ensure the standards and professionals responsible in cybersecurity, certification is a significant matter. Providing certification for professionals and agencies would assist in maintaining high quality standards in cybersecurity. ("Cyberwellness Profile United States," 2015)

Cooperation Measures:

Cooperation should occur at the following levels: Intra-State Cooperation, Intra-Agency Cooperation, Public Sector Partnership and International Cooperation. On an intra-state level the states should be able to share cybersecurity resources across borders or with other nations. The intra-state agency cooperation is where certain national or sector specific programs are available for sharing cybersecurity assets with the public sector. At the public sector level, it would be helpful if the state acknowledged certain cybersecurity programs that are to be shared within the public.

The state could help critical infrastructure owners and operators by providing them with the necessary assets that would enable them to employ cybersecurity measures and deal with their cyber risks. International cooperation could relate to treaties or agreements made concerning cybersecurity measures or providing technical or training assistance to other countries. ("Cyberwellness Profile United States," 2015)

The previous part provides comprehensive information concerning the aspects that need to be included in phase two of the proposed strategy. Table 18 below provides a summary of the essential elements that should be included in phase 2 of a cybersecurity defense strategy; this summary would give states the general framework before going in depth with the recommended detailed information.

Table 18: Essential elements for phase 2 of a cybersecurity defense strategy

Legal	Technical	Organization Measures	Capacity Building	Cooperation
Legal Framework	CSIRT/CERT (Computer Security Incident Response Team, Computer Emergency Response Team)	Government leaders are responsible for establishing a national strategy	Cybersecurity education and awareness	Public-Private
National Cybersecurity Framework	Technical Guidelines	Establishing a Governance roadmap and policies	Cybersecurity workforce skills training	International
Civil Liberties Protection (e.g. Privacy)	Identify Critical Infrastructure	Responsible Agency	Cyber drills	
Child Online Protection	Standards and	National Checklist and National risk assessment method. National Cybersecurity coordinator	General cybersecurity guideline for consumers upon purchase of electronic devices	
National and International Borders	Certification	National Focal Point (a multi-agency which is a local point for all measures that are concerned with protecting the nation against cyber threats.)		
		Multi-stakeholder approach, Contingency plan and promoting Research and Development		

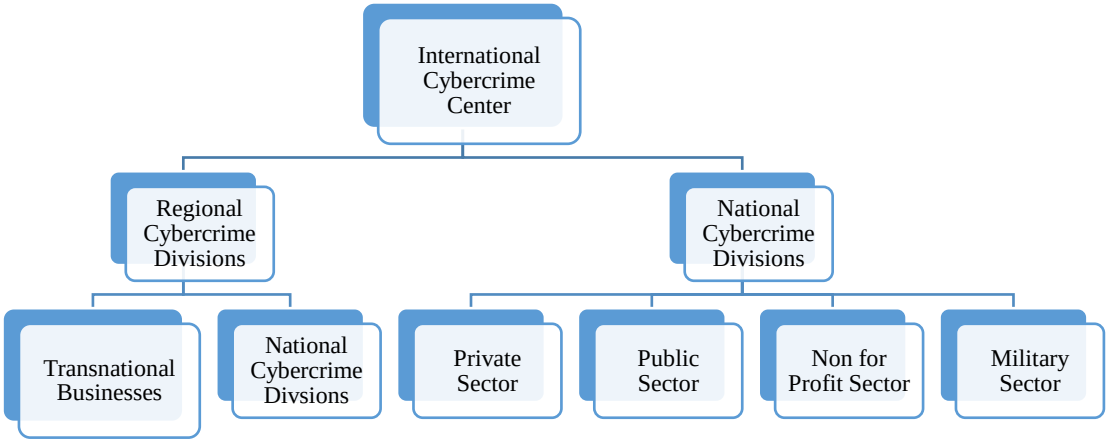
Source: (Leclair A. Jane, Sylvertooth Randall, 2015) ("Cyberwellness Profile United States," 2015)

For regional and international cybersecurity strategies considering the same aspects would be beneficial for states since this would decrease the discrepancy level among states' capabilities in fighting against cybercrime.

5.2.2 Proposed Cybersecurity Defense Strategy on an International Level:

The proposed strategy on an international level is to have an International Cybercrime Center where national and regional cybercrime divisions have a role. The national cybercrime divisions have to monitor cybercrime on 4 levels which include: the private sector, public sector, non-for profit sector and the military sector. It is essential to state that both transnational businesses and the national cybercrime divisions would report to the regional divisions. The regional cybercrime divisions play a role in reporting and updating the international center on the cybersecurity measures, standards and incidents that are present in all the systems (regional, national and transnational businesses).The regional cybercrime divisions would also alert the international center in cases of a possible cybercrime incident that could affect all states on an international level. Figure 5 summarizes the proposed international strategy.

Figure 5: The Proposed Cybersecurity Defense Strategy on an International Level



It would be helpful for regional and international divisions to determine the level of a state's cybersecurity capabilities on a range system. The system includes analyzing the cybersecurity strategies and systems and classifying the states based on certain levels where they are measured on a scale from 0 to 8. Table 19 shows these levels:

Table 19: Classification of states according to levels

No cybersecurity strategies and cybersecurity systems	Low level of cybersecurity strategies and cybersecurity systems	Low level of cybersecurity strategies and medium cybersecurity systems	Medium level of cybersecurity strategies and systems	Medium level of cybersecurity strategies and high cybersecurity systems	High level of cybersecurity strategies and systems
0	1 or 2	3	4	5 or 6	7-8

These levels were formulated based on the fact that some states might put more effort on strategies and less on their cybersecurity defense systems and in some cases they might place more attempts and time in establishing a high level of cybersecurity systems. These levels take into account certain state aspects such as:

- Legal abilities
- Cybersecurity expertise
- Existence or absence of cybersecurity strategies
- Presence of Standards
- The economy
- Expenditure costs on cybersecurity defense systems
- Organizational abilities
- Technological abilities
- Being a developed or developing state
- Cybersecurity awareness and education
- Level of Research and development

This table would assist the international cybercrime center in assessing which states need to further work on their cybersecurity strategies and capabilities. It would also highlight which states are complying with international standards and conforming to generally set international cybersecurity guidelines.

Another recommendation would be to formulate a global international strategy for cyberspace it is advisable to include the following:

- Establishing a cyberspace policy
- Establish principles
- Acknowledging the challenges
- The role of governments
- The role of transnational sectors
- The role of international organizations
- Using the diplomacy approach
- Defense methods
- Developmental measures

Establishing a global international cyberspace strategy would serve as a global guideline for nations, this would empower and enable them to improve their own cybersecurity strategies as well. It would provide more dependable networks and improvement in international security. ("International Strategy for Cyberspace," 2011)

These recommended strategies contribute in providing a guideline for states that have no cybersecurity strategies or are seeking to improve their existing systems, it would assist them in attempting to develop their own by considering the essential aspects. Cybercrime is inevitable in this digital age, it cannot be simply eradicated due to its level of complexity and it provides the cybercriminals with anonymity. It is relevant to state that there is no current existing international organization that is responsible for fighting against cybercrime. The role of the international community is being witnessed

by collaboration of states at a regional level or by taking part in international agreements. No information concerning the usage of cybercrime as an act of rebellion against governmental regimes was found, also no case of cybercrime's ability to change a state's regime was found. Cybercrime is being mostly assessed in terms of the economic, security and state's relations with one another. Continuous efforts are being made to examine how this issue is affecting the state's sovereignty.

In a virtual world, it would be difficult to capture and prosecute the suspects but it is not impossible because new precautionary measures have been developed on a strategical, technical and operative level in many states. These strategies could be adopted since states have already shown some efforts on a regional and international level. This indicates there are initiatives of cooperation, but further collaborative efforts are needed especially at the international level since this would help decrease and at least limit the extent of damage that can be caused by this new phenomenon.

References

Adelson Ian, Ahmerd Z. Mellissa, Coyne Vivian, Lim Han, Jia Zhifan, Paisley L.C., Truong Kim. (2014). *U.S.- China Cybersecurity Cooperation* (pp. pp:1–35). Columbia University. Retrieved from https://sipa.columbia.edu/sites/default/files/AY14_CyberCooperation_FinalReport.pdf

Akhgar Babak, Brewster Benjamin (CENTRIC), Politopoulou Vicky, Kavallieros Dimitrios, Drogkaris Prokopios (KEMEA). (2013). *Engaging Users in Preventing and Fighting Cybercrime* (pp. pp:1–19). DG Home Affairs. Retrieved from http://www.uinfc2.eu/wp/wp-content/uploads/2014/12/UINFC2-D.1.3-Law-Enforcement-Agents-Requirements.pdf

Aldurra Abad Fawaz. (2013, December). *Cybercrime and Penal Code: A Comparative Study between United Arab Emirates and Japan*. Fukuoka University, Japan. Retrieved from http://www.adm.fukuoka-u.ac.jp/fu820/home1/report/pdf/h25/k1475_all.pdf

Avner Levin, Paul Goodrick & Daria Ilkina. (2015). *Securing Cyberspace: Comparative Review of Strategies Worldwide* (pp. 1–58). Ted Rogers School of Ryerson Management University, Privacy and Cyber Crime Institute.

BIAC, CSISAC and ITAC. (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. Orgaization for Economic Co-operation and Development. Retrieved from https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Brenner Susan. (n.d.). *Challenges for Law Enforcement*. Presented at the The University of Dayton School of Law. Retrieved from https://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Brenner-Susan/dc-11-brenner.pdf

Bucci Steven, Rosenzweig Paul, Inserra David. (2013, January 4). A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace. Retrieved March 30, 2016, from http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace

Buzan Barry, Waever Ole, de Wilde Japp. (1998). Security, A New Framework for Analysis. In *Security, A New Framework for Analysis* (pp. pp:1–28). United States of America: Lynne Rienner Publishers, Inc. Retrieved from https://www.uni-erfurt.de/fileadmin/public-docs/Internationale_Beziehungen/BA_Einfuehrung_in_die_IB/BUZAN%20+%20WAEVER+%20WILDE_%201998_Security_CH%201+2.pdf

Center for Strategic and International Studies. (2013). *The Economic Impact of Cybercrime and Cyber Espionage* (pp. pp:1–20). Retrieved from http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf

Center for Strategic and International Studies. (2014). *Net Losses: Estimating the Global Cost of Cybercrime* (pp. pp:1–24). Retrieved from http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf

Chen Jong De Jing. (2014). U.S-China Cybersecurity Relations: Understanding China's Current Environment. *Georgetown Journal of International Affairs*. Retrieved from http://journal.georgetown.edu/u-s-china-cybersecurity-relations-understanding-chinas-current-environment/

Cîrlig-Cristina Carmen. (2014, October). Cyber Defence in the EU Preparing for Cyber Warfare. European Parliamentary Research Service. Retrieved from http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

Council of Europe. (n.d.). Global Action on Cybercrime. Council of Europe. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680300aff

Council of the European Union. (2015, May 6). EU Cybersecurity Strategy: Road map Development. Council of the European Union. Retrieved from http://www.statewatch.org/news/2015/jul/eu-council-cyber-security-road-map-6183-rev-2-15.pdf

Cybercrime Loss as a Percent Of GDP. (2014). McAfee, An Intel Company. Retrieved from http://www.mcafee.com/us/resources/misc/infographic-cybercrime-loss-gdp.pdf

Cybersecurity Industry. (2015, December 18). Retrieved February 19, 2016, from https://ec.europa.eu/digital-agenda/en/cybersecurity-industry

Cyberwellness Profile China. (2015, July 1). International Telecommunication Union. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/China.pdf

Cyberwellness Profile United Arab Emirates. (2015, February 19). International Telecommunication Union. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_Arab_Emirates.pdf

Cyberwellness Profile United States. (2015, January 14). International Telecommunication Union. Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/United_States.pdf

Dani Dani. (n.d.). Copenhagen School's Approach to Security. *Academia*, pp:1–9.

Das Sumanjit,Nayak Tapaswini. (2013). Impact of Cyber Crime: Issues Challenges. *International Journal of Engineering Sciences and Emerging Technologies*, *6*(2), pp:1–12, pp:142–153.

De Muynck (ENISA) Jo, Belasovs Agris, Dufkova Andrea, Portesi Silvia. (2012). *The Fight against Cybercrime Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime* (pp. pp:1–43). European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices

Di Camillio Federica, Miranda Valérie. (2016). Cybersecurity: Toward EU-US Cooperation. *The Internal/External Security Nexus*, (2), pp:1–56.

Digital 21 Strategy Advisory Committee. (2011). *Cyber Security* (No. 9/2011) (pp. pp:1–14). Digital 21 Strategy Advisory Committee. Retrieved from http://www.digital21.gov.hk/eng/D21SAC/attachments/D21SAC_paper_9-2011.pdf

Diskaya Ali. (2013, February 1). Towards a Critical Securitization Theory: the Copenhagen and Aberystwyth Schools of Security Studies. Retrieved January 19, 2016, from http://www.e-ir.info/2013/02/01/towards-a-critical-securitization-theory-the-copenhagen-and-aberystwyth-schools-of-security-studies/

Dr Masadeh M.S. Anwar. (n.d.). *Combating Cyber Crimes - Legislative Approach- A Comparitve Study (Qatar, UAE, UK)* (pp. pp:1–48). Al-Meezan Qatar Legal Portal. Retrieved from http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en

Dr Van Der Meulen Nicole, Jo A Eun, Soesanto Stefan. (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy* (pp. pp:1–152). Policy Department, Citizens' Rights and Constitutional Affairs, European Parliament. Retrieved from 24. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

Dr Wamala Frederick. (2012). *IITU National Cybersecurity Strategy Guide* (PHD). International Telecommunication Union, Geneva. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

El-Guindy N. Mohamed. (2016). Cybercrime Challenges in the Middle East. *Cybersecurity for Energy and Utilities*, pp:1–6.

Eriksson Johan, Giacomello Giampiero. (2006). The Information Revolution, Seurity and International Relations: (IR) Relevant Theory? *International Political Science Review*, *27*(No.3), pp:221–244.

European Commission Migration and Home Affairs. (2015, February 4). CyberCrime. Retrieved May 2, 2016, from http://ec..eu/deuropags/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

European Parliamentary Research Service. (2014, March 31). EU Approach to Cyber-Security. European Parliamentary Research Service. Retrieved from http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI(2014)140775_REV1_EN.pdf

Finkela Kristin, & Theohary A.Catherine. (2015). *Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement* (pp. pp:1–31). Congressional Research Service.

George Mason University (School of Public Policy), Virginia Economic Development Partnership's (VEDP). (2014). *Cyber Security Export Market: United Arab Emirates* (pp. pp:1–28). Retrieved from http://exportvirginia.org/wp-content/uploads/2014/02/Cyber-Security-United-Arab-Emirates.pdf

Gercke Marco. (2012, September). Understanding Cybercrime: Phenomena, Challenges and Legal Response. International Telecommunication Union. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Gilhawley Damian. (2012). Cybercrime: Protecting against the growing threat. *PWC*, *256*, pp:1–55.

Hathaway A.Oona, Crootof Rebecca,Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William, Spiegel Julia. (2011, November 16). The Law of Cyber- Attack. University of Pennsylvania Law School. Retrieved from https://www.law.upenn.edu/live/files/3469-hathaway-a-et-al-the-law-of-cyber-attack-2012]

Hinduja, Sameer. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. *Internet Journal of Criminology*, *1*(1), pp:1–26.

Hong Kong Police Force. (n.d). Cyber Security and Technology Crime Bureau (CSTCB). Retrieved March 2, 2016, from http://www.police.gov.hk/ppp_en/04_crime_matters/tcd/tcd.html

ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector. (2009). *Understanding Cybercrime A Guide for Developing Countries* (pp. pp:1–228). Retrieved from http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFE.pdf

International Strategy for Cyberspace. (2011, May). White House. Retrieved from https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Ionela Maria Ciolan. (2014). Defining Cybersecurity As The Security Issue of The Twenty First Century. A Constructivist Approach, *VI*(12), pp:1–17.

Jervis Robert. (1978). Cooperation Under the Security Dilemma. *World Politics*, *30*(2 (), pp:167–214.

Klingova Katarina. (2013). *Secuirtization of Cyber Space in the United States of America, the Russian Federation and Estonia*. Central European University, Budapest, Hungary.

KPMG. (2011). Cybercrime A Growing Challenge for Governments. *KPMG International*, *8*, pp:1–24.

Lallement Patrick. (n.d). The cybercrime process: an overview of scientific challenges and methods. *Charles Delaunay Institute (ICD), CNRS Joint Research Unit ,Université de Technologie de Troyes*, pp:1–8.

Leclair A. Jane, Sylvertooth Randall. (2015). National Cybersecurity Institute Journal. *National Cybersecurity Institute Journal*, *1*(3), pp:1–68.

Lewis Andrew James. (2014). Cybersecurity and Stability in the Gulf. *Center for Strategic and International Studies, Middle East Program*, pp:1–6.

Lindsay R. Jon. (2014). The Impact of China Cybersecurity Fiction and Friction. *MIT Press Journals*, *39*(3), pp:7–47.

Malby Steven, Mace Robyn, Holterhof Anika, Brown Cameron, Kascherus Stefan, Ignatuschtschenko Eva. (2013, February). Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Marsh and Mclennan Companies. (2014, August 14). Cybercrime in Asia: A Changing Regulatory Environment. Marsh and Mclennan Companies. Retrieved from http://asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20-%20A%20Changing%20Regulatory%20Environment_EN.pdf

Mearsheimer J. John. (n.d). Structural Realism (pp. pp:1–18). University of Chicago. Retrieved from http://mearsheimer.uchicago.edu/pdfs/StructuralRealism.pdf

Mickelberg Kevin, Pollard Neal , Schive Laurie. (2014). *US Cybercrime: Rising risks, reduced readiness* (pp. pp:1–21). PWC. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf

MoyenOrient3. (2014, March 11). United Arab Emirates: Tracking "cyber-criminals" Telecommunications Regulatory Authority and cyber-crime units. Retrieved January 2, 2016, from http://12mars.rsf.org/2014-en/2014/03/11/united-arab-emirates-tracking-cyber-criminals/

Munster Van Rens. (2012, June 26). Securitization. Retrieved February 19, 2016, from http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0091.xml

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity* (No. 1) (pp. pp:1–41). National Institute of Standards and Technology. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Neaimi Abdulla, Ranginya Tago, Lutaaya Philip. (2015). A Framework for Effectiveness of Cyber Security Defenses, a case of the United Arab Emirates (UAE). *Internet Journal of Cyber-Security and Digital Forensics (IJCSDF) The Society of Digital Information and Wireless Communications*, *4*(1), 1–12.

Organization of American States. (n.d). A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach To Creating a Culture of Cybersecurity. Organization of American States. Retrieved from http://www.oas.org/juridico/english/cyb_pry_strategy.pdf

Paganini Pierluigi. (2012, April 23). Analysis of cybercrime and its impact on private and military sectors. Retrieved October 3, 2016, from http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime-and-its-impact-on-private-and-military-sectors.html

Paganini Pierluigi. (2013). *2013,Norton Report, the Impact of Cybercrime according Symantec*. Retrieved from http://securityaffairs.co/wordpress/18475/cyber-crime/2013-norton-report.html

Pawlak Patryk, Dietrich. (2015, June). Cyber Diplomacy: EU Dialogue with Third Countries. European Parliamentary Research Service. Retrieved from http://www..europa.eueuroparl/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf

Petallides J. Constantine. (2012). Cyberterrorism and IR Theory: Realism, Liberalism and Constructivisim in the New Security Threat, *4*(No.3), 1.

Police Executive Research Forum. (2014, April). Critical Issues in Policing Series The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime. Police Executive Research Forum. Retrieved from http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf

Poonia Singh Ajeet. (2014). Cyber Crime: Challenges and its Classifications. *International Journal of Emerging Trends and Technology in Computer Science*, *3*(6), pp:1–3.

Purser Steve. (2014). Standards for Cyber Security European Union Network and Information Security Agency (ENISA). *IOS Press*, pp:1–10.

Purser Steve. (2015, May 26). EU Cybersecurity Policy and Legislation ENISA'S Contribution. European Union Agency for Network and Information Security. Retrieved from https://nettsteder.regjeringen.no/euikt15/files/2015/03/Purser-digital-security.pdf

PWC. (2011). *Cybercrime: protecting against the growing threat , Global Economic Crime Survey* (pp. 1–35). PWC.

Rand Corporation. (n.d). Cyberwarfare. Retrieved April 4, 2016, from http://www.rand.org/topics/cyber-warfare.html

Rueter C. Nicholas. (2011). *The Cybersecurity Dilemma*. Department of Political Science Duke University. Retrieved from http://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/3793/Rueter_duke_0066N_10959.pdf?sequence=1

Saini Hemraj, Rao Shankar Yerra,Panda.T.C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*, *2*(2), pp:1–8, pp:202–209.

Snow. M Gordon. (2011, December 4). Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism. Retrieved July 2, 2016, from https://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism

Spiridon Virgil. (n.d). EU Strategic Prioritiees in Fighting Cybercrime. Romanian National Police, Head of National Cybecrime Unit. Retrieved from http://www.ucd.ie/cci/cync/EU%20Priorities%20on%20Fighting%20Cybercrime.pdf

The Department of Defense CyberStrategy. (2015, April). The Department of Defense. Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

United Nations. (2015, August 31). 2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. Retrieved March 24, 2016, from https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

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

University of California, San Diego. (2012). *China and Cybersecurity: Political, Economic and Strategic Dimensions, Report from Workshops held in the University of California, San Diego* (pp. pp:1–37).

U.S. Immigration and Customs Enforcement. (n.d). Cyber Crimes Center. Retrieved March 2, 2016, from https://www.ice.gov/cyber-crimes

Wallace Ian. (2016, December 16). The Military Role in National Cybersecurity Governance. Retrieved March 31, 2016, from http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace

Wennerström Erik. (2004). EU-Legislationa and Cybercrime A Decade of European Legal Developments. *Scandinavian Studies in Law*, *47*, pp:1–20.