YAŞAR UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

MASTER'S THESIS

CYBER WARFARE MANAGEMENT

SHADAN MOHAMMEDJIHAD ABDALWAHID BABAN

THESIS ADVISOR: ASSOC. PROF. AHMET HASAN KOLTUKSUZ

MSC IN COMPUTER ENGINEERING

PRESENTATION DATE: 23 OCTOBER 2017

BORNOVA / İZMİR
OCTOBER 2017

We certify that we have read this thesis and that in our opinion, it is fully adequate in scope and in quality, as a thesis for the degree of Master of Science.

Jury Members:	**Signature:**
Assoc. Prof. Dr. Ahmet KOLTUKSUZ Yaşar University	
Assoc. Prof. Dr. Murat KOMESLİ Yaşar University	
Assoc. Prof. Dr. Murat Osman ÜNALIR Ege University	

Prof. Dr. Cüneyt GÜZELİŞ

Director of the Graduate School

ABSTRACT

CYBER WARFARE MANAGEMENT

BABAN, SHADAN
MSC, COMPUTER ENGINEERING
ADVISOR: ASSOC. PROF. AHMET KOLTUKSUZ

OCTOBER 2017

With the huge increase in development of computer systems and information technologies and further dependency on information technology, people are focusing on cyberspace, within cyberspace, billions of user connect with each other via the internet all over the world. The management of cyber warfare is one of the biggest challenges facing us, one of the major problems in the management of it is how to protect the system from attacks, reduce the risk of attack, and how to defend sensitive information from potential hackers. This thesis focuses on the main challenges faced in cyber warfare and presents some to avoid it. The most important measure is the need for international laws because strict laws are necessary to avoid cyber warfare. This study analyses and evaluates the risk based on some methodologies such as a Bayesian network for risk assessment that is needed in Cyber Warfare management.

Key Words: cyberspace, Warfare, Cybersecurity, Computer Emergency Response Team (CERT), System Infrastructure, Cyber-attack and Defense, Cyber Crime, International Law.

ÖZ

SİBER SAVAŞ YÖNETİMİ

Baban, Shadan
Yüksek Lisans, Bilgisayar Mühendisliği
Danışman: Doç. Dr. Ahmet Koltuksuz
Ekim 2017

Bilgisayar sistemleri ve bilgi teknolojileri gelişimindeki büyük artış ve giderek artan bilgi teknolojisi bağlılığı soncunda insanlar siber uzaya odaklanmakta, dünyanın dört bir yanındaki milyarlarca kullanıcı siber uzayda birbirleri ile bağlantı kurmaktadır. Siber mücadele yönetimi karşı karşıya olduğumuz en büyük sorunlardan biri olup, siber mücadele yönetimindeki başlıca problemler sistemin saldırılardan nasıl korunacağı, saldırı riskinin nasıl azaltılacağı ve hassas bilgilerin muhtemel bilgisayar korsanlarından nasıl korunacağıdır. Bu tez siber mücadelede karşılaşılan başlıca zorluklar ile bunlardan kaçınmanın bazı yollarını konu almaktadır. Burada en önemli önlem uluslararası kanunlara duyulan ihtiyaçtır, çünkü siber mücadeleden kaçınmak için sıkı kanunlar gerekmektedir. Bu çalışma Siber Mücadele Yönetiminde ihtiyaç duyulan risk değerlendirmeleri için Bayesian ağı gibi bazı metodolojilere dayalı olarak riskleri analiz eder ve değerlendirir.

Anahtar Kelimeler: Siber Saha, Savaş, Siber güvenlik, Bilgisayar Acil Müdahale Ekibi (CERT), Sistem altyapısı, Siber Saldırı ve Savunma, Siber Suç, uluslararası Hukuk.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Assoc. Prof. Dr. Ahmet Koltuksuz for his guidance and patience during this study.

I would like to express my enduring love to my mother and brothers, and sister who are always supportive, loving and caring to me in every possible way in my life.

Finally, I must express my very profound gratitude to my spouse and children for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you

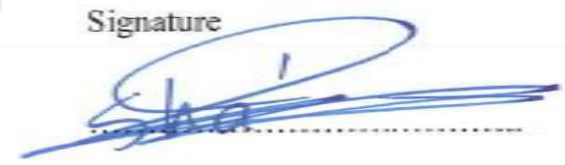
SHADAN BABAN

İzmir, 2017

TEXT OF OATH

I declare and honestly confirm that my study, titled "CYBER WARFARE MANAGEMENT " and presented as a Master's Thesis, has been written without applying to any assistance inconsistent with scientific ethics and traditions. I declare, to the best of my knowledge and belief, that all content and ideas drawn directly or indirectly from external sources are indicated in the text and listed in the list of references.

Shadan Baban



23 October 2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SYMBOLS AND ABBREVIATIONS

DoD	Department of Defense.
CRS	Congressional Research Service.
IBW	Information-based warfare.
EW	Electronic Warfare.
IW	Information Warfare.
EMP	Electromagnetic pulse.
RF	Russian Federation.
NSA	National Security Agency.
JFCC	Joint Functional Component Command.
IC	Intelligence community.
C&C	Ccommand and Control.
CNO	Computer Network Operations
USSTRATCOM	U.S. Strategic Command
JFCC	Joint Functional Component Command
C&C	Command and Control
BKIS	Bach Khoa Internetwork Security Center
OS	Operating System
SCADA	Supervisory Control and Data Acquisition
NIC	National Intelligence Council
CNE	Computer network exploitation
RE	Risk Environments
IA	Information Assurance
DARPA	Defense Advanced Research Projects Agency
CNA	Computer Network Attack .
Pre-CTO	Prepositional Cyber-Task Order.
CSIRT	Computer Security Incident Response Team.
CERT	Computer Emergency Response Team.
ISAC	Information Sharing and Analysis Centers.
CERT/ CC	Computer Emergency Response Team / Coordination Center
SEI	Software Engineering Institute
CIO	Chief Information Officer

CHAPTER ONE
INTRODUCTION

The digital world has imparted a novel kind of silent and current risk: cyber war. Before the internet, and information technology have progressed to such a range that they have turned into the main part of national power, cyber war has turned into the starting day of the country as nation-states are arming themselves up for battlespace in the cyber [1]. Numerous country is making participating in cyber-attacks with terrifying recurrence, developing national strategies, aggressive cyberwar strengths as well as procedure probing missions, cyber reconnaissance, and cyber espionage. Growingly, there are statements of network permeation and cyber-attacks that can be joined to political target and nation-states. What is clearly appeared is that most fiscal policy and ideological capital is being exhausted on finding out how to behavior cyber warfare unless for efforts aiming at how to deny it. In reality, there is an amazing shortage of cosmopolitan discussion and effectiveness with esteem to the inclusion of cyber war. This is regrettable because the cyber scope is a region in which technological invention and skill of running have a way of overridden planning and policy, and in order to stand, cyber warfare is an event which in the final should be intelligently managed [1].

1.1. Definitions

The following are definitions of the terms Cyberspace, Cyber Security, Cyber Crime, Cyber Terrorism, Cyber Warfare, and Information Warfare.

1.1.1 Cyberspace

Cyberspace is the kingdom of communication (behind of it is the user) in which information is saved, communicated online, and shared. Instead of attempting to detect the precise completely worded introduction of cyberspace, it is most helpful to conduct oneself what these introductions are trying attempting to obtain. Cyberspace is initial and primarily milieu of information. It is created up to data digitized that is stored, produced, shared. [2]

1.1.2 Cybersecurity

Cyber security indicates as a rule to the capability to dominance on coming to the information of the system via the communication systems. wherever cyber security

dominances are efficient, cyberspace is deemed an authoritative, trustworthy digital infrastructure, and flexible [3]. Wherever cyber security dominances are deficient, not good (bad) designed, or absent, cyberspace is deemed the nearing the end of digital life. Even those working in the field of protection career shall have a various opinion of cybersecurity based on the parts of cyberspace that interact with personally. While if a system is a physical aperient or a grouping of cyberspace ingredients, the plan for prospect raid and get ready for its ramifications is the function of protection professional appropriated to that system. [3]

At a high level, cyber security is normally expounded in the expression of little trials that explained the targets of safety professionals and their procedure, respective [4]. Three that merge to cover maximum uses of the expression are:

- Disclose, avoid, respond
- The operation, People, technology
- completeness, secrecy, and availability.[3]

1.1.3 Cyber Crime

In recent years, there had been massive concentrated crime related for a computer in criminal justice system. This define as "cyber-crime" has got augmentation awareness in order that computers have turned into central to various areas related to daily life such as social activity, however not restricted to, institutional and personal finances, interpersonal connection, several recordkeeping functions, and so on [5]. Because of its diffuse wide conductivity, the internet advent has moreover a valid to assist ravenous personal offense and property crime obliged with a computer. The U.S. Office reports were presented in 2000, the number of people that used the Internet in the United States is 94 million [6]. This extremely broadens both the criminal pools and prospect sufferer for personal and property crimes together. Furthermore, the nature of this gathering has pliable several possible offenders to play more facilely across existing offender behavior in order to the victim(s) ability be depersonalized in the first stages of an offense. For the Internet, a criminal make not have to turn up face-to-face together with a potential goal, which may do it simpler for the criminal to finish the sacrifice of the goal [7].

Myriam Quéméner analyzes and estimation European and French Union law goal cyber crime introduce cyber crime as offender effectiveness behaves in cyberspace by using the Internet technology. These crimes divided into two groups: 1) the

offender purpose by using accessing data and system by not authorized people, and 2) That includes fake, cheat, deflection of funds, earning illegal meaning, and online service by using defamation. [7]

1.1.4 Cyber Terrorism

The definition of Terrorism is "The illicit use or threatened use of force or vehemence by a person or an organized group against people or property with the intention of alarming or forcing societies or governments, often for ideological or political reasons" [8]. To this moment there was no effective action of cyber terrorism, while attacked in recent years in Kosovo and Middle East via a computer network. A number of funds for a terrorist is limited; the required source of the cyber-attack is a fewer resource and a fewer people (meaning fewer funds). Another benefit of cyber-attacks is that terrorists are able to stay anonymous because they can stay away, maybe is not in the current place where the terrorism may be far away is being carried out. [9]

1.1.5 Cyber Warfare

"Cyber warfare" has been defined as simply as "warfare conducted in the cyberspace" with assurance on the term cyberspace as being the key. This definition is although deficient to understand the term due to the specifics of how warfare in cyberspace is conducted and does not clarify on that point at all [10]. The dictionary of U.S. DoD (United States Department of Defense) Military and Associated Terms defines "cyber operations" as "the employment of cyber capabilities where the essential purpose is to fulfill military objectives or effects in or through cyberspace." and the phrase "computer network attack" as "actions taken through the use of computer networks to deactivate, deny, degrade, or devastate information resident in computers and computer networks, or the computers and networks themselves." CRS Report for Congress from 2001 outlines that "cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same." And CRS Report (Congressional Research Service Reports) for Congress from 2006 introduces the phrase "computer network attack" as "processes to deactivate or destroy information resident in computers and computer networks." Kevin Coleman from Technolytics Institute defined "cyber war" as "a struggle that uses feudal, illegal transactions or attacks on computers and networks in a stress to deactivate

communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses." the admitting that processes of military in cyberspace could be viewed as warfare, the phrase "cyber warfare operations" is the most appropriate for utilizing in testing the vast domain for the processes military in cyberspace [10].

1.1.6 Information Warfare

The definition of Information Warfare is a striped attack by a country or their representative versus computer and information system, software and data that result in enemy damage [11]. An official definition for U.S. DoD of information warfare overlay the three central portions to this form of struggle at the national level: information control, information protection, and information attack. Within the definition, two operational ingredients of warfare are often featured. The term information-based warfare (IBW) is applied to the ingredients whose focus is to acquire, operate, and expand information (or exploit information) to achieve a controlling awareness of the battlespace. This component participates to the information advantage by earning knowledge. The next component protects that knowledge while attacking an opponent's knowledge to earning a differential knowledge advantage. That component includes information attack and information defend (IW-A and IW-D) elements. Both components contribute to the goal of achieving information superiority, but by different means [12].

1.2 Aim of the Thesis

The thesis aim is to analyze, present the cyber warfare, propose strategies for defense against attacks, and how to manage the event of an attack on the system. Presented is the relation between Cyber Warfare and Traditional Warfare, also presented are the challenges of cyber warfare and the difficulties of defense. The other aim is to presents the risk of cyber warfare and how to manage cyber warfare, presents types of CERT, history of CERT, the acronyms, services, framework and organization model of CERT.

1.3 Related Work

In [13] they analyze the unique kind of cyber warfare and establish a foundation for research on the practice of knowledge management and the usage of heterodoxy in cyber security organizations. In [14] the thesis explains how the tools of governments

are increased for cyber warfare's to attack computer systems of the outlandish country and consequently menacing international and national security. The significance shall be critical of the cyber warfare estimate Using powerful analysis and clarification of cyber warfare like the case studies of Georgian and Estonian. The common presumptive happen behind the cyber warfare attacked for Georgia and Estonia is Russia. In [15] they furnish guide post for helping the Air Force of Royal Australian through its voyage during the development of a cyber power. According to the most voyages constantly there are multiple tracks, the choosing track that shall transport an operative cyber capability with obtaining exchequer is the big challenge. In [16] the project is an attempt to develop to common and detailed strategy to be helpful for the company to manage the cyber war security. the administrator of this strategy should be leading to a more secure business environment and as a find out will entice outlandish investments in Arab countries and the Middle East. The capability of this strategy is to deem as the first state across safeguarding companies from cyber war impendence in an efficient method. In [17] case study to evaluate the Cyber Warfare ability and its power to obtain strategic political goals. This research uses Cyber Warfare manage versus Israel and Georgia in 2008 and Estonia in 2007. The Cyber warfare didn't obtain goals on its own for politic strategies in all the cases that have been mentioned above. Cyber Warfare utilize in all cases depended on mainly of website deformation and Denial of Service attacks. These offenses were a considerable annoyance to the influenced country, but the offense was not of the adequate domain, affectation, or period to impose a renunciation from the goals country. Cyber Warfare attacks ability does not overpass vindicatory ability to the area that would permit the accomplishment of strategic political goals over Cyber Warfare alone. The potentially of strategic scale Cyber Warfare remains major, but the ability has not been pretending at this moments. In [18] prepare an evaluation of emerging computer depended on threats in a potential to heading the outstanding issue of protecting the digital infrastructure in our country. The Stuxnet worm is the special case study concentrated on this research, which was arguably initial cyber weapon to infect considerably active destroy. This research will examine Stuxnet, the Iranian nuclear program, and the probability that exist for the comparable threat to industrial control systems in the United States. In [19] the author proposed for pursuit cyber offense depended on the internet called "Correlates of Cyber Warfare" using a theoretical database, they supply an overview of the requirements for that a

database to be practically implemented and the advantages such a database would supply for future research. The beginning by overlay the different databases which occur to the path and observe online damage, former research covers cooperative snooping disclosed systems and the shortage of data ready concerning the transparent volume of cyber-attacks disconnected the internet [19].

CHAPTER TWO
CYBER WARFARE

The development in the domain of communications and computing and the outstanding refinement in the increasing of computerized systems have generated a new space in the world. Cyberspace, a space produced by a human existence, not by nature, has the possibility for enormous advantages as well as anonymous threats. The understanding of this event is the beginning because it exists more than forty years. The interaction amidst a new amidst that presented matchless abilities, a technical domain that needed regular comprehension, and media that contend with the consumer produced- potentially expected - the prospect of confusion [20].

Cyberspace and information uprising had an effective impact on national security. In the case of national security, A quantum jump in the availability and goodness of information, in the frequency of information, transmitted, and in the reliability of weapons was caused by long-term changes that led to the generation of opinion "uprising in military affairs" in the 1990s [20].

2.1 Comparative and Contrasting Approach to the Cyber Warfare and Traditional Warfare

The consultation with scientist was written in the book-length monograph on the war morality, while is the general summary of the existing law [21]. In these approaches are two properties as follow: (1) they consider the theory Just War as a steady state of the idea of the war morality and (2) they agree on the present that the theory of Just War is uprightly serviceable to cyber warfare, without any Edition required. The requirements together with the need to doubt, it is a split doubt whether the present international laws and national laws are applicable to cyber warfare and whether they are enough. Laws (compact, rule, convention, etc.) rarely synchronize with legalization commonly of what is morally allowable and prohibit commonly of what is morally not allowable. The conventional theory of what is morally allowable in war, Theory of Just War, is split into two major part questions. The first part, may morally take part in, or start, a war, by a country: Jus ad Bellum. Second, how morally may fight the war that once one locates herself on it: Jus in Bello. It is consequently an extension to reason a cyber-attack an ‘armed’ offensive since the

artifact act the harm is a computer (prepared for another objective), or, yet extra abstractly, an entity in information-theoretic [21]. Cyber-attack is the most prominent and widespread work on this subject, such as armed attack. But this is not clear. A cyber-attack on more nations by one country is like one of these. Martin Libicki [22] the cyber-attack on Estonia by Russia, NATO explicitly refused allegation that was an doing of war that should make reciprocal vindication commitment [21]. The fundamental of embargo and sanction are split unsatisfactorily by the National Research Council, the first include "just cause", the second not despite the grade of destroyed: this produced excessively of a legal (not moral) uniqueness. An unprovoked cyber-attack by any country on the military or civilian infrastructure of another country is consequently not very much such as paradigmatic, conventional forms of attack or offensive [23]. A cyber-attack does not include obtrusion in the airspace or area by soldiers or plane by the physical target. The best identification would be that a cyber-attack is more similar Electronic Warfare (EW), like strays the radio signaling of another country from outside its fringe, or the purposed use of electromagnetic radiation, like an electromagnetic pulse (EMP) arm to break down, or a laser, or prevent the elaborate of machinery, human act, or infrastructure from beyond a country's fringes [23].

2.2 The Cyberspace Battlefield

The physical world environment of the battleground generally is simple. However, the two countries contemplate war there is formed a battlefront amidst the armies of these countries anywhere appear the active combat. However, the space of the fight is unclear to against terrorism, insurgency, random sabotage and foreign internal defense battles as well as having two different way together with political targets combat on geography [24].

The cooperation together with virtual cyberspace model divided the activities from geography is the master challenge. questionnaire via folks spread across around world can be completed. The groups of fighter which eternally meet caused the completed of the planning. The wherewithal of networking through protect channels prepared by the internet. An offense vector or the resource may be caused by the internet. the complex situation is this new battlespace. For comprehend we should glimpse to the new battlespace environments, how it adopts the war-combat area, the forces we are a confrontation of the galloper, and the required of weapons to conquer

on this virtual forehead. [24].

We visualize three zones to resolves organization, logical and physical while checking the environments of the virtual battlespace. The frontier can be known legally (de jure) such as the fringe amidst the nations or workable such as the partition of the land amidst two parts of the same army; this qualifier is more complex to stratify in the virtual world. The think about the World Wide Web like networking of smaller connection for various configuration essential it is simple to see where to divide it. For the government of U.S, this may be either system with .mil or .gov extensions that are the mixing between the logical and physical. [24].

The U.S. military definition of battlespace is: "A term used to signify a unified military strategy to integrate and combine armed forces for the military theater of operations, including air, information, land, sea, and space to achieve military goals. It includes the environment, factors, and stipulations that should be understood to successfully apply combat power, protect the force, or complete the mission. These include the enemy and friendly armed forces, infrastructure, weather, terrain, and the electromagnetic spectrum within the operational areas and areas of interest" [25].

2.3 The Role of Cyber in Military Doctrine

The U.S.A, Republic of China, and The Russian Federation (RF) are developed the military dogma to the cyber warfare. Meanwhile, 120 countries are involved in this capability enhancement. The more active country for enforcement of cyber-attacks versus its enemy is Russia than other countries like U.S, China, Ingushetia, Estonia, Georgia, Kyrgyzstan, Lithuania, and Chechnya. Whether you accept or not for all or part of this happening appeared for the penalty of the Kremlin, favor policy of RF is pragmatic all these events, as well as the Kremlin, has never performed to stop them [26].

In the mid-1990s while the United States produced a telecommunications panel, Russia bought this product for the phone system, the Sub-Committee has always expressed in the information security about the uncertainty that this production has a secret key make the system shut down when stopped. For this reason, the War Information Strategy (EO) is interested in improvement by the Russian army such as CHAIN. Russia is not the only country that fears the cyber warfare, however, Russia and China believe that the United States is the boss and the scheme race of the cyber

arms and is reported to be involved in cyber snooping in a process called the "moonlight maze" by the Federal Bureau of Investigation (FBI). The Information Technology field is where one country cannot appeal ascendancy, unlike industrial capabilities or military equipment [26]. As a conclusion, the People's Republic of China's pick the most renewable in the military coordinates of information technology, information warfare, that had a massive resource in its the number of rise-goodness science and its population size and math graduates. Meanwhile, internet explorer has become common widely in 1993, start writing about information warfare by Officer of People's Liberation Army (PLA). The cyber process held by All the United State Army, Navy, and Air Force, however, the responsibility of United State Strategic Command(USSTRATCOM) is the instruction of direct Computer Network Operation (CNO), and the defense of All United State Military communication by National Security Agency (NSA). The linkage amidst USSTRATCOM and NASA happen at layer called Joint Functional Component Command (JFCC), familiar as the Joint Functional Component Command (JFCC)- Network Warfare, and the instructable by the director of the NASA. [26].

2.4 The Intelligence Component to Cyber Warfare

By using several models of Intelligence analysis and collection by 16 proxies that include the intelligence community (IC) in the United State through the employee that has professional skills. the inheritance approaches availed fully the regime, however, threats were emerging from the physical scope. The coming of the net-centric world has different threats environment dramatically so that the required of private company and government to review the process of analysis and collection intelligence within emerging threats that caused the effect them [26]. The interesting case still and modernly is unsourced offense versus United State and South Korean regimen websites that started in July 2009 through the unrestraint Day weekend. Both events seek by Project Grey Goose (PGG) interrogators, over and establish US-CERT, the familiar gathering of regime proxies charged with that mission, and companies of Internet security. At the initial step, the Project Grey Goose interrogators get the information about the technical properties of the attacks. The information of the technical properties is engaged amidst firm of the internet security and is fairly objective and not- debatable. The Figure 2-1 show the security company

BKIS in Vietnam which is one of the best technical analysis, the collapse of what was recognized about the offense after BKIS acquired monitoring of both the control and command (C&C) servers. [26].

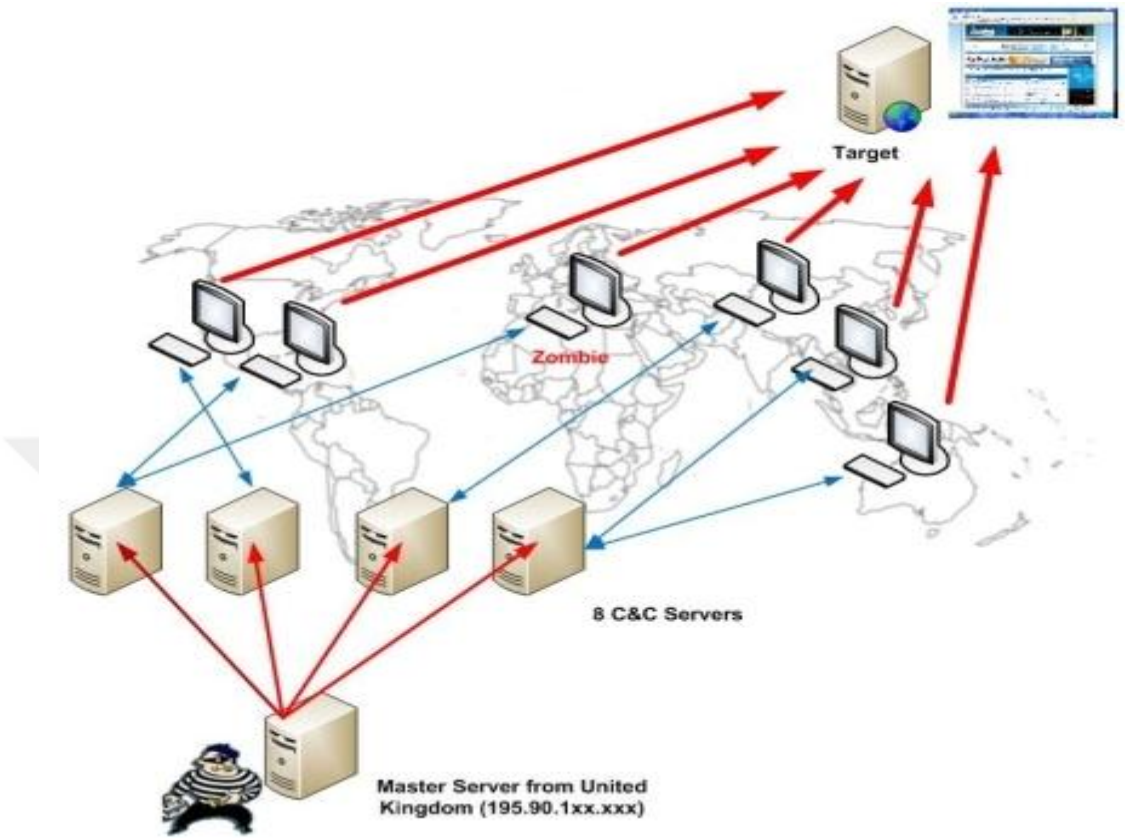


Figure 1 BKIS diagram of the My Doom attack program[26]

The researcher in the BKIS are able to win access to both C&C servers and determined that the botnet after controlled via all the C&C servers. In this botnet, the zombie PCs inform to log onto a several, randomly selected server each three minutes. Additional the researcher explore another server still in the UK, which represented the prime server through controlling all C&C servers [26].

2.5 Risks of the Cyber Warfare

Increased vulnerability System weaknesses affect the network caused by disability to assess the ideal ability of attackers. Supporting technology and the Internet have become the basis of economic communication and expansion, subsequently, there is no need to ensure security in this network infrastructure that can sometimes prove unstable this lead to difficult to track an attack or threat of technology renewal and transformation. There are different methods, include encryption/decryption, physical

protection, password methods, and access control techniques that used for guarantee the total computer network security. However, as investigator persists with research and bequests several measuring of the security effective, cyber-criminals, or cryptanalysts, furthermore the measures of the security may be avoided, infiltrate or broken [27].

2.5.1 Malware Terminology

Deterioration and demand for the overall recovery efforts within most organizations because of malware, which is the most important foreign threats to all hosts. The traditional denominations of malware as follow:

- **Viruses**. A virus reproduced itself by superseding into data files or host programs. The user interaction like opening files or folder or programs execution caused the virus is operated. The classification of the virus as follows:
  - Compiled Viruses. The operating system executes the compiled virus. The contents of compiled viruses are boot sector viruses, which infect the hard drives in main boot record or removable media in boot sector, file infector viruses, in the executable programs they attached themselves to it, and multipartite viruses, which merge the properties of boot sector and file infector viruses.
  - Interpreted Viruses. The software application executes the Interpreted viruses. there are two types of interpreted viruses (scripting virus and macro virus), The operating system has a service for processing script languages and the script that is understanding infect by scripting viruses, while the macro viruses infect the application document and document template by collect the properties of macro programming application capabilities. [28].
- **Worms**. A worm is a self-include program that runs itself normally and not needs a user interface, as well as self-reproducing. There are two types of Worms as follow:
  - Network Service Worms: - collect the characteristic network service vulnerability to infect other host or broadcast itself.
  - Mass Mailing Worms. Like a mail-send virus, however, infect the existing file, rather than self-included [28].
- **Trojan Horses**. The Trojan horse appears as a decent, in fact, they have a secret malignant target as well as its non-reproduce program and independent. They

insert in the host new malicious files or replace the malicious file instead of the original file. However, another attacker tools carry to the hosts.

- **Malicious Mobile Code**. is a software code that transmitted to the local host through the remote host, after that implement on the local host without any instruction from the user. The common languages used in this type include ActiveX, Java, JavaScript, and VBScript.
- **Blended Attacks**. They use various transition concept or infection, such as a blended attack could merge the spread methods of worms and viruses.[28]

2.5.2 Critical Infrastructures Subject to Attack

Attack networks have led to an increase in awareness of the critical infrastructure vulnerability of the countries. The most vulnerable system like (Banking, Energy, Transportation, and Telecommunication) and they targeted through the following attack modes:

- fake hardware
- Insider impendence
- Supervisory Control and Data Acquisition (SCADA) and the Internet caused the unknown to access protected network
- malware spread into the firewall because the Employee perversion of security guidelines

After report "Global Trends 2025." prepared by National Intelligence Council (NIC) they modeled the future threat scenarios. However, it contains several scenarios for assortment cases in national security, The large-scale cyber-event doesn't include in NIC [26].

2.5.3 Meaning of Cyber-attack

The corruption or intentional disturbance by one case of a system of concern to a different case. The former case will be indicating to as the attacker; the latter case will be indicating to as the target. In some contexts, the goal may also become retaliatory. The affected system will be indicating to as the goal system. Note a key ramification of this definition: CNE (computer network exploitation) is not an attack (as corruption and disruption are). Note as well two assumptions: The attacker is a state and the goal is a system of interest to another case. CNE deserves to be distinct from cyber-attack. First, CNE does not forbid the user of the full use of the

computers. The user suffers no coherent harm other than having mysteries stolen. Second, because CNE is trickiest to detect, a deterrence policy could only be stimulated by exception. Harsh punishments for crimes that seldom detected tend to lose truthfulness as law implementation techniques, and this is even truer if such procedures used to try to decide the activities of other states. Third, the legislation of war seldom recognizes espionage as a casus belli, and a good state for changing this has yet to be made, even though the means of espionage have changed. Fourth, everyone does it. Those who try to set deterrence policies to block others from doing what they do themselves perforce detect themselves to be hypocrites or simpleton unless they are so sturdy that they can get away with it [29].

2.5.4 Attack Techniques

There is a standard attack strategy: at the starting, the attacking person or group try to earning access to the network and/or, the computer then to executing malware that can be used to manipulate the data on the computer and/or to steal data. This allows beginning further actions which are shown in figure 2. [30]

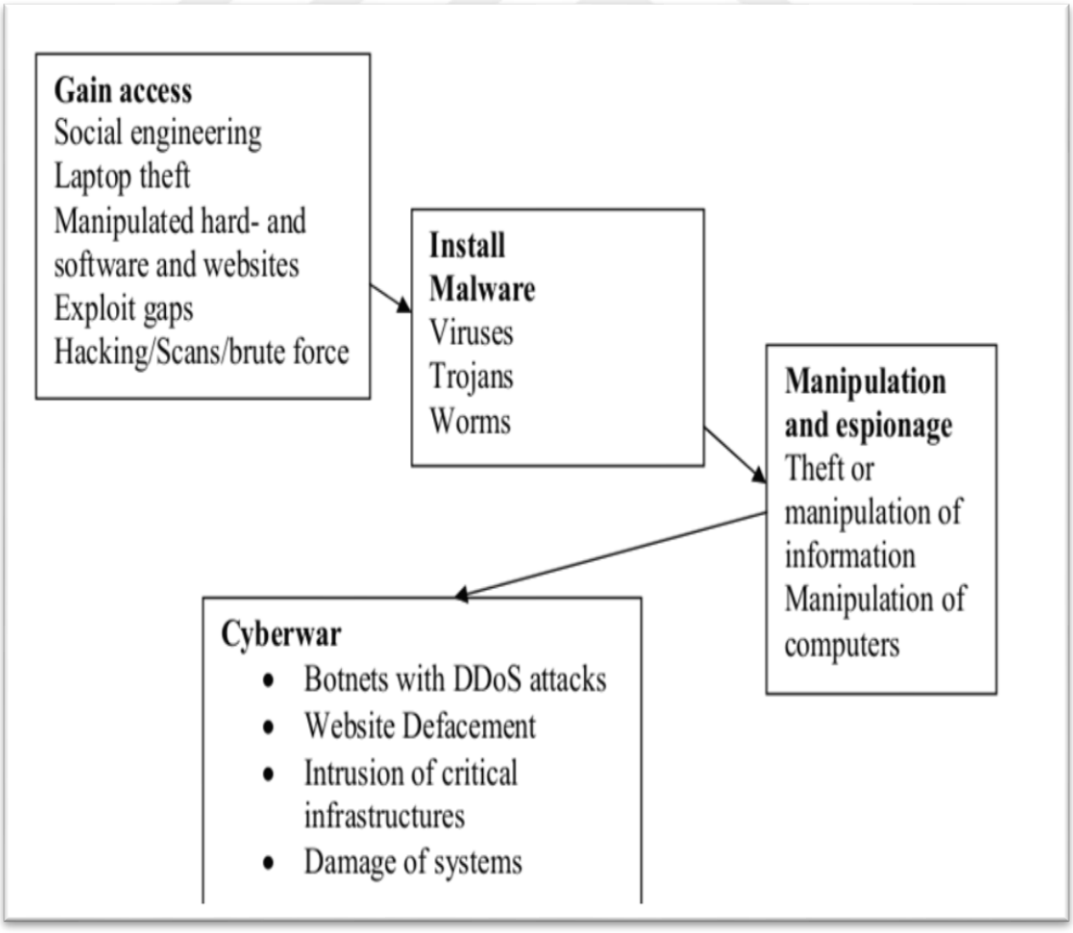


Figure 2 attack strategy [30]

2.5.5 Risk Environments

It is very difficult to analysis cyber environment of every military corps since each of them have their own complex hierarchical authority structure. Moreover, each nation always has their unique plan to manage the military operation. This subsection will raise some main ideas of how to evaluate cyber risk considering to the environment of military operation. A lot more researches and discussions from militarily related specialists needed to grade these topics for cyber security.

From [31], they presented three types of information environment: Physical, Informational, and Cognitive. The first type will be composed of tangible and intangible elements such as information systems and infrastructures, satellites, telecommunication networks and transmission paths in the electromagnetic spectrum. Elements in the physical types exist on air, sea, land, or space. Battle capabilities have measured foremost in this dimension. The types of informational consists of the information itself which indicates to the content of the information such as data, text or image, and flow of the information such as store disseminate, process, collect and display. A range of properties can characterize informational types such as integrity, completeness, accuracy, quality and so on. These types are the necessary link between the physical dimension and the cognitive dimension. The final cognitive type consists of concepts, intentions, values beliefs, and receiving information and perception of transmitting. This type based on any contexts that influence the perception of generating and receiving the information. Decision-making and goal audiences are most inclined to influence and perception management. [32]

2.6 Defense Strategies

A- The DARPA Information Assurance (IA) program is on the securing of computer depended on system and information, as well as the wider perspective operations of information [33], or even more definitions via Information Warfare [34]. These wider points of view typically combine human, committee, and set foresight that scope beyond concentrate for IA program in the technological. Information Assurance concentrate is more carefully the range with defense versus computer network attack(CNA), that introduce with common Pub 3-13 as "... processed to reject, damage, besmear, destroyed information occupant in the network or computers themselves or computer networks and computers [33]. Another substantial difference

is the Information Assurance program's concentrated within defensive sides for combat within the cyber reality. The operations of the cyber offensive are distinctly primary of efficient as the total for military strategy, this activity is not presently supported by program's charter. However, Information Assurance program cannot eliminate the required exactly total attack and defensive abilities, since the defense and attack should be used in tandem to be efficient, such as strategy of the military in the physical realm. Until this termination, potentials should be consumed to supply suitable "rods" amidst the defensive-concentrated abilities enhancement and the attack technique abilities enhancement in the information Assurance program, elsewhere Department of Defense research and community development [35].

B- In Cyberspace The Strategy Cyber Military supremacy in Cyber Warfare, The processing and suggestion excellence cyber military of cyberspace supremacy in cyber warfare. They deemed cyber intelligence capability, manpower in cyber force, and a community for cyber forces to generating strategy in the cyber military. The power domain in cyber force, they must cultivate personals that able to execute operations on the communication as well as occupy technology of cyber security like cyber forensics, cyber intelligence gathering, cyber-attack, and cyber defense. The ability of cyber intelligence covers cyber destroys estimation, pre-CTO, order for combat in cyber, and reconnaissance/surveillance in cyber. The tree structure of cyber force may be mutated to network structure and may be regulated mission or command control committee, by an organization of cyber force. The offer strategy of cyber military supply previous award for behavior to run the required effects in cyberspace [36].

C-Three level of Prevention Model, the proposed a framework of defense system by applying attack tree and misuse monitor for the protection of insider’s malicious behaviors. The concern of network protection is the threat from insiders who run their authorization legitimately to seepage information on the network system. If insider threats his/her system, he/she has caused a server destroyed and loss to adjustment information property. The framework consists of three prohibition modules. It prohibits abnormal conduct by surveillance all activities according to each prohibition are attack tree and misuse monitor. An attack tree is a conceptual structure of insider threats on systems and potential attacks to reach those targets. In addition, a misuse monitor can prohibit the misuse of resources by matching the existing executing process pattern to the predictable processing pattern in pre-defined

current insider executed process profile. [37]

2.6.1 Difficulties in Defense

The wide popular denominator of defense led to the defense of the cyber-attack, That means they prevent for entrance the computer system. Although the defense is concentrated within distinguish unlawful espionage, estimate the effect, determine the root of the issue, prohibit for a spread for infecting inside a network, and to range necessary, rebuild data and the machine that was infected, by using technological procedures. Defenses include the capability into becoming a location at the track of permeation, recognize like an endeavor, and foil this during preemption. Into this goal, using a computer system for observing communications and action; limit permissions; prohibit access tracks; provide encryption checking identification, and enable backup and calamity recovery. However that evidence to be a suitable logical reply to the attacks, cyber- defense needs limited [20]. The size of action single places the guard party in an inferior situation. The try for defense in the region for responsibility is more complicates because of decentralization of network and computer resources. The case in simpler networks compartmentalized: the compartmentalized frame knows that the network is beneath its dominance that known by compartmentalized framework, also should be preserved and defend it. Moreover, this kind of networking is decreasing, as well as increase the industrial system take advantage of information technology as well as become procumbent to cyberspace's threat. The cyberspace had imported the critical infrastructure, the business infrastructure used by cyber force to more of their telecommunications even the burden for negative defense is grown [20].

2.6.2 Strategies for Defense

Rigid technical abilities are more necessary for defense action in cyber, although they are not sufficient. The suitable planning and better technologies are more useful than using only better technologies without good planning for their employment. On the contrary, may want to utilize of defense without awareness for the planning, the domain for technology required for implementing the strategies they cannot completely comprehend. The possible strategies of cyber defense are explained as follow. The description for each of these strategies is different to another because in each strategy shall set different cyber strategies defense cases in the physical world. The nature strategies suggested and without mean exhausts, the space of

approximations, the Strategic of cyber defense may utilize it. In the state, they shall concentrate the starting trail on some principle approximation for every better strategy for defense. As well as the ability to enhance expansion and profundity like start attempt earning insinuation from the behavior attackable together in and outside the DARPA Information Assurance program [38].

A-Deterrence

In the strategy of defense, the basic entity is Deterrence [39]. For each entity hasn't a clear strategy for offensive, the Deterrence is the principle of defense goal can use it. The difference offense and defense keep track like output for defeat for deterrence. To be the Deterrence more efficient, prospect adversary should be convinced of the threat and frivolity for each attempt offenses. Typically, the Deterrence utilizes at the foundation for an adversary shall become specified and chastise accurately and swiftly. The Celerity, Severity, and Certainty are essences of the key causal elements in General Theory of Deterrence [38][40].

B-Defense-in-depth

This strategy utilizes like its name, the objective is to utilize "level" collection for mechanisms of this style like the impairment for several can become alleviated through a power from others. This is tantamount for the thinking that "trustworthy systems can be constructed from untrustworthy elements." The planning for Defense-in-depth based on the participation of technology with the system in nature. Defense-in-depth strategy supposes that in several scales intellectual assailant shall control the amount of felicitous offense shall out balance estimate for they running, or shall finally non-intellectual attacker defeat securing scale in any case of estimation [38].

C-Deception

Deception mechanisms can apply in each layer for war (tactical, strategic, and operations). Current common directing at the deception of defensive action concentrates generally, for using at meter-deception, instead of deception, that is believed to become an attack action [41-42]. Moreover, aggressive IO actions like a deception as well believe for backing defensive functions [43]. In Cyber Defense the goals of deception are to build as much wonder and embarrassment like the potential for the possible offense, concerning the site and amount for critical resources and information systems [44]. For become most effective, like a dynamic strategy in its implementation.

D-Dynamic Compartmentalization

While preventive security measures and deterrence defeats are incapable for prohibiting an offense for penetrating the various scale of defenses, it shall become eligible to depose the influenced also systems for the residue of the infrastructure while the reformative operation able to take. The goal is to include and segmentation effected at a network in a flexible also dynamic manner, while for minimal confusion to the processing task or business infrastructure [38].

E-Isolation of attackers

In this strategy concentrate of isolation on the attacker, instead of isolation for favorable systems and networks like explained at the prior section of segmentation. The isolation strategy split into two special part of actions, long-term and short-term, depended on timeline implementation [38].

2.6.3 Advantage Comparison between Cyber Offense and Cyber Defense

While the attack shall have the properties within cyber warfare, while the event able to differentiate between defensive and offensive cyber weapons, programs, and policies then collaboration is still potential. The distinguishing issue is very connected to the investigation issue in order to pests numerous arms dominance efforts. Unluckily, the forestation here is similar sullen. One defy for discrimination shed is that the equipment required for behavior cyber warfare occur foremost within the virtual world. The physical equipment used at cyber warfare is a computer that is distinguishable only. Both cyber defense and attacks executed through this diffuse and generally non-threatening platform. At the same time, many of the world's massive militaries have systematic cyber warfare programs and units, a fundamental cyber-attack ability only like readily for implementing at a personal home or business. The most defy of distinguishing between defensive with offensive cyber weapons is, subsequently, for distinguishing a weapon at the initial location. Naturally, that issue is incompletely individual to cyber warfare. Nations able similarly detect it hard to evaluate if the enemy nuclear follows up meant to utilize a force or to make bombs. Nevertheless, defy at present is less difficult. Consecrated cleverness efforts mastery ultimately detect if a manufacturer is producing nuclear power or nuclear bombs. A Computers System is away most joint and has away most various uses. Until if a cyber weapon able to be specified, it stays extremely hard for recognize within defensive than offensive abilities. Numerous organizations of Army mission for organizing cyber warfare have together defensive with offensive abilities, both for

that organized over similar instrument and technics. The streak amidst defensive with offensive style is blurry at preferable, also like one commentator set it, “the distinction between being able to probe and penetrate an adversary’s computer network or attack comes down to a couple of keystrokes....” [45]. Paul Kurtz notes: “You can have a small piece of code that can do a whole of a lot of damage or just a little bit of damage depending on how you choose to use it.” [46].

2.7 US and Chinese Military Approaches to Cyber Warfare

Fully a component for the United Nations Army which works in cyber case, the cyber instruction get it, for the military's Ninth Inductive Command to the Navy’s Tenth Fleet (the Fleet Cyber Command). Commonality said the community brags the cyber combatant power for merely less than sixty thousand personnel, the address of the head office in Fort Meade, Maryland. its address was negotiated, investing CYBERCOM like is recognized, the nearer gate to the National Security Agency, the signals, protection, and information intelligence concentrated by the agency of espionage. That authorizes for sharing the resource in the scope plane, like a hundred PhDs engineering, computer science, mathematics, and different areas who work there, complete the road over the best. In any case, inside military of the United Nation, the increasing quickly for the CYBERCOM at volume and perceived significance[2]. Actually, the budget in 2013 for Pentagon plan mentioned the cyber 53 times. The just next year 2014 budget plan debate a cyber increased to 147 times, for the expenditure of the head office of the CYBERCOM alone increased efficiently twice (complete the most special like the rest of the budget shall be cut for the United Nation military). The CYBERCOM guided by strategy designed for comprehensive concept which the cyberspace is modern area for possibilities and threats, The United Nation military act the best extreme for safeguard his strength for utilized in this field (its classical "freedom of maneuver"). The CYBERCOM Deputy Commander of General Jon Davis characterizes the treatment of the cyber problem with complete modern scale for riskiness by United Nation Military. “This is now commander’s business; this is no longer admin tech business” [2]. Existence agenda execute through 30 pages at the categorized version and 12 pages in the Uncategorized version. As a total, concentrate of the CYBERCOM within five goals: terminate a cyberspace according to "operational field" like the military remainder sea, land, or

air, execute a modern protection model for achieving there; partnership with private strip and other agencies; create relationships with global partners; and enhance new talent to stimulate new invention in how the military might combat and win in this area. Like section for that task, three kinds of the cyber force (cyber protection force, combat task force, and national task force) are constructed and driving by CYBERCOM, the "cyber protection force" are responsible for protecting networking and computer of military, "combat task forces" are responsible for support task for trooping at the domain, and "national task force" responsible for assist the securing significant infrastructure. The CYBERCOM is not just frequently processing on the computer networks in government and civilian that should be at present seemingly protect, however, orderly competing between these responsibilities and who have obligated to observe similar network, comprehensive government agencies such as Department of civilian in Homeland Security and the private sector. For producing an equivalent for the expanded role for "national mission forces" while physical money is moving in the bank, The Pentagon doesn't defend on the cash, while actually consolidation of the police and protection. China explained time and again as the destruction of the cyber security world, as the government reports such as published through Congress or essays in Western media (a regular headline: “China: No. 1 Cyber Threat”). Backward these acute fingers are actual attention. If it doesn’t assign one state, the prepared to instruct Cyber Command is the strategies for executing cyberspace in 2011 by Pentagon, obviously, put the China between extremely serious impedance in that realm [2]. Definitely, several are at present framework the Chinese-US relation in the cyberspace as digital echo during the Cold war between Union of Soviet Socialist Republics (USSR) and United State (US) at cyberspace. The country, Analysts in Chinese are fast for thrust back the standing country like a rotten cyber power. “China is accused time and again for launching cyber-attacks abroad but there is never any robust proof. Actually, China has become a victim of such repeated claims,” A person specialized in international security at China Foreign Affairs University summarizes that in 2011 the official Government in China was a goal for approximately 34,000 cyber-attacks by U.S. while in 2012 the number of the cyber-attacks are increased to 90,000 times [2].

CHAPTER THREE
MANAGING AND THE CHALLENGES OF CYBER WARFARE

3.1 Understand the Limits of the State in Cyberspace

The paramount things of cyberspace are the culture, de facto truth, the internet, the network communication between the computer go outside the path in the end of the reality that hardware innovative technologies. Sure that the civilization, environment of scientific, massively social are byproducts of, and entrench in, are embedded in modern information technologies. The rising of consciousness competence to show as a history transfer in the path human civilization explain and demand their worlds [47]. While the author [48] inquiries that knowing the information is same as that having information? Knowing Cordial and additional direct (connaitre) is completely various from knowing about thingummy (savoir) caused this question a key singularity. The float of the cyberspace onto a modernist visualization of space as uniform, and conformable void and indefinite container into an object. In the center of cyberspace, the information is the encoding of the object for the bit and byte and transmits it. When we want to search and access information for any possible subject, we can do it within the internet via search engines. The information exporter caused the internet user for a problem, not lack of information while via a dizzying sensation of becoming lost in the everlasting maze. Demanded and constructed of the cyberspace via the shape of perspectival dimension, Encoded and presented the information around the universe via Overture of the video show screen. While in the middle of the cyberspace, in order to the "real world" not needed the prolonged to avail as a signal or the grapnel for the sight pictorial on the windows terminal of the video display. What we testify today is the maximum appearance of the intellectual reasonable framework operating. Denying other frameworks of awareness to coming inside consciousness while the intellectual picking the center stage of consciousness. In the organ of sense, intellectual turn into over-intellectual, imbalanced, and imperfect, its geniality increase for additive consciousness, separating and breaking the universe to grade the output is an aberration, shattering, and deny in concept thing. In the result, the intellectual-rational framework has not imploded into transformation, perspectival awareness, but in on itself, and into hyperextension of the perspectival universe. Over perspectives, in synchronized for cyberspace, have

formed a modern epistemic request depended on depthless or non-preferentiality, breakdown the uniqueness among signifier and signified. the output is a surface with a cultural magic, images, and the concerned energy notion spot and fugacious requests [48].

3.2 Challenges Pertaining to Cyber War under International Law

In the world, the cyber warfare explained as critical impendence in order that intimidates national security of nation country's in cyberspace [49]. The cyberspace is recognized after Air, sea, land, and exterior domain, as the fifth region that a nation state requires safeguarding while in some case defend. Cyberspace utilization is consequently incorporated for nation state's everyday vigor such as an increasingly vast domain of social (civilization), economic, political, and military efficiencies are based on it and therefore, as will be seen yet, the usurpation of its ability and obstruction of its use both are vulnerable [49]. Regard of the interlinked questions of existing international law (lex lata) focusing of the following:

- How should the nation be defending herself versus the offense if they attacked?
- When ought to degrading state (nation states or that patronized by nation state) intervention in the cyberspace of different nation comprise combat versus the nation(victim nation)?
- For the victim, the nation state is there any refuge shall pick versus the offensive nation state those snooped to its cyberspace If the behavior of a country does not fall in the range of combat.

To confirm whether the current principle effectively processes the confronted defy a nation state of other nation snooping within provincial cyberspace is the major objective. The international law will be enhanced in the case if the current principle of the international law leads to unable. [49]

3.2.1 Application of International law to cyberspace Intrusions

A- The summary of the principle of international law in non-intervention, use power, and the regard to country supremacy (Jus ad Bellum). In nature the international law usually unlawful, and subsequently snoops while licit is subsequently lawful. An issue of dogma forbids a country of interfering in the space affairs of other country,

employing power or attack of power versus other countries or attractive in acts truculence, is the principle of the international law [50][51]. The charter of United Nation states: "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the purposes of the United Nations.". The following nation domain of cyberspace intervention is not allowed by international law: -

- An intrusion.
- The employing of power, attack of, or an armed threat.

These concepts are unknown in international law neither does the international law mention the thresholds of intervention. In the international law shall have the assessment if the intervention framework and involvement, armed threat, employing the power or aggressiveness. Unfortunately, it is not simple to create a group of country intervention falls. While the threshold of country intervention increase for prohibited interference to unlawful utilizes power to combat and when the confirmed criterion shall be set within the state-by-state intervention. The country shall only lawful for utilizes the power it is the victim of an armed threat or if they when it is the victim licensed by United Nation Security Council [50].

B- The Tallinn Manual explanation of the international law in terms and ideas within that intrusion assigned cyber warfare Tallin Manual to assess whether cyber interference assigned an intrusion, utilizes for power and armed threat, the Tallin Manual indicates to various principles. Set while intervention should framework a job of combat, Those principles relevant to the argumentation shall be specified too only [52].

i) States and cyberspace

The cyberspace states are supremacy that mentions in Rule 1. Supply of a lawful liability for the state of framework an infringement of an international obligation and cyberspace that characteristic to it, that is Rule 6. In Rule 9 supply that the victim state shall refuge to commensurate countermeasures versus the accountable state. [52].

ii) Jus ad Bellum (right to use force)

In rule 11 set that cyber process shall framework utilize power while its impact and the size are similar to non-cyber activity increasing to the step for utilizing a power, concerning to utilize the power in the expression of Article 2 of the United Nations

Charter. The rule 13 states that the impact and size required for a processing to be attributed to an armed offense without fail override those qualifying as utilize of power [52].

iii) Ius in Bello (the law governing armed conflict)

A provisions precedent to the implementation of the law for the armed fight is the presence of the armed fight (rule 20)[51]. Another explanation Filder [50] deduce so as to reasonable proof can understand the deployment for Stuxnet frame an unfriendly, willful, country-formed, very complicated and climacteric infrastructure menacing the attack utilize malware, that framed an unlawful utilize the power, armed offense, and an operator truculence. Nevertheless, his opinion though doctrinal testing for international law is considerable, also country practice should be taken into consideration. The nation-States have curiously been peaceful on Stuxnet that is the Filder comments. In [53] the author opinion that the Stuxnet created an armed threat beneath the international law however without Iran formally proclamation it had been attacked, the author sensate that useful opportunity in cyberspace missed the defining the domain of unlawful skill. However, Iran doesn’t satisfy without revenge, doesn't overtly condemn the country accountable for the offense.

3.2.2 Challenges Facing Cyber Intrusion In Terms Of the Current Rules Of International Law

The international law principles prevent confirmed kinds of intervention, however, doesn't determine which intervention place within the black list of intervention neither the thresholds. The attorney has to evaluate it in state-by-state basically. The worthy instructor in defining the kinds of intervention prepared by Tallinn Manual. However, the Tallinn Manual should be eulogized of a summary of the position of the international lawful, forever the professional doesn't correspond to while an intervention framework interface that is obvious, utilize power or attack of and armed offense beneath the international law. [49].

In general Country level intervention is indicated to as cyber war. In an expression of the international law, cyber war able only exists intervention which frames an armed offense. Until this moment, no any cyber intervention reached the threshold for the armed offense, however, the professional for the Tallinn Manual has not shut out the

prospect of any attack [54]. The present principle of international law doesn't include country-state reservation related to cyber force predominance and intervention. International law can not be enforced by the international lawful system because it hasn't centric power. When using power by the country for affairs, the country shall use the countermeasures, however, it is not obvious which shape the countermeasures may select [55][56].

3.3 Methodology and Evaluation of Cyber-attacks

The access to modern technologies within every aspect of human life has expanded to such a grade which, main general section industries, like Government, Education, Health, General Security, National Security Furthermore section like Economics, Power, Nutrition and telecommunication & transmission, are exceeding regarding the modern ICTs. Thus, technologies and telecommunication and information systems are currently playing an important role in ensuring a State’s suitable work and the fully-being of cyberspace and its citizens, the common ground of all these, acts as the connecting link between them [57].

3.3.1 A Cyber-attack Evaluation Methodology

The cyber attack categorization and attribute based on the magnitude of their result. Long-term impact and grade of apparent for the cyber-attack specify crucially factor of its attributes, as well as the utmost degree for the effect for cyber-attack the extra chances for the attribute like a "utilize of power" or at worse like an "armed offense" while its magnitude is as utmost as to cause lack of human lives [57]. The procedure for measurability of the effect of the cyber-attack is a critical situation. While the effect scale for cyber-attacks should be specified by use of quantitative and specific standard, it should probably easier for distinguish and classify them depend on the basic of international law. One able proficiently notice when the same effect factors suggested through the International Group of Expert to classification attributes for cyber-attacks areas well as used like a factor in threat critically testing procedures for infrastructure and distinguishes. A pertinent European Commission Communication specified the standard as the least group of standard that could be deemed through organ country while trying to estimate their crucial infrastructures: (i) general safety‑compromise cases like medical illness, serious injury, population affected, evacuation, loss of life, (ii) the impact of economic ‑ that gather within regard the

GDP impact, the loss is significant for economic and/or the retraction for services or products, (iii) the impact of environmental ‑ i.e. impact on the surrounding and the general environment, (iv) interdependency ‑ while have to do with interdependencies amidst infrastructure crucial objects, (v) impact of political ‑ which is, trustworthy in the regime and (vi) the impact of psychological ‑ i.e. impact of psychological within the population. The determination of this criteria locates venue in explanation of their area (international, state, regional, local) and time (through and next to the event) [58].

For determining the results, National Infrastructure for the U.S. has a Plan for security to distinguished the criteria as follow: (i) general safety and health- comprehensive the impact on physical luxury and human life,(ii) psychological- such as impact to the general mood as well as the grade for dependability for the human in political and economic establishments (iii) economic such as losses regarded direct and indirect (iv) task/ governance that considered the impact of capability for industry or government for conveying primary services, preserve request, guarantee general safety and health and national security execution- within relation to tasks [59]. So there is an explicit link between cyber-attacks and the corresponding methods utilized to estimate communication (ICT) and critical infrastructure while for these situations the effect factors employed for those characterizations are almost the same. In addition, the estimation critical ICTs using assessing criteria are massively for estimating the risks concerning for foreign effects that are effects correlating for socioeconomic output and their impact in citizens, however, they are directly related to the affected critical infrastructures as well as indirectly linked to the degeneration for these critical ICTs or implications of the breakdown for the luxury of citizens. The methodology that used for criticality analysis, who primary role is for utilized as standard for estimate peril related for critical ICTs, able as well serve as a measure for determining the consistency for cyber-attacks furthermore to activate quantification of the "measure and impact criteria, by utilizing specific and specific criteria like in the Tallinn Manual the ones recommended by international Group of Expert, and probably take on other variables. in order to it be easier for distinguishing while acts verge within that called " utilize the power" criteria, which is used for evaluating if or not a country has an offense. Moreover, a similar procedure should be utilized for Mark if the cyber action arrived

at the scale for being attribute like "utilize power" or like " armed offense" delegate so a UN Organ Country for replay through practice it's lawful totally for defense itself depending to the UN Charter Articles. Same as the previous procedure should avail for the level of Senate of Security for deciding while a cyber-attack framework "attack for the peace, violation of the peace or action for offensive", consequently the desired measurement for getting back security and peace for international adopted depended on the UN Charter Article 42 [57].

3.3.2 Evaluating the Impact of Cyber-attacks on Missions

When anyone accesses and made unavailable into source information of weapons like shown in Figure 3 the weapons radix are independent of each other into each specific goal, however, the probability there shall be available territory weapons to entice the goal, in addition, there is a various probability so as to airborne weapons ability be ready. Several weapons are extra appropriate than others into a private model of goal so as to be involved. The following task type explains the author characterization for the different criteria impact task result [61].

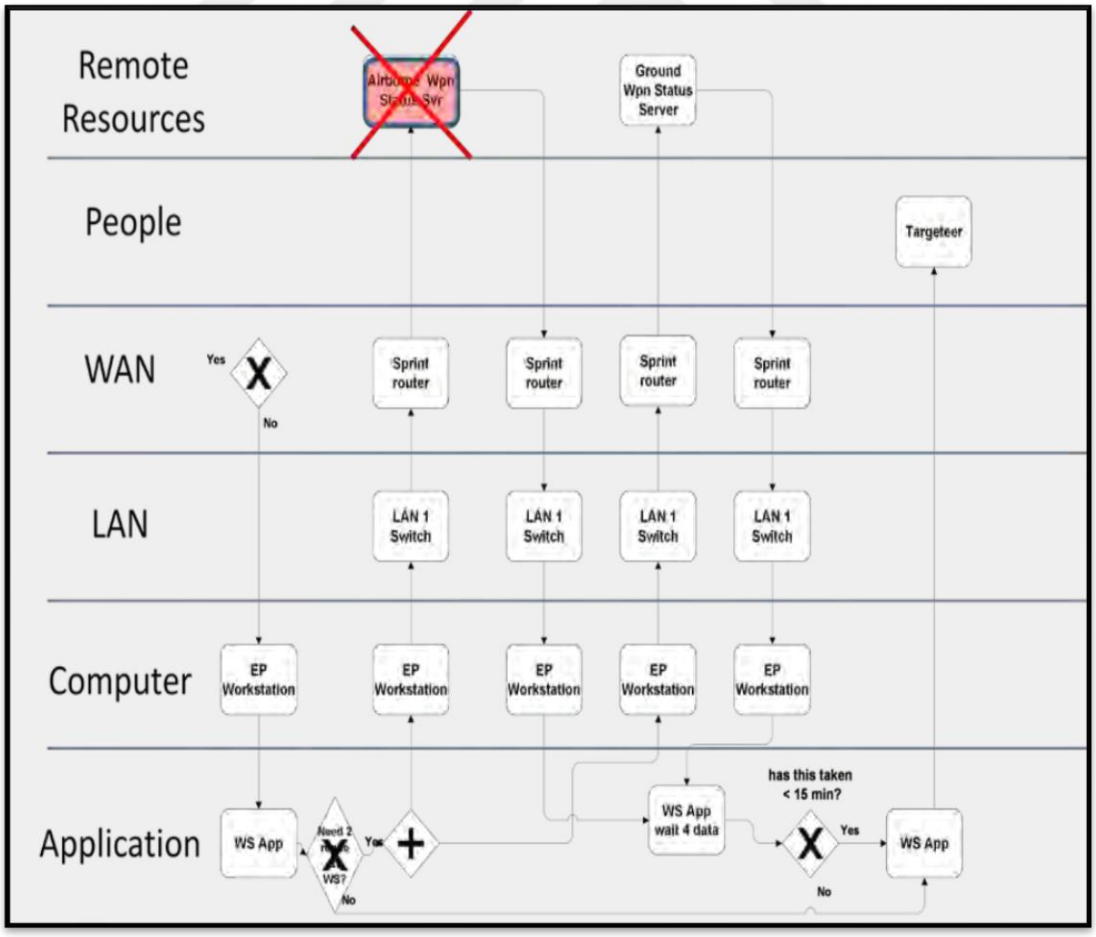


Figure 3: Access to remote mission information becomes unavailable due to an attack.[60]

However, the task attack able to running by using the ready ground weapons information, the task situation resolution posed for task staff is for attempts for comprehension: (1) if they are progressing for the best of proceeding together the task by using the fractional ready information about weapons, (2) if hold off at continuing together the task till next task information about ready weapons be ready, or (3) if into desist the task instance in order that for the accident [61].

3.4 CERT

3.4.1 Definition of CERT

A CERT is a department or an organization within an organization created to study Internet security, find out vulnerabilities and to provide security concerning assistance to the specified community. The KENET CERT offers emergency echo service and shares information for beneficent web and network security. It strives for a safer, powerful Internet for the research community and education via replaying for checking attacks, main accidents, and swapping information about critical cyber security within the community and with other CERTs [61]. As an alternative, the term CSIRT (Computer Security Incident Response Team) also indicate to a group for scientists of IT security particular to respond to computer security incidents. This term, however, is more delicate since it reflects a broader array of security services provided, beyond reactive functions. Although their names suggest an operational responsibility, they are often tasked with similar broad duties as a corporate CERT or CSIRT. The term CERT appears to be more commonly used for national and governmental security teams. Since this paper focuses primarily on (multi-) national or governmental CERT operations, the term CERT is used as an equivalent of CSIRT, SOC and the likes [62].

3.4.2 Acronyms of CERT

Through the years there are several titles and acronyms given for organization of CERT, these contain the following:-

- CSIRC - Computer Security Incident Response Capability or Center.
- IRC - Incident Response Center or Incident Response Capability.
- CIRC - Computer Incident Response Capability or Center.
- CSIRT - Computer Security Incident Response Team.

- SERT - Security Emergency Response Team.
- CIRT - Computer Incident Response Team.
- SIRT - Security Incident Response Team.
- IHT - Incident Handling Team.
- IRT - Incident Response Team. [62]

3.4.3 Types of CERT

There different types of CERT based on the different set of services the following are the types of CERT:-

- A Coordinating CERT coordinator cybersecurity concerning tasks between more specialized CERTs. With a view to getting this overall objective, a Coordinating CERT is likely to concentrate on Coordination, Attribution, Identification and Business Continuity. The outcome, one may anticipate the service portfolio of a Coordinating CERT to contain at least the services in the proactive section, different of the ones in the Security Quality Management Services category, and the coordination services in the reactive section.
- A Servicing CERT provides proactive and reactive security event services. A Servicing CERT concentrates on handling event in different types of IT infrastructure. A Servicing CERT can be a side of an organization where all employees represent its constituency or can be a separate organization that provides its services on a commercial basis to one or more companies. The servicing CERT objectives tend to overlay the full spectrum of security objectives listed, either as an in-house organization or as a commercial company. Therefore, a Servicing CERT can be predicted to cover the full-service portfolio [63].
- A Thematic CERT is a network of collaborating CERTs consolidated by a particular theme (e.g. ICS-CERT for oil & gas). The main concentrate of a Thematic CERT is a proactive exchange of information about particular threats and vulnerabilities and how to counters them, propped by theme-specific tools. Thematic CERTs can have arrangements for mutual support in a cyber emergency. Similar to a Coordinating CERT, a Thematic CERT is likely to concentrate on Coordination, Identification, Attribution and Business Continuity. Additionally, a Thematic CERT will support its organs by

qualifying domain-specific Detection, Mitigation, and ICT resilience. To expanded set of goals, that needs a more detail set of services. Other specialized organizations may select to limit their goals to information sharing only. Such organizations are often called Information Sharing and Analysis Centers (ISAC).

- A Product CERT concentrates on treating security events concerned to a certain (family of) product(s) and is commonly provided by the seller of the product. A seller will offer security services via a Product CERT to its customers as a mean of emphasis that its products will execute as expected. A Product CERT will focus on sharing information concerning threats and vulnerabilities to a special product and mechanisms to handle events and artifacts. With a view to fulfilling the requirement of its constituency, a Product CERT is likely to concentrate on Containment, Detection, Identification, Mitigation and ICT Resilience. A Product CERT will provide many similar services to a Servicing CERT, albeit that they will be limited to the vendor's product(s).[62]

3.4.4 History of CERT

In November 1988 created the internet worm, after that established the Computer Emergency Response Team (CERT) by Defense Advanced Research Projects Agency (DARPA), the location of the Coordination Center (CERT/ CC) at Software Engineering Institute (SEI), Carnegie Mellon University's (CMU) [64]. "The CERT is a society group prepared to expedite society response to computer security events encompassing Internet hosts". CERT Composed of many on very competent recruit during the computer society, Moreover, the personal from the CERT/ CC and from another constraint, replay committee from CERT-System. The CERT/ CC serve as a central spot to restrain for problems in Internet computer security [65]. The Internet System Consortium measured the number of hosts in 1988 and 2014, they present that number of the internet has increased from 60,000 hosts to 1.2 billion hosts. The number of forming CSIRT teams will be growing to proportional the increasing Internet society worldwide, servicing assortment various sizes domains from organizations, regions, and countries. Clearly, such Avast constituency would be ineffectively served by a single CSIRT [64].

3.4.5 CERT in the World

“The Internet is the reality of CSIRTs, and by expansion the world. Many CERT groups around the world are being served by a CSIRT. At some level, these CSIRTs require to interaction to realize their job. Such sharing and coordinate overwork are in the high heart of the CSIRT structure: artlessly statement the task, presenting constituency, and setting the located of the CSIRT’ s in the community are not enough without as well encasement the coordination case [65].

3.4.6 CERT Services

The portfolio of services that exceedingly used as the de-facto set of CERT services has been offered by CMU [66].The portfolio is orderly in three groups:

- Proactive Services: - completed before an events occur or are detected.
- Reactive Services: run when an event becomes known.
- Security Quality Management Services: continuously implemented in order to ensure events can be dealt with.

The table 3.1 had shown the detailed of the services. In order to choose the suitable combination of services that will allow a CERT to achieve its mission, the broad goals stated in the mandate need to be repeated. Although this process of improvement will most likely lead to several results for each individual CERT, the following baseline set of goals that should be included in each CERT’s portfolio is offered:

- Identification of security threats and possible events;
- Detection of security threats and events;
- Coordination of events response activities;
- Inclusion of security events;
- Reduction of security incidents;
- Attribution of security threats and incidents;
- Business Continuity despite security threats; and
- ICT resilience against security threats.

Each one of these services in the portfolio serves one or more CERT objectives, and main objectives can be identified for each service. The table3.2 presents a mapping of CERT services and corresponding main objectives, which can be used to define a clear concentrate for choosing services to be provided by each specific CERT. The mapping does not denote that services cannot obligate other objectives as well. However, the aim is to provide guidance in choosing the maximum relevant services for any particular CERT [67].

3.4.7 CERT Framework

The framework consists of CSIRT Constituency, Organizational locations, Mission and Relationship to other CERTs [68]. These four primary components are directly connected to one another. The CSIRT constituency can be presented as “a special organization, region or country the CSIRT is implementing to provide services”. A CSIRT constituency can be boundless or bounded. Most of the CSIRTs today are bounded meaning that they only serve the funding organization. Understanding the CSIRT's constituency will create the group concentrate for the requirement of organization and assets to be protected. Organizational placement is the varied framework are suggested to CSIRT by tasks, services, objectives, and necessity [68].

Table 1 the portfolio of CERT services [68].

Proactive Services	Reactive Services	Security Quality Management Services

• Announcement
• Technology Watch
• Security Audits or
• Assessments
• Configuration and
• Maintenance of
• Security Tools,
• Applications, and
• Infrastructure
• Development of
• Security Tools
• Intrusion Detection
• Services
• Security-Related
• Information
• Dissemination
	• Alerts and Warnings
	• Incident Handling
	  o Incident Analysis
	  o Incident Response on Site
	  o Incident Response Support
	  o Incident Response Coordination
	• Vulnerability Handling
	  o Vulnerability Analysis
	  o Vulnerability Response
	  o Vulnerability Response Coordination
	• Artifact Handling
	  o Artifact Analysis
	  o Artifact Response
	• Artifact Response
	• Coordination
		• Risk Analysis
		• Business Continuity and Disaster Recovery
		• Planning
		• Security Consulting
		• Awareness Building
		• Education / Training
		• Product Evaluation or Certification

Table 2 CERT services per type of CERT [68].

CERT Services' main focus			Identification	Detection	Coordination	Containment	Mitigation	Attribution	nuity	ICT resilience	CERT	Servicing CERT	Thematic CERT	Product CERT
Proactive Services														
	Announcements		x								x	x	x	x
	Technology Watch		x								x	x	x	x
	Security Audits or Assessment		x	x							o	x		
	Security Tools Application and Infrastructure		x	x							o	x	o	o
	Development of Security Tools		x	x							o	x	o	x
	Security-Related Information Dissemin		x								x	x	x	x
	Intrusion Detection Services			x								x		
ReactiveServices														
	Alerts and Warnings					x	x					x	x	x
	Incident Handling													
		Incident analysis				x	x	x			x	x	x	x
		Incident response on site					x					x		x
		Incident response support					x					x	o	x
		Incident response coordination			x	x		x			x		x	
	Vulnerability Handling													
		Vulnerability analysis				x	x					x		x
		Vulnerability response					x					x	o	x
		Vulnerability response coordination			x	x	x				x		x	
	Artifact Handling													
		Artifact analysis				x		x			x	x		x
		Artifact response				x	x					x	o	x

		Artifact response coordination			x	x		x			x		x	
Security Quality Management Services														
	Risk Analysis									X		x	o	
	Business Continuity and Disaster Recovery Planning								x		x	x	x	
	Security Consulting									X		x	o	x
	Awareness Building								x		x	o	x	o
	Education Training								x		x	x	o	o
	Product Evaluation or Certification									X		x	x	x

The CSIRT mission is typically considered as the organization overall goal and objective. A task statement able to be presented as a style in which the community contacts the business it is into the outside world. The task declaration for each CSIRT within it constituency should be concern giving a suitable security for its constituency. The concentrate of the task declaration of a CSIRT might be the committee prime functions, which is at being a central spot into preventing, replaying and receiving into computer security incidents. Teams shall be formed within specific units like governmental, the business, research work, military, IT and have a diverse framework. Over these streaks, CSIRTs are split by size, style, and mission to domestic, centers of coordination, centers of investigation, national CSIRTs, vendor's team and incidents replay service. In initial the step, CSIRT replies to actual security accidents and lowering impacts of attack [68].

3.4.8 CERT Organizational Model

The CERT organizational formed in the internal style of organization for communication, authority, and relationships. Same, the definition of formed organization is “the network of relationships and roles existing throughout the organization” [61]. The hierarchical form is used for the organizational style; the structure of an organization defines via its system, comprehending commitments, asset allocations, telecommunications, and lines of power. The simple organizational is evaluated via the goals of the organization in additional offers like a connection for that processes action as well as the business is taken out. Thus, the organizational model chooses the number of employees required and their obliged expertise sets, the organizational style chooses a number of employees required in additional their

obliged expertise sets. Diverse CSIRT organizations consist of goals, requests, services, and missions. The organization within different type the team can set up the CSIRT, the classifications of CSIRTs through nature, a scope such as internal or national CSIRTs and the type of services it offers like coordination and analysis, incident response and product team. Currently, The CSIRTs can be classified in more than a single way. The central coordination of the security and communication branch shall be providing backing on site also follow offense at its own region network then record to the committee in central coordination, all these are offered by Central Coordination in CSIRT [61].

3.4.9 CERT Staff

CSIRT action substantially services established, in any case for saving suitable steps and documented policies. As the outcome, there is an ingrained dependence within expert and reliable personals for effectively perform the team's procedures and policies and for offering diplomacy while collaboration together with constituents. Hence staff of CSIRT plays an axial role by guarantee a service also mission for the action. More people wrongly believe a more substantial characteristic within personals of CSIRT to be their technical expertise. Even though experiment technician is an eligible property, by away extra critical criterion is a person can also ready to keep up steps and to supply a uniform interface to customers, constituents, and other groups interact to the CSIRT. It is an extra eligible suggestion to lease person with minimal experience technician and better communication and interpersonal proficiencies after that trains them in CSIRT-special technical skills than vice versa[62]. The staff shall contain (team lead or director, deputy director or deputy team leader, group leaders or supervisors, media relations, triage staff or assistance desk, hotline, sensitivity handlers, incident handlers, platform particularistic, analysis staff for artifact, Display technology, network or system administrators, trainers, support staff, technical writers, crew for CSIRT infrastructure, developers or programmers or (to construct CSIRT tools), maintainers of the web and web developers, legal or paralegal crew or correlation and staff for law enforcement or liaison).

3.4.10 CERT Creation

The procedures of creating and successfully implementing a team begin with planning and the writing of steps. If you do not already have events response procedures that call upon a CIRT, it is time to consider a procedural rewrite. Before you begin rewriting all you are procedures, it is substantial to get support from management. Without their support, the team is not certain sufficient funding or authority and the chances for success are greatly minify. Several managers when the time reaches they select not to create a team but to outsource professionals. There are advantages and disadvantages to this method. It would be a middle of your time to create a plan, and then find out that management has another plan in mind. In addition, if you are company has no created system on securing what so ever, you have a long way ahead of you before you approach anyone with a plan to design a whole team to support a nonexistent security process. Every team member should comprehend the importance of their modulation in the team, and their need to respond fastly when needed. The team organs should recognize the type of status that they will face when they are called upon and what tasks they are predicted to perform when they arrive. This information should not only be clarifying to all team but should also be included in writing the events response procedures. Incident Creating a Computer Response Team is not going be the good solution for all company, but in many if not most settings, it can be an invaluable tool. It will improve response time to any computer base problems you may encounter, ensure that the incident handling methods are supported by the company, and prevent a state of chaos and panic when an actual incident occurs [62].

3.4.11 Roles and Responsibilities of CSIRT/CERTs

To comprehension the role of cooperation among CERT/CSIRT teams in the action of developing the efficiency of combating threats, vulnerabilities and security incidents it is required to discuss advantage of such a collaboration as an important factor in improving services presented by CERTs, as well as barriers that can slow down this process[62]. To render like the top responder for an accident in the computer network at Department also for implementing the necessary function to recognizing, consulting or reviewing, authenticating, management by notifying result or mitigating. Chief Information Officer (CIO) assortments with the CSIRT, while

the responsible straight for the designer or Secretary. The CSIRT is responsible the activities as follow:

- Categorizing Security accident by Department.
- Convention over notification for notifying accident at the computer security.
- Immediate an introductory estimate for selecting source, nature, origin reason, and range of the destroyed.
- Accident of Computer Security shall be recommending echo
- Notified Accident by selecting extra backup members as necessary.
- Preserving privacy for information concerning into computer security incidents.
- Prepared a report for the CIO and Supporting with backup efforts.
- Estimate the origin reason, source, nature, and scope of the loss of the dubious computer security incident.
- Reporting every incident, (Classes 1, 2, and 3) by utilizing the Resource infringement in the Information Technology and/or Accident notifying shape(325-060-04).
- Documenting Accident as suitable. i.e. contain recommended works and lessons learned.
- Prepared a reported accident for the AEIT-OIS.
- Preserve consciousness from, and executing procedures at, an effective reply to computer security incidents.
- Staying present in the process of security and functional into the technologies in their same area of responsibility [62].

3.5 Management in Cyber Defense

The management dimension will be thoughtful under induction, training, and retention. Thereafter, challenges and risks embroiled cybersecurity. According to the find out of a survey [69], technically skilled people generally expressed negative

themes about the military such as: “limited meritocracy, limited creativity, technically ignorant leadership, lack of a technical career path, lack of career advancement,” and so on[70].

3.5.1 Characteristics of cyber warfare professional

A-Education

Depending on the researchers proceed on the workforce information security “half of them have at least a bachelor’s degree, with some comparatively large fraction of that group having a master’s degree as well. Additionally small percentage with [Ph.D.] degrees” [24]. Those people as well have a tendency across education, since they want to hold exploring into modern information so as to stay abreast of emerging technologies; their information skills and standard needed persistent updating [70].

B-Age

An important recruitment agent into the conventional powers given the hardness for action in the military is Age. Nevertheless, being far of the serious for operation in the traditional military, a cyber combatant may older or younger than the middle age for the personnel in the traditional military. Furthermore, the grouping of the nominee for the cyber workforce expanded, ever after age is not a prevailing agent through recruitment. [24]

C-Physical condition

By virtue of cyber fighters vary workplace situation, the predictions of his natural condition are various than that standard predictable for regular forces. As a cyber fighter, the different collection from experiences should act required such as “creativity, mental abilities, technical skills and the ability to sit in a chair for long periods of time, all the while tracking multiple activities on a series of displays, physical fitness may tend to take a back seat.” [24]

3.5.2 Roles in Cyber Workforce

The following are the cyber roles categorized by [71]:

- Processes which "direct, plan and implement offensive and defensive activities in and through cyberspace."
- Practitioners that "provide and sustain assigned portions of cyberspace."
- Targeteers and Analysts that "offer cleverness support to cyber warfare operations."
- Developers which "design and create cyber warfare tools and weapons."

As well as the extra categorization of tasks in cyber workforce via [72] in the condition for specialization kinds:

- Cyber tacticians who "will concentrate at decrease the threat of being fielded systems essentially by the application for suitable protection.
- Cyber strategists who "would concentrate on decreasing the risk of future systems basically through the application of structured and formal system design techniques that reduce system vulnerabilities."

The tasks which are described before should continue appropriate simply of taking out cyber processes, however, extra roles should remain needed into confirming the combination of cyber processes besides another military action [70].

3.5.3 Recruitment

Through fast location, the staffing intricacies of the cyber workforce, armies at the beginning explore to choose cyber attitudes by recruiting of their positions. With each other, all attempted to entice possible cyber combatant of further the military, containing sentenced hackers [70].

A- Recruiting through the ranks: Branch conversion

Every access to cyberspace is the modern field of warfare also the reproduction of cyber warnings stimulated a fast response of governments. As that should get a prolonged time for construct a modern cyber control and a cyber workforce of scribble, armies select to transferring any from the current connections, flag, also every extra pertinent branch within the latest cyber specialization [73]. Although member regeneration should partly help to staff the cyber workforce, transformed cyber combatant should require experience in any fields also act "defensively

focused" [24]. Furthermore, beyond shall be an expense of teaching including instructing those fighters so be proficient in cyber warfare issues. Therefore, armies are non-growing theirs cyber workforce only of theirs individual levels. People are attending since special expertise fill cyber warfare points, essentially this needing creativity, expertise, and other abilities [70].

B- Recruiting outside the military

Armies required on reach outer including the resumption about possible cyber warriors, after transforming the suitable staff into cyber combatant incompletely supplies the force of cyber workforce. Currently, armies are preparing till continue their cyber workforce. The development is a section from a universal scheme on development cyber consciousness that shall consult staff in the ministry's cyber unit twice including a number of cyber-concerning knowledge to ternary" [74]. Through promoting and applying recruiting social media, and homepages, armies continue attempting on interest possible cyber warriors. Moreover, in[55] proposed that cyber security organizations required to stretch out to the special society, and send "speakers to hacker conferences, competing in network warfare contests, and publishing research papers at academic conferences". In addition, armies stay regarding the recruitment from hackers – seldom still the sentenced ones – and people requiring protection approvals [70].

3.5.4 Training

Cyber threats increased in type and number whereas technological advances carry on. Subsequently, cyber security professionals require having a wish for training, considering they want to seek new information for to stay up-to-date about developing technologies. Furthermore, their information base and proficiencies may readily be expired. Traineeship significant cyber workforce, either newly recruited or already existing – raise the rate in cyber warfare. Numerous countries are explicit their strategy for evolving cyber workforce in theirs cyber security strategies. In additional any of these state cyber strategies quickly talk about the significance and need to take the genuine personal capability, there are a few of them providing accurate knowledge around the applications of research activities and cyber learning

[75]. Cyber interests became to the attentiveness of fighting circles and fighting teaching at institutions focused on this case through increasing cyber-concerning courses in their course book and dispatching "groups to an assortment of competitions, wherever they face off against each other" [76]. In [77] they design a vision for the career pathway and cyber learning in the work as shown in Figure 4, the professions pathway should ingress, performer, practitioner, and proficient levels. The teaching blocks are constructed accumulatively: kernel cyber proficiencies take the initial level and expertise practice, task of defense and offense, supporting functions and the command block like the subsequent steps. In another concept, kernel cyber proficiencies are analyzed in detail and it is suggested that cyber specialists attempt the identical primary learning. In [72] puts upwards kernel principles of information affirmation as follows:

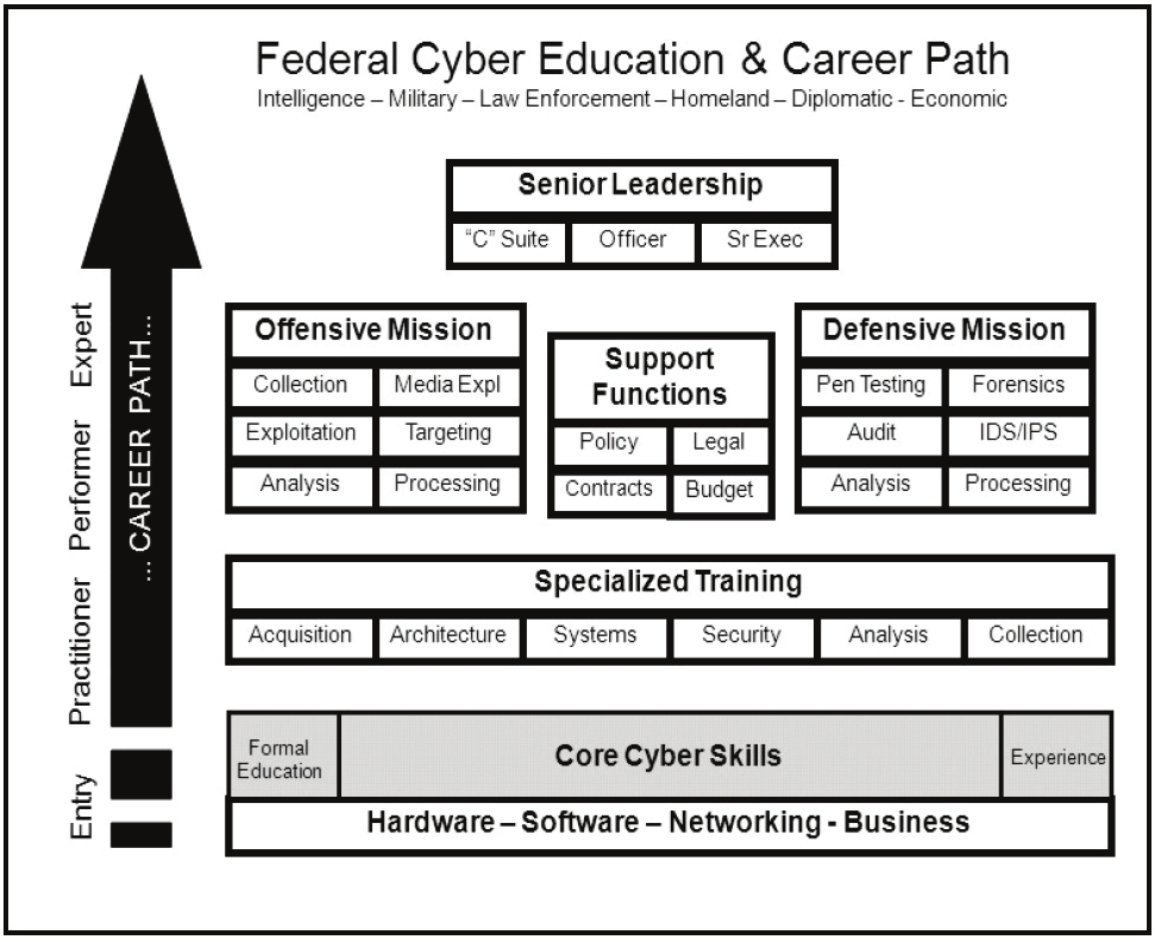


Figure 4: A concept of the research ceremony [70]

- The Reference Monitor (RM) connotation that "preserve that access control is at the heart of data security."

- The equation of The Risk Management, which set up the state that "protection applied to alleviate incipient risk will reduce that risk to some degree, resulting in residual risk."

- Defense - In - Depth that "dictates that practitioners of IA should not depend on any monocular device, technology, or security area (e.g., personnel security, physical security) while working to reduce system risks."

- The Precept of minimum Prerogative which states that "critical information should receive no more solely to potential disclosure or amendment risk than which is under no conditions necessary for task accomplishment."

3.5.5 Managing the Cyber Workforce

Another paramount part of detained that cyber workforce is how they accomplished. These people are perspective to visualize outer the case, be innovative and originative. In [69] they suggest, "You don't have to overly administrate them, only point in the pathway you need them to go. Cyber warriors deserve evenly tech-savvy leaders who grasped and appreciate their achievements; who authorize originative problem fixing and encourage out of the box thinking; who can authorize individual efforts and yet successfully concentrate these efforts into a concrete team" [69].

3.6 Knowledge Management

Knowledge "conclude from information as information concludes from data". This finally indicates that information is the felicitous processing within a nation in whichever the data turn into beneficial. Moreover, "whether the information is to become knowledge, humans must make virtually all the action". That conversion happens by the simile of status, the result, and modulation for choices and works, the link of whereby information join to knowledge, and how people transform what they think about information [78]. Knowledge can be to classified in couple classes: explicit and tacit. Information is Tacit knowledge, like continued practice, while should not be codified [79]. Traditionally the Tacit knowledge like spoke or obtained by practice, however, the process for register this knowledge within the database, a book, or unformed transcription. Before-Mentioned knowledge is obviously

inefficient to future productions while have not owned these practices. The tacit knowledge spiral of learn-teach-learn constructs a cooperative operation. The cooperative or learned operation spiral depends on a community of experience to collect and disseminate the information [80]. Explicit knowledge, furthermore, is the knowledge that has been converting into a registered and codified case. A future production able to learn themselves at those passes also failures about previous productions while explicit knowledge is ready at a problem. Information concluded from sensors or extra information collecting "resides in the information domain, this information is converted into consciousness and knowledge in the cognitive domain and forms of decision-making [sic]". This captured tacit information or data is at the point of conversion – readily transcribed into readily distribute knowledge. Prior to this conversion, the information was a silent kernel asset to the community of experience. Although the information is a focal asset, it may have been hiding in the community and its collective knowledge pool. Thus, this conversion knowledge readily becomes a cooperative and non-competitive body of knowledge [81]. Once knowledge should be capturing and codifying, modification suits a novel target for widening the value of that information. Create product innovations, co-operation, and cases sufficient. Approaches are considered as important ideas, that make also incentivizes reform. Nonaka explained the core of innovation as "to rebuild the world according to a particular seeing or ideal" [82]. Cybersecurity processes depend on at intelligence. The intelligence is creating through the special gathering about information and its capture and codification to knowledge. Moreover, management act requiring manufacturers to be innovative extra now than regularly by allocating contractual duties on this subject. In brief, effective knowledge building is an output of production information sharing. Information sharing "is critical because of mental assets, unlike physical assets, growing in value with use. All educational and experience curves have this characteristic. The Communications theory states that a network's potential benefits up exponentially as the nodes it can successfully interconnect expand numerically" [83].

3.7 Identity Management Systems

At the standard about an Identity Management System (IMS), the author notifies that each client utilizing an Identity Management Applications (IMA) could be understood like a – probably threatening data operation entity" so requires the sufficiently responding via utilizing for an IMA. This title "Identity Management System" (IMS) must explain the foundation in what Identity Management Applications are coordinated like elements. So as to guarantee performing identity management into such a style that it shall determine global agreement amidst users, consider that an Identity Management Protocol (IMP) required being done introduce that facilitates communication for the kind of wanted connection (or social status), therefore the level for alias into being used should be calculated automatically in the receiver and the sender side. the author supposed that enhancing for an IMP is compulsory in order to an IMP should comparatively simply authorize any useful, certain translation for different kinds of telecommunication, i.e., sub-identities activation. Nevertheless, it's necessary to move the user's susceptibility right into explain underlying parts about networking in any time because of the suitable level of security for data security and date protection. The output on a needed since donation entrance on collections of precepts also may be coded in a program. An IMS, depending on the specialization, indicates the foundation inside the unit or within different organizations, who own for one accord in a common form of confidence in maintaining also utilizing individualities. Furthermore, IMS able also denotes an enforcement of individuality management covers a full community. An IMS able just get the grasp over a community wherever it is near position amidst the framework from common systems. That indicates the enforcement, in addition to the benefit of systems, wants to be politically reasonable, economically measurable, scientifically controllable, and rightfully conformable. As well as, IMS depends on a specialized foundation qualifying some processing of digital signatures for authentication also the individual-evident utilize about unknown communication. This is tiny a specialized inquiry than a legitimate also federal one, into whence away entrance on characteristics for a digital integrity is carpetbagger into the user or community. As need through government, a community-enormous executed IMS must act for the nation-from-the-art plan concerning legitimate parts in addition to appearances of privacy safeguard technology and data protection technology – insofar it would be a "Privacy-Enhancing Identity Management System".

Admittedly, there is the risk that organizations or company, that offer and apply IMA in an initial stage, build confidence-succeed, as political and legitimate counteracting tools interact comparably lazy therefore the result should not certainly be secrecy-developing or to limited privacy-submissive[84].

3.8 Event Management

The supportive works at the domain administrator challenging the emergency need a favorable determination for a crisis. Until recently, the bargain with traditional terror is needed by the information system society. the author describes a mass casualty’s case like an event that the equivalence within wanted and resources are undermined and the information system is a crash. Therefore, the management system offers an enormous objection for the information system. The principle object of the total system administration of the case is to reduce destroy part of the whole system changed, indeed to the charge of implementing the solution on the destroyed part of the system.

3.8.1 Pre-Event Phase

The component from the highest interest in predicting achievement into the administration from the system and decreasing from the confusion associated is extensive early preparations. Planning is beginning step for determining also understand the menaces; The plan of the System Administration must include couple rules. The initial associate on the organization from the pre-system situation case and communication and the association within the different saving groups and management systems center at the area. The second associates on the system situation and covers the common algorithm of the system management throughout Information System Management Center (ISMC). Those rules are completed through other important elements that contact into the specific rules of any governmental division and system department. The second stage is a resource, the system staffing must be reassigned to the various department allow to the efficient plans. The property must be evaluated. Areas into the extra system emergency must be pre-designed. Recovery system facilities must be planned. Another crucial facility like certain communication systems, Critical gaps should be sources and sketched for support, whenever required, must be mapped. The final step is training; the team

training must be provided utilizing a number of various formats and methods. Tutorials are to be performed by multimedia devices, lectures, and written materials were given to somebody at a special level. At a next step, aforementioned information must be strengthened and enhanced via training mission-oriented groups. The numerous superior step of training depended on two types of trains (Managers', and Full-scale train).

3.8.2 Immediate preparations phase

The explosion from some ISMC does traditional guided through a short time from confusion. Accordingly, Managers must act approving on this rules (Confirm information, Gather data: position, Type of event, , measured amount of casualties, estimated time of solving problem, Call for extra staff, Notify operating rooms, Decide whether solving destroyed will be needed, Open command station, Open public information center). Intuition should be avoided if possible. This is followed by finding out as many information as potential concerning that system position and estimated a quantity from casualties. It should be realized that starting information force be problematic, incorrect or indeed absent. ISMC situation must be notified just subsequent verification from the validated data, preferably by crosschecking with a different reference. The event can denote abbreviated term. These should be including clearly visible nametags defining the role of the staff member, later evidence from the ISMC declaration; the team organ getting the message must notify the system manager. Optional services continue on do finished as soon as potential. In conformity for the measured, amount of losses also the command center should be equipped with all requisite communication aids and computers.

3.8.3 Treatment process

The part of the system crash must be rehabilitation by ISMC staff. Thus, system crash should be divided into two major categories: those parts should be solved or treatments a problem without replacing the system software or hardware, those who need to replace the system component. A System Manager is put in the assessment from any processing site, each transfer from information should be documented to facilitate follow-up. The part of the system crash should more do transferred to the different system having on special techniques that need processing in special tools either outstanding on the inadequate resource in this admitting system.

3.8.4 Post-event procedures

The prompting meeting should do taken at the earliest likely following terminus of the event. During this meeting, all site directors will provide a short description, showed simply and naturally while this explicit information is fundamental for determining and evaluating the impact of the process. The discussion of all participants will do observed and reported. Results and tutorings to be learned will be distributed to other System, to the ISMC. Protocols should be corrected and updated in accordance with the inducement process. Monitoring should be maintained to enhance our alertness. Gaps in the workforce, equipment, and knowledge must be chosen at the earliest likely.

3.9 Warfare decision making

Information warfare combat that conflict among the current from information can defy the remainder of groups and people. This is more significant that both machines and humans able for making choices that guarantee the integrity to autonomous systems, communication, and information [85]. The purposes of information warfare offense like crime, damage or modification of information, or the damage the infrastructure of information. Certain main purposes should provide subsequent purposes like the possession of money, generation or energy of worry. The operations in information warfare have several kinds, containing categorizations of the set theirs based on the characteristics, like the situation they happen, whether they are defensive or offensive, or the players in the procedure [85]. In [86] the author present in information warfare needs at minimum two different kinds of players. In this kind who preserve information resource is defense, while the attack information resource by the offense. Such players should act correlated with nations, organizations, or individuals. Offensive players cover hackers, corporations, insiders, terrorists, criminals, governments. The purpose of offensive operations in information warfare to the criminal does raise the integrity or availability of information, while the purpose of the defender is to minimize the integrity or availability of information. This has the impact of actual payoff on the criminal and absent payoff to the protector. Of aforementioned perspective, information warfare can be formed like a game that does work among defensive and offensive players who choose tactics by

several payoffs. Designing information warfare into a game-theoretic behavior recommends that processes in information warfare can be examined by methods in game-theoretical. A game represents the cooperation between mutually aware, rational players, wherever the choices by any players change the payoffs from others. A Bayesian game [87] is a play in which information on payoff and the plans to another player is unfinished also a player selects a “type” or “prior” to different players at the start of the match. The Bayesian examination managed to predict the result of the match also for doing Decision for playing attack and protection. A stochastic game [88] is a powerful game with probabilistic developments within any events. The game starts with a first state. The players get payoff depended on the work that they take also the existing state of the game. At any stage of the game, the game developments within a modern state including a possibility that depended on the effects that the players take and the current state. the effect depended on the decision making to the chosen the succeeding state. We can complete the Bayesian network or stochastic methods as a decision making for information warfare.

CHAPTER FOUR
CONCLUSIONS AND FUTURE RESEARCH

4.1 Conclusion:-

The Existing protocols of the International law are deficient at packages among intervention status, accordingly, the principles make no- protect, the situation versus interference. Unbounded interference and cyber distinction may produce in cyberspace become disordered. In some dispute, it has disordered formerly and presupposed mediation on the global level. The properties and classification of the cyber-attacks depended on the size for this effect. Cyber-attack classification based on the impact stage in the loss of human lives and amount of havoc in critical infrastructure.

For constructing an efficacious cyber army, the required for the candidates should have the training, skill, retaining, talent, and recruiting. There is a relatively passive understanding from the army between it performs recruiting, and technical community greatly difficult in a violent tournament to shining talents. The managing of the cyber workforce has different obstacles. For some reason distinction among cyber and classical force, the age does not pick a dominated power for recruiting. The area of cyber is extremely susceptible, has several factors and alert In addition to asymmetric effect. Policy produced need to construct suitable recruitment rules, aperient rescue operation if needed, and confirm a fertile career way with actual rewarding. Moreover, might support cyber power-man. It should be known some different pieces of knowledge like the policy, cyber strategies, and tactics, as well as it should be eloquent in the cyber process, and have knowledge about cyber information gathering, cyber-attack and defense technology, and cyber psychological process. The arranging of cyber force should be arranged in network structures for distributed and sharing information in real time.

Based on the new research in Classification for cyber security and network security traffic the Bayesian network is appropriate classification model for analyzing the network traffic and classify Denial of Service (DoS) attack, and classify the user to Root (U2R) attack.

The US cyber security community implemented the Knowledge management system as unwell. The operation absence rewarding for many benefit and importance of the

knowledge acquired has been limited. The administration team and the governances faced as well as unorganized structure and deficiency of harmonious usage. The Government and cyber security proficient accept to use Knowledge management system and its importance for having it. In practice the knowledge management is not well understood and not flexible used, including the fast is required.

Any big or importance organized and community system becomes more vulnerable to cybersecurity mishap as well as the grown based on the ICT infrastructure and communicate with other organization. Confidence is an important key and effective communion for sharing information in a cyber domain. While the cyber-attack is growing real menace to the community every day, the different modes and types of cyber-attack encompass a new domain of Warfare that desired outstanding activities at all levels of protection. Continues planning on service of all components of the managing staff will improve the power and durability of a community against traditional and cyber-attack. The operation of information and network that support the military in cyberspace become critical elements to gain advantages and adversary. the thing of the significant procedures for security in the network is evaluating the risk of a penetration test and vulnerability detection. There are different best risk evaluations like network risk metric (NRM) and risk Environment.

The concept of CERT is an important model for cyber security operation and mishaps. The mishaps in CERT do not enforce structure boundaries, national or network and that the meddler repeatedly contribution unfastened security process. Many mishaps appear while the software implementation or design lacks are exploited. The communication of sensitivity information and threat across the network is the basis for fixing the particular event and enhancing the operating system security. The CERT-system will elevate the attention and informed between site management for the more the management source of support in time of computer emergencies. The growing knowledge level of the CERT made all members is for active and professional for computer security events.

4.2 Future Work

The demand for sufficient also effective protection the system cannot be over-assert because of the dependence on Internet. Accordingly, suggested that offense or attack at regular network transactions data set must be fine-vetted utilizing the classification

of the Bayesian network for reducing the difficulty. Since DoS offense is concerning the rise due to the availability of easy mechanisms at the network, it must be properly secured versus and a reliable firewall is supported. Clean pipes are a different new approach of working DoS offense.

REFERENCES

1- Fred Schreier “On cyber warfare ”, DCAF HORIZON 2015 WORKING PAPER No. 7

2- P. W. Singer And Allan Friedman “ cybersecurity And Cyberwar What Everyone Needs To Know®”, Published in the United States of America by Oxford University Press 198 Madison Avenue, New York, NY 10016,© P. W. Singer and Allan Friedman 2014.

3- Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss.“Cyber Security Policy Guidebook”, First Edition. © 2012 John Wiley & Sons, Inc. Published 2012 by John Wiley & Sons, Inc.

4- Bayuk, J. (2010). Enterprise Security for the Executive: Setting the Tone at the Top. Santa Barbara, CA: Praeger.

5- Toby Finnie, Tom Petee, John Jarvis, “Future Challenges of Cybercrime ” Volume 5: Proceedings of the Futures Working Group.Quantico, Virginia 2010.

6- Newburger, E. C. (2001). Home computers and Internet use in the United States: August 2000 (Current Population Reports). Washington, DC: US Bureau of Census.

7- Glenn Curtis , Ronald Dolan ,Seth Elan , Noël Ivey , Carl Minkus , Eric Solsten , Taru Spiegel Tomoko Steen , and Project Manager: Alice R. Buchalter , “ Cybercrime: An Annotated Bibliography Of Select Foreign-Language Academic Literature ” , An Annotated Bibliography Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the National Institute of Justice . November 2009.

8- Denning, D. (2000, May 23). Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services U.S. House of Representatives, Georgetown University.

9- Kevin Curran, Kevin Concannon, Sean McKeever “Cyber Terrorism Attacks ”, Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

10- Darius Kazinec “ Issues Of Cyber Warfare In International Law ”, Master Thesis, Darius Kazinec, Faculty Of Law, Department Of International And European Law, 2011.

11- Andrew M. Colarik and Lech J. Janczewski, “Cyber Warfare and Cyber

Terrorism ", Information Science Reference Hershey-New York, © 2008 by IGI Global.

12- Edward Waltz "Information Warfare Principles and Operations", Library of Congress Cataloging-in-Publication Data, ISBN 0-89006-511-X, 1998.

13- Quinn E. Lanzendorfer and Scott C. Spangler " Innovating Knowledge Management In Cyber Warfare " Issues in Information Systems, Volume 16, Issue II, pp. 246-254, 2015.

14- Alexia Kasparian, "Cyberspace: The New Battlefield The Cyber Warfare on the Internet Infrastructure of Estonia in 2007 and of Georgia in 2008", International Conflict Msc, 2013/2014.

15- Squadron Leader Craig Stallard and Royal Australian Air Force "At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force ", Thesis, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama.

16- Walid Al-Ahmad, "A Detailed Strategy for Managing Corporation Cyber War Security ", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(4): 1-9 The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012).

17- Major Bradley L. Boyd, " Cyber Warfare: Armageddon In A Teacup? ", Master's Thesis, U.S. Army Command, and General Staff College, 2009.

18- Daniel Louis Gold, " Information Warfare On An Evolving Battlefield ", Master Thesis In Homeland Security, San Diego State University,2012.

19- Charles Debeck " The Correlates of Cyber Warfare: A database for the modern era ", Master Thesis, Graduate Theses and Dissertations, Graduate College,2011.

20- Lior Tabansky, "Basic Concepts in Cyber Warfare ", Military and Strategic Affairs, Volume 3, No1, May 2011.

21- Owens, W., Dam, K. & Lin, H. (Eds) (2009) Technology, Law, and Ethics Regarding US Acquisition of Cyberattack Capabilities (Washington, DC: National Research Council of the National Academies of Science).

22- Libicki, M. (2009) Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND Project Air Force, RAND Corporation).

23- Randall R. Dipert, "The Ethics of Cyber Warfare ", State University of New York, 16 Dec 2010, Journal of Military Ethics, 9:4, 384-410.

24- Jason Andress, Steve Winterfeld, and Lillian Ablon "Cyber Warfare

Techniques, Tactics and Tools for Security Practitioners ", Second Edition,2014 Elsevier Inc.

25- Taleb N. NY Times first chapters,http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html; 2007.

26- Jeffrey Carr, "Inside Cyber Warfare", 2010 Published by O'Reilly Media, Inc.

27- Moyinoluwa Abidemi Bode, Boniface Kayode Alese, Samuel Adebayo Oluwadare & Aderonke Favour-Bethy Thompson "Risk Analysis In Cyber Situation Awareness Using Bayesian Approach ", Department of Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria, 2014.

28- Murugiah Souppaya, Karen Scarfone " Guide to Malware Incident Prevention and Handling for Desktops and Laptops", NIST Special Publication 800-83 Revision 1, 2013.

29- Martin C. Libicki "Cyber deterrence and Cyberwar ", © Copyright 2009 RAND Corporation.

30- apl. Prof. Dr. K. Saalbach "Cyber war Methods and Practice Version 9.0 ", University of Osnabruck, Jun 2014.

31- FM 3-13 Inform and Influence Activities, Department of the Anny, Washington DC, January 25, 2013.

32- Aniwat Hemanidhi, Sanon Chimmanee & Chom Kimpan "Cyber Risk Evaluation Framework based on Risk Environment of Military Operation ", 2015 Asian Conference on Defence Technology (ACDT),©2015 IEEE.

33- ICs, Joint Pub 3-13, 1998, p. 1-9.

34- M. C. Libicki, What is Information Warfare?, National Defense University, 1995.

35- Mr. Walt Tirenin & Mr. Don Faatz "A Concept for Strategic Cyber Defense ", © 1999 IEEE.

36- Jung-Ho Eom, Nam-UK Kim, Sung-Hwan Kim and Tai-Myoung Chung, " Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare", International Conference on Cybersecurity, Cyber Warfare and Digital Forensic (CyberSec),2012, IEEE.

37- Jung-Ho Eom, Min-Woo Park, Seon-Ho Park and Tai-Myoung Chunk " A Framework of Defense System for prevention of Insider's Malicious Behaviors", Advanced Communication Technology (ICACT), 13th International Conference on 2011.

38- Mr. Walt Tirenin & Mr. Don Faatz "A Concept for Strategic Cyber Defense ", © 1999 IEEE

39- D. S. Alberts, Defensive Information Warfare, Washington, D.C., National Defense University Press, 1996.

40- R. E. Hayes, and G. Wheatley, Information Warfare and Deterrence, Strategic Forum Number 87, National Defense University, October 1996.

41- JCS, Joint Publication 3-58, Joint Doctrine for Military Deception, 3 1 May 1996.

42- U.S. Army Field Manual 90-2, Battlefield Deception, 3 October 1988, (Rescinded). ~tto://www.fas.ore/im/doddir/armv/fm90-2/toc

43- JCS, Joint Doctrine for Information Operations, Joint Pub 3-13, 9 October 1998, p. 11-14.

44- O. S. Saydjari, DARPA Information Assurance program manager, electronic mail, 28 January 1999.

45- Ben Bain, "Military Wrestles with Cyber War Battle Planning" DefenseSystems.com, July 26, 2010, p. 3, http://defensesystems.com/Articles/2010/07/26/FEAT-Cyber-Command-tackles-cyber- war.aspx?Page=1.

46- Nicholas C. Rueter "The cybersecurity Dilemma ", Master thesis of Arts in the Department of Political Science in the Graduate School of Duke University 2011.

47- Ronald E. Purser, "Cyberspace and Its Limits: Hypermodern Detours in the Evolution of Consciousness", Global CyberTech & Integral Consciousness XXV Annual Gebser Conference October 21–24 1999.

48- Borgmann, Albert, "Crossing the Postmodern Divide", Chicago: University of Chicago Press,1992.

49- Murdoch Watney, "Challenges Pertaining to Cyber War under International Law ", Cybersecurity, Cyber Warfare and Digital Forensic (CyberSec), 2014 Third International Conference on, 2014.

50- D.P. Fidler, Aug 1, 2011, "Was Stuxnet an Act of War? Decoding a Cyber-attack" , IEEE Security & Privacy , Volume: 9, Issue: 4, 2011.

51- J. Dugard, International Law: A South African Perspective, Capetown, South Africa: Juta, 2011, pp. 495 – 513, 519 – 525.

52- N. Melzer, May 7, 2013, "Cyberwarfare and International Law" http://www.unidir.org/files/publications/pdfs/cyberwarfare-andinternational-law-382.pdf

53- G.D. Brown, November 14, 2011, “Why Iran didn’t admit Stuxnet was an attack”, issue 63, 4 the quarter 2011 / JFQ.

54- M.N. Smitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, New York, USA: Cambridge University Press, 2013.

55- E Iasiello, February 23, 2014, “Cyber Attack: A Dull Tool to Shape Foreign Policy,”, http://www.ccdcoe.org/publicatoins/2013/proceedings/d3r1s3_Iasiello.pdf.

56- R.L. Kruger, “Deterrence of Cyber Attacks: in Cyberpower and National Security, F.D. Kramer, S.H. Starr and L.K Wentz, Eds. Washington, D.C: National Defense University Press, 2009, pp. 317

57- Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis, Theodore Apostolopoulos “A CYBER-ATTACK EVALUATION METHODOLOGY ” , ECCWS_2014.

58- Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2009) “Risk-based criticality analysis”, Critical Infrastructure Protection III, Springer, Vol. 311 pp 35-49.

59- U.S. Department of Homeland Security, National Infrastructure Protection Plan 2009, Washington, DC.

60- Scott Musman, Aeron Temin, Mike Tanner, Dick Fox, and Brian Pridemore,“ Evaluating the Impact of Cyber-attacks on Missions”, MITRE Corp, McLean, VA, 22102, July 2010.

61- Peter MUIA, Meoli KASHORDA, Kennedy ASEDA, Ronald OSURE, Martin NJAU, “Building a Cybersecurity Emergency Response Team (CERT) for the NREN Community – The case of KENET CERT ”, 8th UbuntuNet Alliance annual conference, 2015.

62- Tom Campbell, CISSP, ABCP “An Introduction to the Computer Security Incident Response Team (CSIRT) Set-Up and Operational Considerations”, March 2003, SANS Institute.

63- Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle and Mark Zajicek, “Handbook for Computer Security Incident Response Teams (CSIRTs)” , Copyright 2003 by Carnegie Mellon University.

64- Scherlis, W., ‘‘DARPA Establishes Computer Emergency Response Team,’’ DARPA Press Release, December 6, 1988.

65- Denning, P., Computers Under Attack, ACM Press, 1990.

66- Carnegie Mellon University, 2002. CSIRT Services. Software Engineering Institute. CERT Coordination Center. Stelvio bv, The Netherlands; PRESECURE

Consulting GmbH, Germany. [online] Available at: <http://www.cert.org/csirts/services.html> [Accessed 15 October 2013].

67- Olaf Kruidhof,“Evolution of National and Corporate CERTs - Trust, the Key Factor”, Best Practices in Computer Network Defense: Incident Detection and Response M.E. Hathaway (Ed.), IOS Press, 2014.

68- Melissa E. Hathaway, “Best Practices in Computer Network Defense: Incident Detection and Response” , NATO Science for Peace and Security Series, Sep 2013.

69- Conti, G., & Easterly, J.“Recruiting, development, and retention of cyber warriors despite an inhospitable culture”,Small Wars Journal, 2010.

70- Ilker Kilaz, Akif Onder and Murat Yanik, “ Manpower Planning and Management in Cyber Defense”, Turkish Army War College, Istanbul, Turkey.

71- Franz, T., "The Cyber Warfare Professional: Realizations for Developing the Next Generation", Air & Space Power Journal, vol. 25, no. 2, pp. 87-99, 2011.

72- Fulp, J. D., “Training the cyber warrior”, in Security education and critical infrastructures, eds C Irvine & H Armstrong, The International Federation for Information Processing, vol.125, pp. 261-273. Springer, US, 2003.

73- Boland, R. "Military Branch Undertakes Massive Troop Conversion", Signal, vol. 64, no. 6, pp. 49-51, 2010.

74- McGarry, B. (2013) “NSA Chief: What Cyberwarrior Shortage?”,Availablefrom: http:// defensetech.org/2013/10/14/nsachief-what-cyberwarrior- shortage/>. [15 December 2013].

75- National cybersecurity Strategy and 2013-2014 Action Plan (Turkey), (2013) Available from: <http://www.ccdcoe.org/strategies/TUR_Cyber security.pdf>. [13 February 2014].

76- Beidel, E.“Military Academies Look to Fill Nation’s cybersecurity Gaps” Available from: http://www.nationaldefensemagazine.org/archive/2012 /January / Pages/MilitaryAcademiesLooktoFillNation%E2%8 0%99sCyber securityGaps.aspx. [30 December 2013].

77- Evans, K., & Reeder, F. (2010),”A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters”. Center for Strategic and International Studies (CSIS).

78- Davenport, T. H., & Prusak. (2000). Working knowledge: how organizations manage what they know. Boston, Mass.: Harvard Business School Press.

79- Polanyi, M., & Sen, A. (2009). The tacit dimension. Chicago; London:

University of Chicago Press.

80- Perry, W.L., Moffat, J. (2004). “Information sharing among military headquarters: The effects on decision making”. RAND Corporation National Security Research Division.

81- Logan, D., King, J. & Fischer, H (2008). Tribal Leadership: Leveraging Natural Groups to build a thriving organization. New York, NY: Harper Collins.

82- Nonaka (1998) The knowledge-creating company. Harvard Business Review on Knowledge Management. Pp.21-48.

83- Quinn, Anderson, and Finkelstein (1998). Managing professional intellect: making the most of the best. Harvard Business Review on Knowledge Management. pp. 181-205.

84- Schleswig-Holstein and Studio Notarile Genghini (SNG),“Identity Management Systems (IMS): Identification and Comparison Study” , Independent Centre for Privacy Protection (ICPP) 2003.

85- Kathryn Merrick *, Medria Hardhienata, Kamran Shafi and Jiankun Hu, “A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios ”, Future Internet 2016, 8, 34; doi:10.3390/fi8030034.

86- Denning, D.E.R. Information Warfare, and Security; Addison-Wesley Reading: Essex, UK, 1999; Volume 4.

87- Liu, Y.; Comaniciu, C.; Man, H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. Proceeding from the 2006Workshop on Game Theory for Communications and Networks, Pisa, Italy, 14 October 2006; p. 4.

88- Sallhammar, K.; Knapskog, S.J.; Helvik, B.E. Using stochastic game theory to compute the expected behavior of attackers. In Proceedings of the IEEE 2005 Symposium on Applications and the Internet Workshops, Trento, Italy, 31 January–4 February 2005; pp. 102–105.