T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# INVESTIGATION OF AFGHANISTAN NETWORK INFRASTRUCTURE FOR CYBER SECURITY

**M.Sc. THESIS**

**Sayed Zakariya HABIB**

|  |  |  |
|---|---|---|
| **Enstitü Anabilim Dalı** | **:** | **COMPUTER ENGINEERING** |
| **Tez Danışmanı** | **:** | **Doç. Dr. Ahmet ZENGİN** |

**Jaunary 2018**

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# INVESTIGATION OF AFGHANISTAN NETWORK INFRASTRUCTURE FOR CYBER SECURITY

M.Sc. THESIS

Sayed Zakariya HABIB

Enstitü Anabilim Dalı : COMPUTER ENGINEERING

This thesis has been accepted unanimously / with majority of votes by the examination committee on ………….

| | | |
|---|---|---|
| Doç.Dr.Ahmet ÖZMEN | Doç. Dr. Müfit ÇETİN<br>……………… | DocDr. Ahmet Zeyn<br>……………… |
| Head of Jury | Jury Member | Jury Member |

# DECLARATION

I have learned many new things along the new era of communication systems and the era which I have perceived to dedicate my times for understanding, during four years of my studies at Kabul Polytechnic University KPU and especially, two years of my continuous research in the field of cyber security at Sakarya university, I have learned for instance, a bunch of techniques with emphasize in academic procedures. More importantly, I have learned the honesty because it is one of the significant equivalent to human wealth, this honesty is deserved and provoked me for going to raise my hands up and declare that all the data in this thesis was obtained by myself in academic rules, all visual and written information and results were presented in accordance with academic and ethical rules, there is no distortion in the presented data, in case of utilizing other people's works they were refereed properly to scientific norms, the data presented in this thesis has not been used in any other thesis in this university or in any other university.

Sayed Zakariya HABIB
10.12.2017

# ACKNOWLEDGEMENT

First of all, I am thankful to my supervisor associate Doç. Dr. Ahmet ZENGİN for his support and necessary guidance concerning to this effort as my final graduate thesis. He has motivated me by technically supporting in each steps, from investigation up to simulation steps, without his superior supports, the accomplishment of this thesis was hard, and thus his support has been essential in each part up to finalization.

Gratefully, I would like to continue my appreciation to my gentle professor Mr. Daniel F. Garcia who took my supervision at Oviedo University, Gijon in Spain, when I attended to ERASMUS plus at this university under his supervision. It is really being appreciated for his comments, helping and hardworking to collaborate me in each steps of this effort. His knowledge and experiences made me feel much more confident and encouraged me comprehensively.

Secondly, I would also like to thankful from colleagues who helped me by giving their valuable information, suggestions, comments, and animadversions to improve more enough and excited me to finalizing this thesis within the limitation of time. Finally, I would like to express my sincere thanks towards researchers who devoted their time and pieces of knowledge in either simulation or investigation parts. As well as, thanks and gratitude toward my family and friends for their encouragements which also helped me in the completion of this dissertation.

# TABLE OF CONTENTS

CHAPTER 3.

# LIST OF ABBREVIATION

| | |
|---|---|
| ACS | : Access Control System |
| AI | : Artificial Intelligence |
| AL | : Application Layer |
| ANDS | : Afghan National Development Strategy |
| AOFN | : Afghan Optical Fiber Network |
| ARP | : Address Resolution Protocol |
| AWCC | : Afghan Wireless Communication Company |
| BAS | : Biometric Authentication System |
| BN | : Bayesian Network |
| BOF | : Buffer Overflow |
| CASA | : Central Asia Southern Asia |
| CC | : Cyber Challenges |
| CDN | : Content Delivery Network |
| CIA | : Confidentiality, Availability and Integrity |
| CII | : Critical Information Infrastructures |
| CIS | : Critical Information System |
| COPP | : Child Online Protection Policy |
| CPT | : Curious Packet Tracer |
| CS | : Cyber Security |
| CT | : Cyber Threat |
| CW | : Cyber War |
| CWF | : Cyber warfare |
| CyC | : Cyber Crime |

| | |
|---|---|
| DA | : Data Acquisition |
| DAC | : Discretionary Access Control |
| DBR | : Database Resource |
| DCS | : Distributed Control System |
| DDOS | : Distributed Denial Of Services |
| DLP | : Data Loss Prevention |
| DOF | : Data Overflow |
| DoI&CS | : Directorate of Information and Cyber Security |
| DOS | : Denial Of Services |
| EID | : Extended Influence Diagrams |
| ENB | : External Network Backbone |
| ESCAP | : Economic and Social Commission for Asia and Pacific |
| ExNA | : External Network Architecture |
| FS | : Frequency Spectrum |
| GDoL | : General Department of Legislative |
| GSM | : Global System for Mobile |
| HerS | : Herat Server |
| HMI | : Human Machine Interface |
| HNLAL | : High-secret Network Logical Architecture Layer |
| IEEE | : Institute of Electrical and Electronic Engineers |
| IJNSA | : International Journal of Network Security and its Application |
| IL | : Internet Layer |
| IMEI | : International Mobile Equipment Identification |
| INB | : International Network Backbone |
| InNA | : Internal Network Architecture |
| IoT | : Internet of Things |
| IP | : Internet Protocol |
| IS | : Information System |
| ISISMS | : International Standards for Information Security Management System |
| ISO | : International Standard Organization |

| | |
|---|---|
| ISP | : Internet Service Provider |
| ISSD | : Information Systems Security Directorate |
| ITP | : Information Technology Professional |
| ITRC | : Information Technology and Research Center |
| KabS | : Kabul Server |
| L&HFB | : Low and High Frequency Bands |
| LAN | : Local Area Network |
| MAC | : Mandatory Access Control |
| MAC | : Media Access Control |
| MaSS | : Maszar-e-Sharif Server |
| MCIT | : Ministry of Communication and Information Technology |
| MFAS | : Multi Factor Authentication System |
| MoJ | : Ministry of Justice |
| NAL | : Network Access Layer |
| NATO | : North Atlantic Treaty Organization |
| NCSSA | : National Cyber Security Strategy of Afghanistan |
| NDOS | : National Directorate Of Security |
| NLAP | : Network Logical Architecture Policy |
| OAP | : Open Access Policy |
| OSI | : Open System Interconnection |
| OSIS | : Online Service and Information System |
| OSN | : Online Social Network |
| PGS | : Power Grid System |
| PL&SL | : Presentation Layer and Session Layer |
| PNLAL | : Public Network Logical Architecture Layer |
| PSN | : Products Serial Number |
| PTCL | : Pakistan Telecommunication Company Limited |
| RACS | : Role-based Access Control System |
| RTOS | : Real-Time Operating System |
| RTU | : Remote Terminal Unit |

| | |
|---|---|
| SCADA | : Supervisory Control And Data Acquisition |
| SDL | : Scenario Definition Language |
| SDLC | : Software Development Life Cycle |
| SIM | : Subscriber Identity Module |
| SNLAL | : Secret Network Logical Architecture Layer |
| SQL | : Structure Query Language |
| SQLI | : SQL injection |
| SSFD | : Cyber Security Strategy for Defense |
| SVM | : Support Victor Machine |
| TAPI | : Turkmenistan, Afghanistan, Pakistan and India |
| TAS | : Token Authentication System |
| TCP | : Transmission Control Protocol |
| TICoI | : Telecom Infrastructure Company Of Iran |
| TL | : Transport Layer |
| TOE | : Technology Organization Environment |
| TUTAP | : Turkmenistan, Uzbekistan, Tajikistan, Afghanistan and Pakistan |
| VCT | : Virtual Cyber Terrain |
| VPN | : Virtual Private Network |
| W&ES | : Web and Email Server |
| WAN | : Wide Area Network |
| WiMAX | : Worldwide interpretability for Microwave Access |
| WSN | : Wireless Sensor Network |
| XSS | : Cross-side scripting |

## LIST OF FIGURES

## LIST OF TABLES

# AFGANİSTAN İLETİŞİM ALTYAPISININ SİBER GÜVENLİK AÇISINDAN ARAŞTIRILMASI

## ÖZET

Anahtar Kelimeler: Siber güvenlik, siber saldırılar, siber savaşlar, güvenlik açığı, gizlilik, bütünlük, ağ altyapısı, iletişim ve bilgi sistemleri.

Global endüstriler büyük ölçüde bilgi ve veri güvenliğine yatırım yapıyor. Sanal iletişim zamanında, herhangi bir topolojisinde, öncelikle geçerlik ve güvenliği garanti altına almalı. Aksi takdirde bu tür iletişim karmaşık sorunlara ve kaynakların ağlar üzerinde zarar görmesine neden olur. Halbuki iletişim sistemleri savunmasızdır, Ülkenin bilgi bütünlüğüne, gizliliğine ve kullanılabilirliğine güvenmesi, siber güvenliğinin yetersizliğinden tam tersidir. Aslında, iletişim sistemleri veya internet öncelikle odaklı veya insan zihnindeki güvenlikle tasarlanmamıştır. Diğer bir deyişle, çok sayıda ağ bileşeninin koordinasyonu, öncelikle hava-arayüzü üzerinden kurulan veya ağ üzerinden önceden tanımlanmış protokoller altında fiziksel olarak entegre edilmiş güvenli bir bağlantıya ihtiyaç duyar.

Ayrıca, bir hükümetin gerçekleştirme sorumluluğundan biri, siber ortamda ya da gerçekçi saldırı ve tehditlerle mücadele etmek için bir caydırma ekibi ya da teşkilatı oluşturmaktır. Modern iletişim sistemlerinde, siber saldırılar casusluk açısından gittikçe artmaktadır ve bilgi sistemlerine ciddi zarar vermek suretiyle siber alanın geleceğinde büyük bir sorun çıkarmaktadır. Öte yandan, Afganistan hükümeti, herhangi bir dışa bağımlı siber saldırılara karşı iyi tanımlanmış bir stratejiye sahip değilken, casusluktan sorumlu olan ve Afganistan'daki siber alanda katastrofik sorunlar çıkaran ülkelerden aktarılan değiştirilebilir verilerin büyük bir çoğunluğu bulunmaktadır. Bu sorunlar dikkate alındığında, bu çalışma Afganistan'da siber saldırılar ve siber istismar, bilgi güvenliği ile ilgili zorluklar, siber saldırıların mevcut Afganistan ağ altyapıları üzerindeki etkileri ve analizleri de dahil olmak üzere siber tehditlerle ilgilidir. Siberayla ilgili belirgin ve belirgin olmayan siber saldırılar için bir şekilde çözümün yanı sıra, mevcut ve gelecekteki siber krizin, modellerin ve simülasyon özelliklerinin bu raporun kısmen bir bölümünde analizi tanımlanmıştır. Bununla birlikte, güvenlik açısından Afganistan'ın mevcut siber durumuna, yaygın gelecekteki siber güvenlik ve siber güvenlik zorluklarına ilişkin sorunlar da bu raporda gösterilmektedir.

# SUMMARY

Keywords: Cybersecurity, cyberattacks, cyber wars, vulnerability, confidentiality, integrity, network infrastructure, communication and information systems.

Global industries are investing heavily in information and data security. At the time of virtual communication under any types of topologies, firstly, the validity and security must be guaranteed. Otherwise, such communication cause complex problems and resources damage over the networks. However, communication systems are vulnerable, the nation's reliance on the integrities, confidentialities, and availabilities of information stand in stark contrast to the inadequacy of their cybersecurity. In fact, communication systems or internet was not primarily designed with security in oriented or human minds. On the other word, coordinating of huge numbers of network components, first of all, need to a secure connection, either such connection established via air-interface or integrated physically under predefined protocols over the network.

Additionally, one of the accomplishment responsibility of a government is creating a deterrence team or military to combat any types of attack and threat either on cyberspace or on realistic. In modern communication systems cyber-attacks becoming increasingly in terms of espionage, and it would make a big challenge in the future of cyberspace by causing serious damage to information systems. From the other hand, the government of Afghanistan does not have a well-defined strategy against any types of outsider cyberattacks while the huge amount of the exchangeable data transferring from the countries who are in charge of espionage and attempt to make catastrophic problems on Afghanistan's cyberspace.

In consideration to these issues, this study concerned in Afghanistan’s cyber-threats including cyber-attacks and cyber-exploit, information security challenges, analysis and effects of cyber-attacks on current Afghanistan network infrastructures. Definition of somewhat solution for distinctive and non-distinctive cyber-attacks over cyberspace, as well as the analysis of current and future cyberspace crisis, models and simulations aspect in some partial part of this report, has been also covered. However, current cyberspace status of Afghanistan in term of security, challenges of prevalent future cyber security and cyber security difficulties have also illustrated in this report.

# CHAPTER 1. INTRODUCTION

In para-industrial communities, information is a significant source of strategies that conducts through information systems and information systems have an impressive and effective role into industrial society in terms of investments by having valuable wealth in such society, however, cyber-threats commonly target the source of strategies or information being contributed to multi-dimensional source of human life. Industrial lives, intelligent sensor networks and smart processors that operate interactivity are not only the target of malicious, slightly, the human life and community's safety also being conclusively threatened by cyber-threats and inauspicious plans in function of cyber-attacks and cyber-exploits.

Many international organizations and foundations including national communities have found and reported multi-types of crimes that basically called cybercrimes, in deep consideration to cybercrimes, it is actually a modern type of crimes easily could be carry out through malicious and spams emails, many types of malware, malicious codes, malicious and inauspicious strategies in ambition of cyber-attacks into victims physical infrastructure. Whatever, this modern crimes which are being managed individually or groups of malicious teams work to gather to arrange, enumerate as the biggest challenges for investments and para-industrial communities.

Generally speaking about cyber-attacks could be seen as kind of similar to silent warriors in virtual space. This virtual space is known as cyberspace. Hackers and attackers attempt to target network infrastructures for gaining access, taking over authority and control of information systems. In such kinds of attacks, any types of information could be at risk, wherever those pieces of information are archived, whether that's, virtually over the internet or saved in data centers and even stored on the cloud [1].

Cyber-security has become as one of the largest arguable phenomena in modern technology and communication society, as far as, security and risks of online applications and offline software, directly depend on development and architecture phases of software productions, the security risks and security vacuums in information systems connects dependably to our current cyber-security issues. Cyber-security and security risks are not passed a long history equal to other human development counterpoises; slightly it is introduced in last decades and almost the cyber-threats have impressive effect newly in modern communication and information systems. Nonetheless, in many concepts cyber-security risks and cyber-threats calculate as modern types of threats that threaten information and communication systems; these risks precisely cause catastrophic cybercrimes in all around the continents. Many national and multi-national organizations around the world concern about the security risks and risks management which are raise generally from cyberspace.

On the other side, the efforts of cybercriminals have become more sophisticated, as these have acquired substantial resources, improved their organizational structures and implemented a clear division of labor between disparate criminal networks. Attacks via the Internet have become systematic and may often be aimed at specific high-value yet vulnerable targets. Moreover, the state of malware for cybercrime has become increasingly more sophisticated and the activities of criminal groups that organize cyber-attacks are continuously expanding in scope. Other forms of cybercrime include harassment, fraud, the distribution of illegal materials or the violation of intellectual property rights. In continuation to the risks of cyberspace, it includes a wide range area of the cyber-threats contains cyber-attacks and cyber-exploits, it is not just a society or group for protection of natural and national investments, rather the cyber-security is often counted beyond human knowledge due to the productions of application and software are not easily preventable for current nations and even though the penetration into negative points of software is also not that much impossible, hackers and attackers can easily penetrate and then can exploit the applicable software installed on victims systems by understanding the basic functionality of software and hardware technology.

Cyberspace deserve a serious preservation that comprehensively safe human lives. As it is all cleared, modern communication systems have changed our daily activities, our behaviors and even our minds. However, from the other point of view, parallel to human needs and necessary technology, digital world has improved, within these changes and improvements of the digital world accommodatingly human societies faced lots of problems through the cyber space. Today large amount of investments are spent to prevent cold war among countries. One of the extremely valuable and sensitive areas of cold war is cyber war.

In demonstrations and discoveries regarding the cyber war, many types of cybercrimes are also proceed-able in human daily life at all around the world, but this phenomena is almost new in our people minds in Afghanistan, the cyber-security risks and risks management including risk assessments are the biggest challengeable case study in our current and future cyberspace for both of public and private sectors. Therefore, this report prepared for two important goals, first, it has been prepared for personal improvement and increments of high scientific potential knowledge concerning cyber-threats, modern technology and specifically perceive of cyberspace; and then as final thesis. In general, this report commonly concentrate into four phases of modern technology and cyber-threats, the first phase contains the basic underlining about cyber-security and risks which threaten our current and future communication and information systems, in the second phase is concerned regarding the common types of cyber-threats including cyber-attacks and cyber-exploits, while in the third phase is concentrated about the solutions and modulations of the cyber-threats and in the final phase the simulation and conclusion have been demonstrated. Security is the protection operation of archived information, which denies any unauthorized users trying to take any authority over the systems. In brief, security is defined as the process of preventing hackers from entering into systems and protecting any unauthorized access to systems, networks and the data in cyberspace [2]. In consideration to the current internal network backbone, Afghanistan is not well equipped with wired network communications except in some locations. Therefore, wireless and telecommunication are the common and popular networks for data transmission and internet service providing. Currently, wireless and GSM services have made up for approximately 80 percent of Afghanistan's communication systems [3].

According to a new statistics survey from the ministry of communication and information, there are more internet users and so forth the number of information systems are constantly increasing, which deserve to use meaning full techniques to prevent emerging threats in cyberspace [4]. The understanding of cyber threats is a key parameter for future cybersecurity development, due to the data leakage or damage of communication infrastructure and information systems must be ranked on priority.

Nevertheless, from the other side, the movement of current network infrastructures from wireless to software-based modes often needs more resources and sufficient maintenance, in both hardware based and software based communication sides. Certainly, in the case of security, the lack of non-existence and inadequate facilities, all types of communications might be at risk from each portion of the transmission. In agreement with worldwide updated internet security threat reports, nowadays personal identities are impressively under threats, Afghanistan also suffers from these kinds of vulnerabilities.

In terms of information and systems implementation, computerization and especially communication systems, Afghanistan has to start from the beginning and currently, attempts to supply information systems in different areas. Such as commercial and banking systems; industrial contribution and transportation systems; the distribution of national identifications; the digitalization of health services; online law consultancy and social services systems; online learning and training systems; military and national security systems [5]. As an example, the ministry of communication and information technology with the aid of the ministry of interior affairs, presently have begun digital distribution of national identity or birth certificates to people. This project is one of the major projects which might have an extensive security problem in the future. However, development communication projects like e-government which covers mobile government services and innovation grants program are the other project that can be at risk of cyber-attacks in the future [6]. Additionally, the usage of software and developed applications increase and spread over all, nearly all of the in used software in Afghanistan, are not legally distributed and mostly are not developed inside of this country. The security of such applications have made an arguably challenge in current and although would make bigger issue in the future.

Furthermore, military and police biometric and registration systems are the exceedingly largest projects which ministry of defense and interior affair presently work on them, these projects would have a big security challenge in the future if considerably do not concern about current cyber-threats and cyber-malicious tools [7]. From the other side, Afghanistan’s internal conflictions and powerful countries like Russia, China, United States of America and other regional countries competencies have the co-relation with our current and the future cyberspace, in part 2.1, the argumentative review of cyber-attacks proof that Afghanistan is not slightly safe.

Generally, in this report the illustration of the general network architecture of Afghanistan, general connection links with international and regional countries network backbone, data transmission, network topology and cyber security issues presented. More specifically the aim of this report is to concentrate on current and future cybersecurity issues, such as: analyzing the risks caused by cyber-attacks in cyberspace and mitigate the risk of attacks that target the credential information or critical systems. In addition, further this report concerned about a predefined scenario, and a model including simulation of typical cyber threats that may target current and future parts of the Afghani developed cyberspace. While in first chapter looked forward to find some important academic aspects for giving the readers more reliability and making contains of this report understandable from academic perspectives which a short review of academic related works in consideration to the subjected issues have brought in chapter one of this thesis. In the second chapter of this research-based thesis, the histories of cyber-attacks on critical information systems including public, health, aviation, energy and even communication sectors will be reviewed. As well as, previous research results will be assessed to combine with the scope of this project in this chapter. The second chapter is focuses on different aspects of security challenges and risks on current and likelihood on future cyberspace, along with a brief review of network fundamental infrastructures, security strategies and procedures in cyberspace also presented in this chapter.

Most importantly, the main aim of this report is to analyze and simulate Afghanistan's current and future cyber threats, which are presented in the third chapter. Also in this chapter, the particular cyber challenges and threat solutions have also shown by a predefined scenario of cyber warfare, in terms of cyberattacks and cyber warriors (hackers). Based on this scenario modeling and simulation of cyber-attacks will be covered in some part of this chapter. Additionally, in this chapter, general analysis of cyber threats proposed solutions and future plans on cyberspace including types of cyber-attacks, future security challenges and a short review of network infrastructures have also presented.

Finally, the conclusion of all the analyzed information combined with information from the predetermined scenario will be contained in chapter four, along with all the project references. Moreover, I have also brought the appendices to the end of this chapter for illustration of issues which are not explained during the discussion.

## 1.1. Literature Review

Since the fall of Taliban regime in 2001, many governmental sectors allocate the annually huge amount of budgets for providing secure virtual connection systems and reliable internet, but still, there is a serious concern about the cybersecurity and cyber challenges. Basically, Information Technology Research Center (ITRC), being supported by

Afghanistan National Security Council and Cyber Research Center of ministry of telecommunication financed by government of Afghanistan, and world bank are the organizations who involve regarding the current cybersecurity, cyber threats and moving forward to establish reliable strong e-governments to ensure the efficiency and transparency in all social and governmental systems for keeping data privacy. For instance, in 2014 the (MCIT) published a paper by the name of National Cyber Security Strategy of Afghanistan (NCSA), vision, mission includes protections of ICT and secure cyberspace in Afghanistan, information and data security and network security have evaluated in this paper, however cyber capabilities of Afghanistan, definition of security framework are also the other major consideration of this effort. In addition, monitoring, troubleshooting of network infrastructure and analyze of network capacity in case of traffics and strategies of future cyber capabilities measurements are also the plenty common concern of this paper. Moreover, MCIT has started to publish journals and articles concern about cybersecurity and cyber capabilities of governmental organizations. As well as the MCIT started training cyber professional teams like Cyber Emergency Response Team (CERT) which founded in 2009, aimed at security assurance and cyber challenges.

The paper: Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation which has presented by Doddapaneni. Krishna Chaitanya, Ghosh. Arindam, at Middlesex University, the Burroughs, Hendon, London. NW44BT. Consequently, as we understand the Denial-of-Service (DoS) attacks are recognized as one of the serious threats due to the resources constrained property in Wireless Sensor Networks WSN. Based on it, they evaluated the WSN and impact of the Denial Of Service DOS impact on such sensor networks by presenting of  Zigbee model provided in OPNET, further,  in this model Numerical results, discussions and comparisons are provided for various simulation scenarios. Moreover, in this paper, a survey of attacks on WSN, discuss the various DoS attacks, and the impact of DoS on the performance of the system has presented. The simulation results show that the impact of DoS attacks on the performance of WSN can be more severe.

NATIONAL STRATEGY FOR CYBERSPACE SECURITY INDIA written by S R. R. Aiyengar, in this paper he concerns about cyber-security and cybercrimes includes threats scenario and assessment of vulnerabilities, cyber-attacks on critical infrastructure and national strategy to secure Indian cyberspace, cyber defense strategies and threats to the national security. Additionally, he has attempted to cover the cyber-threats characteristics and foreign threats like Chinese and Pakistani threats to India cyberspace as well.

In IEEE 18th international conference on parallel and distributed systems Jinyu Wu, Lihua Yin and  Yunchuan Guo presented the risk management of cyber-attacks by name of CYBER ATTACKS PREDICTION MODEL BASED ON BAYESIAN NETWORK. In this article, a model of cyber-attack and cyber-attacks risk management in performing evaluations of network security has been developed. The authors presented a graphical and prediction model of cyber-attacks based on Bayesian network (BN) by considering to value of assets in the network, different usage status of the network and a brief overview of cyber-attack events on network infrastructure.

In terms of cyber-security, analysis of past and present cybersecurity has presented by Jason R. C. Nurse Sadie Creese, Michael Goldsmith & Koen Lamberts under the title of GUIDELINES FOR USABLE CYBER SECURITY: PAST AND PRESENT in 2007, Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications conference.

The objective of this paper is recap some of the major developments in cybersecurity, usability and Human-Computer Interaction and Security HCIS domains, furthermore, he evaluates particularly three demission of cybersecurity issues same as, usability issues, review of up to date cybersecurity problems and evaluations techniques applied in day to day security issues. Simulating Cyber Operations: A Cyber Security Training Framework which has written by Bryan K. Fite in February 2014. In this paper, an innovative way to model Cyber & Operations by representing the core Simulation elements as Objects and describing their interactions via a Scenario Definition  Language (SDL), which dictates the rules governing object interactions has described. Furthermore, an approach used to create an intendment based cyber operation simulation and fundamental cyber object types have already illustrated by details in this paper.

Cybersecurity strategies for defense, ACST–Strategy-Cyber Security-001 Ed 001 / Rev 000/ 30-09-2014 published by defense strategies department of United States of America. The main concern of this document is to describe the Cyber Security Strategy for Defense (SSFD) in order to obtain a horizontal concept for the establishment of a cyber-capability for Defense. The cyber-attacks strategies, cyber-procedures and policies defense strategies and deterrence of cyber-attacks has been deeply has made cleared and annotated in this paper.

In consideration to the defense of cyber-attacks, Teodor Sommestad, Mathias Ekstedt and Pontus Johnson in proceedings of the 42nd Hawaii international conference on system sciences in 2009 presented a model-based applicable framework for analyzing the cyber-security and cyber security challenges by providing different architectural scenarios under the title of CYBER SECURITY RISKS ASSESSMENT WITH BAYESIAN DEFENSE GRAPHS AND ARCHITECTURAL MODELS. They used Bayesian statistics according to Extended Influence Diagrams (EID) to carry on cyber-attacks graphs and related countermeasures. They proved the attacks graphs structure that how such structure can be captured in an abstract model to support analysis based on architectural models and permits calculating the likelihood that cyber-attacks will proceed, succeed and the expected loss of these given the instantiated architectural scenario in this effort. However, they described the uncertainties framework of cyber-attacks with analysis, and as well as, in this paper, they have shown that the information system analysis framework dealing with uncertainty can be merged with architecture models by using a concept called abstract model.

Related to software privacy, a multi-dimension scenario include the descriptions of risks caused by software has been presented by Andrew J. Setterstrom, John M. Pearson and Hassan Aleassa in Northern Illinois University, Southern Illinois University Carbondale and the university of Yarmouk by the name of An Exploratory Examination of

Antecedents to Software Piracy: A Cross-Cultural Comparison. In this article, they concern about software privacy and problem on a global scale for software developers. The effort is determined to conduct a cross-cultural comparison of a model predicting the intent of individuals to pirate software using two subsamples: Jordan and the US. However, cultural efficiency roles on software privacy, individual behavior and hypothesis development of software explained by details.

Thamer Alhussain, Steve Drew, Osama Aljarraj presented an article under title of "BIOMETRIC AUTHENTICATION FOR MOBILE GOVERNMENT SECURITY". In this effort, they tried to outline the issue of broadcast signals on public airwaves and the process of the grounded theory application to information system security research, to develop a substantive theory for the successful implementation of biometric authentication in m-government security. However, they explained the common issues such as Personal Authentication Number PIN approach of biometric authentication systems currently in use for mobile government. A model of authentication process and security has presented in this paper by involving a trusted third party authenticator. Thus, the grounded theory approach fits the ambition of this study, which is to develop a theoretical framework for successful implementation of biometric authentication in m-government security. Moreover, the methodologies and data collections processes including the coding processes to achieve goals for m-government service also have elucidated in partial part of this effort.

TERRAIN AND BEHAVIOR MODELING FOR PROJECTING MULTISTAGECYBER ATTACKS described by Daniel Fava, Jared Holsopple, Shanchieh Jay and YangBrian Argauer. The concept of decomposing of the modeling of network and systems configuration from the extraction of cyber-attacks behavior, predictions and necessary of critical information of a computer and automatically loss of information a model called Virtual Cyber Terrain VCT has revealed in this effort. This model shows the accessibility of vulnerabilities at different network accessibility domains. However, in this direct graph model critical topological and systems configuration for the situation and threats assessment caused by cyber-attacks includes the traced pattern of cyber-attacks, exploit sequences and cyber-attacks capabilities in actions brought out in this paper. Moreover, the authors use traditional work prediction which has important overlap with the study of information compression a customized suffix tree for trends examine developed in connection to projecting multistage of cyber-attacks.

ADDRESSING CYBER SECURITY FOR THE OIL, GAS AND ENERGY SECTOR which has presented by Rafat Rob, Gareth W. McLorn, Tolga Tural, Abdullah Sheikh, Ahmad Hassan, in Saudi Aramco Dhahran, KSA. In this paper they have analyzed different dimension of cyber-threats, cyber-security, and security of Oil and Gas stations under the SCADA systems configuration. However, cyber-attacks risks on assessments especially the risks overcome by DoS and DDoS attacks, and cybersecurity measurements are their popular consideration in this effort. Moreover, this paper, properly explicated the vulnerabilities of SCADA systems and impressive critical structure of this system, when an attacks targeted such systems.

SECURITY RISK ANALYSIS AND EVALUATION has been presented by Fotios Harmantzis and Manu Malek in IEEE Communications Society 0-7803-8533-0/04 in 2004. In this paper, they have considered about the huge amount of internet users, governmental cooperate institutions risk and financial loss due to the breach of data in the United States of America. Focusing on key industries of governmental organizational services that are more vulnerable of cyber-attacks have analyzed by a quantitative estimation. Moreover, in this effort authors collected data based on different types of cyber-attacks and organized a view on network security, statics related to the significance of cyber-attacks, cyber-attacks impact, and formulation of the problems in a quantitative manner have genuinely overviewed by details.

PREDICTION OF MALICIOUS OBJECTS IN COMPUTER NETWORK AND DEFENSE which has written by Hemraj Saini, T. C. Panda, and Minaketan Panda, where presented in the international journal of network security and its application (IJNSA) November 2014. In this research, the authors analyzed different types of network topologies and envisage defense of sensitive information accompanied in computer networks and communication systems. However, in this effort, they have developed a model for prediction of malicious traffic from incoming traffic by using Black Scholes. Moreover, the authors used MATLAB for simulation of realistic values and models, as well as the framework for the treatment of predicated malicious traffic by details and security measurements are also have illustrated in deep consideration to network security.

ANALYSIS AND IMPACT OF CYBER THREATS ON ONLINE SOCIAL NETWORK which has been written by Seema D. Trivedi, Dhaivat Dave and R. Sridharan at Marwadi Education Foundation's Group of Institutions, India. In this paper they concerned about security risks and risks assessment of Online Social Network (OSN) which may cause harms in terms of social, economic or even at psychological levels. In this survey, analysis of some of the most popular cyber threats is mentioned along with their impact in Online Social Network OSN. However, in this article, they have described the different types and methods of cyber-attacks like Spammer and phishing, stalking and account compromise, locations leakage, and fake profile attacks. Additionally, in this effort, they analyzed and presented the classical and modern types of cyber-threats including cyber-attacks and cyber-exploits on the online social network.

Cyber-security policy which has been evaluated by Times of India in 2013 published, NATIONAL CYBER SECURITY POLICY 2013, this organization aims at building a secure and resilient cyberspace for citizens, businesses, and the government, communications and IT Minister. In this paper, the necessary of the policies and vulnerabilities of cyber-attacks from state and non-state actors, corporate and terrorists have characterized considerably. Moreover, the critical infrastructures such as; nuclear plants, air defense systems, power infrastructures and telecommunications system risks evaluated. As well as, the distinctive feature of the cybersecurity policy is to create a mechanism to obtain information regarding information and communications technology (ICT) infrastructure threats, the methods to respond to it and solve security challenges delineated and sketched in this paper. With reference to intelligent network architectures an article by name of

INTELLIGENT NETWORK INFRASTRUCTURE SYSTEMS ARCHITECTURE AND INTEGRATION, RISK MANAGEMENT AND VALIDATION prepared by Emmanuel Hooper, concerned about effective risks management and risks assessment of the intelligent detections and response strategies, processes and policies responsibility evaluation. He had has exemplified the technical and management processes, risks management implementation, and management of the project risks profile of intelligent detections in Virtual Private Network VPN, as well as, the design and response and even firewall systems response. Additionally, he also has epitomized the risks analysis, risks treatment, evaluation of risks management processes and risks monitoring of the intelligent detections and response strategies in last part of this article.

In terms of cyber insurance and IT instruments risks, Tridib Bandyopadhyay attempts to illustrate the cyber insurance in risks management of and has introduced an adoption of innovation framework grounded on the context based Technology Organization Environment TOE entitled ORGANIZATIONAL ADOPTION OF CYBER INSURANCE INSTRUMENTS IN IT SECURITY RISK MANAGEMENT in Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA March 23rd-24th, 2012. In this paper, the contextual factors that affect successful organizational adoption of cyber insurance and extend the TOE adoption of innovation theory in the area of IT security risks management have illuminated.

He also has explained that how the Cyber insurance can be an effective instrument to transfer cyber risks and complement the benefits of technological controls that guard the IS (information and network) assets in organizations. However, the main discussion of the authors in this paper is to provide an efficient model for organizational adoption of cyber insurance in information systems IS risks management and risks mitigation at structural and organizational adoption. Finally, there are many types of academic research, investigations and related works expressly discuss the general types of cyber threats, cyber events, and cyberspace. Based on above research and investigations hereby particularly, the lack of cyber-security simulation, cyber-threats modulation and cyber-attacks simulation in Afghanistan, I have been individually motivated, to concern regarding such lacks and start calligraphy of this effort as my final thesis. As an overview to the key performances and activities of CERT and ITRC teams of Afghanistan, apparently, they are busy with consulting and advisory services, cyber resource capacity developments, information security and technology standardization mostly by considering to expand the development projects, resource planning optimizations and electronic government audits.

Supplementary, these governmental organizations recently started publishing monthly journals regarding the cyber-security and cyber-events which are available on their official journals and websites, but the publication of these journals are concerned about the cyber-events, cyber-crisis, and public awareness. Since they started publishing academic journals, technical development efforts public awareness documents and cyber-security strategies technical journals. Unfortunately, I couldn’t find any paper to be concerned about analyzing of cybersecurity in Afghanistan, simulation and/or modulation of cyber-threats (cyber-attacks and cyber-exploit) in Afghanistan includes cyber challenges, threats vulnerabilities, and cyber-attacks risks, or even risks management. Definitely, the interrogation regarding above difficulties requires deeper investigations and essential explorations to be done as an intentional academic document, but, this reported has prepared in hope of starting points considering to intimated perplexities and bafflements of cyber threats that our current generation struggling with and the next generation would be faced bigger challenges.

# CHAPTER 2. INFORMATION SECURITY AND THREATS

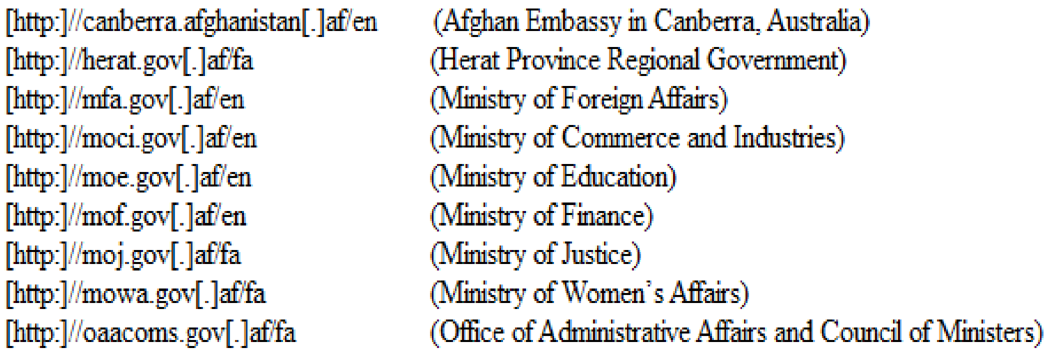
## 2.1. Brief Review of Cyber-Attack in Afghanistan

The temperament of this report preserved to outline some significant events of cyber-attacks which took place and affected directly on government official websites accompanied by the huge amount of data leakage and sensitive information. However cyber warfare attacks on military infrastructures, government's communication systems, and financial markets pose a rapidly growing, but little-understood threats to international security and could become a decisive weapon of choice in future conflicts between countries. Certainly, Afghanistan is not an exception or safe from these types of decisive weapon.

The systematic modeling and methods of cyber-attacks on critical information systems (CIS) with non-respect to virgin network communication of Afghanistan had has catastrophic destructions, largely due to lack of knowledge and contextual information including lack of experts such offensive attacks which countered as the major reason of opening the new season of threats on virtual communication systems. In this part, a brief review of the troublesome of unpleasant cyber-attacks is overviewed, since these attacks had happened on official websites, targeted governmental intelligence assessments and the huge amount of personal information of employees also had been stolen by hackers.

There is two main perspective that usually causes cyber-conflicts in Afghanistan, first: according to the geographical location of Afghanistan, this country confined from southeastern and northern sides by China, Pakistan, and Russia, as well, from western side by the Islamic Republic of Iran. As well as, this country also has an attractive strategic location slightly closed to Middle East countries, therefore predominantly battlefield of cyber wars consequences because of Afghanistan geographical location and it's close border to Middle East countries. Second: interior challenges and competitions are also might be the challengeable presumption, and key factors that immersed Afghanistan in the battle of digital wars.

Based on, Threat Connect Intelligence Research Team (TCIRT) reports [8], on 16 December 2014, group of Chinese hackers allegedly used a targeted cross-site- scripting (XSS) method attack on Content Delivery Network CDN (Refers to Appendices A.1. discussed CDN) being used in Afghanistan [9]. and the domains in which is shown in Figure 2.1. were targeted, and already possessed by ministries of education, Finance, Foreign affairs, Justice, Women affairs, Commerce and Industries, Regional government of Herat and foreign websites that receive contents from, in addition to internal conflicts this attack also continued outside of Afghanistan same as attack on CDN embassy of Afghanistan in Australia have been also affected from Chinese group of hackers attacks, ministry of communication and information technology MCIT of Afghanistan confirmed an announced that a group of Chinese injected a malicious script on mentioned governmental CDN domains.



| | |
|---|---|
| [http:]//canberra.afghanistan[.]af/en | (Afghan Embassy in Canberra, Australia) |
| [http:]//herat.gov[.]af/fa | (Herat Province Regional Government) |
| [http:]//mfa.gov[.]af/en | (Ministry of Foreign Affairs) |
| [http:]//moci.gov[.]af/en | (Ministry of Commerce and Industries) |
| [http:]//moe.gov[.]af/en | (Ministry of Education) |
| [http:]//mof.gov[.]af/en | (Ministry of Finance) |
| [http:]//moj.gov[.]af/fa | (Ministry of Justice) |
| [http:]//mowa.gov[.]af/fa | (Ministry of Women's Affairs) |
| [http:]//oaacoms.gov[.]af/fa | (Office of Administrative Affairs and Council of Ministers) |

Figure 2.1. List of official targeted domains

In coming next parts technically will discuss the circumstances of this kind of attacks by details in term of security and solution [10]. On the other hand, while the of fundamentalist radicals group like Al Qaeda spread all around the world, especially in

Afghanistan, Taliban influence contributed greatly Al Qaeda’s involvements to the past and current state of Afghanistan, thereupon on 5 March 2012 group of hackers had been supported by Al Qaeda, attacked on national security council of Afghanistan website, by taking control of the website, hackers then published the Osama bin Laden picture on national security council of Afghanistan website [11].

In addition to reporting, again earlier in 2016 group of hackers were supported by radicalisms party inside of Afghanistan attacked national security council of Afghanistan claimed for justice, specifically accused the Afghan governors to financially assistances of ISIS [12]. deliberate cyber-attacks and cyber wars in animus of Afghanistan official governments distributed websites domains and subdomains, but in fact, the intention of hackers who were supported by a country do not target only the governmental financial assets.

From another side, international troops or NATO participants work in Afghanistan after the American invasion in 2001, attack and taking control of communication systems by hacking, for instance, on 23 September 2016 the sentence "German military carried out first foreign cyber-attack in Afghan hostage op – report" makes an outline of the daily news. Where groups of German hackers tried to hack the GSM networks in Afghanistan to identify their abducted German Army Force’s location [13].

This offensive attack on GMS networks of Afghanistan was because of backtracking GSM's signals in peer to peer communications. The threat of attacks is not only concerned with governmental organizations alleged on small-medium business and social affiliation affairs as well [14]. Last recently, Taliban, ISIS, the Haqqani Network, and other violent extremists carrying out cyber-attacks on numerous governmental and nongovernmental websites. Generally, in such above attacks, attackers intent to steal intellectuals property, disable the network infrastructures, destroy the communication systems and enthusiastic of network infrastructure manipulations or taking control of systems. Thus, attackers deliberately attempt to overflow computers network and target servers with too much traffic to sustain operations, proceed until possessing the undertaken server's control [15].

## 2.2. Information Data Security and Security Challenges

In common concern to data privacy, the theft of data or information always existed, annually enormous and huge amount of data are stolen in different purposes in all around the world. But particularly after 17 years of modern technology and computer revolution in Afghanistan, nowadays internet and computer technology have brought an unprecedented stolen of data in cyberspace. Nevertheless, it is the time to concern about future cyber threats and cyber security accurately, to obtain a semi model of the secure cyber area on Afghanistan's current and future cyberspace. However, to make sense and the better understanding of security challenges, it has approbated, easily to comprehend data security from multilateral perspectives, specifically data security or data being collected, stored and analyzed inside of the virtual storages.

Before facing numerous challenges or certain problems in cyberspace we must have sagacious and essential knowledge of cyber and information security. Therefore a brief overview of data and information security is comprehensibly covered in this part [16]. In term of data transformation through different network protocols, similar to, peer to peer network connection, hardware-based (Packet switching and Circuit switching) and software-based or visualization protocols. Any types of information which are stored, collected and analyzed inside of the virtual storage including transactions of data over the network and iteration of data berthed on cyberspaces could be at risks. In general, security is the processes of protecting and preventing of information from stolen and damage on cyberspaces and virtual storage, where cyber-security is the art of defense and avert of information from theft and aggravation of information damage on cyberspace. In contrast, to earn a secure space, first of all nations need particular definitions and strategies related to cyber challenges on cyberspaces because the future economy and national security directly depends on information technologies and communication systems. Especially, while the new banking and communication systems being established over the network or started servicing online. All the financial chains and economical markets would be stopped and cease completely functioning in terms of insecure data transmission [17]. The basic terminology of information or data security (Confidentiality, Integrity, and Availability) are the significant components and principles of information systems, servicing either online, functioning under local area network or even stored on cloud computing systems. However, from the other side, authentication and non-reputation of data could also be calculated as the main concepts of information or data security. In order to, provide a secure communication above mention key factors must be preserved [18].

### 2.2.1. Confidentiality of data

The valuable assets of an organization is confidentiality of data, in term of information security, any types of personal or data must be kept on secret or be confidential and only be read by right authorized and must be prevented from reaching wrong persons, otherwise, information is not confidential if proliferated or being disclosure. Leakage of personal information, intellectual properties, the proliferation of individual information and secret information regarding business’s plans and strategies are the prevalent risks [19]. Additionally, information which reveals the authority of a nation in a realm and relating to any action taken or to is taken in connection to a national security and governmental procedures and policies all includes confidentiality of information.

Particularly, over the network and communication systems, bilateral confirmation from both pre-defined transmitter and receiver sides refer to confidentiality of data. Technically data confidentiality defined as discloser of received, viewed visually, electronically or orally which includes bunch of techniques for saving the privacy such as; without having and instructions, technical information, business and marketing strategies, databases, qualifications, conceptions and constitutions, tooling, prototypes, sketches, models, drawings, specifications, procurement requirements, engineering information, samples, computer software (source and object codes), forecasts, identity of or details about actual or potential customers or projects, techniques, inventions, discoveries [20].

### 2.2.2. Integrity of data

Integrity is the case to be concerned with sustain the steadfastness, accuracy, and dependability of data over its flawless life cycle. Often integrity of data refers to prevention of unauthorized people from reading and writing data over networks, where such data been stored over virtual space similar to, the cloud or collected on data centers. In both cases, data must not be changed, modified and altered by unauthorized users [21]. On the other word, data integrity is important in both hierarchical and relational database models, in the relational databases, technically data integrity includes entity integrity, referential integrity, and domain integrity. Additionally, data integrity in database systems ensures that the data is stored and collected in database and table fields can be traced and connected to another data. According to data security, a well-defined data integrity increases the system’s stabilities. Sometimes the non-human events such as electromagnetic pulse or sever crash cause the non-integrity of data. In such case, checksum techniques and data cryptography partially and full encryption must be considered accurately for verification of integrity [22].

### 2.2.3. Availability of data

The information and communication systems which service the users, anywhere and anytime must be available when it is being called and accessed by someone. Calculates and processes of the data, collecting information, protecting the security controls and using the transformation channels for access must be performing properly. Availability of the information systems concerns, the availability of organizational public assets in all the times, and averting of the service interruption in consequence of electric pulses, systems upgrades, and hardware failures are totally the key parameters to make data available. In addition, the availability of information systems also involves averting Denial of Service DoS as assaults as well, for instance, while the flood of messages or requests ramp out and cease the source systems. In such a situation, primarily, the occurrence imposes the system turned off or shout down [23]. However significant amount of information requires particular attention and monitoring, specifically, when the improper handle of the information causes financial punishments, identities were stolen, financial losses, and invasion of data privacy or unauthorized access by a person or groups in case of availability of information systems [24].

### 2.2.4. Non-repudiation and authentication of data

Non-reputation and authentication of data are also the important key factors of information systems which must be in proper functioning, means while the huge amount of requests target to overload systems, primary information systems must be able to authenticate the demands, otherwise, the flood of requests cause the system failure or non-functioning. Data and information security critical points have been illustrated in general up to now, assembling of security challenges emerge if any of mentioned concept would not be functioned correctly by information and communication systems. On the other word, protecting information and data security is the end goals of information and communication systems. In each steps, the information security measures correctly for servicing. When a hacker or hijacker attempts to take controls of the systems, firstly, targets one of the above concepts; and regularly cyber challenges cause intrusion of servers, web servers, web clients, operating systems, networks and even database management systems.

## 2.3. Afghanistan’s Current Network Infrastructures

In term of data and information security, network infrastructures have significant role for controlling the security measurements and monitoring of the data transmission, basically data and information security directly related to network configurations and distributed networks structures. A clear predefined network architectures help maintainers to evaluate manifestly data exchange and information transactions overall. Afghanistan has been dealing with cyber challenges and cyber security challenges approximately in last two decades especially since 2001. For instance, many private, public organizations and social media networks dealing within insecure connection over all the country, in fact, complexity of network structure and acrostic network fundamentals have made big problems, a large amount of personal identities being theft because of complex and unknown definition of network infrastructures. The majority of the private organizations includes telecommunication companies and internet service providers (ISPs) are connected through satellites which the transmissions of information is controlled by themselves or consequently by private sectors.

On another hand, the increase of internet users, incredible expand of computer network infrastructures especially, the networks that are directly or indirectly connected to new projects of fiber optic have made this country to the battle of hallucinations network architectures. As we know, the nature of creation of the first generation of computer network it had been developed for data transaction between two users. During the time that computer networks had been introduced, the security and security challenges was not placed in human minds, same as the first generation of computer networks.

Currently Afghanistan government just concentrates on developments and expands of networks and increase of internet, telecom and internet services, except on some rare situations, and no one cares about data and cyber-security or even cyber-security challenges. These abnormalities will make the serious problems and catastrophic vulnerabilities in the future of cyber-security procedures and cyberspace from multidimensional perspectives of cybersecurity.

Comparatively, the satellite communications and transaction security, air interfaces or wireless broadband security and physical interface or cabling establishment’s security can be the clear example of current security circumstances. However, from the other side, according to the last investigation of ministry of telecommunications, over 65 percent of internet users are connected through.

a. Telecommunications Company and GSM services like 3G, newly 4G and in the future the 5 and upper generation will also be introduced to the markets. The bulk of the internet users are connected through telecommunication internet services.
b. Private internet service provider (ISP) companies, the fundamental and backbone of both telecommunications and private ISPs are currently connected to satellites, for providing internet services in Afghanistan.
c. The remaining part is serviced by the governmental new project of fiber optic which is expanding and developing in many provinces and traditional communication systems.

As a review of the general network infrastructure of Afghanistan, the backbone of internet and communication systems dependently linked and have the direct connection to neighbor countries communication backbone.

As an example, the fiber optic project which already started distribution over Afghanistan either from the northern and southern side or western side connected to international backbone networks via Iran, Russia, and other Asian countries like Tajikistan, Uzbekistan and especially Pakistan. Based on MCIT administration reports, basically the ministry of information and technology attempts to expand the coverage area of internet across to country, in moment of the time this governmental organization concerns about three vital factors of communication systems.

The drop of price through fiber optic, increase of the consumers though copper Cabling networks and expands of Optical Fiber Networks. The internet users in Afghanistan currently are serviced via Microwave Networks, WiMAX Networks and also through GSM network backbones, Digital Phones, Dial-up, and DSL technology that counts the significant service providers for providing internet services and communication facilities, but there are two main elements which the governmental organizations do not concern about them. First, in terms of security and safety of data, the MCIT does not publish a particular standard definition for long or short terms in the future in public.

Second, in the manner of internet and network connection, fiber optic has connected Afghanistan's internal networks to international networks backbone. Later in this part, the international connectivity links has explained that totally the network backbones and infrastructures are dependently connected across the globe through the neighbor countries network infrastructures. Such as: PTCL Pakistan and TIC in Iran.

From the Northern side Afghanistan's network backbone is connected through Tajikistan, Uzbekistan and Turkmenistan network infrastructure to international network backbone, means that the nature of Afghan Optical Fiber Network AOFN is not an independent network infrastructure provider in general.

The fiber optic is the largest project on hands of MCIT, implementation of this project deserves the biggest and significant budget of MCIT annually, and this project makes the main building block of network backbone that connects Afghanistan to World Wide Web/global physical network infrastructures.

Here are the main connectivity links of this large project has divided into (External and Internal infrastructure) and analyzed the connection links from multi-connectivity parts, at the end of this part the risks and future challenges of the AOFN have also outlined and analyzed.

### 2.3.1. External connectivity links of AOFN

As earlier in this report the architecture and orderly of the network elements outlined, in order to help security maintainers for monitoring and pinging the network traffics and even controlling of the security events and overloads over all networks and transaction gateways. In a short general overview, modern networks designed based on the broadcast logic and broadcast logic of local networks is designed based on a special order for easily transportation, which is also applies the same logic in source and destination. Basically, orderly nodes only accept the traffics which come from another orderly node, and traffic will also be seen by multiple orderly nodes. Nevertheless, network architecture plays an important role for providing reliable connections, communications and interconnections systems in data communication. From another side, unorderly and complexity of network elements like switches, hubs, routers even cabling cause dangerous results with high probabilities of risks, damages and data destructions. While the heavy amount of risks are because of the unorderly design of network architecture, confidentiality of data and information depends on upon settlement of network elements.

As concentrate to general network infrastructure of Afghanistan, this country has connected to all of its neighbor countries via terrestrial fiber optic connections, with some exception of China, however this country also has dual fiber links to Turkmenistan and Pakistan same as linked to other neighbor countries (Iran, Tajikistan, and Uzbekistan) through hyper-connected links of fiber optic. In connectivity manner of the telecom and infrastructure correspondents for trans-border connectivity to Pakistan Telecommunication Company Limited PTCL (refer to Appendices A.2.). In this regard, Pakistan operating two links across the countries' border, between Torkham, Afghanistan and Torkham, Pakistan at the north and the southern border crossing between Spin Boldak in Kandahar Province, Afghanistan and Chaman, in Pakistan. However, this connection links have connected Afghanistan to Telecom Infrastructure Company TIC (refer to Appendices A.3.) in Iran operating a link between Islam Qala, Afghanistan (Borderland line of Afghanistan with Iran located at West of Herat) and Dogharoun, in Iran (Borderland line of Iran with Afghanistan located at East of Taybad) that are supported by hyper connectivity fiber optic links [25].

Additionally, to trans-border connectivity of Afghanistan from northern side, a single network link connected through Sher-Khan border (Afghanistan) across the border with

Panji Poyon (Tajikistan) operate by Afghan Telecom and Tajiktelecom. Although, the fiber optic hyper link has connected to Turkmenistan across the border via Afghan Telecom and Turkmentelecom operate two diverse links across the border of these countries, where western link has connected Serhetabat, Mary Province, Turkmenistan and Torghundi, Herat Province, Afghanistan. Moreover, an eastern hyper fiber optic link connects Lebap, Turkmenistan and Aquinas, Afghanistan. As well as, the hyper fiber connectivity links between Afghanistan and Uzbekistan, operate by a hyper fiber links over the Amu Dharia River via a one-kilometer bridge between Hairatan, Afghanistan and Akhunbabaev, in Uzbekistan. Finally, regarding the connections links between Afghanistan and China, currently there are no transport links between these two countries at the time of writing this thesis, but in the future there will a hyper connection fiber links between these two countries; the only future possibility for a transport connection would be though Wakhjir Pass in the Pamir Mountains. On the Afghanistan’s side, there are no immediate plans for telecommunications infrastructure east of Faizabad or Panjshir to connected southeastern sides of Afghanistan with Chinese telecommunication and communication systems [26].

In addition to hyper fiber optical links between China and Afghanistan, it is not that much hard for China to create a fiber optic link over the border between Afghanistan and China. But for Afghanistan, it can be a serious problem in the current situation due to the existence of mountains in Badakhshan Afghanistan which are prevented the implementation of optical fiber link, and also, it needs the necessary funding and budgets. These might be the reasons which the government has not carefully reviewed this connection link yet, but, totally this agreement will be signed and implemented by both sides in the near future.

### 2.3.2. Internal structural design of (AOFN)

Consequently, according to external network infrastructure connectivity links of Afghanistan with the neighbor countries, the major network infrastructures of this country is connected to Iran and Pakistan communication backbone. Mostly, the Afghan Fiber Optical Network AOFN domestically connects main internal connectivity links inside of Afghanistan. The implementation of his project consists of a backbone built primarily, along the country's circular Highway also known as the ring road because from one side, as already described earlier the AOFN connects Afghanistan networks across the globe through trans-border connectivity links and also it connects the overall internal connectivity links of network backbone inside of Afghanistan.

From another side, the internal structure of this project runs as a cyclic network cabling that connects all corner Afghanistan's provinces by providing domestic wireless connections through microwaves, physical cable connectivity or fiber optic and telecom facilities Figure 2.. and Figure 2.2. show the general structure and on Figure 2.. has shown the technical structure and connectivity links of this project.

According to the plans and description of this project that has newly published by the ministry of communication and information technology MCIT of Afghanistan, United Nations Economic and Social Commission for Asia and Pacific (ESCAP) about the new project of fiber optic. In fact, this project makes the main building black of Afghanistan current domestic network connectivity backbone. Based on geographical domestic provinces of Afghanistan the map of this project (AOFN) has segmented into to three below parts. Moreover, this project has planned to be contacted over three phases of implementation covering the internal or domestic network infrastructure over all the country.

a. The core segment: More than the dozen central provinces of Afghanistan have covered by this part of Afghan Optical Fiber Network AOFN.
b. Eastern segments: Along the ring road start from Kandahar and finishes to Faryab covers the provinces of Kandahar, Zabul, Ghazni, Maidan Wardak, Kabul, Parwan, Baghlan, Kunduz, Samangan, Mazar-i-Sharif, Jawzjan, and Faryab includes the province's central cities and countryside. Moreover, the extension of this segment

of AOFN connects the provinces such as; Nangarhar, Laghman, Logar, and Paktika, Additionally, the provinces of Bamyan, Parwan, Ghor, and Daykundi are also expected to be covered by expanding of this segment of the project.

c. Western segments: The provinces that connected by this segment of AOFN are Herat and Farah along the ring road in the west of Afghanistan.

In addition, to technical specification of Afghan Optical Fiber Network the core ring network comprises 18 fiber pairs in a 40 millimeter, high-density polyethylene duct operating at an initial capacity of STM-16 (2.5 Gbps), upgradeable to STM-64 (10 Gbps) [25].

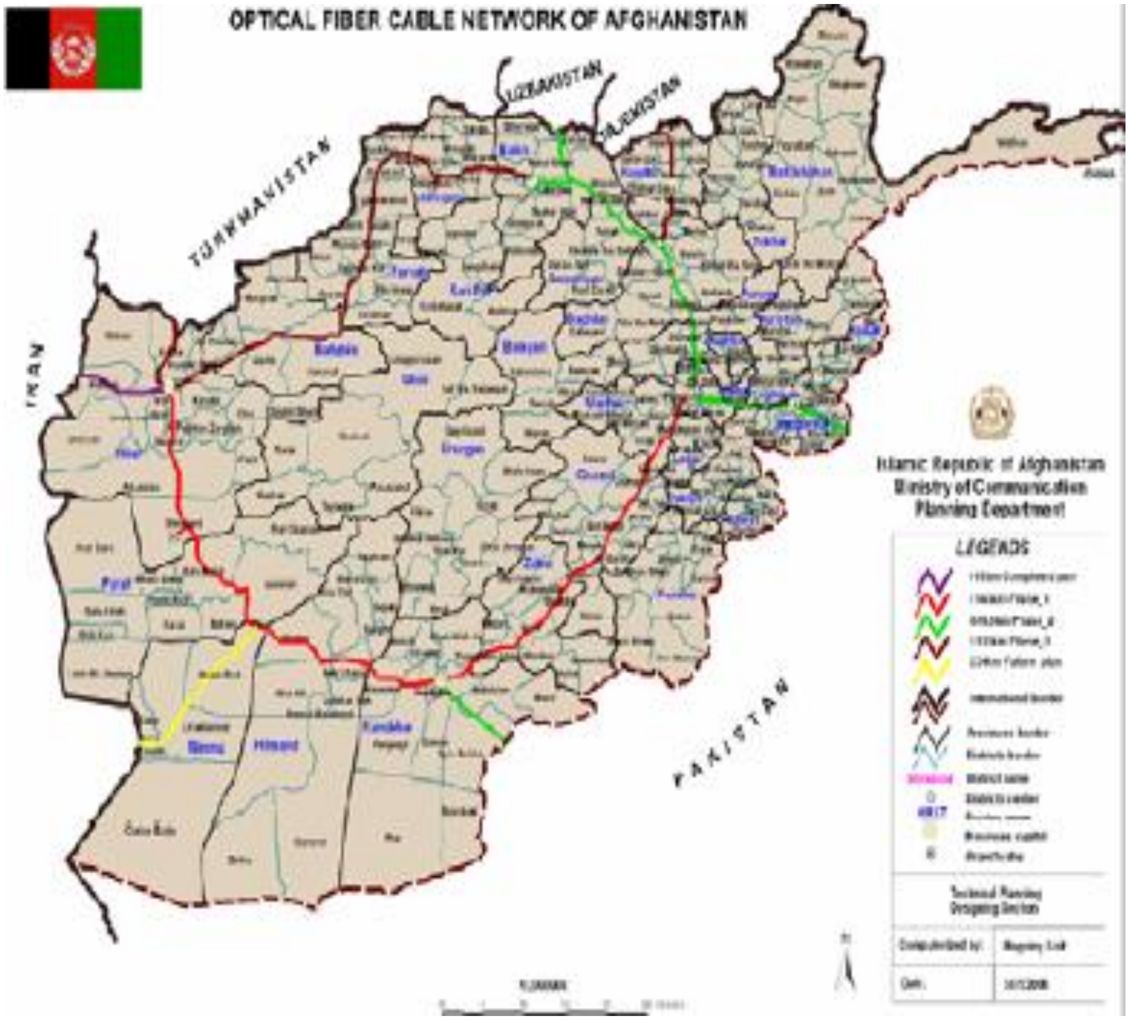

OPTICAL FIBER CABLE NETWORK OF AFGHANISTAN
UZBAKISTAN
TAJIKISTAN
TURKMANISTAN
IRAN
PAKISTAN
Islamic Republic of Afghanistan
Ministry of Communication
Planning Department
LEGENDS

Figure 2.2. AOFN cyclic general structure (MICT, 2008)

Moreover, equipment installed to connect South-Eastern Provincial OSN 3500 with STM-16 (2.5Gbps) capacity and all other Provincial Capital Cities is S390 with STM-64 (10Gbps) capacity. However, there are two Chinese companies (ZTE and Huawei) who are working under the agreement of Ministry of Communication and Information technology MCIT of Afghanistan for the technical implementation of this project include the upgradeable contribution in future of technical maintaining of Afghan Optical Fiber Network project [27].

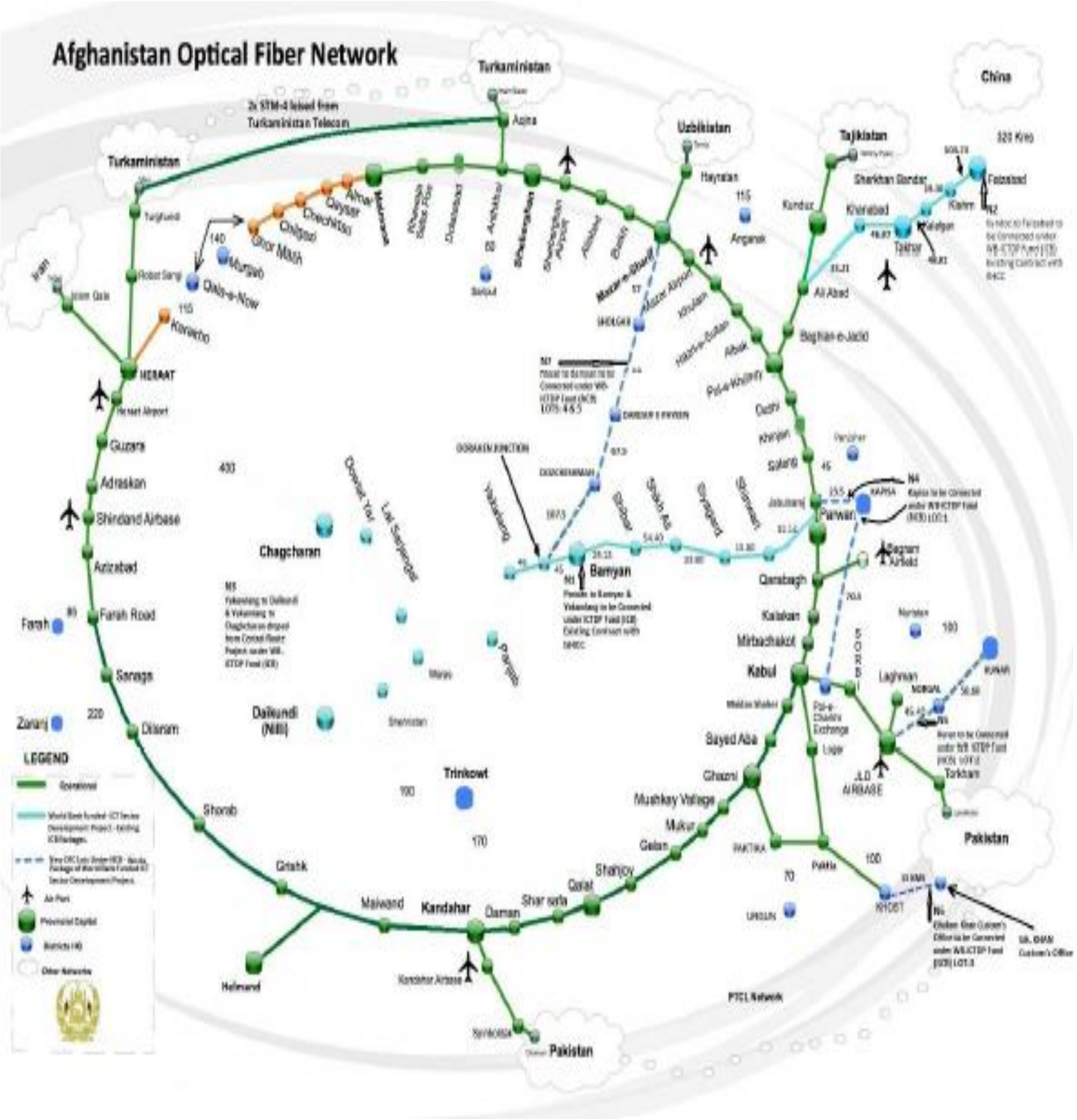


Figure 2.3. AOFN cyclic technical structure (MICT, 2010)

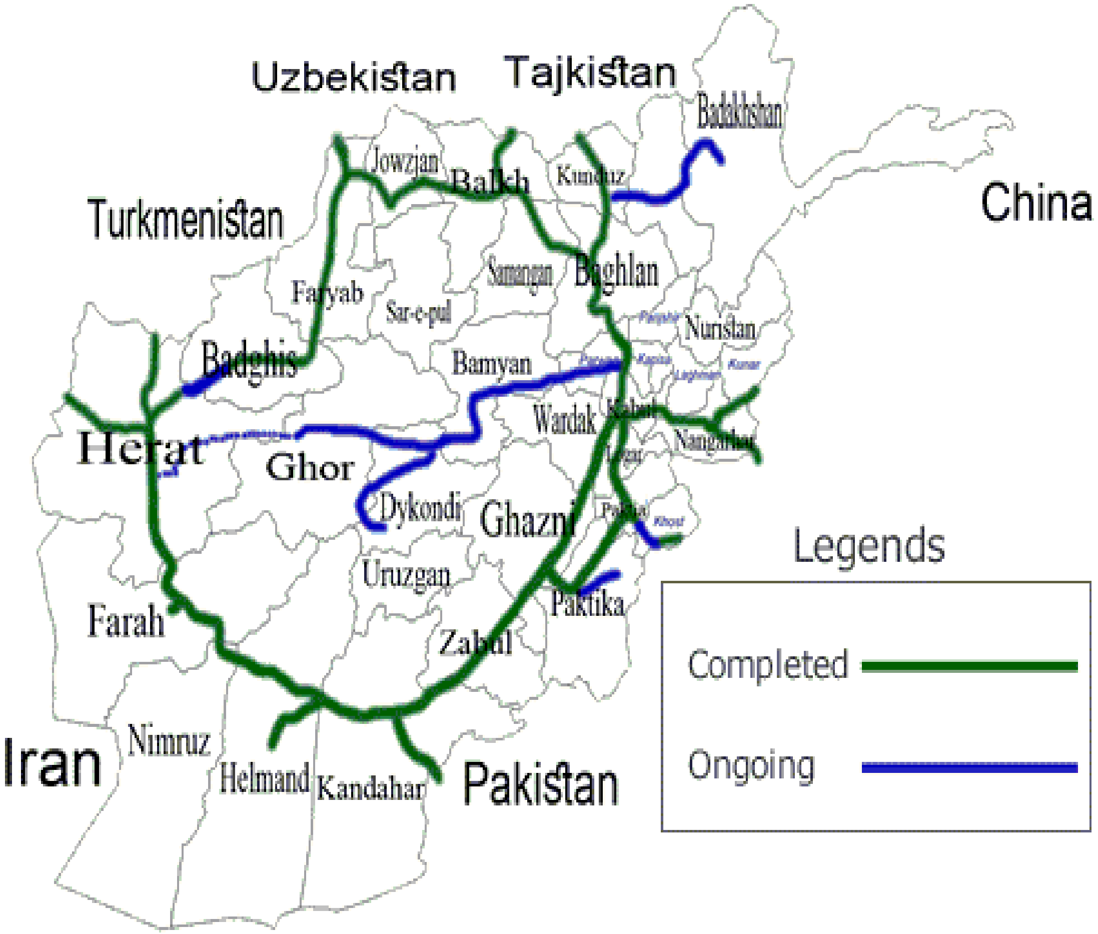


Figure 2.2. AOFN cyclic general structure (MICT, 2010)

### 2.3.3. Security risks of (AOFN)

The sentence: “The Optical Fiber Network is governed by the Open Access Policy of the Afghanistan Ministry of Communications and Information Technology, which was enacted in 2012 in order to make sure retail telecommunications providers each have access to technologies such as high-speed fiber, enabling all providers to serve Afghans at the lowest possible price and still turn a reasonable profit. The policy sets forth core principles of non-discrimination, transparency, and cost-based pricing." Has been taken from AOFN instruction description and Open Access Policy documents are clear the current circumstance of this project. There are two main factors that are not cleared in these papers which are current and future risks of AOFN and the both side security challenges. On one side, according to dependency of network infrastructure as we reviewed previously in this report, the dependency of Afghanistan's network backbone the connection of links of this project depends on two significant neighbor countries network-backbones (Iran and Pakistan). Consequently Afghanistan cannot be as an autonomous member in terms of packet transactions and accelerate of network capacities for providing high speed internet without cooperation of these two neighbors.

Since Afghanistan's network capacities, packet transactions and even network security relatively depend on these two neighbor countries network-backbone meaning that they can easily control the data transactions over the network. If so, this can cause big challenges in future cyberspace in terms of confidentiality, integrity, and availability of data on current and future of Afghanistan's cybersecurity. Additionally, data damages, the high pressure of electric voltage to Afghanistan network systems causing network alteration and data damage, network infrastructure devastations and disabling of network connections are some of the common suspected future risks of Afghan Optical Fiber Network (AOFN) due to its dependency. On another side, the physical security issues and internal conflicts has brought big challenges across the implementation of Afghan Optical Fiber Network AOFN, as a main member of Afghan National Development Strategy (ANDS) of communications MCIT is responsible for accelerating and developing the network capabilities especially by expansion of the big technological projects and identified as a strategic vision for information and communications sector of Afghanistan, this ministry is a realistic strategic implementer of AOFN for providing affordable information and communications services in all around the country.

But unfortunately, the internal conflicts and issues like irresponsible militant groups same as Taliban and ISIS including official corruptions prevent and cut off the millstones of AOFN from implementation. Alongside, since the AOFN project has started, many physical security challenges reported, in addition to physical security issue, the major challenges that prevent the achievements of telecommunications goals and spreads of

AOFN are national security, administration and financial bureaucracy, late approval of the annual budgets and development projects. As well as, weak implementation and lack of technical capacity, which are the major concerns. Therefore, a strong capacity building effort including technician's safety is required to upgrade and intensify the capability of networks establishment infrastructures on lands at all around the country and grantee the safety of personnel, the governmental technicians, stockholders and engineers.

## 2.4. Current Cyber Procedures and Policies

As it is clear that the assessment of threat and vulnerability (especially on cyberspace) is one of the main concerns of the security authorities in a country, either the assessments would deserve to be implemented technically or even needs assistance to be done strategically.

Infinitely, the risks assessment issue is an important challenge because in many cases, it can lead to reduce the risks significantly or reduce the consequence of the risks and vulnerabilities in the lower rate.  Literally, the illustration of the threats, risks, and vulnerabilities concerning the national network infrastructure, and it is a framework for analyzing, managing and figuring out the risks conducted the occurring accidentally or deliberately cyber-attacks against our critical, none critical infrastructures and national security.

Accordingly, our main goals in here are to assess the current cyber-security level of Afghanistan which are defined by governmental organizations in a particular framework and the evaluation of the security associated with cyber-attacks against our current infrastructure, expressly, our future critical and even non critical network fundamentals. It is also clear that access to a lots of information especially, information regarding the security plans and important information in regard to the cyber-strategies of organizations is impossible. Because of, both governmental and private organizations never make and let such information available on public, but here, the issues of current network infrastructure, information security challenges and future cyber threats in concerning to our behave public documents and information analyzed and evaluated based on the public available data and information.

When discussing digital security or computer codes means that the future public, private companies, and nations rely on virtual communication systems called cyberspace and from every side, financial assets to the movement of national industries and military forces, data security is one of the considerable phenomena on cyberspaces. Malicious actors are able to benefit from the internet by using simple tools to steal data and intellectual property for their own political and economic goals which such destructive cyber-attacks and data loss present a significant risk at political, economic, business infrastructure and psychological effect on nations. Earlier in part 2.1. we discuss significant events of cyber-attacks on network infrastructures, this destructive occurrence is clearly alarming that Afghanistan goes into a battlefield of cyber war from each side close to neighbor countries includes Russian, China and even international troops. The cyber-attacks would be continued in short and long term in the future, especially while the economical projects such as; TUTAP, TAPI and CASA-1000 being implemented. The implementation of these projects have an important financial benefits for all of Afghanistan's neighbor countries, China and Russia, as well as, have vital role in future of Afghanistan economic and industrial facilities.

The implementation of these projects is unacceptable for our neighboring countries in two reasonable argues. First, completion of these projects improve the basic infrastructures inside of Afghanistan and lead this country to self-sufficiency. Therefore, countries that have been engaging in various competitions in Afghanistan for years, certainly, they do not want Afghanistan to become a self-sufficient and independent society. Second, the implementation of these projects will provide the necessary financial benefits for the countries involved in the conflicts in Afghanistan. Like, the big challenges about TUTAP in Afghanistan, which several people were martyred and then thousands political conflicts also raised. In such a case, the cyber security of these projects cannot be protected from cyber-attacks in the future, and the countries involved in competing on these projects will not refrain from any types of cyber-attacks.

Hence, security of supplemented power grids and critical systems must be accomplished. Otherwise, damages of such system have disastrous effects. Again for instance, TUTAP is a by-contractual project that provides energy to current and future of Afghanistan industries and this project is one of the famous compiling economical project being supported by Asian bank. However, TUTAP transmits electricity from Central Asian countries to South Asia bypassing Afghan lands.

In perspective to cybersecurity, on one word, such projects, digital CASA (Refer to Appendices B.2. for more details) and CASA-1000, TUTAP and similar economical projects are partial part of Supervisory Control and Data Acquisition (SCADA) system. The future of these projects must be isolated and networked under a particular architecture of networks. Safety and security, of SCADA and Distributed Control System (DCS), would be one of the main consideration of Afghanistan's government.

On the other word, the safety and security of these economical projects directly depend on safety and security of the public internet. Due to, in concern to cybersecurity theories, such critical networked systems (SCADA and DCS include other critical fundamentals) infrastructure are often easy to be accessed from public internet. However, for commercializing and commoditizing of such big commercial and economic projects that Afghan government has on hand deserve and might be reasonable to be connected to at least public networked infrastructure, in order to enhance the accessibility and quality of services. Thus, it also might be considered that the cyber-threats and attacks are unavoidable because of multiple reasons and argues. In case of cyber-attacks on such systems, and fundamentals of industrial, military, economy and power infrastructure systems. As we also understand that the nature of threats and vulnerabilities avoid servicing or stops performing of the systems. So first of all the security and safety of these systems must be verified by competent and transparent processes. Whilst the distribution and supplementation of such kinds of systems are frequently developing and increasing in modern technology societies, and as a powerful networks backbone in Afghanistan.

Commonly, SCADA and DCS are configured under Internet Protocol (IP) and transmission control protocol (TCP) or over Ethernet, which cyber-attacks on such systems leads serious consequence by pushing down the physical infrastructure components into abnormal conditions. Particularly, physical infrastructure is a usual sensitive point that cyber attackers tents on it [28]. Due to current competition on economic projects in Afghanistan, cyberattacks enumerate as a strong instrument to make serious problem in future of Afghanistan's regional and international relations. From the other side, the involvement of NATO, China, Russia and neighbor countries in current political and economic situation are also the major reasons for future cyber challenges.

Conclusively, the government organizations includes ministry of communications and information technology by collaborating of the ministry of justices that is in charge of cyber-crimes prevention laws and prosecutions, implement the cyber procedures and policies in both cyber-attacks preventions and prosecutions. In fact, as already pointed out some key performance of MCIT in case of offensive cyber-attacks, over the network, this governmental organization also plays an important role in cyber-attacks prevention. Based on, monthly and annual journals that the MCIT and ministry of justices publish, in common, there are two types of procedures and policies which are illustrated in two separate sections as below by details.

### 2.4.1. Preventions procedures and policies

As previously, outlined the significant risks of the different network settlements and infrastructures. Generally, in this section, concerned about the cyber-attacks preventions, the definition of cyber-attacks preventions and efficiency of cyber-attacks prevention. Spastically, the main and key responsibility of MCIT of Afghanistan especially, the security directorate of MCIT which directly involve cyber-attacks prevention is the technical and none-technical preventions security policies, where outlined in general as below.

1. Network security and definition of specific rules and policies in case of offensive cyber-attacks over the public and private network facilities, physical infrastructure implementation procedures, cyber-security policies implementation over all the networks, and risk assessments cause by an offensive cyber-attacks.
2. Network topologies strategy and implementation, aversion of offensive cyber-attacks over the public and private sectors. In terms of awareness, this governmental organization is also responsible to provide training for employees and robust technical prevention controls. How and with what kinds of technologies they implement, is a secret strategy that is not accessible to the public.
3. As well as this governmental organization also has a directorate by the name of cyber-security directory who performs the activities to save the business trade secrets, personal information theft, coordinate security strategies, public awareness in term of cyber-attacks and implements necessary policies against any kinds of cyber-threats and cyber-attacks. Totally, this security directorate is in charge of measurements of critical information infrastructures in the country, in order to make sure that the confidentiality, integrity, and availability of information systems within the government are in place.

In fact, according to cyberspaces safety, the prevention is a standard method that denies any types of cyber-attacks over the network infrastructures, whatever, such networks are configured under LAN, WAN, and internet or has been settle up under air interface network same as, GSM communications, wireless broadband network and being served by satellite broadcast services.

The cyber-attack has not only effects over the physical network infrastructure also the injection of malicious scripts and codes have multiple choices and flexible possibilities to be run all over the networks [29]. According to data loss preventions policies (DLP), the prevention of a cyber-attack is one the noteworthy and momentous performances of the organizations, if an organization manage and arrange a well implacable prevention policy against cyber-attacks.

Rarely, such organization effects from malicious attacks over its network because of malicious scripts and codes being filtered based on predefined data leakage and damages prevention policies. As far as, the prevention policies also decrease the cyber-attack possibilities and also the cost of preventions is many times cheaper than prosecutions procedures.

### 2.4.2. Prosecutions procedures and policies

In this part, particularly outlined some important prosecutions rules and policies of cyber-attacks based on official journals and official gazette of the ministry of justice of Afghanistan which is newly approved by Afghanistan’s president and ministry legislative board by name of criminal code (کدجزا). However, the ministry of justice and especially, the general department of legislative by collaborating of MCIT are in charge of legislative laws and prosecution policies of cyber-attacks. Hereby, they have defined and approved some persecution laws that are generally outlined in Table 2.1. and the information in this table converted from Persian.

There is no need to argue about the prosecution policies deeply and it is not important to be analyzed in this report because the philosophy of this report is not arranged and managed regarding prosecution rules and policies that are being implemented by authorized governmental organizations.

As well as, the legislative authorities also have their own definition about cybercrimes and cybercriminals. As a general overview, some of the ministries of justice's cybercrime prosecution policies has mentioned in this table for information and understanding of the basic persecution procedures. It should also be noticed that the prosecution policy paper is approved and published newly on 25/02/1396 (15/05/2017) for more information refer to [30].

Table 2.1. Legislative prosecution laws and policies in case of cyber-attacks

| Titles | | Commandments or sentenced punishment la |
|---|---|---|
| Cybercriminals punishment | | |
| Paragraph 875 | (1) | The cybercrimes are those, which are implemented by using modern information technology tools, digital communications, and internet on virtual communications space (Cyberspace). |
| | (2) | Cyberspace is the virtual nonsense space that is created and configured under computer networks or internet. |
| | (3) | The perpetrator of cybercrimes punishes according to this chapter commandments or sentences. |
| Illegal access to information systems, computer applications, and computer information. | | |
| Paragraph 876 | (1) | The persons who access illegally to information systems, private computer applications or personal information will be punished on pain of imprisonment. |
| | (2) | The perpetrator who does the cybercrimes according to the first dorsal of this paragraph (1), cause financial harms, vital threats and moral harms to another person or people will be convicted to first dorsal of this paragraph (1) and will also punish to crimes punishment procedures. |
| Illegal changes to information and computer systems or computer applications. | | |
| Paragraph 877 | (1) | The persons who illegally perpetrates temporarily or permanently to one of the following crimes will be |

Table 2.1. (Continue)

| | | |
|---|---|---|
| | | convicted to medium imprisonment and financial fines from 60000 AFG to 300,000 AFG ($900 - $4400).<br>1. Changes, legal users deny and cause performance damage to computer systems.<br>2. Products, changes, trammel or vulnerabilities to computer systems, applications, and information systems.<br>3. Denial of services, inaccessibility, absurd or insensate of information systems, computer applications, and computer systems.<br>4. The prevention of legal user's access to information systems computer networks and computer applications.<br>5. Bring change to security level or breaking the security level of computer systems, computer applications, and information systems.<br>6. Injection of malicious codes or malware and viruses to computer systems, information and communication systems include computer applications. |
| Element and damage to computer systems, information systems, and computer applications. | | |
| Paragraph 878 | (1) | The persons who access illegally to above systems and elements, damage and inactive them that cause financial and moral harms will be convicted to medium imprisonment and financial punishments from 60,000 AFG to 300,000 AFG ($900 - $4400).<br>If the punishment of the crime of the first dorsal of paragraph 878 related to above systems and public or governmental systems perpetrate financial harms more than |

Table 2.1. (Continue)

| | | |
|---|---|---|
| | | billion Afghani the perpetrator will be punished to life imprisonment up to ten years. |
| | (2) | According to dorsal (1 and 2) of this paragraph, if a person who breaks down, harms or damages the air and lands transportation systems, energy production basements and other sensitive public basements, or even if the criminal financial harms or damages to other persons, organizations or companies the criminal will be punished to life imprisonment. In addition, if the cyber-attack cause homicide or murder the criminal absolutely will be punished to permanent life imprisonment. |
| Password and credential disclosure. | | |
| Paragraph 879 | (1) | If a person who discloses credential codes passwords or other credential access codes to information systems he/she will be punished to double financial that has done to people, organizations or companies. |
| | (2) | If the person who discloses dorsal (1) of this paragraph related to governmental organizations, companies, and public projects he/she will be convicted to medium imprisonment and financial punishment from 60,000 AFG to 100,000 AFG ($900 - $1250). |

Conclusively, there are also many prosecution rules and policies regarding cybercrimes, cyber-threats, and cyber-criminals mentioned by details in this official gazette of the ministry of justice of Islamic Republic of Afghanistan. Commonly, these rules and policies are sufficient for internal prosecution of the cybercriminals who attempt to destruct the internal network infrastructure, information and communication systems. However, in case of external cyber-threats and cyber-warfare, the authorized persons and organizations continuously need professional cyber-attacks prevention teams and adequate facilities.

## 2.5. Current Cyber Threats and Vulnerabilities

Cyber threats are the new phenomenon in recent decades, with the evolution of information technology and communications world, the threat has emerged through an extensive network of the worldwide Internet. Thus, the challenge of cyber threats is important and complex.

In common, there are many types of threats and different methods which the hackers and attackers designed for targeting complex manufacturers and networks, as we understood the nature of security and threats, many different parameters could be the deathful threats on cyberspace. Whatever, here the popular vulnerabilities and threats that seriously take place and prevent security strategies briefly illustrate in this part. Based on research and investigations according to the current status of cyberspace of Afghanistan, this country significantly impacted the cyber-attacks being managed by powerful nations and neighbor countries.

In fact, interfering of neighbor countries, the competition of international troops and regional nations in economic, political and industrial changed Afghanistan into a negative competitive market, which such negative competition had has unpleasant and direct effects on cyberspace and security of the virtual space. However, competition in politics and large economy projects is the contest between multiple international countries, neighbors and internal extremists in Afghanistan, as already proved that the attacks on cyberspaces of Afghanistan were supported officially by a legitimate government same as the cyber-attack had recently happened on official domains of multiple ministries.

Particularly, in this part concerned about two types of threats that Afghanistan is experiencing every day, based on the cyber-events had occurred, cyberattacks categorized in two general below parts and as well the general structure of the threats that cause cyber threats and data leakage already classified on Figure 2.3.

### 2.5.1. External threats

The cyber challenge manages from outside of a country by authorized governments as slightly pointed out also in part 2.1. in such method, significant horrible devastative cyber-attacks officially organize by an official organizer nation from outside of the country, those organizers have competent evidence and are legally authorized for establishing an official cyber-attack on network infrastructure and information systems of the other nations.

In terms of cybersecurity strategies, in both cases, either external cyber-attacks or internal cyber-attacks, the victims' national security agencies are in charge of defense, recognize and deterrence the cyber-attacks. Whatever such attack targets public online services or private sections and industrial companies. In such kinds of cyber-attacks socially or politically being motivated, cyber-attacks carried out primarily, through the Internet, the attacker groups allocate times and sufficient budgets to target a specific destination and build an appropriate legislative framework in form of cyber-attacks on critical fundamentals. The key factors that outsiders target listed as below, similarly, there are also some methods illustrated in part 2.8 that can be used in internal attacks.

1. Targeting fault point of none up to date software, attackers ambush the security vacuum and critical fault of software that installed on victims servers or systems, for instance, the attack happened on Panama papers in July 2016.
2. Targeting power grid systems, power grid systems or energy stations considers as one of the critical instrument that being targeted by outsiders, sometimes attackers by the distributed denial of service (DDOS) or denial of service (DOS) methods attempt to destroy fundamental of power systems, as an example, attacks on Aramco oil stations.
3. Network infrastructures and communication systems, in fact, the network infrastructure is one of the popular instrument being affected by cyber-attacks, in this method hackers attempt to target fundamental of the network for overloading,

overflowing, destruction and devastation by generating high electromagnetic pulse over the network and data transmissions facilities.

4. Economical and online service, attacker attempt to target the online services to stop functioning, they effectively coordinating their activity and develop appropriate applicable malicious software aspired to data leakage, data stolen, and financial benefits or even nearly all of them are interested in political beneficiaries.
5. The cyber-attack targets source applications and databases, in this kind of attacks attackers, involve information theft, economical beneficiary, credential theft and theft of sensitive documents and identity. SQL injection, cross-site scripting, and buffer overflow could be the regular live examples of such kinds of attacks [31].

### 2.5.2. Internal cyber threat’s instruments

In general, the threat is an approach for troubleshooting fault of the systems and sources. Specifically, internal threat is also an event for analyzing the internal cybersecurity faults. It is a semi-completed experience that enables security expertise to identify, classify, and address the security risks associated with insiders.

Insiders are significantly more dangerous and major problems than external vulnerabilities because the destruction of data on internal infrastructure highly effects on the daily activity of public and private resources like an economic institution, education institution and etc. Insiders could be easily discovered because they use the instruments allocated by internal IP addresses or even if they use fake IPs still the government and security team can discover them. Nevertheless, the main internal threat instruments that cause conflict and problems in cyberspace are point out on below.

1. Selling of illegal SIM-Cards: The international and national companies who are providing the telecommunication services, internet and text messaging services, manufacture and sell the Subscriber Identity Module SIM- cards without permission of legal government authority, nearly all the Afghan civilians use 3G

and 4G services to be connected on the internet. However, intense of the insiders are using and being connected through telecommunication internet that government or often the telecommunication companies do not register them. This process can cause and have serious consequences on cyberspace, due to, it makes the backtracking and monitoring issues overall in general. Similar to, the cyber-attack on the website of National Directorate Of Security (NDOS) of Afghanistan had happened on 25 November 2016 was by insiders [11]. The hacker who called for justice. In this case, normally the cyber-attacks can be denied or monitor if the government register and monitor all the internet users.

2. Black market, selling of cracked and out of date software: Generally, controlling of black markets in all around the world is a big problem, but in the other countries software products and licenses are under the guise of state or an official authorized organization. Basically, based on the software product company's agreements, illegal use of software in commercial and none commercial is completely prohibited, but unfortunately, in Afghanistan, almost the government does not involve to the selling of cracked and out of date software, and sometimes such software is used by official government agencies. Regional and neighbor countries, especially Iran and Pakistan cracking the Microsoft products, inject malicious codes into software source codes and then export them to Afghanistan.

3. Illegal use of Café-nets and internet services: Billions of computers and electronic devices are connected to the internet at café nets in all around the country and every day increases, particularly in Kabul. The licensed café nets protected by simple firewalls configured under the main network routers. Many Internet cafes have big security problems and also other similar public access points security has not covered by a predefined protection policy. The insiders attack from café nets with an unknown identity. The security team is not able to trace and find them easily, which distinguish between an insider who uses café net internet service is impossible. However, the security of café nets must be provided by government or

an official authorized security team includes the requirements for physical protection, access controls, encryption, backups and virus protection. As well as, the café nets should include rules and advice on connecting shared or mobile devices to corporate networks and guidance on their use in public places.

4. Non-transparent deal of telecommunication companies and internet service providers: Over the 20 million population of Afghanistan use GSM services (Voice transmission, Short Messaging Service and Internet 3G and 4G Service). The government can't control the telecommunication products in black markets, and due to the inability of government, usually, telecommunication companies export SIM-card, 3G-4G Dongles, and mediums without registration to an official government agency.

5. This problem has made a big deal on current communication systems and it would make a bigger challenge in the future cybersecurity. However, the existence of unlicensed internet service provider ISP makes the other major problem, the majority of ISPs directly benefits from satellites and working without having official license.

6. None accountability of risk management: This is the major issues appear for governmental organizations, many of them never concern about the risks of cyber and cyber-attacks. Inadequate risk assessments can be particularly dangerous because they instill a false sense of security. A false sense of security can lead to devastating consequences.

7. In this part, concerned about critical issues that could be crucial challenges on current and future cyberspace, but still many of such problem not being covered in this part, because the analysis and evaluation of the current cyber situation and future strategy by details deeply need sufficient time and investigation. For instance, the evaluation of frequency spectrums that are distributing by the

government and GSM security. Basically the transmission of voice and data over the GSM networks, data and voice being encrypted by one of the standard encryption methods but still the encryption method is not secure and GSM transmission could be compromised easily by new and modern technology [32].

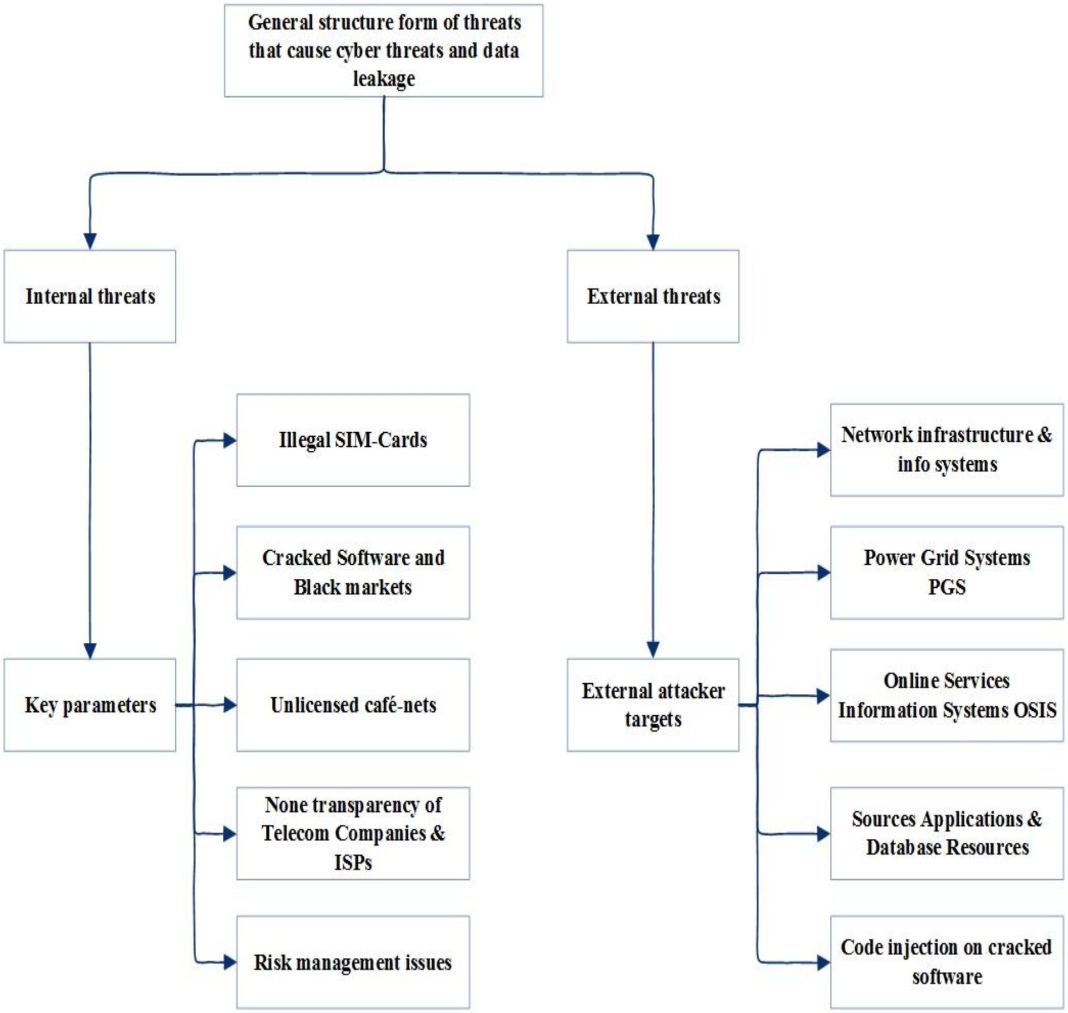

General structure form of threats that cause cyber threats and data leakage
Internal threats
External threats
Key parameters
Illegal SIM-Cards
Cracked Software and Black markets
Unlicensed café-nets
None transparency of Telecom Companies & ISPs
Risk management issues
External attacker targets
Network infrastructure & info systems
Power Grid Systems PGS
Online Services Information Systems OSIS
Sources Applications & Database Resources
Code injection on cracked software

Figure 2.3. General issues that cause cyber-threats and data leakage

## 2.6. Obstacles to Current Cybersecurity

By reviewing the goals and visions of cybersecurity team, absolutely we can recognize the impediments of cybersecurity, and then also the impact of cyber challenges can be analyzed. However, the major concern of all the states and the citizens are the security and data privacy of the communication and information systems within their home country. Primary, there are significant problems and obstacles that prevent the implementation of security strategies, generally listed as below which the government and particularly MCIT slightly can't control by their own current capabilities. Coordination: Effectively coordinating of national cybersecurity team in all across the country by following a preplan, well define a method and build an appropriate legislative framework for cybersecurity on cyberspaces, with the participation of the private sectors, civil society and even participants of national and international expertise.

a. Confidentiality, Availability and Integrity CIA assurance: Build an appropriate feasible and managing framework for cybersecurity on cyberspaces, sketching on international experience to establish a national cybersecurity system and computer emergency response teams then develop the necessary infrastructure to ensure confidentiality, availability, and integrity of data and digital transmissions.

b. Intellectual property: Implement effective activity to build the necessary human capacity and activation of an e-government systems for all sectors, especially in cooperation with the private economy, industrial sectors and banks, as well as, cooperate with other countries and relevant international organizations in case of international cyber-attacks on cyberspaces and providing confidence national consulate with international cybersecurity teams.

c. Public awareness: Advertising and announcing public awareness, defining public and private data privacy, the sensitivity of data and personal identity, benefits of digital services for individual and public usages or e-governments and even alarming the public awareness in case of cyber-attacks on public and private critical information systems.

d. Interoperability: Control of the internal and external network capacities and overloading of data on network nodes, absolutely, control of frequency spectrums and private sectors telecommunication channels in case of misusage or unlicensed usage of radio frequencies in low and high-frequency bands (L&HFB) [33].

## 2.7. Current Cyber Strategies

In referring to current cyber-strategy, some of our government’s key performances outlined previously under the title of current cyber policies and procedures. Actually, to analyze precisely the organizational strategies, first of all, it is hard to access strategies of an organization, because such information quarantine secretly and mostly is not accessible to the public. Therefore, under this title, some of the key issues which are impacting the cyberspace and communication systems been signified by bringing a simple example. Firstly, the importance of cyber power, cyber strategy and then cyber-threats including cyber-attacks and exploits. When I was a child around ten years old, I experienced an incident of my real life, one day I was running quickly toward home, returning back from educational center where bunch of my colleagues had been playing football on the street.

They stopped playing soccer by whispering each other when I was getting closer to them, however, I have been asked to participate them in playing. There were two problems which made me nervous, I couldn’t play very well and I was also so happy to be asked for joining them.

I abandoned my books and tried to play with them. I pushed to the ground by one of them directly, as soon as, I had made it over the players. Then I had been assumed as a ball to be beaten as much as they can instead of the real ball. I couldn’t do anything, they all began fully kicking me and curled up to avoid getting hit on my head. It was a great spectacle for them in order to laugh that finally, I escaped when they were all laughing.

In today's cyberspace poor cyber power nations are same as my childhood, without having powers, abilities and human resources the cyber powerful countries invite them just to make laugh and for their entertainment. What happens if the cyber-attacks manage by such a powerful country? The countries that have not Cyber-power and human intellectual resources will be a battle of cyber wars like Afghanistan, internal conflicts, the existence of the international and national terrorist groups that equipped by adequate cyber resources are the biggest challenges of current cyberspace and will make the biggest future cyber threats. Almost, currently, the government works on cybersecurity and has established a cyber-department for transparency of the future cyberspace.

However, the governors attempt to define prosecution law framework for cyber-attacks preventions and protections which is already explained in part 2.4. The Afghan Telecommunications Regulatory Authority ATRA working with MCIT of Afghanistan to control the frequency spectrum and optimizations. Absolutely, these organizations have developed strategies and deeply concentrate regarding spreads of current technological projects and improvements criteria in the field of digitalization. By referring back to literature part of this report, as MCIT has published an academic journal explaining the current cyber-strategies. This effort “National Cyber-security Strategy of Afghanistan” which is published in 2014, explained the cooperation and integrity of multiple governmental agencies such as the ministry of communication and information technology MCIT, the ministry of Justice MoJ, Information system Security Directorate ISSD and national parliament in act of demonstrating laws and policies, specifically connected to cybercrimes.

The mission and vision of MCIT including the cyber-strategies and objectives of this governmental agencies have contented in this report, commonly, a description of the public and private sectors responsibilities on cyberspace underlined. Additionally, in partial parts of this report the strategy of government regarding the cyberspace demonstrated as an example the text “The ISSD of MCIT enforce the adaptation of ISO 2700 series and other International standards for Information Security Management System (ISMS).

Information assurance, information systems and IT infrastructure audits, vulnerability assessment, risk management of the critical information infrastructures (CII), Business continuity, ensure Application security through Software Development Life Cycle

(SDLC) and best practices and Penetration testing of IT infrastructures" which has been copied directly from this effort, relatively conducted to this report. However, how an offensive cyber-attack can be deterred or can be mitigated technically and relatively in connection to the cooperation of government cyber-teams agencies they have not explained either technically or politically.

The conferences which is establishes among government agencies regarding cyberspace also is one the significant priorities mentioned in this effort, such as draft of laws, draft of e-Transaction and e-Signature lawful procedures, draft of National Cyber/Information security Policy, draft of Intergovernmental IT security, Router, Switch, Firewall Policies, draft of Computer crime incident response procedure, draft of IT security training curriculum/schedule and Child Online Protection Policy by cooperating to the Ministry of Justice and other government agencies have brought optimistic results, in this paper.Moreover, the classification of data and information at government and none government agencies have also synopsized in this effort. In referring to this effort, a framework to solve technically or politically the digital wars and cyber-conflicts or a framework to explain the current technology circumstances of cyberspace which annoy by streams of trillions of logic bombs and threaten our current and future network infrastructure is not defined in this paper.

In a general manner, the outlined framework which is mentioned in this effort totally have written on paper, practically, I could find a cyber-event or attack that indicate being deterred or retailed by these organizations. Our current network infrastructure and our future critical network infrastructure is heavily threatened by logic bombs.

## 2.8. General Methods and Types of Attacks

We all understand the nature of cyber-attacks, which are the negative vacuum of our installed hardware and software tools on our systems. IP addresses, network topologies, and network infrastructures are the preliminary steps for adversaries that attempt to discover and select as their targets, usually, collections of such information are easily possible from internet the production companies issue and share their product instructions publicly on internet, the instruction includes the hardware and software even types and version of the settlement software. Thus, such prime internet search helps the attacker to fully understand about network infrastructure of victims, then easily, they will be able to penetrate on target systems by using the flexible method of cyber-attacks that considerate in this part of this report.

However, the threats adequately categorized briefly in previous parts, but in this part the essentially concerned about the types of threats (Exploit and attacks), also, the methods that consequence a big destruction over all systems.

Whatever, such attack manages either by insiders or outsiders, they both exploit and follow particular methods, nevertheless, of course, there are many types of threats and method of cyber-attacks that can't be explained by details in this report because of time-consuming, but in short, the popular types of threats are explained in here.

The identification of threats help us to understand the nature of cyber-attacks, when we understand the nature of attacks then could be able to define a well-defined strategy for defense, therefore, here firstly, we want to recognize the variety of attacks and evaluate the risks and at the end, the vulnerabilities and threats of cyber-attacks will be decomposed and analyzed by details.

Several methods could be performed by attackers, especially, nowadays the cyber-attacks intensifying or sometimes a cyber-attack can result in the variety of fields and comes from indistinguishable sources like the attack in systematizing of cyber terror and death of the human.

But the method of attacks depend on cyber-attacks and directly contacted on target systems, such as: cyber-attacks aimed for stealing and theft of intellectual property and personal information, the attacks designed in format of Distributed Denial Of Service DDOS and Denial Of Service DOS, the assaults targets SCADA grid systems and attacks designed for political and financial intentions, and eventually the attacks on nuclear facilities, sensitive communication network and military systems infrastructure.

A primarily step where the attackers attempt to learn and gain the useful information like target’s IP address, the topology of target’s network infrastructure various of software and hardware installed on victims systems. Frequently, this information is easily accessible from the internet which the attackers are able to learn about them or mightily all of the manufactured companies publish installation guides and instructions specification about the hardware and software products on the internet. Secondly, gaining of the primary information regarding the victim systems directly or indirectly excites adversaries to select an appropriate method of attacks for penetrating on targeted systems. Here we discussed general methods of attacks and attackers final targets, which placed and targeted sensitive infrastructure nuclear facilities, military fundamentals, health services and financial collaboration organizations in the history of hacking, keying as below.

### 2.8.1. DDoS and DoS

As an overview, cybersecurity and security of system's infrastructure is a region of increasing interest as the nations has become increasingly impacted by its inability to promise and assure that both information on virtual space and system infrastructure remain secure.

As we know, the concept of protection, data privacy, and security has a long history and started from along with human life,  people were trying to be protected from malicious behaviors, continues until now, and it has become one of the high value in modern society. However, parallel to the protection and privacy the challenge and threat also become strong and increasingly has appeared as a destructive instrument in modern technology. In modern society especially, in today’s global village and communication systems, malicious parties try to find different method against data protection. Cybersecurity and information privacy which DDoS and DoS concern as effective methods against assets and protection of data on cyberspace. In short, both DDoS and DoS have designed for destruction and damage of information or data stored on virtual relational sources and relies on virtual space and even the DDoS and DoS have the strong capability to damage and destroy the network infrastructure. Moreover, the malicious groups have tried many times to target the physical infrastructure such as SCADA grid systems to stop them from functioning by using DDoS and DoS methods which is shown in Figure 2.4. However, these types of threats are the largest dangerous instruments in today’s digital communication and information systems which are configured under the network or partially connected to the internet. In general DDOS and DoS disable the virtual services and compromise the availability of servers.

Particularly, in such kinds of cyber-attacks, the attackers attempt to take the control of the infected hosts and use the hosts to flood the victim systems, either by consuming the bandwidth or resources of the victim systems. Furthermore, the attacks continue until disable the network components and compromise the victim resources (Socket, CPU, memory desk, database bandwidth and even I/O bandwidth) [34]. Many internet service providers, web hosting services, online service providers and even SCADA infrastructures being seriously suffered from DDOS and DoS attacks in all around. There are many methods, complex algorithms and defense mechanisms had have presented by multinational cybersecurity companies and academic scholars characterized to decrease, monitor or mitigate the DDoS or DoS attacks. Further, in solution part 3.1. of this report, we will review some of the solutions and defense mechanisms against DDoS and DoS, but here we concern, about the risks assessments and description of the risks that are executed by DDoS and DoS attacks.

Nevertheless, also the main focus of this report is about the simulation of DDoS and DDoS risks, defense mechanisms, and simulation of the DDOS. The risks assessments and risks analysis are the other important parameters of organizations to identify and then classify them through vectors para-diagram. The DDoS and DoS can be resulted many types of risks according to victim's infrastructure, but below are the most common risks that can be overwhelmed through these type of attacks.

a. Effects on critical network infrastructures and consumption of three main components of the network such as; consumption of resources, consumption of network bandwidth and overflow on network connectivity links includes gateways, routers, switches and etc.
b. Misuse and abuse of the commercial logic, the DoS and DDoS aims to target the structural logic of business and network infrastructure components.
c. Destruction, modification and alteration physical structure of the network elements, which accounted as the biggest issues to physical infrastructures including business, public and critical infrastructures.

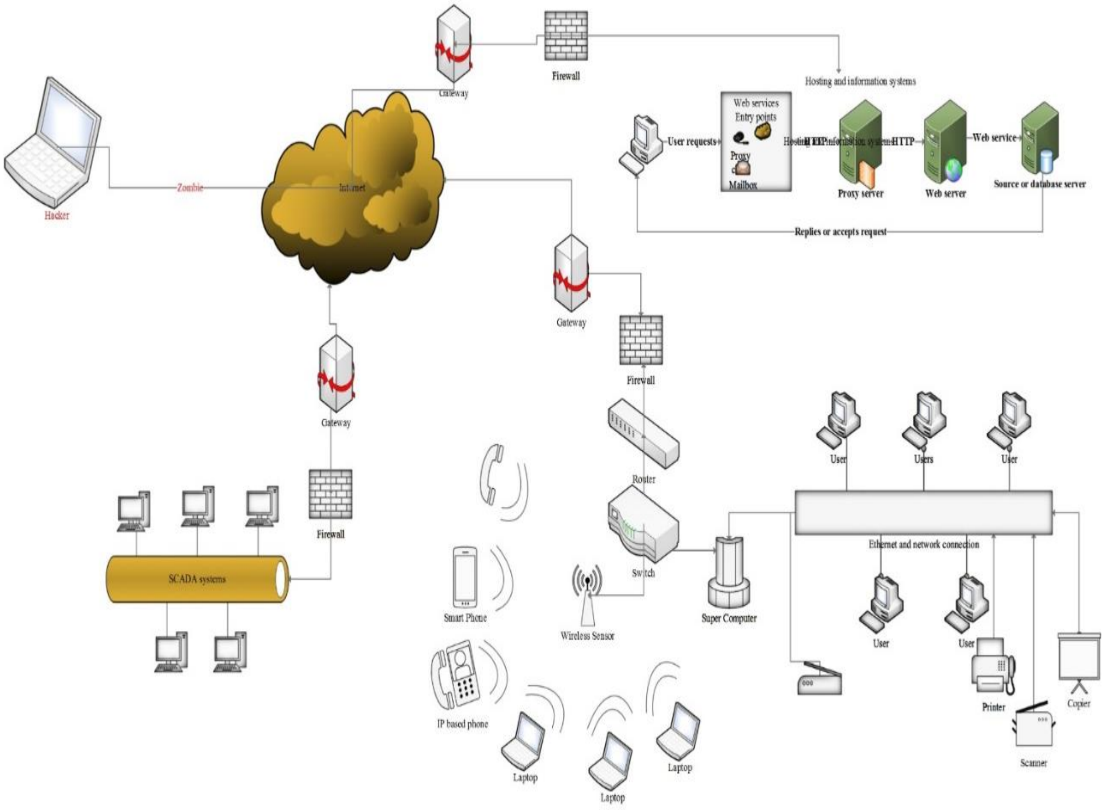


Figure 2.4. DDoS on network infrastructure, information & SCADA systems

### 2.8.2. SQL injection and cross-site scripting

1. SQL injection: Recently in last 15 years, the popular organizations' concern about the new methods of dangerous attacks on web applications called SQL injection and XSS. Both of them ranked as destructive logical analyzer method of hacking. The attackers analyze the logical structure of SQL queries and then execute SQL queries into database application servers.

Generally, the SQL injection runs through web applications into databases server of web application, based on, the logic of SQL statement back in or databases server of web application authenticates the input data without proper validation. Then designed SQL queries are used by an attacker with an intention to bypass the validation of the legal credentials, in such processes the attacker easily grants access without having any legitimate access right into sources of the systems and users accounts [31].

SQL injection enumerate as one of the common attacks on web servers and web application servers, there are many types of static and dynamic protection and detection method against SQL injection like parameterization of the coding, definition of the parameterized function, procedures and relational paragraphing on the logic of coding. The logical structure and flow of SQL injection method has shown in Figure 2.5.

In addition, the vulnerabilities of SQL injection particularly in the web applications are distinctly very ample and certainly a bulky security threat to stored personal data on web application servers.

2. XSS: this is also a method of hacking and dangerous vulnerabilities that enable the hackers to inject the malicious scripts to web browsers, usually, the cross-site scripting concern as, the hacking method on online applications includes banking systems, application for registrations and etc. Attackers use this method for targeting web applications to run their malicious script via browsers.

The XSS creates various security violations such as theft of cookie, data theft, web content manipulation and even denial of services [35]. XSS is commonly occurs because of none validation of user inputs on both web server sides, and client-side where with proper validation in both web server side and users side the application developer can be able to prevent the XSS attacks.

There are also many other methods of prevention that generally the application developers concern about, such as; client side and server-side validations, validation on user interface pages and finally, the attractive effective method for both XSS and SQL injection is parameterized programming [31].

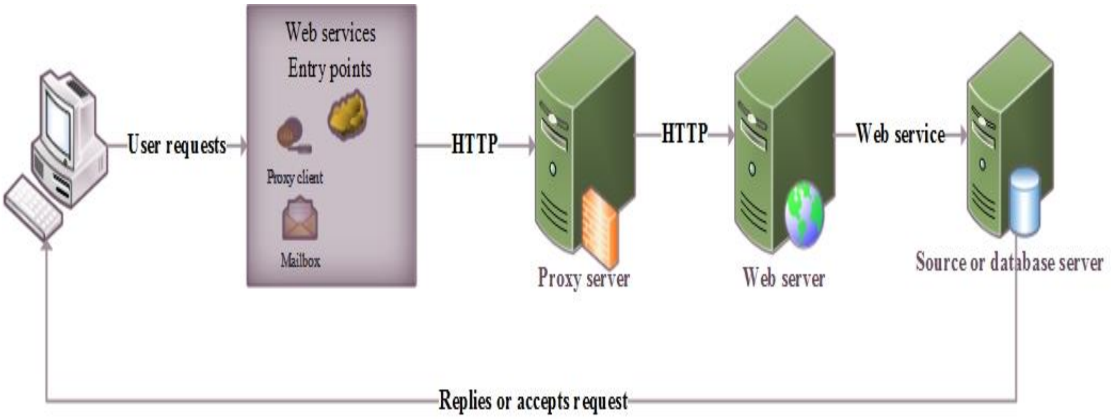


Figure 2.5. Flow of SQL injection

### 2.8.3. Physical infrastructure vulnerabilities

There are many types of risks that chronologically growth within the improvement of technology and globalization. Since the cold war started, many nation's networks and critical infrastructures have targeted in purpose of prominence competitive without caring about the supremacy laws and procedures in all around the world where cyber-threat is one of the well-known instruments of cold war. However, here the physical architectures of such critical infrastructure especially SCADA and their potential risks have discussed. Since 1982, when the Soviet Union attacked the Siberian energy pipelines (Gas and Oil), for the first time [36]. and exploded it.

The security of SCADA systems collapsed, parallel to the development of industrial technologies, manufacture of SCADA systems and improvement of communication technologies, the security risks of SCADA systems increased within the high potential of risks**.** Recently in 2010, a number of security companies reported the existence of malware that was targeted particular systems a modern worm with the unusual payload that would impress specific type of Siemens SCADA systems by the name of Stuxnet. This malware was the powerful self-replicate exploited long list of vulnerabilities in Middle East countries, especially on Iran nuclear facilities [37].

It had the capability to break down the installed system's security such and antiviruses and update itself over the network to command and control server for executing malicious codes. More than half of the spotty computers which had been infected by Stuxnet were in Iran. Consequently, after this incident especially in Iranian nuclear facilities, the world scientists and politicians characteristically, interested in SCADA systems. As a general review on architecture of SCADA systems, these systems are widely used in modern industries, in power supply stations, gas and oil stations, transportation and water stations, as well as, in many more determinations. In fact, the structure and concept of SCADA systems are newly introduced in modern industries. The most important challenges similar to monitoring and controlling of industrial processes such as power plants and power grid systems, oil and gas distribution systems, food production systems water source systems and many other basic systems are managed by SCADA systems. Damage or even disability of SCADA systems has significant negative impacts on industrial infrastructures, SCADA systems architected as distributed architecture with multiple servers configured under a single LAN within the IP distribution of network procedures and network security.

Each server is responsible for a different internal meaning, but now the SCADA systems increasingly networked and configured over the large geographical areas which delivers service for WAN and the internet. While the internet itself has another virtual impacts on these systems that are required meaningful security treatments [38].

Different generations of SCADA systems have introduced on industrial societies parallel to the development of technologies the SCADA systems are also developed significantly. As you can see the Table 2. 2. has shown the comparison among different generations of such systems. However, SCADA architectures, protocols, and technologies can be in various considers, it would be impractical to list the numerous vulnerabilities and threats that may apply to each configuration. Nevertheless, it should be noted commonly, that the vulnerabilities in SCADA are largely the same as the ones encountered in conventional computer systems because such systems can be remotely controlled.

Table 2. 2. Comparison and description of different SCADA generations

| Generations | General names | Description and property |
|---|---|---|
| 1th generation | Monolithic | Remote terminal unit RTU SCADA primary servers, standby servers, field devices. |
| 2th generation | Distributed | Application servers, configuration servers, historian servers, database servers, human-machine interface HMI, data acquisition, RTUs engineering workstations and configured under control network or LAN. |
| 3th generation | Networked | Corporate PCs, business servers, application servers, configuration servers, primary historian servers, secondary historian servers, database servers, RTUs, HMI, data acquisitions, external partners, remote access, widely control network or internet, corporate network, web and email servers W&ES. |
| 4th generation | Internet of things | Under process … |

Many reasons can be caused the unavailability of SCADA systems, mostly the cyber-attacks are dreadful and make serious problems on SCADA systems, when targeted these systems. The cyber-attacks could be implemented remotely or physically by injecting malicious codes, and by having physical access to overflow the systems. Firstly, the typical cyber-attack type which is targeting these systems are distributed denial of service DDoS and denial of service DoS.

Nonetheless, cyber-attacks on SCADA systems cause multiple risks and dangerous outcomes such as; hardware failure, software failure, and even network failure, the failure on these systems results the disability of them. Secondly, by having physical access to the systems, the attackers can destroy and disable the key factors of the SCADA systems by entering the high-voltage of electricity, the high-voltage of power produce high power potential and uncontrollable circumstances on stations and infrastructure.

Thus, the network fundamentals and components alternatively disable, same as having access to a component of network to compromise a Real Time Unit RTU and gain access to control networks like injecting a USB stick and replace malicious codes into SCADA systems. Buffer overflow, the other matter that arises from the requirement of continuous availability is that SCADA field devices may run for years without rebooting. In the process, they accumulate fragmentation, which makes them particularly vulnerable to buffer overflow. However, buffer overflow is one the frequent matter of an attack on SCADA systems it can affect field devices that are embedded systems running real-time operating systems RTOS, buffer overflow also can be the matter of malware designed for purpose of SCADA networks or computer network may well infect a SCADA servers [39].

In addition to types of attacks, however, the SCADA systems can be targeted through two types of attacks that are commonly designed in this aims, the attacks which are being implemented via Denial of Service DoS and Distributed Denial of Service DDoS. DoS is the semi-traditional type of attack that generally targets a single source of victims, where DDoS is not only target the multiple sources of victims, it has also the distributed flexibility according to victims sources. Three complicated entanglements of DoS and DDoS have been identified that generally attempt to disable electrical source systems. They are the attacks targeting network protocols, the attacks on network infrastructures and the attacks on network bandwidth [40].

### 2.8.4. Black hole/ Gray Hole

Primarily, Black Hole/ Gray Hole is a method of cyber-attacks used for targeting the smart grid and SCADA systems, the attackers used this method to target the networks that transmit large volumes of traffics. Prevention of data availability, compromising a network node by attackers and dropping of the voyager packets through networks are the popular types of black hole cyber-attack.

Once the attackers will be able to drop all the network transaction packets by implementing this kind of attacks known as the Black hole, then exploit the systems and resources as much as they want. However, sometimes drops of network packets happen selectively, in this case, the detection of attacks is hard because nobody can recognize and recovers the dropped packets. This type of attacks is similar to Denial of Service DoS, and it has the impressive impacts on network nodes because the attackers can be able to breach the network systems integrity at the compromised node and cause the loss of network availability overall.

### 2.8.5. Watering hole

The watering hole is a wiretapping or eavesdropping hacking method that enables the attackers to target the websites and theft especially, the username and passwords of the user who visits the websites. Watering hole strategies could be run on websites that have frequently (individual, groups, organizations and industrial companies) visitors. In this method, the attackers guess what websites a particular target visits frequently and then run and implant malware on that website. In 2012, watering hole encountered as a considerable threat to critical national infrastructure and fundamentals [38]. Primarily, the attackers target the people who recruited by large organizations and companies, such as governmental authorized responsible, military members and groups of authorized people in important roles, or even more sensitively the persons who are the member of an important organization like top organizers and planners.

The target of watering hole clearly has presented on Figure 2.6. and the victim organizations. On the other hand, this method of attack is a big threat to stealing personal information from citizens, civilians and people, and even it can be unique as well. This means that hackers can easily capture all the personal information of any citizens or persons and then benefits from lost information for themselves.

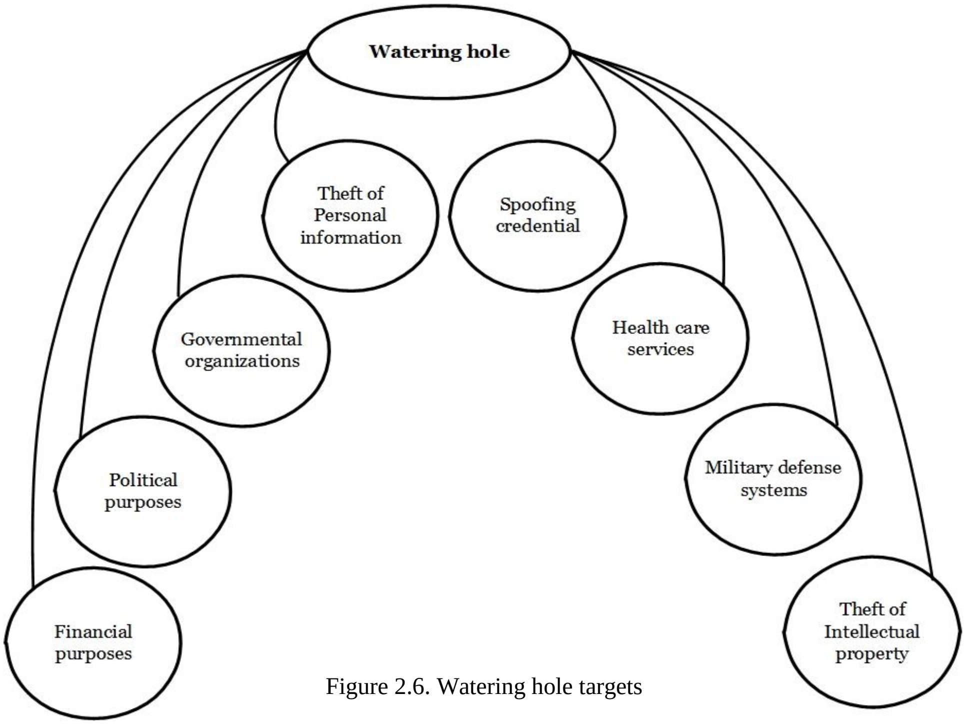


Figure 2.6. Watering hole targets

### 2.8.6. The third party cracked software

Today's communication and information systems rely on third-party software and applications such as; smartphones, utilizing mobile computing and clouds. Commonly, the communication and information systems need third party software, in concern to the production of applications and software, many errors and faults could be exist in development of software. The security vacuum and risks always encounter in either both open sources or close sources software due to the fact of human faults. Earlier in the threats part, we mentioned some of the risks that come out because of cracked software that neighbor country export to black markets in Afghanistan. Here, we describe the common issues and security risks of cracked software, many security organizations discovered fatal issues of such software. The cracked software significantly can always be infected to malicious codes which have dangerous risks on commercial applications, communications systems and also information systems, particularly, the injection of malicious codes, exploitable in logic of coding and a more serious problems can also be run on cracked software. In the large organizations that are generally use the vendors developed applications or third party software, they also have security measurement teams who are responsible for checking and monitoring of the installed applications performances.

If a unique service of software does not use very frequently, the security responsible disables or removes from both clients and servers side. When the applications and software use in large data centers and under big network configurations, the security teams disable the useless feature of the product because the useless features of third party software allocate the resources, create huge security risks, and have significant effects in both servers and clients.

In fact, the weakness of security and infected malicious codes into third-party software enables cyber- attacks and the vulnerabilities on systems reason the compromising business data, personal information, and theft of intellectual property and even organization's assets. As we already mentioned previously, Afghanistan has become and changed into a black market of the back door and cracked software including clients and server's operating systems, official documentation instruments like Microsoft office, outlooks or even the software uses for the designing similar to AutoCAD and etc.

The public and private organizations such as: educational institutions, financial, construction companies, transportations and even communications firms are typically use the cracked software without having knowledge and sufficient information about the malicious codes, spyware and malware that are being injected into such cracked software for spying.

Theft of data and intellectual properties and many other sophisticated challenges can be raised due to such application and software. In abundant cases, big international and private companies like telecommunications, social services, and transportation companies train and aware their employees including their stockholders and shareholders, but mostly, the middle and small business companies and principally governmental agencies encounter issues in usage of cracked software.

### 2.8.7. Zero-day attack

A variety and remarkable of target could be actualized by using of zero-day attack method especially, when the newer versions of third-party software including close sources and open sources operating systems with unknown hole ramp to markets and/or installed to critical shared embedded systems and computers. Zero-day attack takes unconditional roles to target cyber-physical systems and infrastructures that such software is installed on them. A zero-day attack is a type of attack operation designed for exploiting the vulnerabilities of the software and products, in general, this type of attack refers to a hole in software or products that are unknown to the vendor. Attackers can penetrate into this vulnerable hole before the vendors become aware of it. A zero-day attack can include spyware dealt espionages, infiltrating and allowing the unwanted access to user information. Precisely, the Zero-day attack is a mechanism of cyber-attacks that may cause remarkable damages and has destructive impacts even in both cyber-physical systems and cyberspace.

### 2.8.8. Spear phishing

Spear phishing: A method of hacking without any targets and there is no specific definition to be targeted by a spear phishing hacking method, the preliminary concept of spear phishing is slightly closed to social engineering. Adversaries attempt to target individually the famous persons or the key personals in organizations by spear phishing hacking method, and it has demonstrated an aberrant method and effective in opposite to cyber security-aware individuals. Similar to the watering hole, the spear phishing also is a method for spoofing the credentials such as usernames/passwords of individual persons by injections of malware into target systems. Sometimes both watering hole and spear phishing may influences to backdoor malware on locally configured network finding the path to be injected into employee's personal computers. The malware can be injected through social media, spam emails, and sometimes the email contains official instructions about underwork projects or instructions regarding the responsibility of employees. Attacker impersonates the official identity of an organization by an official format then send it to the employees via emails that contains a link or an attachments that will allow the attacker to be taken the supervision of target personal computer.

When an employee or a user clicks on shared links or opens the shared attachments, then the malware can be able to infect the victim system or personal computers. Undoubtedly, these are not all the hacking methods and exploiting instruments that have been evaluated in here. There are many different methods of hacking in today’s cyber world and cyberspace, where these methods evolve over the time and is changed parallel to the advancement of technology and the integrity of the communication and information systems. The methods which have evaluated and analyzed here are usually the methods that the cyber world has suffered and experienced up to meantime. They have been brought here as examples of cyber threats which commonly is threatened our future virtual safety.

# CHAPTER 3. PROPOSAL SOLUTIONS and STRATEGIES

## 3.1. Cyber Challenges Solution

In concern to the growth of internet users and massive communication devices including smartphones, smart TVs, computers and many other IP based electrical and communication devices, especially, since 2001-2002. When the first mobile telecommunication company Afghan Wireless telecommunication Company (AWCC) is substituted instead of traditional wired communication systems into telecommunication market in Afghanistan as a legal communication company for providing telecom and communication services. It was not constantly appeared as a secure communication company in minds, the aims of this company were giving GSM services (voice, SMS, and later poor data transaction), whatever, connecting urban and non-urban areas (cities and rural) to modern communication systems.

During the times, this company connected nearly all of the Afghanistan's provinces though GSM services via using frequency spectrums, but later when the new door of modern communication technologies had been opened, especially, when the ministry of telecommunications and information technology established in 2002. Communications systems started growing in multi-dimensional phases, but parallel to the increasingly growth of the communication and information systems multidimensional risks have also grown, and still increase in a wide range of espionage at large, medium and even small governmental and none government enterprises. Nowadays, millions of devices are connected to World Wide Web WWW through GSM signals and AOFN at all around in Afghanistan that sense good, because this development has brought big changes in a country with traditional and conservative customs and also convey large, medium and small business firms to online services and advertisements for their businesses. In concern to the recent report of MCIT, exhibits the remarkable growth of internet users, indicates that each one would possess at least two smartphones and this might spread in soonest future at all over.

During that time, the people might be faced latency of challenges in terms of security and safety of their personal data. From the security perspective, the large amount of national sensitive data are at risk through widespread distribution and connection of modern devices over the networks, it also might bring big challenges in the future, no one can estimate that how much data might be at risks or will be lost and stolen in behave of such situation.

Insiders, outsiders and international criminal enterprises including interior and foreign malicious groups attempt to penetrate into Afghanistan's sensitive network infrastructure, economic development projects, business firms, and even critical infrastructure through cyberspace to obtain their inaccurate goals. Of course, it might emerge social, economic, health and public services into a battle of digital wars in the next near future. There is multi lack of security experts and IT professionals in the country.

Seriously, public and private sectors might be at risks because the government is not able to support security institutions, training centers and cyber-experts inside and outside of Afghanistan, currently, a few governmental organization by helping of international organizations just try to train IT professionals and cyber-experts for the safety of their own communication and information systems. In connection to projects that MCIT has on hand, same as e-government, m-government and other digital developments projects (Refer to Appendices B.1.) deserve sufficient cyber-security experts and consultants for at least to fulfill the pre-security standard requirements. As we partially reviewed in literature part of this report, from basic networked communication systems and sensitive systems architecture up to critical network infrastructure, many types or strategies including conceptual, theoretical and practical cyber-warfare solutions have been simulated and presented. Indiscriminately, in consideration to the review of cyber-attacks in Afghanistan, indicate the notable cyber-incidents, risks and enormous damageable incidents on current and future cyberspace in this country. Currently, the majority of private and public sectors use traditional documentation and manual systems, exclusively, nearly all of them are safe and they are not under any types of serious cyber-attacks because of manual systems and traditional official documentation, but by upgrading the communication and information systems, automation and computerization or even development of technological projects immerge cyber-functionality performances into higher hazardous cyber-incidents like damages and risks.

However, form the other side, the dysfunctionality of cyber-deterrence also grows up day by day in this country. Certainly the government by cooperation of international organization invests hugely in multiple developments of technological projects. This technological projects are highly automated and connected to the transactional systems in all over, which this advantages, however, heavily depend on variety of communication and information systems, but there are also many disadvantages came out at the expense of security. Primarily, in this part a solution, based on cyber risks and data privacy categorization presented. Generally, the risks which threaten information and communication systems are slightly split up into three types in this report.

Lose of the information (lose because of hacking and cyber-attacks, logical systems failure and physical systems failure or even power failure) count as the significant risks regarding the cyber-security procedures, logical systems interruptions which insiders and outsider (attackers) try to exploit by penetrating into systems through abuse of essence negative patch of information and communication systems. Due to recent reports, there are millions of terabytes of information lose in all over the world because of logical and physical systems failure or even the information which are being hacked in all over the world. There are multinational technology companies who are in charge of providing security instruments and software (Antivirus, Antimalware, firewalls and many other tools) which is not concerned about their performances in this report. In addition, these companies also have some standard roles and definition of security and risks and risks assessments for visualized systems on cyberspace.

In particular review of solutions against an attack especially, DoS and DDoS, mainly two major factor is arguable, one is the prevention of an attack before happing, in this term, examiners, and administrators looking to answer the question that how they can find or define an effective prevention policy to deter an attack before it happens. There are many concepts and models are represented to answer this question, a cloud-based open-flow firewall for mitigation against DDoS attack in smart grid network concept and model is an example of academic presentations [41].

In this paper has proposed a cloud-based model of firewall for mitigation of DDoS attacks in smart grid Advance Metering Infrastructure AMI network, however, in this paper claimed that the proposed cloud-based firewall does not have only the ability of mitigating the effect of DDoS attack it also has the ability to prevent the attacks before it launches. In this concept, a model and a simulation of such firewall within high Volumatic legitimate and illegitimate terrific has also described. Moreover, there many other academic types of research and presentations on international conferences that concerned to answer the above question by designing complex algorithms, mathematical and statistical solutions that could not be discussed here because of limitation.

Computer systems, IP based electrical devices, physical network infrastructures, smartphones, telecommunication and information systems or any other devices which rely on networks are threatened by various kinds of threats. In referring to the cybersecurity, approximately all of the methodologies and solutions that introduced by many Scientifics, have been accepted that such systems are always at risks. Basically, many scholars have modeled, simulated and presented multiple solutions for mitigating the cyber-attack risks, for instance, prevention and even prosecution cyber-strategies. But, practically they are not able to prevent dangerous aggressive cyber-attacks in numerous circumstances. However, plurality of the cyberattacks especially DDoS and DoS are reformed to disrupt and devastate by aggressive efforts, meaning that the hackers try to arrange an attack that targets infrastructures sequentially, in such a situation. Probably the prevention policies similar to firewalls and other security technology tools might be able to prevent the first stage of attack, but absolutely fail to deter the other sequential parts of attack. Therefore, this solution proposed and described in this report by considering to both prevention and deterrence against the cyberattacks.

### 3.1.1. Logical network architecture policy (LNAP)

In this part, on behave of the current and huge possibility of future security risks which are threatened virtual communications and information systems, the exploration of the potential risks of security and subsequently, the proposed solution in considering to the sensitivity of communication networks and network architecture, especially in consideration to AOFN, has presented.

Notwithstanding, this achievement has particularly gotten around the obstacles, based on the sensitivity of information and networks, the new applicable hypothetical and conceptual network structure by the name of Logical Network Architecture Policy LNAP which has shown in Figure 3.1. demonstrated by details. This figure shows two LANs that is configured under internal intranet or Ethernet as an example, in this conceptual architecture policy, however, three secure layers of networks including inbound and outbound gateways simulated, in connection to decrease the security risks.

However, in subcontinents of this part attended about the sorting and sensitivity of network and information by setting up "Curious Packet Tracer CPT", The Curious Packet Tracer, is inspecting all the incoming and outgoing traffic bite by bite. In terms, if any suspicious packets, malicious behaviors, and connections observe at filtering point, then CPT would have to omit, analyze and quarantine or even report them. Basically, this hypothetical architecture proposed hypothetically, but the physical path or connection link also has to be divided into three logical channels.In this proposal many technical issues could be raised simultaneously, the initial problem may be the complexity and miscellaneous of big data classification, how it would be possible to classify big data?

In consideration of this issue and impact of it concerned, regularly, among scientists and politicians, dramatically multi-dimensional mechanisms and techniques for clustering and classifying of data also have been presented. Some traditional mechanisms, like Support Victor Machine (SVM) that calculated as an effective classification method, which tends to map data to a high dimensional space via kernel functions and performs linear classification [42].

Current big data processing tools, like Hadoop [43]. and BigTable [44]. represented to store data in distributed sets and assign calculation components to each set to process data have mainly considered at nearly all of the organization where the tools can handle large-scale data, the large amount of them require additional devices or deserve implementation costs.

However, regarding the costs and complexity of data on the dataset and the problem raises because of these traditional methods, some modern solutions and mechanisms also have presented, in involvement to large data classifications such as "Efficient classification method for large dataset" [45]. "efficient clustering algorithm for large databases" [46] "Online training of support vector classifier" [47]. and "Reducing the search space for big data mining for interesting patterns from uncertain data" [48].

Finally the prevailing and applicable big data classification which presented under the title of "Big data classification based on multi-view method" [49]. have simply concentrated on the clustering method with different parameters have applied to simplify the dataset in order to obtain datasets with different information classification of big data overall. As well as, the multi-dimensional application including complex algorithms "Classification Application Based on Mutual Information and Random Forest Method for High Dimensional Data" [50]. a concern in this issue has been developed and represented.

The technical issues have been solved by reviewing proposal and algorithms, but who would classify the information? In facts, in standard data classification strategy, this process runs by the authorized organizational management board. Primarily, these logical channels designed, based on sensitivity and public availability of information and based on, strategies which authorized decision makers to define. In each logical channel, also can be called layer, a particular bunch of transactional information dedicated into a particular network logical channel, each channel or layer is responsible to transfer its own dedicated packets, same as, each logical layer has its own authority to sorts and then transfers the streams of zeros and ones over the network, but, due to security reason before moving from checking points all the packets are being scanned and filtered and then dedicated into a particular channel in concern to the packet's header and footer addresses. For instance, when the data related to secret communication which originates from a secret source must be routed to a secret destination.

In this case, the source and destination are determined by sender and receiver, but probably while the packet transfers over the network, it might encounter multiple devastating (Damages, hack, interruption because of physical systems failure and many other issues that generally happen all around in daily data communication), many solutions already handled to prevent and recover the hacking like encryption, hacking prevention policy and comprehensively standard security policy already defined by many security enterprises.

In addition to, the physical damages or physical systems failure also could be handled by regenerating and supplying of multi backup policies into source and destination, but considerably for transferring such packets, specific route must be established and dedicated for each logical layer of proposed solution (LNAP), until the next packets related to the other layer come over or it is also possible to direct different routes simultaneously by dedicating logical channel over the transaction network. In modern technology and facilities on hands of technologist, many standard broadcast theories have introduced. During the transformation of specific packets in none-simultaneous communications, the possibility of interruption of other packets exclusively must be reduced to zero, because of interferences, collisions and more uniquely because of the reliable transit of secret packets which originates from a defined secure source and transfers toward a secure destination.

In the real world, the sorting and filtering of the transactional packets are possible to be executed on any nodes of the network. This proposal slightly fulfills the internal pre-requirements of security over the network and presented two important factors which are easily doable to recognize new unauthorized connections or packets. Firstly, filtering; how it is possible to filter each packet transfers over the network? Filtering and scanning might cause big challenges in delay and traffic routes or it might slow down the speed of the transactions.

But, it is possible by applying a predefined procedure on the network nodes cyber-deterrence response team is also able to set up this policy (An imaginary hypothetical Logical Network Architecture Policy LNAP proposed in this report) on each node of the network. There is two significant complexity in scanning and filtering. Firstly, recognize malicious packets and suspicious transactional data is not that much easy? Probably, filtering deserves more resources and absolutely decrease the load of traffics over the network, and no one wants to slow down the network traffics in direction of looking up for malware or malicious packets. Commonly, by using current technologies and facilities, it can be overcome.

There are many technology companies demonstrated modern hardware/software combinations that can scan and filter the packets bite by bite over the networks. Basically, the scanning and filtering can be run fast as the electromagnetic pulse moves over without having the latency of routes or delay. However, in this case, prediction of malicious packets easily can be marked by reading the header, footer and deserved channel of packets including the packets source and destination address, these attributes help to recognize the malicious packets properly without speeding down the traffic, where the suspicious packets also can be omitted before drop in into networks or channels.

Another, problem that might be raised, is the privacy of transactional packets, because no one wants, either the government or even the Internet Service Provider ISPs break down their privacy by reading and/or changing the transactional packets on network nodes. This problem also easily can be solved by implementing and defining the privacy roles in the design of LNAP.

It would not be searching for a specific word, keywords, and tags, consequently, LNAP would be looking forward to finding the specific property on the header, footer, source and destination of packets to check if there are a predestined sample of bite that predicate malicious or suspicious packets movements and attack malware. From the other side, it is also possible to LNAP to looking for signatures of transactional packets. If a suspicious packets found then, then it could be just dropped the suspicious packets, dump them into cyber oblivion, as well as, such suspicious packets could be quarantine for next review and even report then to cyber-deterrence response team for review and even it could be left aside to be analyzed in the next inspection.

Secondly, controlling and monitoring of data and even traffic easily can be performed, suspicious packets, abnormal network traffic and any kinds of kinetic cyber-attacks are possible to be handled on transactional network nodes. In addition to protecting the network, sorting of the transactional packets conducts them into a secure preserved logical channel which helps the network maintainers in deeper action. Indeed, generally, there are some key attributes on network nodes and gateways in concern to disruption attacks, when an emergency offensive cyber-attacks especially denial of service or distributed denial of service performs, the below listed changes over the transmission network nodes easily could be the monitor.

a. The balance of traffic loads alternatively changes in each pule of time, and the electromagnetic transactions which are named terabytes continuously shown different indicator graphs per second at all over the network's nodes. Probably, indicator graph shows the high increase of packets transformation or even high decrease of transformable packets on conductor network nodes.

b. Hosting servers and even back up servers target by malicious injected codes or malware installed on them, in this case, both hosting and back up servers would not be able to establish a session between demanders and servers.

c. Traffic routes originate from unknown sources, alternatively, the routes transfer from different gateways, and the attacks intensifying in each pule of time until exploit the targets.

d. Significantly, above primordial indicators encourage the cyber-incidents response team to prevent or deter the attacks by resorting to their predefined cyber-deterrence policy.

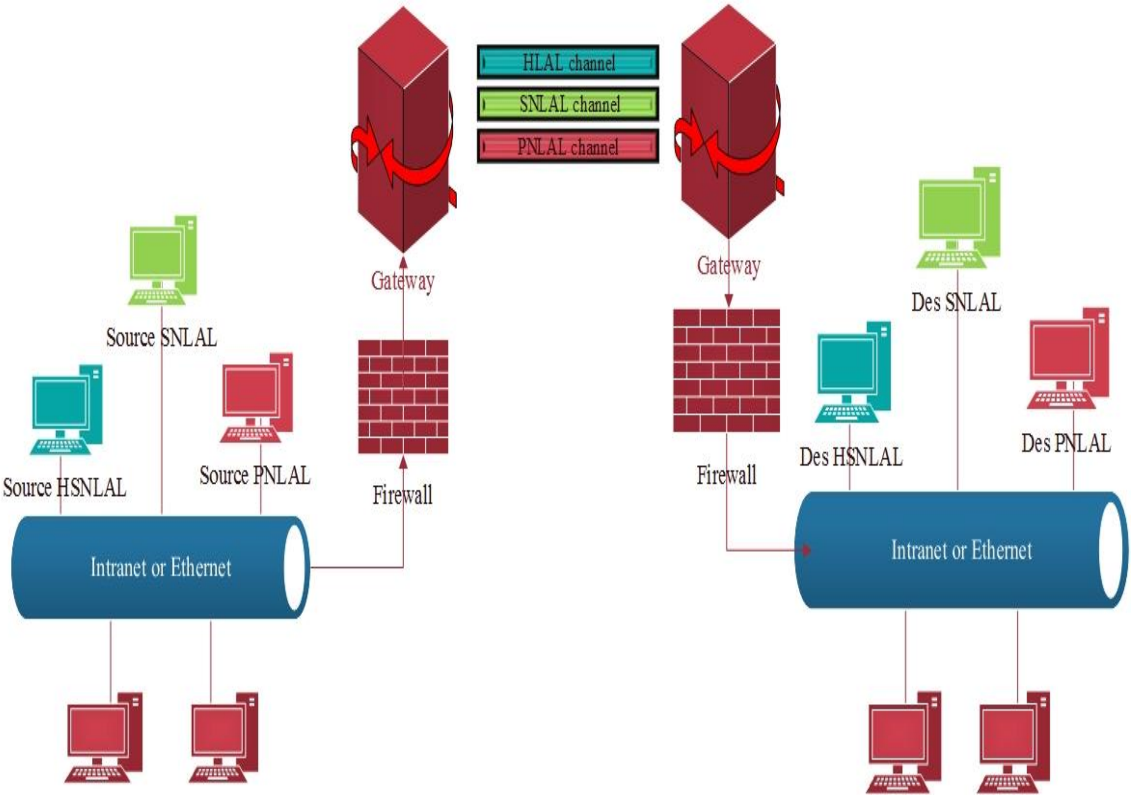


Figure 3.1. Conceptual LNAP architecture under LAN

Consequently, in this scenario we have illustrated the proposal of LNAP solution in terms of offensive cyber-attacks over the network, imagine, there are trillion terabytes streams of ones and zeros inform of electromagnetic pulses drop in from international backbone network per second into Afghanistan's network backbone, a small shock of electrical pulse can disrupt a huge amount of this vital information inside of and/or outside, primarily, these electromagnetic pulses or data are not completely pure and useable, a quarter of half of these data are infected via malicious zeros and ones streams. In this terms, the LNAP is a good and clear solution that intelligently can be executed on main entrance gateways which connect our network backbone to international network backbone.

However, the fact that we deemed all the technological systems are so vulnerable to cyber war also increases crisis instability, as long as our economic and military systems develop, our cyber-enemies constantly increase and slightly the offensive cyber-attacks enforce us into catastrophic cyber vulnerabilities. As the network backbone architecture analyzed previously, our network backbone from land wired connectivity up to aerial connectivity dependently being connected to our neighbor's network backbone.

Moreover, the privacy, privacy of our network backbone including all our sensitive information closed to our way of thinking and understanding of cyber-warriors, currently this space is in our hand, we already started the modernization and virtualization, if no one cares about today's cyber-security, this would be a big deal of our future generation safety. Whatever, the applicable of this proposal is comprehensively possible at each node of network especially, along with AOFN which is distributed and wired at all corner of Afghanistan.

By scanning, filtering and then sorting of information bite by bite at entrance gateways which drop the transactional packets in from international backbone network especially, the data comes from our neighbor’s network backbone, properly any types of suspicious connections, malware, malicious packets can be monitored, handled and annihilated at these gateways. Moreover to threats, the other problem which can be internally handled is inside of Afghanistan. Internally, first of all, the black markets are a big threat in both real world and cyber-space, because there are many electrical devices and cyber tools (Refers to Appendence B.3.) especially cracked software that generally import from our neighbor countries and internationally to black markets, then overall the medium private sectors including all of the governmental organizations use them officially or unofficially. In this terms, absolutely the government is responsible to avoid the distribution of such illegal activities or businesses.

In terms of data classification, by texturing the big aspirations in this field, we understand the nature of data and information classification which is the substantial part of organizational strategies. The processes of classifying and categorizing of strategic data based on organizations procedure concerned the basic step of data classification, and this process defined as fundamental of security.

In addition, data security, risk management, and compliance completely enumerate the coefficients of data classifications. In case of confidentiality, availability and integrity of assets, generally organization labels and tags the data, the tagging and labeling have many advantages and efficiencies for assets such as: searching, sorting and retrieving, however, the data classification uses abundantly as essential policy of most of the national and international corporations and enterprises.

By referring to definition" Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the institutions should that data be disclosed, altered or destroyed without authorization” [51]. which already express the importance of data classification.

Almost, this process carried out over the organization procedures and allocated internally, but what would happen? If the data transfer over the network? Who would access such classified data? And when such data would be transferred?

What about the security measurement while data converted into electromagnetic signals? How many people and important members of organization been suffered because of damages and devastates of the amplified electromagnetic pulse? Based on all these questions a model of network proposed and illustrated previously, and classified as below. The conceptual network categorization has the potential to transfer classified data according to organizations procedures and assets strategies.

### 3.1.2. Public network logical architecture layer (PNLAL)

As an overview to data classification, in fact, assets management and arrangement or data classification is an extremely significant initial principle, procedure, and policy to secure organization's assets, where the process of categorizing of data based on organizations policy and sensitivity of data is called data classification.

It is not far away from the truth, if we say organizational data classification is a few step to our national security because the ordinary goals of cyber-attacks is targeting the assets which stored in large data centers or stored internally into companies internal servers, relatively, this network classification architected based on standard organizational data classification processes.

The main important point of this logical architecture is to connect internal network nodes for transferring a large amount of data publically. As earlier explained simply about this layer of the network, in this layer particularly concerned regarding the flow of information that may or must be opened on public access, the conceptual of this layer has been prepared based on the availability of data that normally have categorized and defined by organizations.

However, the key functionalities of this channel is to transfer data between two peer-to-peer network connection or may broadcast from a single source to public broadcast stations such as: broadcast of radio and television signals and furthermore the services giving by public servers or might transfer the voice, data and text services using on telecommunication companies.

As well as, the information pertains public announcements, advertisements in format of voice, data, audio and/or the information without having any restrictions. By looking up to below functionalities explains more accurately the processes of scanning, filtering and transferring of the data over the network.

In addition, this logical channel that supports the public network connectivity can participate in three key elements of public services, the first one is managing the public internal network connectivity in all around the country.

Secondly, the transaction of data over the network to give access to users for connecting to public governmental and private services, and the last one is connectivity of AOFN to private sectors network infrastructure to be receiving m-government services and service deliveries, which would be provided by telecommunication companies. This task is one of the significant responsibility of this channel.

a. Labeling and classification of data are possible to define by organizations who make the decisions regarding the sensitivity of data to be shared publically or not.
b. "Curious Packets Tracer" CPT reads the labels of packets, evaluates the source and distention of data and then marks as the suspicious or non-suspicious packet.
c. Access nodes which are in charge of scanning the data comprehensively scan the data based on the marked labels.
d. Once the packet's label been read by "Curious Packet Tracer" CPT then data ought to be filtered or redirected to this channel for transferring to the destination.
e. Suspicious packets ought to be quarantined, reported or be omitted on access node which CPT been installed.
f. Finally, CPT marks the packets as public availability and then direct them to public accessibility channels or PNLAL.

### 3.1.3. Secret network logical architecture layer (SNLAL)

According to earlier argues, sensitivity of this logical layer is more valuable in terms of data and information communication, basically the logic of this layer has designed to transfer sensitive information according to strategic definition which organizations concern sensitively on them, and the logic of layer has potential of secret data transmission among large development national and international companies such as industrial companies, transportation company except public shared information, production companies, health insurance and services, institutional and educational organizations, agricultural and many other development companies that play important roles on national developments. Based on this architecture the only data would be possible to transfers from this layer which are frequently shared among large development companies, industrial manufactures companies and many other national private and public organizations about large development plans, procedures and strategies.

In consider to data volubility and its significances, in this terms, however, the data classification would be concluded by higher management board of such development private and public companies or it may also possible that the government directly involve in decision making to most of the data classifications. Of course, all of the companies have their own "Corporate Policy and Procedure Manual" and data classification based on their own processes, but here, the discussion concerned to transmission of information over the network. Commonly, below functionalities considered as the primary initialization of packets.

a. Labeling and classification of data are might be defined by organizations who plans and decide regarding the sensitivity of data to be shared among the development companies, institutional organizations, health services or shortly label the sensitivity of data as secret, generally such data probably contains plans, development strategies, and many other sensitive data might be possible.

b. "Curious Packets Tracer" CPT reads the labels of packets, evaluates the source and distention of data and then marks as the suspicious or non-suspicious packet, in case, if the data labeled as non-suspicious then CPT dedicates the transfer channels based on label and attributes of packets.
c. Access nodes which are in charge of scanning the data comprehensively scan the data based on the marked labels.
d. Once the packet's label been read by "Curious Packet Tracer" CPT then data ought to be filtered or redirected to dedicated channel for transmission.
e. Suspicious packets ought to be quarantined, reported or be omitted on access node which CPT been installed on.
f. Finally, the CPT marks the sensitivity of packets as secret or marks to not be on public availability and then direct them to secret accessibility channels or SNLAL.

#### 3.1.4. High-secret network logical architecture layer (HNLAL)

National security risk management, legal discoveries and compliances, national security issues and challenges, national political and economic decision making embracing national strategies, international relations circumstances high secret importance plans, large investment  in charge of national development, military and national conceal security, highly sensitive data regarding the critical systems and significantly high secret information would be transmitted by using this channel. The functionalities involve in this layer highly criticized. The logic of this channel deserves to neither unauthorized persons and nor suspicious packets intruders to be involved on both communications and internal data categorizations, classifications procedures, highly secret administratively authorized governments or private consortiums and high level of organization administrators plan and classify the data based on sensitivity and critical availability.

a. Labeling and classification of data are possible to be defined by organizations who plan and decide regarding the sensitivity of data to be shared among the development companies, institutional organizations, health services or shortly label the sensitivity of data as secret, generally such data probably contains plans, development strategies, and many other sensitive data might be possible.

b. "Curious Packets Tracer" CPT reads the labels of packets, evaluates the source and distention of data and then marks as the suspicious or non-suspicious packet, in case, if the data labeled as non-suspicious then CPT dedicates the transfer channels based on label and attributes of packets.
c. Access nodes which are in charge of scanning the data comprehensively scan the data based on the marked labels.
d. Once the packet's label been read by "Curious Packet Tracer" CPT then data ought to be filtered or redirected to dedicated channel for transmission.
e. Suspicious packets ought to be quarantined, reported or be omitted on access node which CPT been installed on.
f. Finally, the CPT marks the sensitivity of packets as secret or marks to not be on public availability and then direct them to high secret accessibility channels or HSNLAL.

### 3.2. Scenario of Cyber Threats

As large numbers of organizations concern about cloud computing and its advantages for their information storage to safe assets, primarily, because of cyber-threats (cyber-attacks and cyber-exploit that are carry through DDoS and DoS), further from the other side, the reliance of computer and information systems intensify on networks and remote systems, thus, security interests move to the forefront of modern communication and information systems. In referring to our previous arguments about the Denial of Service DoS and Distributed Denial of Service DDoS, these two types of attacks enumerate as the dangerous attacks that threaten remote control, information and computer systems, anyhow, these attacks intend to cease the undertaking operations on the target systems.

On the other hand, newly virtualization of networks like software defines network has introduced for intensifying the packets transition over the networks, where one of the newest targets of the DDoS and DoS is software define network [52], in modern communication systems, there are many solutions presented concern to three phases (Recognition, Prevention, and Deterrence) to deter such kinds of attacks [53], such as: Neural network intelligent algorithms and many other complex algorithms designed in this area to mitigate or at least decrease the risks of the threats. Particularly, the DDoS attacks probably constitute and contribute in the form of unexpectedly low network performance, slowness in access to websites, cuts in networks connections, increase in the number of spam e-mails or inability to access certain parts of a website [54]. As well as, the deep packet inspection concepts in considering to the deterrence of DDoS [55]. and also many other conservation methods in this terms have presented up to now. In this paper, a specific kind of attack called denial of service DoS designed, based on an imaginary scenario, outstandingly, based on communication which is provided through AOFN, as we also review the network architecture of Afghanistan Optical Fiber Network AOFN, its distribution to all across the country and probability spreads to all corner of the cities and rural areas in Afghanistan. In this imaginary scenario, considered about a company (can be a public company or a private company), and cyber-security of this company which has three important branches located in Kabul, Mazar-i-Sharif and Kandahar (The three popular cities including that the Two provinces Mazar and Kandahar are the commercial ports which valuable amount of the commercial and business goods export and import by passing these two border provinces) have evaluated.

The main goal of the hosting company is protections of the three servers including the backup server which is set up in large cities, however, these sever have configured under a wide area network by managing of one switch. The only security layer that the company has considered is installing of a firewall excluding of Antivirus on personal employees computers. The firewall has installed in Bamyan Province (This province is the central province the company has set upped firewall) due to low costs and also this province plays a central role for the company in terms of security challenges. In addition, the company has multiple agencies at all around of Afghanistan, but its main servers are located at these three provinces shown on figures in part 3.4 of this report. However, this company has three servers specifically, in Kabul, Mazar-e-Sharif, and Kandahar by having below compatibilities and geographical locations.

a. The server located in Kabul (Capital of Afghanistan) called central server or in short Kabul-Server or even can be called shorter Kab-Server. This server has the much operating application installed on it and has the important central high operability for giving service to customers. Additionally, another server which plays the backup roles has also set up and configured in this provinces under the same network.

b. The second server which also has the operating application installed located in Mazar-e-Sharif called MeS-Server. Half of the AOFN hyper connectivity links passing from this city and connects Afghanistan's internal networks to central Asian countries backbones such as Tajikistan, Uzbekistan, and Turkmenistan and significantly it has direct connectivity links to Russia.

c. And finally, the third server which is located in Kandahar is one of the famous city and also estimates as one of the important commercial ports, as well as, the AOFN connects internal networks to international backbone network by passing this city and connecting the southern network infrastructure to Pakistan’s network backbone, this server would be called Kandahar server of in short Kand-Server.

There are many application and operating software installed on these servers for giving service to customers and company’s stallholders internally and externally. Attackers especially, cyber-sniffers designed an inappropriate and malicious goal to target the central server which located in Kabul by using Denial of Service DoS attack.

There are many attributes regarding these networked servers as below that can be outlined as significant notifications, by referring back in solution part 3.1, there are approximately more than six entrance gateways and more than two central gateways have assumed, but as sample the links that connect two entrance gateway and one central gate have concerned and simulated in this conceptual and imaginary scenario.

1. Servers located in different cities probably shared many resources such as processing the tasks, shared processors, hosting services and it is also possible that these three servers being configured as cluster systems or even distributed systems for interoperations under a shared network.

2. These provinces have been selected because, firstly, they are business attractive cities the internal and external companies have business branches in these cities, secondly, in addition, that Kabul is capital of Afghanistan, the well-known commercial companies, and official agencies are located in this city, and finally, Kandahar and Mazar-e-Sharif connects AOFN to international backbone and also these two provinces calculate as the border and commercial important ports cities in Afghanistan.

3. Third of the servers have connected under the Afghan Fiber Optic Network AOFN which is one of the high-speed network providers in Afghanistan.
4. Hosting services might be hosted internally or it might be possible to configure in intention to external hosting. In conclusion, third of servers might be used as backup servers to each other for both internal and external hosting services.
5. The critical role of the Kabul server is computing the central services capabilities and mainly plays the considerable role to control the other server located in Mazar-e-Sharif and Kandahar and also takes backup for maintains.
6. The Mazar-e-Sharif's server is responsible to share its resources with servers which are located in Kabul and Kandahar, additionally, this server is also physically connected to external backbone network via internal connectivity links of AOFN to central Asian countries.
7. Same as Mazar-e-Sharif server, the Kandahar server's resources have to be shared among Kandahar, Mazar-e-Sharif and Kabul servers, this server hosts the web

contains and also being connected to international backbone infrastructure via entrance gateway which is connected to Iran network backbone.

8. Based on this imaginary scenario, three important gateways also configured, into three important provinces, the gateway which is located in Herat (Is a border province connects eastern Afghanistan network infrastructure to Iran’s network backbone), pretty near, the Kabul servers getting service and being configured under Herat gateway, where the Kandahar server which set upped under the entrance border gateway, same as the Kandahar’s server and Mazar-e-Sharif’s server also benefits from internal and international connectivity links under border gateways because of their geographical locations.

As reviewed previously, A Denial of Service DoS attack is a kind of attacks or being executed by a group of attacks (Such as: Military cyber performing groups, international groups of attacks executers and specifically, in Afghanistan national harassment cyber groups that already carried out and arranged cyber-attacks many times) in which attackers attempt to get access to network fundamentals and data applications layer to make the applications out of reach of those who are allowed to use them. DoS attacks cause a challengeable disruption to the machine's service in the network and are costly requires high bandwidth, it can be created or done through many techniques, for instance, the familiar techniques that can be used and generally uses on database systems is the systems overflows, in this technique attackers attempt to overflow the systems by getting access to resources and/or assaulting the target systems to occupy the resource of systems such as memory, central unit processor CPU, and other resources which the servers are being ceased by DoS attacks and they are not able to give access to authorized users [56].

Additionally, DoS attacks are often concluded as a big threat to many organizations, and the hidden motivation could be behind the DoS attacks, as well as this kind of attacks, often linked to inappropriate schemes being adopted by organizations. In this terms, attackers continue the repeated attacks to stop the servers until the victims respond to the attacker's inappropriate demands, or sometimes these attacks can perform in many other spots such as cease of the information systems, espionages revealing the cyber-powers, maneuvering national cyber-powers or many other reasons.

### 3.3. Model and Simulation of Threats

By referring to the precedent scenario and its property that illustrated. In this scenario, three branches of a company which are located in Herat, Kabul, and Mazar-e-Sharif explained by details, commonly, disruptions and devastations of victim systems directly depend on the type of attacks and victim technologies including the software and software types they use in their systems.

As we reviewed in chapter two the different types of attacks that cause multi-dimensional difficulties. Particularly, the simulation of an unintentional DoS cyber-attacks would be simulated based on particular input data and antecedent scenario in part 3.2. then the results will also be evaluated in part 3.4. In this simulation an unintentional DoS attack which placed on one of the company's branches (No matter that the company is a private or it can be a public company for giving social services) will have been considered, the attacker enthusiastically attempts to disable large, sensitive and critical systems by DDoS and DoS, where a specific type (DoS) has been selected to be simulated, inclusively, the models of cyber-threats and proposed solution models are discussed in this part.

#### 3.3.1. A model of attacks

Proceeding to modulation of the cyber-threat and its direct impressiveness helps to develop further step that is called simulation, as far as, a model underline the common literature of cyber-threats in general and understanding of the inefficiency and effectiveness of cyber-attacks on network infrastructure in particular, in terms of network-based communication systems. The nature of a model express the efficiency of an effect, for instance in Software Life Cycle SLC, the theory of a model present the gaps between software and problems, through the use of models software engineers reconnaissance the issues then represent the issue into through a model to mitigate and evaluate all the problems.

In referring to a specific definition of a model “A model is an abstraction of some aspect of an existing or planned system. Models are created to serve particular purposes, for example, to present a human-understandable description of some aspect of a system or to present information in a form that can be mechanically analyzed” [57]. explore mainly two important aspects, firstly, the understanding of problems are much easier, when the issues are represented in the models. Secondly, a model helps us to analyze and evaluate technical problems of the systems are not understandable for the human.

Based on this definition, the basic concepts of a model discussed here in general and the concepts of models being implemented and customized according to our problem in particular. Many Scholars, Professionals, and Scientifics tried to define the models and then present them into maturity framework in entanglement to cyber-security and challenges that are mentioned somehow in literature part of this report, but, to explore technically the models of cyber-attacks, cyber-risks and solutions in contrast to cyber-attacks some of them also inspected here, however, at the end by inspiration and adaptation from such standard definition and presented models, a model of threat in consistency to our previous scenario has circumscribed and holistically operation of a specific types of cyber-attack drawn on Figure 3.2.

In normal communication between a user for receiving service and a server for giving servers, the user sends session properties request to the server for authentication, then the server controls the user's property either it is valid or not.

In case, the server determines authentication of a user by validating its property, if the demanded property of users verified by the server then it allows and authorizes the user for servicing, otherwise the connection fails between users and servers. DDoS and DoS attack actually interference within authentication and authorization processes between a server and a user. In pursuance of authentication and authorization processes Figure 3.2. explains a simple interruption series of attacks in form of DDoS and DoS, however, the impressiveness effect of DDoS and DoS on a model describes that when a valid user attempts to access the server, then the servers validate and authenticate users. Almost entirely, when servers reply to user's requests by sending acknowledgments. In normal communication, the session between users and servers establish when both sides confirm the requests and acknowledgments, what the attacks inference here is the interruption of acknowledgment meaning that because of attack interruption the user is not able to receive the acknowledgment which being sent by servers.

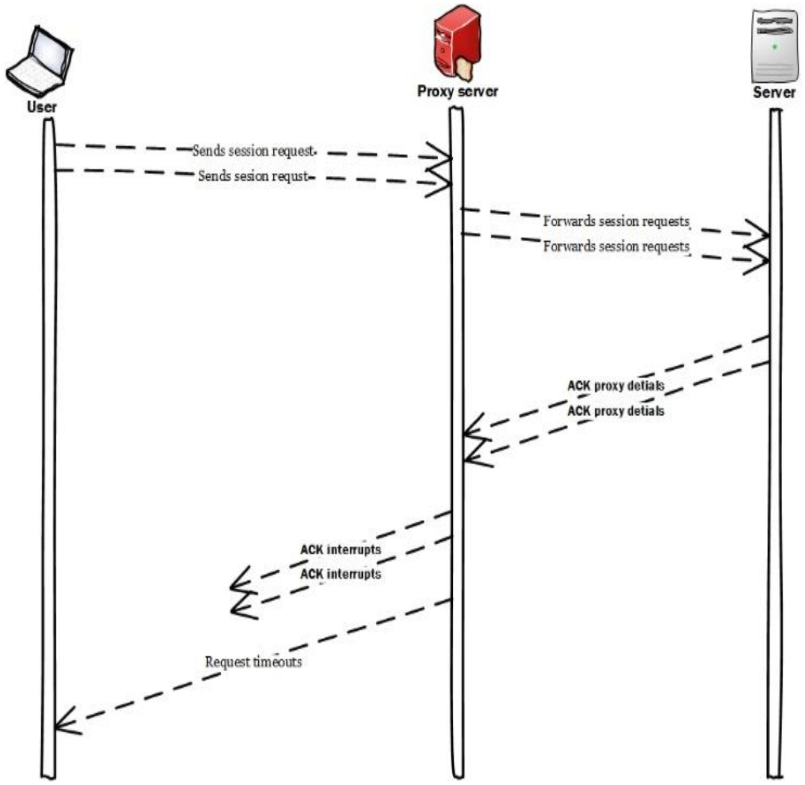


Figure 3.2. Effect of DDoS and DoS on network infrastructure

### 3.3.2. Models of proposal security solution

In Software Life Cycle SLC theory, the threat modeling is a structured approach that enables the application developers and maintainers to recognize, quantify, and address the security risks associated with an application, however, the huge amount of risks raise because of software and application difficulties on cyberspace. From the other side, today the main focus of programmers is on software and application risks, as we already know that the cyberspace is a space rely on applications and information systems which the security on cyberspace directly depends on the security of information systems and applications. What a significant roles being played by a model is to present the risk gaps between coding of an application and application developer [58].

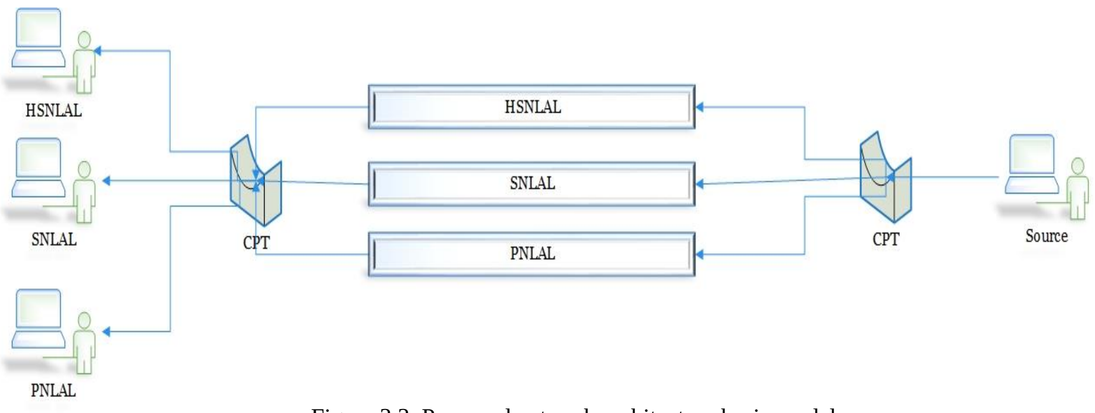


Figure 3.3. Proposed network architecture basic model

According to this theory and proposed solution, hereafter has been tried to obtain an ideal model of threat solution on cyberspace and then evaluated the model by showing a flowchart of this ideal model, comprehensively, the theory of modeling and simulation has a widespread of scope and defined specifically for each system based on system's requirements. In general, this ideal model has been obtained by adopting the definitions and widespread of the theory of modeling that has explained in this regard. Beforehand on a basic model the effect of DDoS and DoS presented, in fact, the anterior model collaborates to design the main proposal solution models in contrast to cyberattacks in this part, by referring to part 2.1. and its sub-tittles this model has combined from three important schemed network layers, as already shown on Figure 3.4. but technically Figure 3.3. has shown the basic model of three proposed network architecture and Figure 3.4. is presented the logic flow of proposed network architecture. In fact, both of them engaging practical experiences and enabled to provide evidence of basic network architecture which has been urged earlier in this report.  This model has presented in order to reduce the complexity conducted to our earlier proposal security solution.

### 3.3.3. Threat types and a model of risks assessment

Threats refer to the source of the vulnerability on victim systems in devastation and damages determinations (risks) that rely on cyberspace, but a model of threat refers to the gaps between disruptions and human interface. Threats or expressly the cyber-threats are not only considered to the vulnerabilities and damages carrying on by cyber-attacks, the threats represent a general meaning, means that the practically the threats always exist, whether a cyber-attack occurs or not.

Threat and vulnerability are not even two synonyms words, in most cases, these two words are often mistaken in meaning in act of cyber-attack. To understand the exact meaning of these vocabularies that generally result from the big risks, a simple scenario has supposed to expresses superlatively.

Living in a beautiful vocational house without any defects and problems is nice and appreciable for everyone; assume that living in such a house that everything has managed built properly at an awesome vocational location which most people buy such houses for their vocations especially for living in the summer and Christmas.

The house estimations and engineering calculated precisely against natural pests and incidents such as resistance to earthquakes seasonal and monsoon storms including flowing daily normal wind and calculation of lateral and side loads that coming from each direction on house. Same as the inside of the house equipped by modem power source systems for clarity and in any country they use electricity for cooking by having a high secure electrical protection systems and backup power sources.

In case of power outages, pipeline (water supply systems and sewage systems), heating and air condition systems or even in modern engineering, civil engineers and construction professionals by try to use the modem smart sensors for cooling and heating systems on intelligent building.

As well as, the high resistance PVC windows, standard electrical and mechanical gateways and doors, event alarms and fire alarm systems including many other facilities and equipment that are normally set up on the residential building are accomplished accurately. Additionally, all the rooms, halls and kitchens inside of this house are connected to a secure broadband high-speed internet connection, being serviced by a telecommunication company or Internet Service Providers ISP, finally, all the materials like sands, types of cement, plasters, and bricks which are used in this house have tested and confirmed, also the resistance of walls and ceilings evaluated, calculated and done with precision instruments carefully. Now the house is ready for utilization, a rich man buy this house, normally for living without caring to anything else because before buying, he has checked everything that is confirmed by the municipality and he also can see that all stuff work correctly.

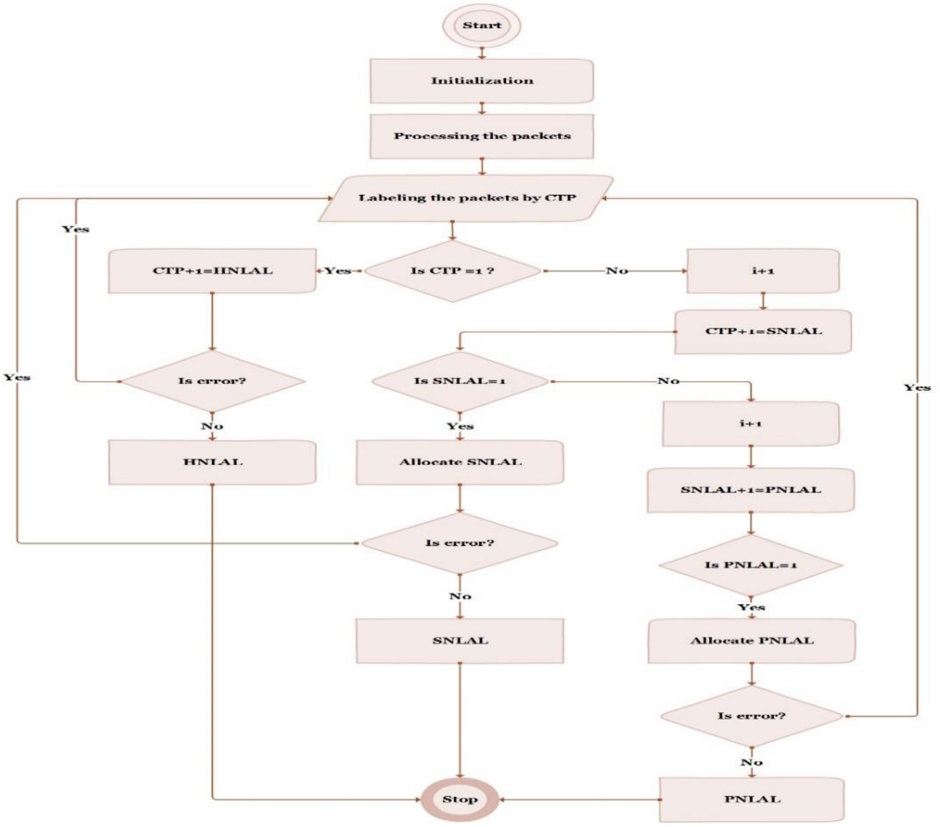


Figure 3.4. Flow of proposed solution

After passing a tedious and boring official day with plenty bargained he had have related to his business, he returned back to home for resting and thinking about his next day that what must be done by tomorrow, by the time of entering to house, he saw the pieces of cropped money that he had put inside of the clothes cabinet long times ago, he noticed that something went wrong. Immediately he walked to check what happen, when he was walking fast, also noticed the pieces of scattered sausages and chopped meat that he had in the kitchen along the way.

a. What you think about the scenario up to now, and what about the result of the scenario its dependency to the subject of our discussion, and the relations of this scenario with cyberspace, cyber-threats, and cyber-security?

b. Do you think the businessman has bought an ideal vocational house without having any shortages or issues, in case, what types of an issue might exist?

c. What about the risks, have you noticed that what kind of risks might exist inside or outside of business man's ideal house? At least, the small risks are cleared a little bit until now.

d. What about the threats, what kind of simple or complicated threats might or might not exist in consider to the engineering of business man's house?
e. In case, if the threats exist what you think about the vulnerability of the house, that the threats can easily penetrate into the house, which typically consequences the risks and big challenges?

To answer the rest of above questions, let's continue the scenario. The businessman quickly got inside of the bedroom and saw that half of his money was torn, he asks himself that how such an unbelievable and strange can happen because he was assured of the security and resistance of house against many natural and non-natural problems. By the time he was thinking, he was eager to rest a little bit, laid down on the bed and turned on the television, meantime the phone rings, he picked up the phone and said: Hello, this is my new home's phone number, how can I help you? The guy on the phone said: Good evening, I am calling from the backup power source of the regional residence houses, as we noticed the rats have penetrated into some of our backup rooms. I have called you to know if you faced the same problem. Then the businessman understood that the rats pierced and havoc his money and eaten half of the sausages in the kitchen, it was interesting for him to know how the rats barged inside? By started looking forward he found that there is a small hole in the kitchen generally related to unused pipeline systems, lets the rats drop themselves inside of the kitchen and spreads out at all corners of the house.

Genuinely, the scenario aimed at conceiving main problems and get clear ideas for the better understanding of three essential and important words (Threat, vulnerability, and risk) to answer the questions and compare with the subjected discussion. Additionally, based on this scenario we have understood the rest of the cyber instruments and tools that how a malware can easily break the security layer of applications and information systems, then penetrate into source of the information,

Fundamentally, in this scenario all the rats calculate as threats that have targeted the kitchen of businessman by trying to pierce the unused pipeline (vulnerability) and then stated devastating and disruption of the business man's kitchen pieces of stuff and his money (risks).

Firstly, the threats always exist anywhere in our daily life like the existence of rats on business man's scenario. Secondly, if the businessman or the house builders were supposed to close the unused hole of the pipeline (that is enumerated as a big vulnerability) accurately in the kitchen then the rats never been able to pierced inside of the kitchen (The mechanism of deterrence or prevention procedure on cyberspace that commonly being supported by technical and strategies in this report refer to part 3.5 for more details).

Same as regarding the holes on software and applications including the neglected point on the hardware of the systems which the applications are installed on them accounted as contemplative and challengeable vulnerabilities. Thirdly, the simple scenario thought us to perceive the basic meaning of risks on application and information systems, once we understand the risks of the systems then, it will be easy to find a good solution for decreasing or mitigating the risks which are mostly being threatened by cyber-threats. Attackers target such vulnerabilities of the information systems, applications and even hardware failure point of the systems to exploit the victim's systems by using many types of attack mechanisms.

Finally, as a result, the phrase "existence and association of vulnerabilities on systems cause cyber-attacks in action or the nature of threats return to system’s vulnerabilities” conclude our discussion on business man’s scenario. In addition to the vulnerability of pipelines in this scenario, there can be many arguable reasons about the pipeline that the rats pierced from. For instance, the pipeline might be broken or corrupted from the fundamental of the house (where most of the software expires and/or needs to be updated, upgraded or even needs to be maintained according to organization requirements and procedures changes, in this case, the application or software needs to be modified or completely substituted by an up to date one).

The other reason, probably the manufacturer of the pipe had not tested the pipes during the construction and production or the raw materials of pipes had had serious problems (As the application and information systems are not architected and produced properly based on organizations requirements). Finally, it might not be necessary to install the pipes in the kitchen (while in production of the applications and information systems there are many unnecessary features that are not used by users or even they are added by developer and system engineers during the production of application based on organization requirements, but momently there is no need to be on information systems anymore). As we already understand the basic meaning and nature of especially two words (Threat and vulnerability), both of these words accepted as threat for modeling in this argumentation Figure 3.5. expresses the threats model, in this model cyber-threats divided into two main parts (cyber-attacks and cyber-exploit), however, the cyber-threats sequences the risks, then the risks might be possible to be reviewed by reviewing the systems fundamental and sources as presented on mentioned figure.

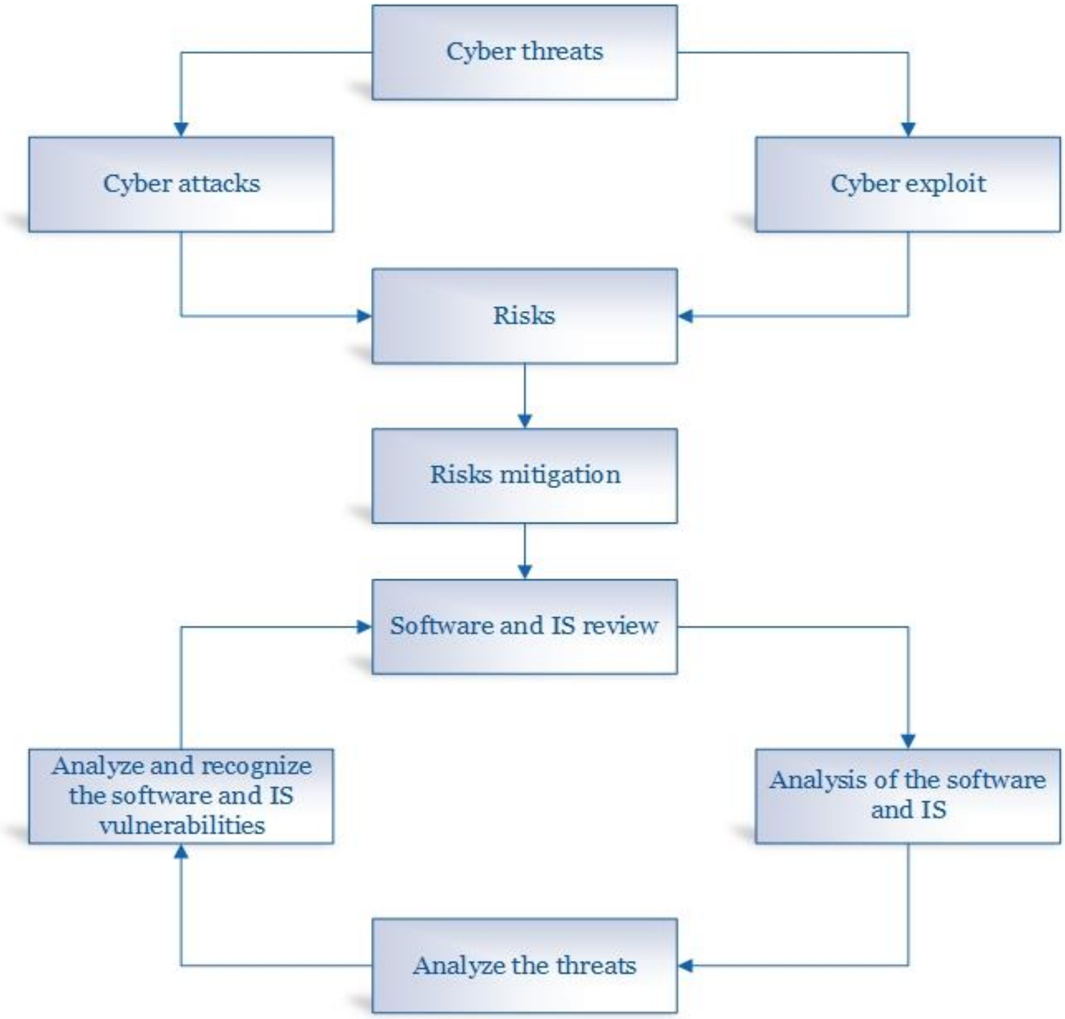


Figure 3.5. Threat types and risks assessment

### 3.4. General Analysis and Simulation of Threats

Analysis and anatomization of the issues to achieve a satisfactory result in fragment of this part are based on two essential pivotal controversies, asseveration of scenario which antecedently described, and the model that is presented in Figure 3.6. Our main focus on this argument is to get the results at three conspicuous notes of the network that route heavy traffic, deter the latency cyber-attacks and consume the resources. This means that we first evaluate the traffic in the gateways, switch, routers and the firewall, and then the main sources of servers or central process unit of the servers. By getting our expectation evaluation at above notes the simulation repercussion will be our desired outcomes.

Nonetheless, the latency cyber-attacks assume to be Denial of Service DoS that is being executed by an outsider of an insider. As cleared on presented model the company's infrastructure has configured under the wide area network being connected through AOFN, same as, the firm's employees personal computers, shared resources, local administrators personal computers are also networked under the same range of the network. The three main gateways (Mazar-e-Sharif, Herat and Kandahar gateways) plays important roles for inbounding and out-bounding data transmission, as well as, the traffic routes from these gateways in general.

Simulation is the other important of part of our discussion where all general routing gateways, company's servers, and firewalls by using an OPNET simulator based on the designed presented model, to deal with risks assessment and understanding of system vulnerabilities. In fact, the model and simulation are the suitable instruments to achieve our arbitrary consequences that are executed through threats. Moreover, the simulation also helps us to demonstrate the results of threat (specifically the cyber-attack in the type of DoS) via displayed graphs and analyzed statistical outcomes of cyber-attacks on the backbone.

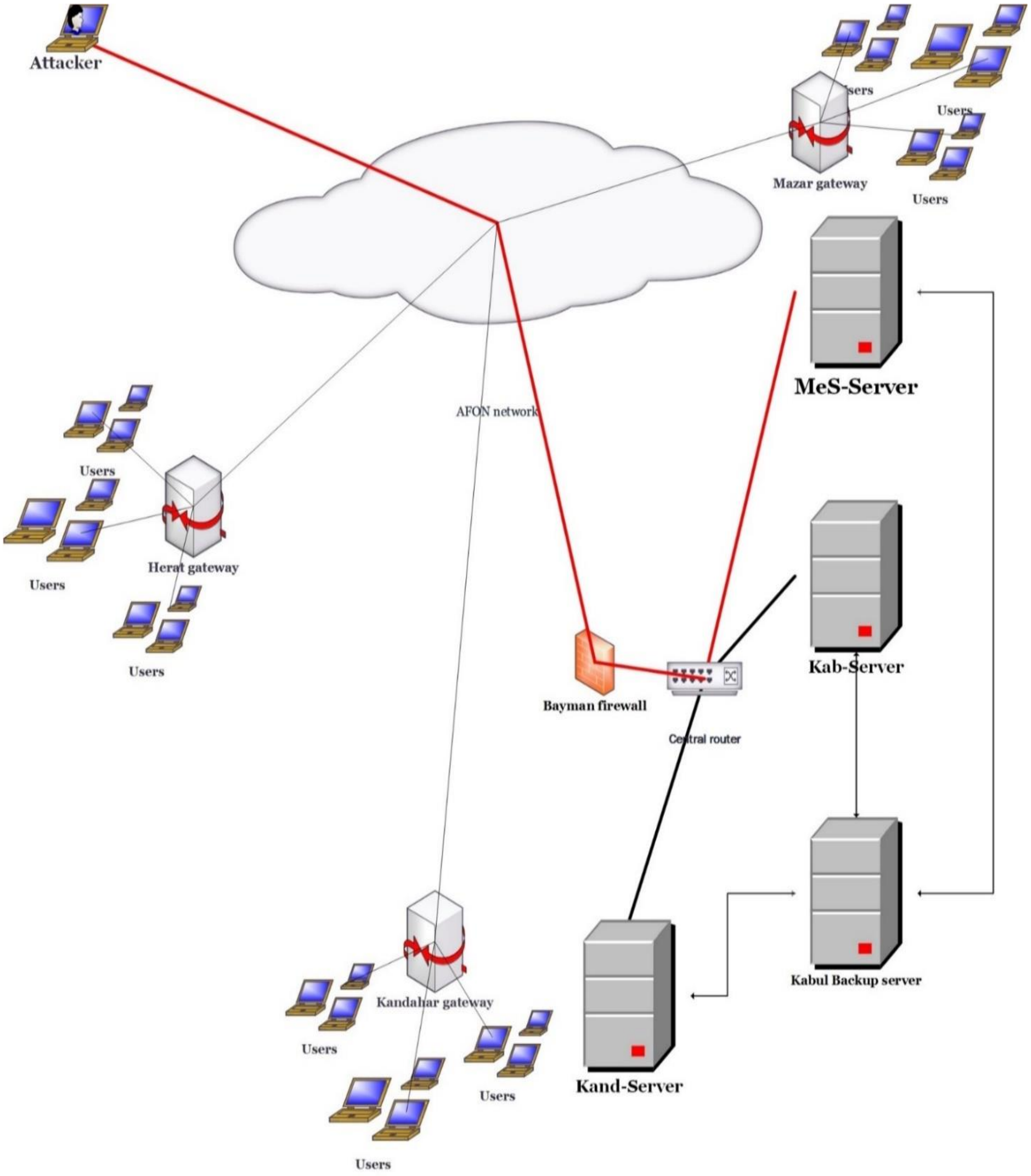


Figure 3.6. A model of enterprise infrastructure under wide area network topology

There are four major parts that are considered in this simulation, firstly attempt to show the cyber-attack via animation which is shown on Figure 3.6. analysis and evaluation of the cyber-attack results and result of the cyber-attack within the different frames of time, or starting and ending times of cyber-attack, displaying the results of the cyber-attack that how much the attacker exploited the resources of the company's servers and network security policy of the organization. The main consideration of the attackers is to penetrate on the source of the system by breaking the security level of firewall, in this scenario, the terrific loads on below three main components of the systems have analyzed.

However, the simulation has run within the specific frame of time for one hour in average, but commonly the simulation of DoS attack has designed for four hours repeatedly attack continuation.

1. Traffic loads (which already have shown on Figure 3.8. and Figure 3.10. on firewall, gateways (Mazar-e-Sharif, Herat and Kandahar) and whole of the network. Generally local domain and users are configured under the local switches and all the servers are installed under a main switch that is called central switch in this scenario. This switch plays an important roles and has protected by a layer of security or firewall, where the hackers successfully takes the control of all these components that are already presented on Figure 3.7. and Figure 3.8.

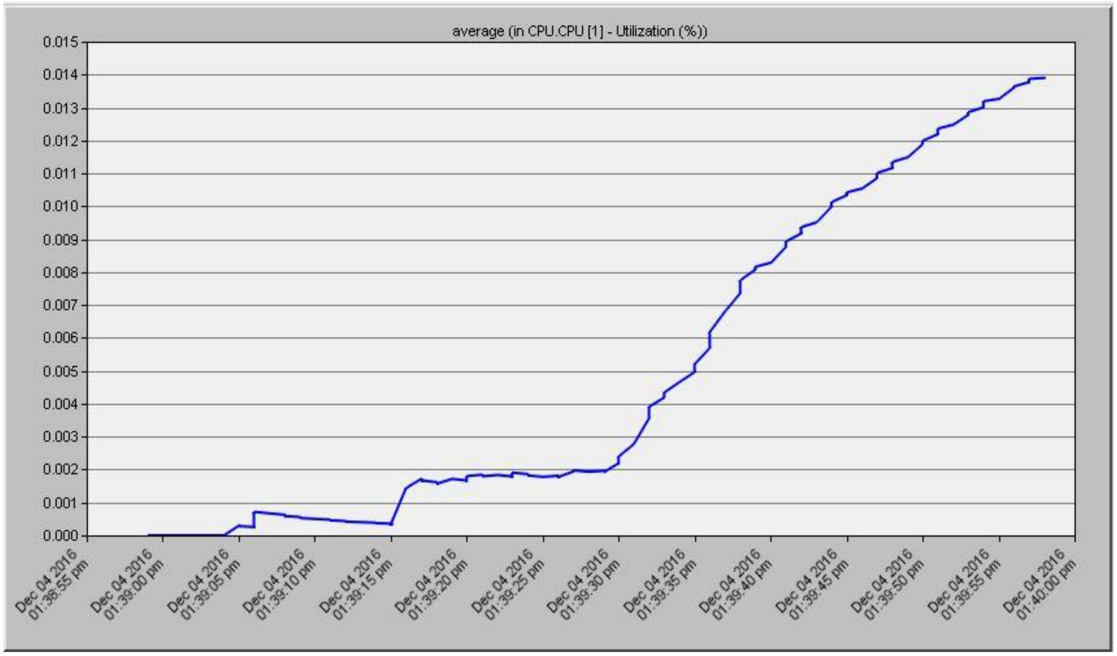


Figure 3.7. Average result of DoS attack on security layer or firewall

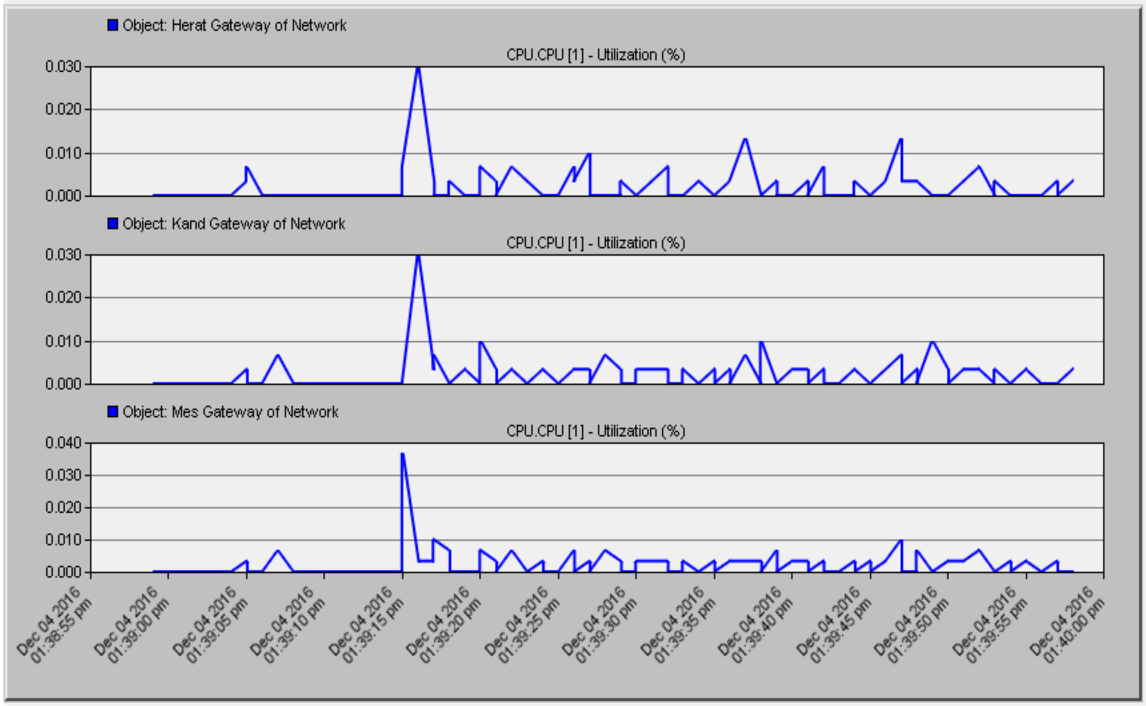


Figure 3.9. Statistics traffic loads on gateways

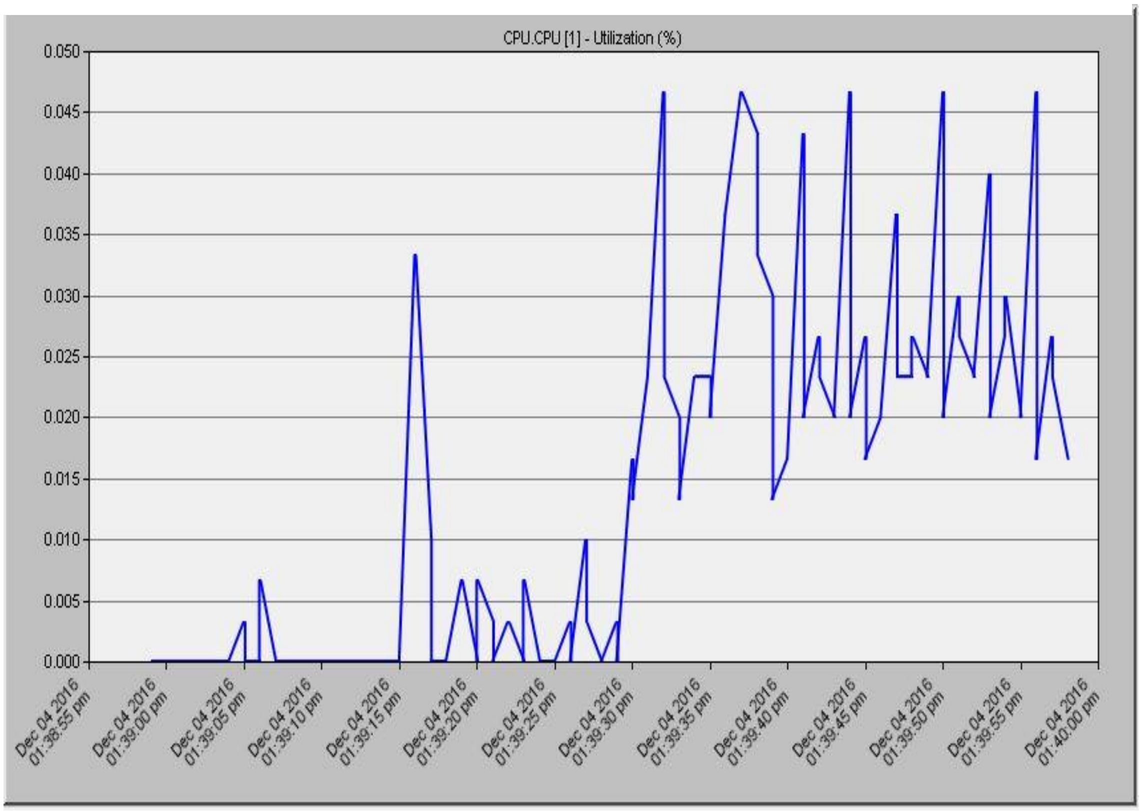


Figure 3.8. Overlaid result of DoS attack on security layer or firewall

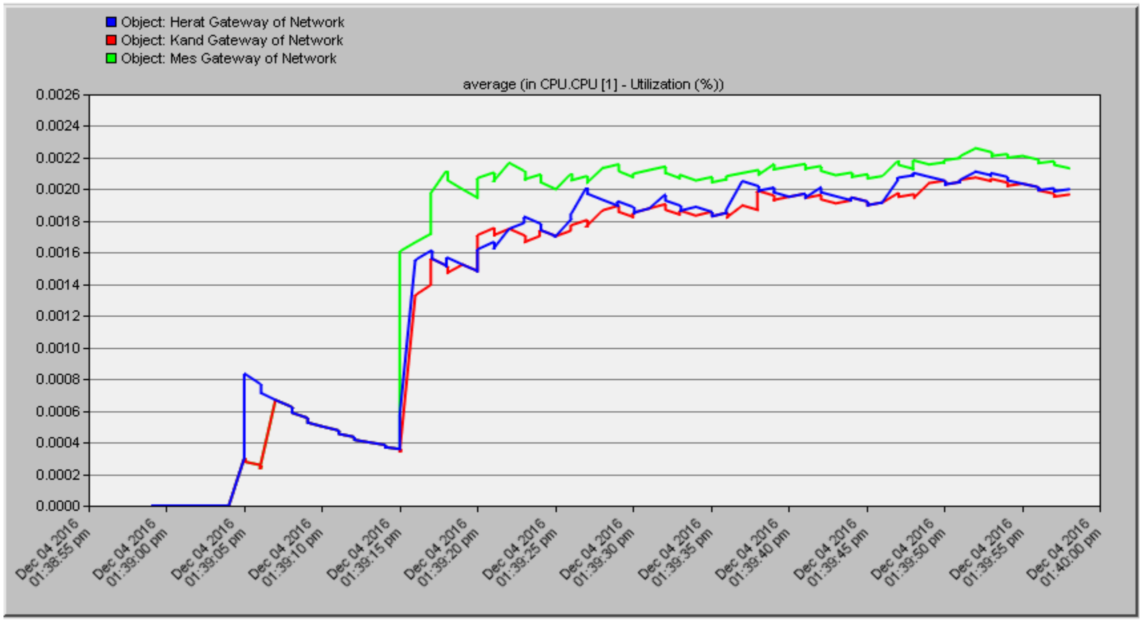


Figure 3.11. Overlaid average results of  traffic loads on gateways

2. The loads on servers especially, on Mes_Server or Mazar-e-Sharif server due to hierarchy attacks of the hacker to get access and control of this server, however, this server is the main target of the attacker. The outcome loads after and before attack are presented on Figure 3.10. and Figure 3.12.

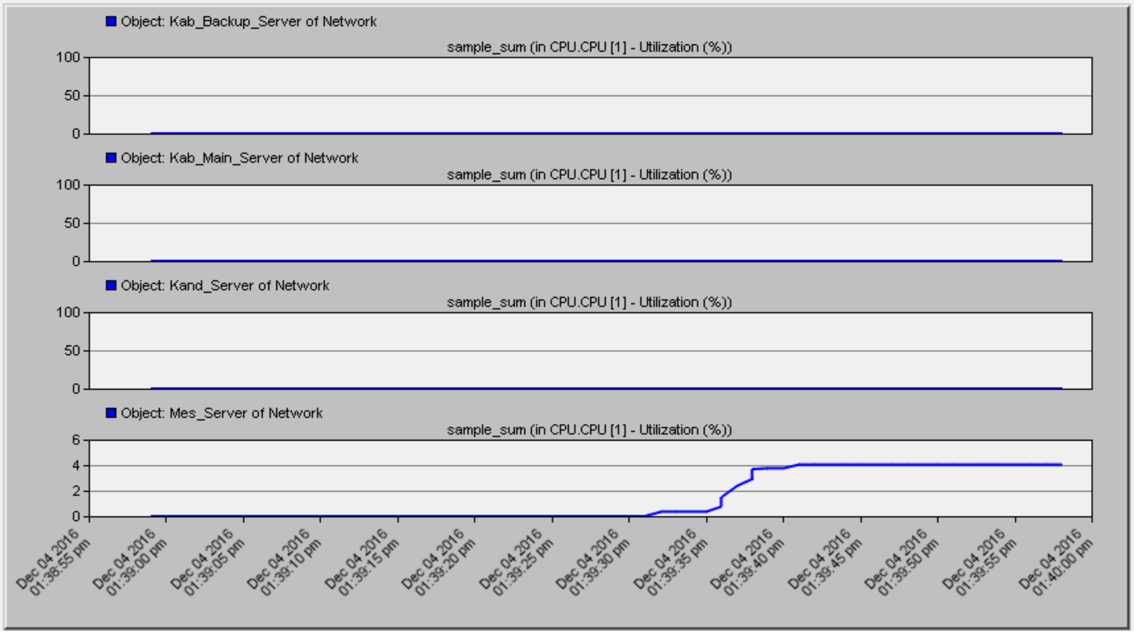


Figure 3.10. Server's CUP utilization at the time attack

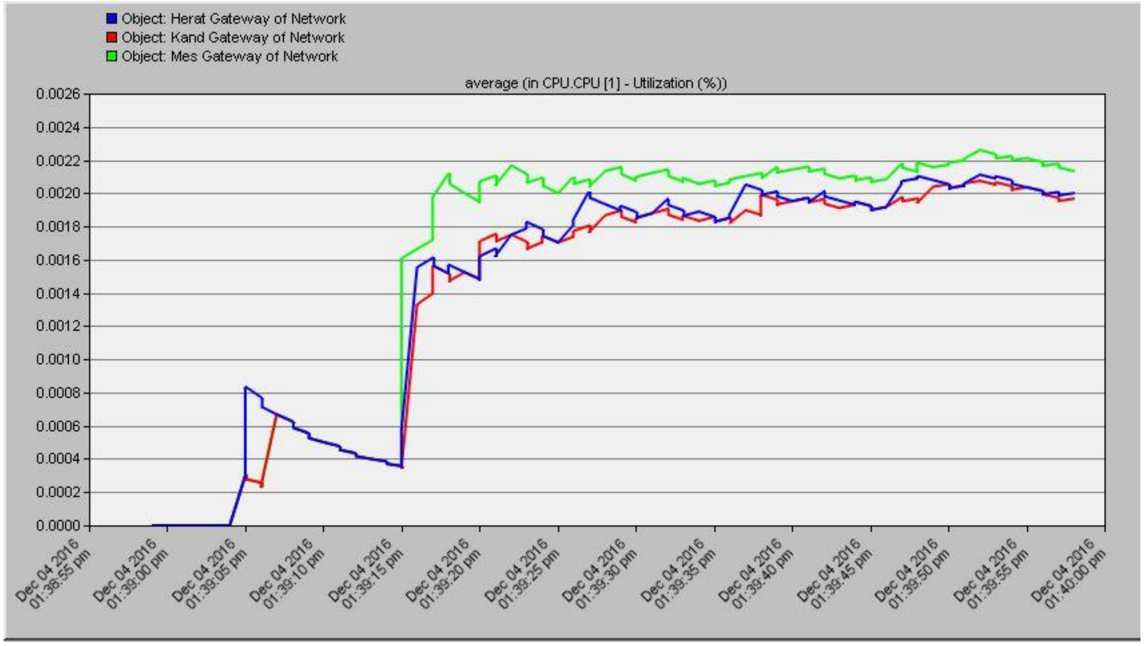


Figure 3.12. Overlaid average of Server's CUP utilization at the time attack

3. The overall results of the other network components and controls includes protocols such as; HTTP, IP and more importantly delay on network including data send/receive or data transmission over the network, which are shown on Figure 3.12., Figure 3.13. and Figure 3.14.

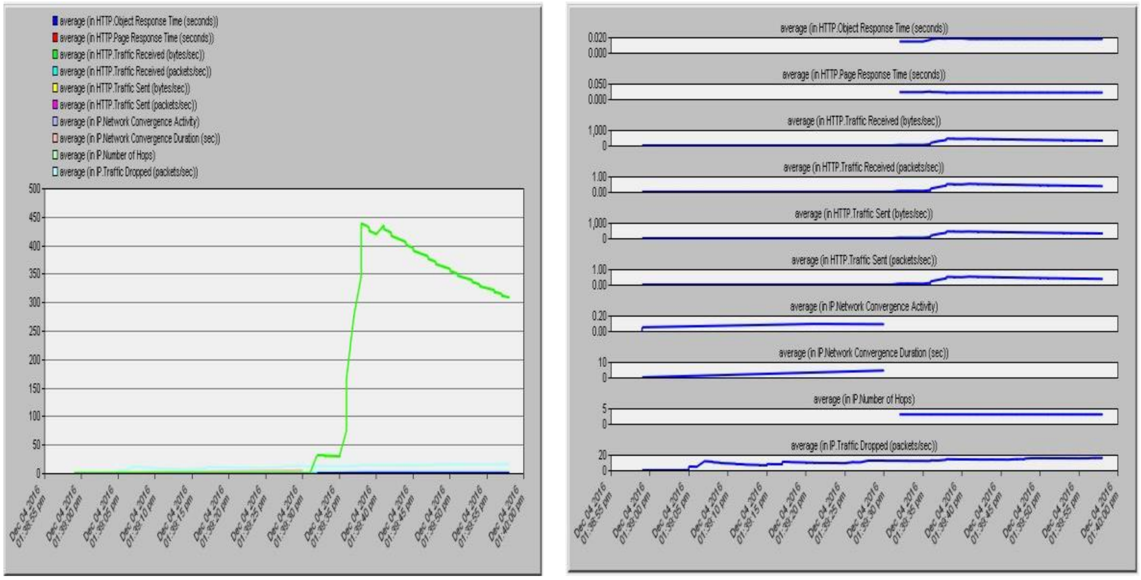


Figure 3.13. Results on HTTP

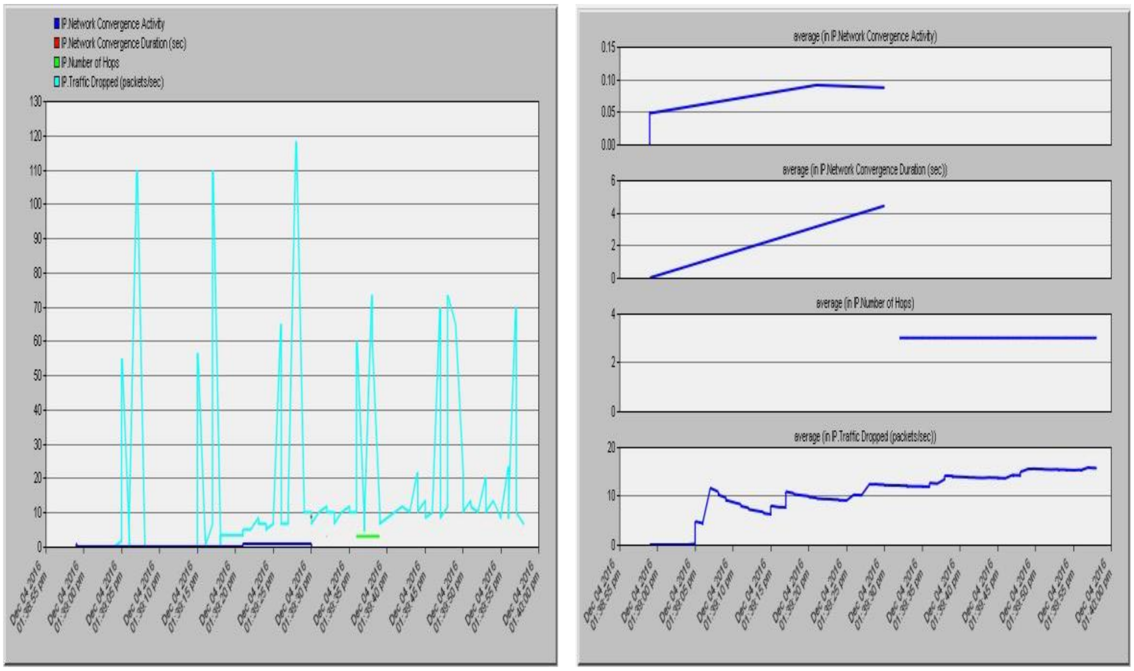


Figure 3.14. Average and Overlaid loads for IPs

## 3.5. Proposal Strategies Concerned to Our National Safety

We talk about a strategy, about the demonstration building to arrange, manage and save our national security comprehensively, our cybersecurity in connection to all of our assets (financial, cultural, semantic, vital and agricultural, although our intellectual property and finally all the assessments that the history has given to us), we save our community, our society, our economics our all of investments by a well-defined strategy. It is not just the matter of cyberspace, a well-defined strategy concludes all of the nation's life and it must be able to incorporate transparently and conspicuously in a large area of different and heterogeneous ecosystem environments in general and security on cyberspace in particular. Nowadays multi difficulties cultivate on cyberspace because of none presence of well-defined cyber plans and strategies.

In the manner of national security procedures a strategy is not exclusively restricted in virtual communications, similarity, it has many concerned, such as inoperability of national government and none government sectors, internal consistency of governmental security and cyber teams, understanding of cyberspace and then cybercrimes, cyber-espionage and publically cyber awareness all could be included in this reference. A strategy has a couple of visages, one the plans related to the development of a society or a nation that generally signs by supreme administration authorities and the other side which can be technically concentrated. Here, the strategy related to both technical and none technical illustrated, but just in concern to cyberspace.

In terms of national cybersecurity and in consideration to the international organization's cyberspace privacy, nations applied demonstrative policies to avoid illegal actions and safe their cyberspace in the past, but our government administration was not able to control internal illegal activity, since 2001 until now. Optimistically, based on investigations, annual reports of World Bank and other suppliers reveal that MCIT invests heavily in development projects, but seems the cyber-security and security challenges newly interacts within Afghanistan and threat fully would be continued in the future. Here are some key performances outlined that already other nations apply to control their cyberspaces and internal cyber-tools challenges. In this part, we concentrated on a strategy intervolving technically or none technically, howsoever, in both cases, the government directly has responsibility to involve any issues threaten national security. In terms of current virtual communication and information systems status, here are some solutions and strategy proposed based on the current Afghanistan’s network architecture, academic journals and proposal of technological projects materials which the government by supporting of international donors working on them.

### 3.5.1. Technical strategies

The strategies that can be proposed and solved based on academic investigations, research, technical instrument developments and specifically technically configuration of electronic instruments in consider to national budgets and resources. There are huge amount of information and sensitive credential being stolen, theft, disrupted and ruined because of unawareness of nations and lack of technical resources. In fact, technical properties of the information systems is one of the consequential factors that can be target by hackers and insiders, hackers easily have access to these properties by reading the instructions of any hardware and software products or electrical instruments. Therefore, the support of internal technicians under a well-defined political strategies with interact of national public and provide sectors including the human intellectual properties and technicians, government would be able to mitigate the virtual risks and threats, whatever, in this aim some strategies have underlined as below that might help to understand basic technical strategies in order to restrict cyber-threats and vulnerabilities on our current and might on our future cyberspaces.

#### 3.5.1.1. Electronic device productions

The production of electronic devices and instruments similar to personal computers including laptop and desktop, smartphones, television, webcams and consequentially the production of electrical chips are the best solutions to keep safe our nation, but unfortunately, this is impossible in our current capacities and inside of our current resources comprising financial budgets and human resources (Coordinators, administrators, technicians, managers, and intellectuals plus talents). Probably our future generation would be succeeded to think about it.

Thus, the electronic chips might have capabilities to set up small electronic tags into them for espionage and tagging when having connected to the network or at least the producers would understand how to breach them and/or how to get access into these chips which have already designed and produced by themselves. What can we do now? Is to prepare an applicable and lawful strategy via allocating sufficient resources for next our generations to save them from threaten in parts.

Additionally, at current technology market, the only responsibility of government is to control these electronic chips exquisitely, with official usages to import particular and secure kinds of them. The chips that set up on shared resources printers, personal computers and embedded systems can be easily breached by executing a simple malware or malicious codes. Or either, assume if a small chip constituted on a shared printer, scanner or copier and it is also possible to design the capability of electrical chips to take a copy from all the secret information, where have been shared among authorized military, national conceal or other secret associations and then send them to its organizers, how much risks would threaten the national assets, no one even can imagine.

#### 3.5.1.2. Aerial bands and frequency spectrum

Primarily the safety of nations is on hand of their government, it is impossible to save a nation without intervolving of the governors and as well as, the safety of government directly depends on the safety of the nations. Regarding to current cyberspace status of Afghanistan, what the government can do is to control all of the aerial space including the frequency spectrum, aerial bands, radio frequencies and other aerial communication systems. Many possibilities could be magnified in terms improper usage of similar aerial communications bands.

The safety of radio, television channels, satellite communications bands, channel bands related to telecommunication service and more importantly the military secret communication systems which embrace the secret strategies of national military, dependently connected to aerial spectrum.

Since 2002, there are many national and international organizations being facilitated by aerial frequency spectrums legally or illegally. During the time hemisphere contact, commonly is an appropriate communication system for internal terrorist groups inside of Afghanistan, however, the restricted range and control of frequency spectrum extremely help to save our national security in both virtual and real world. Of course there are many rules and policies defined by MCIT and ATRA in usage of radio frequency spectrum, but controlling and prosecution seems impossible by having current technology and management board.

### 3.5.1.3. Network security policy

In fact, threats on networks outgrowth the uncountable disruptions in confidentiality, availability, integrity and non-reputation of data in referring to cyber-security, however, implement of the network security policy and standard network protocols is almost compulsory and already applied everywhere. Correspondingly, this terms also being used in network infrastructure and configuration is Afghanistan as well, by referring to this case, MCIT applying multiple version of International Standard Organization ISO, a particular version ISO 27000 and upgrading continuously for more reliable services. But, in communication fundamentals traditional and out of date application cause challenges, where an up to date technical strategy, makes more realistic excitation to our network communities. In connection to network security, standard network security policy has a wide arguable discussion, technical and practical implementation and also it is time consumer that cannot be illustrated in this report comprehensively, but by defining a particular procedure in this terms and an applicable strategy our government would be succeed to safe many parts of our current and future cyberspace. Modern secure facilities such as: Biometric Authentication Systems BAS, Token Authentication Systems, finger print biometric scanner system or Multi Factor Authentication Systems MFAS, Access Control (Role-based Access Control System RACS, Discretionary Access Control DAC and Mandatory Access Control MAC) systems, access remote control authentication systems and Kerberos protocol authentication systems (Refer to Appendence C.1. for more details regarding these systems). Finally data filtering and digital signature all can be considered underneath of standard network security policy, because the implementation of advanced and modern authenticator and authorizer dependently related to network security policy.

### 3.5.1.4. Electronic device acceptable use policy

Acceptable policy in contemplation to cyber-security and cyber-warriors gives common meaning which the nation critically concern in this terms. For instance, the USA, China, Russian even Iran annually approve new policies regarding the use of electronic and electronic devices, especially the devices which are not compatible with their terms and conditions. By registration of electronic devices which import into Afghanistan daily, contribute to control suspicious internal cyber illegal activities, harassments and cyber-attacks. Moreover policy has also financial beneficiaries to our national budgets and taxes systems. Each electronic device has a unique identification number (For instance: on smartphones International Mobile Equipment Identification IMEI or serial numbers and for personal computer Media Access Control MAC addresses also called physical address that is globally unique and unchangeable) grants to register them into standard official systems. In this terms, first of all, a strategy to manage and arrange all the electronic devices need to be approved by legal government authorities.

Many foreigners who are working and cooperating in different field in Afghanistan, especially in industrial companies, economical projects, development projects, technological projects and other developments enterprises benefit from free communication services without giving taxes or payment for their electrical devices. In general, this is not threaten our national cybersecurity, but inside up to present time, the terrorists groups and radicals also benefit from such services almost without knowing the government. Therefore, this policy handle and mitigate salient amount of cyber-threats on our cyberspace. Another possibility to control and mitigate internal illegal cyber activities in Afghanistan, is the standard distribution of logical address (Internet Protocol IP), currently many of industrial technology markets use version four of IP(IPv4) address, because of huge latency of electronic devices the new version of logical address (IPv6) is also introduced to technology markets.

The communication model which was introduced by International Standard Organization ISO, particularly Open Systems Interconnections OSI (Refer to Appendices C.2.) use in current network communication systems in Afghanistan, especially version ISO 2700 upgrading to higher versions. Transmission Control Protocol and IP TCP/IP operability interact each other in terms of data communications over the network, the combination of four layers such as: Network Access Layer NAL, Internet Layer IL, Transport Layer TL and importantly Application Layer AP make the real data communication and transmissions. In both basic and advanced network security, the security of TCP/IP is one of the important concern of transmissions for service delivering, there are many methods and types of attacks also designed to interrupt and spoof these layers. IP spoofing, SYN flooding attacks which is a form of Denial of Service DoS attack and Address Resolution Protocol (Refer to Appendices C.3.) Spoofing including Domain Name Systems spoofing attacks are the common reported which are targeted to flood the layers related to TCP/IP and MAC address. The issue that how it would be possible to record millions of electrical devices attributes that imports daily in Afghanistan, technically can be solved easily.

A Real-Time System RTS catch simply the problem (It is hard and need sufficient resources, but the development is simply possible), developer of RTS uses many kinds of intelligent algorithms to monitor the variety of challenges according to difficulties. Imagine, if we create a source center to store all attributes related to electrical devices then by developing a smart or Real-Time System the new devices also will be possible to be caught and stored constantly into this resource centers. However, once the new devices recognized and authorized by source center then the TRS system permit them for receiving public services. A well-defined technical strategy absolutely survive our current and future assets. In addition, in the near future, Internet of Things IoT would be also an extensive challenges if the private and government sectors, especially the government internal bureaus compatibility do not cooperate each other for preparing a commonwealth defense and deterrence well-defined strategies in opposite to cyber threats.

### 3.5.1.5. Apply of standard data encryption policy

Encryption is a level of security in terms of none raw bites transmission, technically encryption defines in application layer of TCP/IP or equal to Application, Presentation and Session layer of OSI model. These layers easily can be captured by hackers and attackers, because readable data transmits from these layers and transaction is easily catchable by hackers in these layers. A simple network analyzer software which is known packets sniffer can be run away, once the data and traffic been captured by sniffer, this software also has the ability to sniff the content of packets and then captures the network sensitive information such as: user credentials, account information and other credential transmit over the network.

Practically, by encrypting transactional data probably we safe the credentials as far as possible, the main two types classical and modern encryption algorithms and procedures explained widely in current technology. Classical encryption is not use superabundant in modern technology anymore because of unsafety, and there are also many methods of cracking or decrypting of encrypted data as well.

However, in modern encryption methodologies complex algorithms and statistical consumption contended, the decryption of the modern encryption algorithms are slightly impossible because of its complexity, where such complex modern encryption systems can be implemented and used in current and more precisely in future data transmission systems in Afghanistan. Coordination and arrangement would excited to motivate private and public companies for using a standard secure modern encryption systems at their virtual communication service especially on online banking systems and high secret communication which mostly the secret data transfer over the network.

### 3.5.1.6. Software productions

Reliability of software refers to the first condition of cyber-security due to systems flexibility with application and software, and referring to previous parts the risks and black holes, faults and errors on software have made unchallengeable issues, in modern technology, escalated cyber-violence and threats raise because of faults in online and offline applications, technically, the counterparts of insiders and outsiders is these deficiencies in software or applications.

In here, we assumed that the software and application included all types of untouchable instruments which used in cyberspace for servicing such as operating systems, web-based, Windows-based information systems and applications. If the government can produce such application and software, certainly, it might be possible to decrease the internal and external cyber-threats and violence. But same as the production of electrical chips, it is also impossible in current situation, especially production of operating system with our on-hand facilities and lack of experts. But, the possibility of customizing open sources operating systems such as: Linux and Unix is closed to real.

What we can do is to concern firstly, about the customizing of open source operating systems and then a deep consideration to internal production of information systems based on our social needs. Whatever, the production of customized software has many efficiencies in both private and public sectors. The admissible strategy that our government can pursues is to maintain our current systems accurately and then constitute with internal information systems products shortly in near future. Obviously, it is believable that some of private companies by interoperability of public agencies work in this field by developing business applications and small software in purpose of social servicing, but, if we consider to huge amount of a nation requirements, our current productions do not fulfill our requirements, especially in connection to critical information systems, this dream has not jointed to reality.

### 3.5.2. Political and lawful strategies

Concerning to the technical system's problems and instruments, it can be solved easily, in modern technology and investments in this fields even if the government do not concern seriously in technical treatments, it would be resolved by dedicating budgets and contracting with private sectors because of human resources and intellectuals.  In terms of human capabilities and intellectuals the private sectors invest heavily more than governments world widely especially in Afghanistan. But, the political arrangement and management government has to be involved for defining an effective applicable strategy to defense cyber-attacks on critical systems and critical infrastructures. Here are, some key performances annotated on. In reference to our currents network geopolitical structure and according to cyber-attacks on resources of national security conceal NSC of Afghanistan and many other governmental official domains, thereafter the attacks nor MCIT and not NSC reactions been reported, the only official report that has published on MCIT website confirmed that the official domains have been targeted by Chinese hackers.

In this report MCIT confirmed that an unknown scripts had been injected on some of hosting servers. The reason that the governors ignore similar cyber-attacks which target continuously official websites and public services is not clear. Likely, it is because to save their political prestige or maybe it is because of the inconsistency of intergovernmental security response teams. However, lack of human resources and intellectuals also might be possible. In any case, the management and intervolving of authorized governmental management board by well-defined of lawful strategy and cooperation with private sectors, probably government would be able to appease future cyber-threats (Exploit and attacks).

#### 3.5.2.1. Control of black market

As many times concerned regarding the black markets in this report, In fact, the challenges of black markets is not only concerned in Afghanistan, rather it causes significant challenges at all around the world in both cyberspaces and physically effective illegal activities. But, regularly the other nations such: China, United State of America, European Union, Russia and even our neighbors countries slightly have abilities and resources to control and prevent at the least the export of cyber-tools in concern to their national security, especially, among the list, the USA, China, Russia and Iran.

There are many types of cyber-tools exporting to Afghanistan that are not being controlled or it might impossible to control them in black markets. Regarding to the current cyberspace situations, partially, government is able to prevent and of course MCIT is planning to control incomprehensively in some parts such as: control of radio frequency spectrum, ISPs and other technological firms, but is not enough because unregistered SIM cards, electrical devices, insecure public internet and none control of café nets make challenges and threaten our daily life. How such activity threaten our cyberspaces? Let's imagine a simple scenario. A professional insider or hacker or even it is also doable by none professionals with having a preplan attack buys a SIM card from black market and a computer which also bought from black markets, the hacker can easily use either 3G services or public internet in terms of approaching her/his goals. First of all, he/she attempts to run a malicious script in purpose of espionage or offensive denial service attack DoS into sensitive servers depend on one of the ministry of defense and ministry of interior (which the plans and programs of the ministries including the identification of soldiers and biometric properties have been stored on them), public services and institutions or even social data centers (A data center is supposed to be developed by MCIT for saving e-government services such as: electronic passport, electronic identification number, electronic driving license plus health insurance and online banking servers) within approximately ten minutes. Secondly, he/she can easily break down the basic security policies and firewalls by penetrating into one of above systems or servers, however, he can kidnap millions of terabyte of data or he/she is also able to disrupt and disable all social services and military services for a long time, nevertheless, these are the possibilities of attacks on our current services that can be done by an insider or an attacker.

Assume, if the critical systems like SCADA come in the future, what such attack can destroy, and how much such systems would be secure, no one can assume to be done. Finally, how our government and governmental security team can handle the issue or are they able to catch the hacker? Slightly impossible because inconsistencies of our current systems and none cooperation with private sectors. Generally, the 3G services are provided by private telecommunication companies except for Afghan Telecom AFT and public internet by café nets (Which are connected directly to satellites or connected to an

ISP and/or either being serviced by both cabling or air interfaces) at all across the country, thus, the monitoring of insider simultaneously needs highly secured systems and private sectors cooperation.

As well as, handling of the issues are also impossible at time of attack, due to monitoring of issues and then troubleshooting the problems for averting the risks that cause significant damages, is the other major problem. Contentiously, the attackers conspicuously will able to disrupt, destroy and kidnap as much as sensitive information they need, and likewise they can do whatever they want.

#### 3.5.2.2. Prevention of cracked software

Prevention of cracked and out of date software at least on public or from official usage: By preventing of the cracked and out of date antiviruses and other applicable software products such as client-side and server operating systems at least on official organizations help to safe the organizational and personal data one employee's official personal computers. New study revealed that installed out of date software products on servers or on clients is a big deal because, as we already considered previously about the patch and dispatch of software, many types and methods of cyber-attacks perform to collapse through targeting the black hole of software as had happened to Panama papers. In Panama paper, a small software was out of date, hackers easily breached into targeted server by backtracking and monitoring. The black hole on out of date software can easily be handled by updating the software products, it is hard to determine the black hole of software products before installation into systems, through updating the software black hole dispatches automatically.  Another big and dangerous challenge is the cracked software which are being imported from our neighbors. The usage of cracked software especially in official terms, causes catastrophic difficulties.

In fact, when a software produced, the producers define a security level on software (operating systems and other developed software products web based and windows based applications) by cracking somehow the security level of software breaks down, and then crackers customize the source code and inject malicious codes on them. In reference to growing presence of such software in Afghanistan, our national security risks also grows up, the influential role of government is to prevent the usage of such software in official institution and social services. I remember, when I was an undergraduate student at Kabul Polytechnic University, thousands of students and alumni who were studying in different fields, and were staying at dorm, at this dorm which is close to campus wide area network, students widely use cracked software because of being free and easily available to black market many times cheaper than their original price, at the same time, many types of malware (viruses, worms and Trojan horses), malicious codes and malicious scripts were been found on each personal computer of students.

Same as, these types of software being used on many other official organizations as well. Theft of personal information, threats to institutional privacy, theft of the governmental and private institutions and threaten to public network are the undistinguished issues which probably raise due to usage of such software, in addition to, injected malicious codes would also apparently instigate crackers and insiders to carry out their inauspicious goals successfully in desire of either espionage or collapse of the communication and information systems.

#### 3.5.2.3. Flexible prosecution policy

Since along times ago cybercrimes have escalated and have repeatedly increased after 1990. Cybercrime consists of criminal acts that committed by using electronic communications network and information systems. However, hacking, Theft of personal data, Copyright infringement, online scam and Fraud, Child violence and pornography, Cyber stalking and Bullying are also well-known types of cybercrimes, typically cyber-crimes revealing the new types of crimes especially in modern technology. When the violence has been starting from first cyber-attacks until now this types of crimes increase constantly, the cybercrime could be performed by using a wide range of different attacks, where a type of this crime explained earlier in this report. Recently, the MICT, ATRA and ISSD by inter-operation of ministry of Justice and intervolving of parliament have approved a precaution policy regarding condemnation of cybercrimes consummators.

Optimistically, implementation and improvement of such laws is appreciable in all sincerity. But here, the flexible prosecution policy have strong performance and effective role in capturing and entrapping the criminals (insiders and outsiders) who modify, threaten seriously our nation and disrupts information in concern to our civilians and national services. Flexible prosecution policy has two common meaning in here that our government with intervolving private sectors could handle both of them easily, the establishment of emergency teams consists of technical experts and legislators in response to cyber-attacks. The technical experts and intellectuals commonly try to defense or deter cyber-attacks and sometimes retaliate in response to cyber-attacks technically. The legislator's team comprehensively could define a lawful precaution strategy in consider to disruptions affected by cyber-attacks. As we understand the cybercrime have newly interacted in traditional Afghani society, our people and almost our legislators are not familiar precisely with this type of crime. The combination and cooperation of both legislators and technical experts might help partially to mitigate the vulnerabilities threaten our present and future cyberspace.

### 3.5.2.4. Control of official personal computers

Safety of personal computer on official public (military institution associations and training centers, public service organizations like health insurance and hospitals, driving license, public identification data centers and digital passport issuers centers, public and private institutions, transportations public and private sectors and more importantly advice to public internet providers café nets to safe their personal computers) offices and private sectors (agricultural sectors, industrial sectors, telecommunications sectors and their agencies, and finally the internet service providers ISPs) including the individual and public awareness. In this terms, what the government can do is to autograph legitimate law( which is not defined on newly approved and issued by ministry of justice by the name of Jaza code in Persian کدجزا regarding the cyber-laws), in  reference to public and private sectors personal computer, this legitimate law would enforce the public, especially private companies and institutions to manage their own personal employee’s computers, however, there are also multiple ways like data access policy, personal computer safety and many other standard methods have intensively defined about safety of personal computers. In military and official organizations, an up to date antivirus is sufficient to detect and protect personal computers belongs to authorized official management board.

### 3.5.2.5.  Control of ISPs and Café nets

Safety of public internet service providers including ISPs and public café nets, as it is clear that public internet service providers threaten most of public social and economic services such as health insurance services banking systems, public transportation systems and even online transactions if they infected by suspicious codes and malware. Therefore, the safety of public internet providers has significant roles on public and social service, in terms of security and safety of personal computers, that how to save and monitor especially café nets to do not infected by cyberattacks, rapidly an official movement is necessary.

By enforcing the owner of such public service providers, possibly the government would be able to compel them for saving their personal computers and other device like shared webcams, networked scanners, shared domains and shared printers. The other problem is monitoring of them, in case, if an insider arrange an attacks by using of public internet services, the café nets itself would be possible to be monitored by security cameras that is already illustrated previously in this report. But, if an attack arranges by hacking Wi-Fi of the public internet, slightly the prevention is impossible and besides the government must aware them to save their internal resources via technical consulting and other national safety cares. But tracking and finding such attack is possible by tracing logical address (IP) and physical address (MAC) of electronic devices that insiders and attackers used them by defining acceptable electronic devices use policy.

### 3.5.2.6. Countermeasure and retaliation

Countermeasure and retaliation: Cyber-threats in act of cyber-attacks and aims of critical infrastructure exploitation, espionage, theft of sensitive information dramatically have thought us the art of creating “logic bombs”; along the history our people suffered from many types internal skirmish, external political and competitive interferences. A land with purely traditional cultures and customs newly joins and mostly suffers to/from modern type of cold war, during the cold wars, especially after second worldwide war, the art of cyber-wars launched significantly among the nations and almost Afghanistan was not included. In referring definition of cyberspace that Martin C. Libicki has illustrated "Cyberspace is a thing of contrasts: It is a space and is thus similar to such other media of contention as the land and sea. It is also a space unlike any other, making it dissimilar. Cyberspace has to be appreciated on its own merits; it is a man-made construct." In contemplating to this definition and respecting to other peaceful nations except of those who have devastating goals in regional and international countries, our current situations and nearly future cyber vulnerabilities deserve to make sense of countermeasure and retaliation.

In many terms, these two important factors are mentality defined as key performances as defensive strategies. The way to defense our cyberspace in general and cyber-deterrence in particular, arrangement and management of internal human capacity is almost assist us in terms for creating cyber-deterrence, cyber countermeasure and retaliation team, and finally equipped cyber-army. Firstly, the strategy to determine our exact cyberspace, could be able to monitor all types of suspicious and harmful cyber-activities including cyber-attacks and exploitation, and detect all of such vulnerabilities, in case, if the protections or deterrence failed, then the revenge is an appropriate appreciation and countermeasure to be supported by defining such strategy.

# CHAPTER 4. CONCLUSION AND FUTURE WORKS

## 4.1. Conclusion

A short inspection in consideration to contain of this report, the first chapter of this report is concerned on general introduction and information regarding information, data security, and cybersecurity of Afghanistan. Where in the second chapter, the information and data security, security challenges on cyberspace, confidentiality, integrity and availability of data including Non-repudiation and authentication of data are deeply detailed. However, the main argumentation of this two chapters are providing the general knowledge in terms of cyber security and security challenges.

Afghanistan's current network infrastructures, External connectivity links of AOFN Internal structural design of AOFN also have described in the second chapter. Imperceptibly, the valuable argumentation about security risks of Afghan Optical Fiber Network (AOFN), current cyber procedures and policies of the Afghan government, more precisely the current cyber threats and vulnerabilities that outcome significant risks illuminated as well in this chapter. Types of cyber-attacks and attacks mechanisms (such as: Distributed Denial of Service and Denial of Service, SQL injection and cross-site scripting, Physical infrastructure vulnerabilities, Black hole/ Gray Hole, Watering hole, the risks and vulnerabilities of third-party cracked software, zero-day attack and Spear phishing) including obstacles to current cyber security and current government cyber strategies by details have particularized step by step as well as in second chapter.

The main focus of this research-based thesis is on the third chapter of this report; in this chapter the two general important perspectives  (solutions and strategies) introduced by implementing conceptual network splitting into three logical phases; the theory of above three phases regarding to information and data security challenges and cyber security challenges firstly, named as Logical Network Architecture Policy and subtitled Public Network Logical Architecture Layer Secret Network Logical Architecture Layer, High-secret Network and Logical Architecture Layer then made clear the technical and non-technical challenges and solutions.

However, in this chapter, these solutions from multi-perspectives such as: defining scenarios, Modeling and simulating the threats argued and applicably analyzed successfully. As well as, Models of proposal security solution, threat types and a model of risks assessment based on a scenario stressed also isolated in this chapter, further the general analysis and simulation of threats and proposal strategies concerned to our national safety from both point of view technical and political concentrated at last partial part of the third chapter.

In the fourth chapter, an overall review regarding the future work of thesis and conclusion have successfully completed. Although the first and second chapters of this report are more reliant on external information academic theories and concepts, bur these chapters considered as  essential for starting and hardworking, because of, firstly, these two chapters make everyone who read and understand, then  the information in these chapters were needed for the new design of each step of working loads.

Secondly, these chapters, individually helped me greatly to gain more knowledge and understanding details problems about the cyberspace and cybersecurity in the first movement, and then, with self-interior support, motivated to solve all the argues related to cyberspace such as proposal define for mitigating or slightly analyzing the risks and solve the challenges of the cyberattacks. In this research-based effort as my final thesis, the general investigations of cyber-threats, cyber-vulnerabilities including cyber-attacks and cybercrimes evaluated by collecting data and information from international academic organizations conferences, famous publishers, ACM digital libraries google scholar because of a general evaluation of the above-mentioned criteria. This research is deserved to be accomplished according to academic, technical theories and implementation. The part 2.1. of this report or the brief review of important cyber-events including cyber-threats (cyber-attacks and cyber-exploits) and risks of cyber-attacks on official domains of Afghanistan's governmental agencies and ministries have shown the none-stability of current systems and technology which are being established and used by most of the government agencies.

As well as, in this part also the general academic review of the threats, risks, and vulnerabilities of systems containing all the categories of the complex algorithms, conferences, presentations, simulations, and modeling have consummated according to the subjected title. Besides of general threats, common risks, conventional vulnerabilities of information systems, applications and software which rely on cyberspace, the sensitivity of the information, information systems and security of them have evaluated by comparison of Afghanistan current technologies with new modern technologies.

In general, these academic research and journals are based on articles and theories that have been produced and published by academic cyber scientists and cyber professionals individually or collectively. Our main goal in discussing and bringing such articles in this project is that this report has a direct, structurally or adaptively interconnection with them. Thus, in many parts of this research, various innovative approaches, concepts, and ideas have illustrated and designed, by relying on these scientific papers, especially the definition of the comprehensive strategies that we have gained an overall understanding of the implementation of these strategies in the real cyber world.

Defining different scenarios in the diverse parts of this research is one of the simplest methods that evaluates and makes our discussion easier to understand fundamental of important cyber challenges in general. For instance, in research, there are three major scenarios have characterized in various parts in connection to the issues, and intended to evaluate, analyze, and conclude the security challenges and challenges of the information systems in particular. Like the businessman's scenario, in this scenario, three basic elements, such as threats of the systems, vulnerabilities of the systems and system's risks, have evaluated. Wherever, the basic scenario in which the simulation of this project is implemented based on it, in fact, in this scenario three important gateways in two border provinces and capital of Afghanistan is defined and because the conceptual idea is that all internal packets being dropped in from these three gateways, an imaginary denial of service DoS type of cyber-attack performed and the results of cyber-attack analyzed and evaluated from different perspective in this scenario.

By referring to the substantial parts of this research which is solution, in order to mitigate, control, monitor and decrease the risks of future cyber threats, the theories and strategies have presented in this purpose by showing the diagrams and the flow model for emphasis of mentioned factors on information system. Such diagrams were designed to support the future information system and application developers because as he also outlined in part 4.2. of this research such diagrams and flows enumerate a start point for development of algorithms and the implementation of algorithms in real world. These figures and models help developer in observing a system or algorithm from various perspectives, as well these figures and models the future developers to improve their understanding of structures and ideas/abstractions in designing and defining the applicable algorithm.

The overall consequences which can point out from analysis and study of this research are that the cyber threats and cybercrimes make big challenges at everywhere and all corners of the world, although these threats, pose a significant threat to the communication systems and economic infrastructures of all countries. But the risks of threats in the other countries are lesser than the risks of cyber threats in Afghanistan, this country is more affected by these threats basically, due to lack of sufficient knowledge, human intellectual resources, mismanagement and disarrangement of cyber measurements. Nowadays, as most manual information and administrative systems at governmental and non-governmental organizations, cyber threat is not that many serious problems, but in the near future, when all the cultural and economic infrastructures, politics and banking systems, agriculture and internal products become automated or especially while the important sensitive governmental and non-governmental official information systems networked under public connection systems, the cyber threats will make major and serious challenges.

From the other point, the overall cyber challenge is a perpetual challenge on information and communication systems, it means that the threats of the cyber world always resolutely exist, especially when Internet of things will be introduced in new modern communication systems and information technology societies. In this term, there will be two major problems; firstly, in case of cyber-attack on information systems all the infrastructures will be under contemplative risks, including personal information and many other economic, politics and social services; secondly, the security of IP addresses distribution itself will have major issues such as the security problems of IP based home and public devices, security issue of protocols that will be implemented and security incompatibility of devices which will be configured under local domains.

However, another major problem of interest of things is the arrangement and organization of IP addresses in terms of monitoring and backtracking of the insiders and even outsiders. Additionally, the analysis and simulation of cyber-attack based on denial of service DoS have prepared by using OPNET simulator tool, where the simulation requirements and instruments such as modeling and drawing of the flowchart are executed by Microsoft product VISO based on flexibility of the tools and requirements of this research.

Consequently, increasing the nation’s cyber forces potential on the virtual communication systems and the convergence of digital wars are the common challenges that threaten our future generations. However, today’s necessary measures and prevention strategies are our main indicators in hope of having a safe future virtual space. Additionally, our society and culture are newly experiencing these types of wars especially, modern types of crimes, from the other point of view, our people do not have necessary and sufficient knowledge in this regards because these phenomena introduced recently in our communities, especially, in the recent decades. Therefore, the cyber-wars and cyber-threats on communication systems are considered as a dangerous instrument for our current communication systems, likely, would be changed into critical case in the future.

### 4.2. Future Plan Regarding Cyberspace Security (Future Work)

The topic which has been selected under the subjected simulation of cyber threats of a country as master final thesis is not limited into a small range of work, rather, it's widespread of complex virtual world with sophisticated arguable directions. Because for a precise examination and an accurate assessment of such sophisticated things, firstly, is out of ability of a single person, assuredly no one has such abilities. Secondly, from the other perspective, it is absolutely necessary to assess and analyze Afghanistan's serious cyber threats problems, which is completely a new phenomenon in this country especially cyber wars and cyber terrorists. Therefore, to achieve these goals and to gain a successful outcome research by having acceptable argues, completely needs more time and deserve a wide bunch of investigations with cooperation of authorized and qualified people.

In this research-based paper, what you have seen is the starting point or it might motivate our next generation to keep in touch and deal with according to time and requirements of newer modern technology. if so, the future necessary performances are the investigation precisely on network security and risks of network infrastructure includes critical and non-critical networks fundamentals because such critical systems are not introduced in our current industrial society, The main concern of this reports associated on proposal solution a wide investigation and analysis is necessarily required to develop an applicable algorithm and the implementation of the algorithm, and development of applicable application and information systems to fulfill the proposed most of technical strategies.

# REFERENCES

[1] https://www.Itgovernance.co.uk what-is-cybersecurity, Access Date: 15.01.2017.

[2] https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, Access Date: 18.01.2017.

[3] Wafa, Z., National Cyber Security Strategy of Afghanistan (NCSA), Islamic Republic of Afghanistan Ministry of Communications and IT, November, 15, 2014.

[4] https://www.rt.com/news/360436-german-military-cyber-attack, Access Date: 14.01.2017.

[5] Macdonnell, N., Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. April, 2011.

[6] Knapp, J., K., Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions U.S. Air Force Academy, Colorado.

[7] Tural, T., Sheikh, A. and Hassan, A., Addressing Cyber Security for the Oil, Gas and Energy Sector, Rob R., Power Systems, Gareth W. McLorn, Power Systems Renewables, Saudi Aramco, Dhahran, KSA. April, 2015.

[8] https://www.threatconnect.com/company/intelligence-research-team, Access Date: 30.01.2017.

[9] http://securityaffairs.co/wordpress/31480/ cyber-crime/afghanistan-cdn-network-hacked.html, Access Date: 18.02.2017.

[10] http://www.bbc.com/persian/ afghanistan/ 2012/03/120305_k02-afg-net-security. html, Access Date: 19.02.2017.

[11] http://www.bbc.com/persian/afghanistan-38103569, Access Date: 21.02.2017.

[12] http://www.bbc.com/persian/afghanistan/2014/12/141222_k03_afghan_electronic_gov_threats, Access Date: 27.02.2017.

[13] https://www.theguardian.com/technology/2010/feb/03/cyber-warfare-growing-threat, Access Date: 07.03.2017.

[14] https://www.scmagazineuk.com/ cyber-attack-among-world-economic-forums-top-global- risks/article/531363/, Access Date: 10.03.2017.

[15] http://its.ucsc.edu/security/training/intro.html, Access Date: 25.03.2017.

[16] http://whatis.techtarget.com/definition/CIA, Access Date: 25.03.2017.

[17] https://www.out-law.com/page-389, Access Date: 27.03.2017.

[18] https://www.techopedia.com/definition/, Access Date: 29.03.2017.

[19] Elizabeth, R., and Denning, L., Cryptography and data Security, Purdue University, May, 2016.

[20] Guttmann, P., Cryptography and the Data Security, University of Auckland, January, 2016.

[21] Djambazova, E., Almgren, K., Dimitrov, K. and Jonsson, E., Industrial Control System and Communications (SSIC) Emerging and Future Cyber Threats to BAS, Sofia, Bulgaria. Critical Systems, International Conference on Cyber Security of Smart cities, Institute for Parallel Processing, 2015.

[22] Drias, Z., Serhrouchni, A. and Vogel, O., Analysis of Cyber Security for Industrial Control Systems, Paris, France, 2016.

[23] http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm/, Access Date: 05.04.2017.

[24] https://www.techopedia.com/definition/ 25830/cia-triad-of-information-security, Access Date: 05.03.2017.

[25] United Nations, Economic and Social Commission for Asia and the Pacific, An In-Depth Study of the Broadband Infrastructure in Afghanistan and Mongolia, April, 2015.

[26] Hamdard, J., The state of telecommunication and internet in Afghanistan, MICT of Afghanistan, Assistant report, Six years later (2006-2012).

[27] MCIT, Presentation on Afghan Fiber Optic Ring, Practical steps towards a knowledge-based economy International Conference, and the Seventh session of the SPECA, Project, Working Group on Knowledge-based Development, Dushanbe, Tajikistan, 16-17 June. 2015.

[28] Michael J., McDonald, J., John, M., Richardson, T., Regis, H., Chavez, N.D., Schwrtz, D., Atking, D. and Ronald, D., Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications, text books, 2014.

[29] Loukas, G., Cyber-physical attacks on industrial control systems How They Work and How to Protect Against Them? A Growing Invisible Threat, chapter 4 and chapter 5, 2015.

[30] Ministry of Justice of the Islamic Republic of Afghanistan, The official gazette, Crimes code, sequence number 1260, 25/02/1396 (15/05/2017), published by ministry of Justice and approval of national parlement of Afghanistan and technical help of MCIT.

[31] Kumar Gupta, M., Govil, M. and Singh, G., Static Analysis Approaches to Detect SQL Injection and Cross Site Scripting, Vulnerabilities in Web Applications, Department of Computer Engineering, Malviya National Institute of Technology, Jaipur, India, 2012.

[32] http://spectrum.ieee.org/telecom/wireless/ open-source-effort-to-hack-gsm, Access Date: 19.07.2017.

[33] United States, Cyber Strategy and Policy, Committee on Armed Services, Senate, One Hundred Fifteenth Congress, First Session, Second March, 2017.

[34] Zargar, S.T., Joshi, J. and Tipper, D., A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE, Communications Surveys & Tutorials, June, 2011.

[35] Khing Shar, L. and Beng Kuan Tan, H., Automated Removal of Cross Site Scripting Vulnerabilities in Web Applications in Information and Software Technology, Vol. 54, Issue 5, PP 467-478, May, 2012.

[36] Reed, T., At the Abyss: An insider's history of the cold war. Presidio Press, October, 2005.

[37] Cordesman, A.H., Iran and Nuclear Weapons. Background Paper for the Senate Foreign Relations Committee, Center for Strategic and International Studies, Washington, DC., July, 2000.

[38] Kumar Pandey, R. and Mishra, M., Cyber Security Threats - Smart Grid Infrastructure, the risks and effect of cyber threats on physical systems, Department of Electrical Engineering, Indian Institute of Technology (BHU) Varanasi, India, 2016.

[39] Bretasab, A.S., Bretasab, N.G., Carvalhoa, B., Baeyensc, E. and Pramod P., Smart grids cyber-physical security as a malicious data attack: An innovation approach, Khargonekarda Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL 32611-6200, USA, Department of Electrical & Computer Engineering, University of Sao Paulo, Sao Carlos, SP 13566-590, Brazil, Department of Systems Engineering and Automation, University of Valladolid, Valladolid 47002, USA, Irvine, 92697-5615, August, 2014.

[40] Diovu, R.C. and Agee, J.T., A cloud-based open-flow firewall for mitigation against DDoS attacks in smart grid AMI network, Discipline of Electrical, Electronic and the Computer Engineering, University of KwaZulu-Natal, IEEE, 978-1-5090-4746-8/17, July, 2017.

[41] Ong Y., and Qiao M., Context-Aware Data Loss Prevention for Cloud Storage Services, College of Engineering, IBM Almaden Research Center, San Jose, CA, USA, IEEE, 2159-6190/17, 2017.

[42] Liu Y., Chen, M. and MAO S., Big data: A survey Mobile network and Application, Vol. 19, no. 2, PP. 171-209, 2014.

[43] Hadoop A., Hadoop, URL:http://hadoop.apache.org, April 2015, Access date 27.08.2017.

[44] Chang, F., Dean J., Ghemawat, S., Hsieh, W.C., Wallach, D.A., Burrows, M., Chandra, T., Fikes, A., and Gruber, R.E., Bigtable: A distributed storage systems for structured data, ACM Transactions on Computer Systems, Vol. 26, no. 2, PP. 4, 2008.

[45] Jiang, S.Y., Efficient classification method for large dataset, Machine Learning and Cybernetics, International Conference on. IEEE, PP-1190-1194, 2006.

[46] Guha, S., Rastogi, R., and Shim, K., Cure: an efficient clustering algorithm for large databases, ACM sigmoid Record. ACM, vol. 27, no. 2, PP. 73-84 June, 1998.

[47] Lau K, W., and Wu, Q.H., Online training of support vector classifier, Pattern Recognition, Vol. 36, No. 8, PP. 1913-1920, 2003.

[48] Leung, C.K.S., Mackinnon, R.K., and Jiang, F., Reducing the search space for big data mining for interesting patterns from uncertain data, Big Data, International Congress on. IEEE, PP. 315-322, June, 2014.

[49] Weiwen, L., and Danni, C., Big data classification based on multi-view method Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition, Guangzhou, 12-15, July, 2015.

[50] Kong, Q., Gong, H., Ding, X. and Hou, R., Classification Application Based on Mutual Information and Random Forest Method for High Dimensional Data, College of Information Science and Engineering, Ocean University of China, 9th International Conference on Intelligent Human-Machine Systems and Cybernetics, 2016.

[51] https://www.cmu.edu/iso/governance/guidelines/data-classification.html#nav, Access date 08/09/2017.

[52] Haque, M., Tan, R., S.C., Sameer A, Kaspin, R., Yusoff, Z., Ziri, S.R., and Kwang, L.C., Motivation of DDoS Attack-Aware in Software Defined Networking Controller Placement, International Conference on Computer and Applications (ICCA), IEEE, 978-1-5386-2752-5/17/, 2017.

[53] Ruswin, S., Lakshminarasimman, S. and Sundrakantham, K., Detecting DDoS Attacks using Decision Tree Algorithm, Department of Computer Science and Engineering Thiagarajar College of Engineering Tamil Nadu, India, International Conference on Signal Processing, Communications and Networking (ICSCN - 2017), March 16, 2017.

[54] Gezgin, D.M., Buluş, E., Kablosuz ağlar için bir DoS saldırısı tasarımı, 2013.

[55] Özer, E., İskefıyeli, M., Detection of DDoS Attack via Deep Packet Analysis in Real-Time Systems, Department of computer engineering, Sakarya University, Second international conference on Computer Science and Engineering, IEEE, 978-1-5386-0930-9/17, 2016.

[56] Yu, K., Ivanov, S.A., Golodov, V.A. and Sinkov, A.S., Development of a Mathematical Model of the Control Beginning of DDoS-Attacks and Malicious Traffic, School of Electrical Engineering and Computer Science, South Ural State University and national research university, Chelyabinsk, Russia, IEEE, 978-1-5386-0703-9/17, 2017.

[57] Atlee, J.M., France, R., Georg, G. and Zschaler, S., Modeling in Software Engineering, 29th International Conference on Software Engineering, IEEE, 0-7695-2892-9/07, 2007.

[58] Bishop, C.M., How a Scientific Theory of Modeling Can Benefit Industry, Associate Technical Fellow, The Boeing Company, Huntsville, Alabama 35824, 2011.

[59] http://www.webopedia.com/TERM/C/CDN.html, Access Date: 11.01.2017.

[60] https://www.cloudflare.com/cdn/, Access Date: 11.01.2017.

[61] https://www.pinterest.com/explore/content-delivery-network/, Access Date: 11.01.2017.

[62] https://aws.amazon.com/cloudfront/, Access Date: 23.04.2017.

[63] https://ptcl.com.pk/Home/PageDetail?ItemId=41&linkId=110, Access Date: 11.04.2017.

[64] https://www.tic.ir/en/history, Access Date: 17.05.2017.

[65] http://www. mcit.gov.af/en, Access Date: 19.04.2017.

[66] Cabral, J.M., Environmental and Social Management Framework for Digital CASA Afghanistan Project, Consultancy services to prepare environmental and social management framework (EAMF) and to carry out relevant capacity building for digital CASA, Islamic Republic of Afghanistan, Ministry of Communications and Information Technology, Environmental Consultant, June, 2015.

[67] http://itfreetraining.com/, the exact access date of this web address was on: 25.05.2017.

[68] http://www.omnisecu.com/security/index.php, the exact access date of this website on: 19.08.2017.

[69] http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html, Access Date: 26.08.2017.

[70] https://www.lifewire.com/address-resolution-protocol-817941, Access Date: 22.09.2017.

[71] Costante, E., Fauri, D., Etalle, S. and Hartog, J., Hybrid Framework for Data Loss Prevention and Detection, Nicola Zannone,Eindhoven University of Technology, Symposium on Security and Privacy Workshops, IEEE, DOI 10.1109/SPW, 2016.

[72] Alhusain, T., Drew, S. and Aljarraj, O., Biometric Authentication for Mobile Government Security an application of grounded theory, school ICT, Griffith University, IEEE, 978-1-4244-6585-9/10, 2010.

[73] Zefferer, T., and Teufl P, Policy-based Security Assessment of Mobile End-user Devices An Alternative to Mobile Device Management Solutions for Android Smartphones, Institute for Applied Information Processing and Communications, Graz University of Technology, Austria, Graz, Inffeldgasse, 16a, 8010,2016.

[74] Clarke, A. and Knake, R., Cyber War, The next threat to national security and what to do about it, Text book, April, 2012.

# APPENDICES

## Appendices A.1. Content Delivery Network (CDN):

The content delivery network is platforms which work under distributed servers, CDN counts as a system under distributed network of servers which delivers content of a webpage include texts, pictures, videos and any kinds of information from servers to users, in this kinds of integrated system many domains can be configured [59]. In addition, the content of any webpage can be distributed by CDN system based on geographical location of users. On such configuration of the servers, if any user calls access tags to handle services, the nearest sever closed to user responses to user request shown in Figure 4.1. These kinds of services are used to accelerate the static content of web pages, increases the dynamic content of webpage and gives fast services to mobile context [60]. In case of any issue, or service failed backup servers handle the nearest request of users [61], [62].

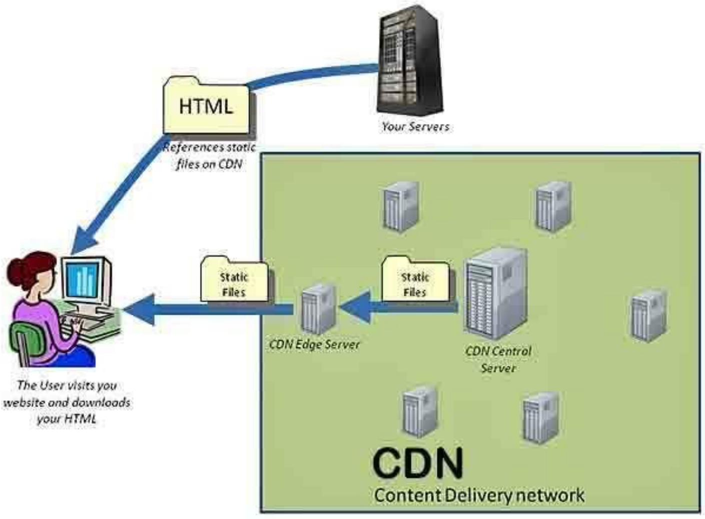


Figure 4.1. The CDN configuration and implementation

### A.2. PTCL Pakistan

PTCL is a wireless fast broadband network links communication connections internally inside of Pakistan and submarine fiber connectivity across the globe, this organization is actually a member of IMEWE Cable Consortium with its landing station at Karachi from point of view, the Afghanistan fiber optic links dependently connected to this global infrastructures via fiber optic. Based on internal and external connectivity gateway below three types of network connection is providing this company.

a. Satellite communications
b. Internally landline connections
c. International connection services

Mostly, the first two facilities (Satellite communications and Landlines connectivity services) interactively operate inside of Pakistan but the third feature which directly connects network infrastructure to international network backbone for providing Terabit capacity.

However, the network backbone of this company is connected across border connections links from two main sides to South (East Asia- Middle East and Western Europe) and as well as (India Middle East and Western Europe) [63].

### A.3. Telecom Infrastructure Company of Iran

This is the main member of governmental telecommunication network that provides three main functions.

a. Responsible for the main telecommunication networks in Iran.
b. Telecommunications hob of the Middle East region.
c. A gateway connected the East and the West.

This company is working as the governmental organization of Information and Communication Technology ICT Ministry with the aim of creating, developing, managing, organizing, supervising, maintaining and implementing the main communications backbone of the country and continues its infrastructural activities [64].

### B.1. MCIT technology projects

During the time of writing this report, according to the annual report of MCIT on their website current running projects included.

1. E-government

This is a component of large and significant digital projects by the name of electric government aims the development of important digitalized projects. MCIT attempt to provide Value Added Services VAS by implementation of this projects. In common below components are covered under implementation of this project.

a. Distribution of Afghan National Card or Identification Card.
b. E-government resources centers at all the corners of country.
c. Development of service delivery and interoperability websites.
d. ID cards, Passports and other licenses.
e. Establishing an ICT village.
f. Development of e-government application over all the country.
g. Improving ICT training and digital literacy.

Driver license, Resident Management & National ID, Vehicle Registration, Digital Signature and Biometrics systems are common components that covered under this digitalization and development projects. The ministry of communication and information technology of Afghanistan with cooperation of other national and international organizations invest heavily in implementation of this project.

2. M-Government

This is also a component aims to provide government services using mobile telephony to increase their efficiency and effectiveness. This digitalization project covers components consequently in intention of digital services.

a. Enabling Mobile Government.
b. Innovations Grant Program.

3. Postal Sector Modernization

This component aims to modernize the postal sector to improve its reach and service delivery. It is going to be actualized straight forwarding the below elements.

a. Renovation, improvement, modernization and assembly of Afghan Post Organizations APO, which is an active and main responsible of governmental agency at all across the country for serving the postal services.
b. Rephrasing of postal procedural laws.
c. Implementing a postal basic regulator in the scheme of an independent agency concealed by Ministry of Communication and Information Technology MCIT.

4. Exacerbation and intensification of Ministry itself

This element goals to strengthen the MICT that can catch the current and future issues competently and impressively in our current and slightly in future modern society. This development element will be carried out via the below important sub-components.

a. Reorganizing the ministry.
b. Rebuilding the cyber security central office at aims of combats to cyber challenges and issues.

c. Soak up ability of the ministry and increasing the capacity of MCIT also the capacity increment of other ministries of Islamic Republic of Afghanistan IROA.
d. Determine of the Chief Information Officer CIO framework rules into all the government offices and agencies.
e. Rebuilding a resourcefulness core agency at goals of ICT improvements and developments for government, communication training centers and ICT institutions at across the country.

5. Extending the network infrastructure especially the telecommunication networks

Extending of the physical infrastructure of networks including telecommunication network that will fulfill the physical backbone of ICT network sector by dedicating adequate resources and essential fundamental framework.

a. Building Telephone Lines Network
b. Building Internet Exchange Point
c. Optic Fiber Network
d. Broadband Connectivity

Note: Most of the above texts about the currents projects running in MCIT have been copied from proposal of the projects and MCIT website for more information refer [65].

### B.2. Digital CASA project

This project is established based on digital requirements and services of Afghanistan, government of Afghanistan with accomplished of international society try to implement this project to increase access to digital services throughout Afghanistan, via a regionally integrated, secure and affordable digital infrastructure, including the expansion of e-Government services and digital job opportunities. The implementation of this project has defined in three phases and components which covers Afghanistan's digital services internally and externally, meaning that the main building block of digital service and network connectivity are being conducted by implementation of this project. However, the three main components consists

a. Supply side: which is covered digital connectivity of network cross border strengthen fiber optic links neighbor countries like China, Uzbekistan, Tajikistan and Turkmenistan as well as domestic digital services of greater access affordable domestic high speed internet, improvement of domestic network capabilities in urban and rural areas, financing the pre-purchase and rise of internet bandwidth for government usage, financing the government network GovNet for providing broadband connectivity to government institutions, including schools, universities, government offices in Kabul and provinces and finally to financing of investments in Internet exchange point that may be facilitated at the regional level, and for upgrading of the National Internet Exchange of Afghanistan.

b. The automation of shared platforms via e-services, deployment of a government shared e-Procurement platform, enhancement of the National Data Center located within MCIT for enabling a shared digital platform across government (e.g. leveraging cloud computing technologies) including options for backup disaster recovery, targeted interventions aimed at the development of the IT/ITES industry, GIS mapping and lastly digital jobs and skills development are being supplemented by this component of this digital development project.

c. The last components which are more conversable is providing technical supports to MCIT and Afghanistan Telecom Regulatory Authority ATRA, promoting a competitive ICT market, private sector investment and digital jobs facilitation, facilitating cross-sector infrastructure sharing, facilitating e-Government standards and interoperability frameworks, developing digital leadership within the government and signed the last one is developing and implementing robust cybersecurity frameworks are the key details being covered by this components of CASA digital project. For more details, refer to the reference [66]. full access about the implementation of this project and consequently the coverage areas being

> actualized by implementation of this digital CASA development project. In concern to impact of this project MCIT mentioned some natural impact such as: limited impact on some productive assets, agricultural crops and fruit trees, ornamental assets like plants and trees.

In terms of developments and social especially modern progression of Afghanistan, this project has the high potential positive impacts at all, because Afghanistan backbone network is connected through implementation of this projected to international network infrastructures, however, high speed internet and landline facilities and including modern technology services will also be provided in conservative society of Afghanistan, as well the substantial is that the internal connectivity networks of Afghanistan will be accomplished though this project. But, there are two risks across the implementation of this projects.

Firstly, Afghanistan's government won't be able to grantee the physical security or land lines of this project on mountains and deserts, further it is a big challenge from two dimensional arguable challenges that internal security capability of Afghani government is not sufficient to maintains and deters the malicious groups from destruction and physical attacks in short and long terms in the future, and the significant challenge that the neighbor countries involve in developments projects in Afghanistan, mostly they create challenges across the deployments of developments projects especially, technological and economical projects by supporting some internal malicious groups.

Secondly, the cyber-security of this projects is arguable and has negative impacts in the future, in terms of none negative risks this project categorized as B types in World Bank who financially supports, but if the physical connection of this project faces problems, it will have the worst negative impacts on connectivity infrastructures, there are many likelihood risks raise such as: financial negative impacts, loss of sensitive information, loss of connectivity and most important the government has to connect the sensitive network infrastructure in the future through physical cabling of this project, which will cause high-level risks at military assets, oil and gas stations, and critical communication and information systems, as well as other development economical projects.

### B.3. Cyber-tools

In this report, cyber-tools concerned regarding any types of instrument that can be used to flood and exploit enumerates as threats to cyberspace including hardware such as: any types of IP based electrical devices like unregistered or registered SIM cards and smart phones, personal computers (Laptop, Desktop, Micro laptop and etc.), and any types of personal electrical tablets, iPads and none IP-based tools like USBs, flash, dongles as well as software such as:  cracked antivirus, dangerous malware, ransom-ware, third parity cracked software, viruses, worms and Trojan horses.

### C.1. Network authentication system

In this part the network authentication systems concerned as common because it gives a general meaning in considering to authentication procedures and processes, however, particularly the authentication has a single meaning which is a process of either allowing or denying the devices which have compatibility of using the network or a user access to the network. There are many protocols that are developed in terms of network authentication systems, such as NTLM and Kerberos authentication protocols which are commonly used in networks to authenticate users against the domain controller. In fact, the authentication processes are involved with users credential including all the IP based electrical devices and it is enumerated as one of the important partial parts of network security, where the network security itself accounted the significant elements of cyberspaces. The three main components concern in terms of authentication as below [67].

a. Network authentication: which are include NTLM and Kerberos protocols.
b. Remote authentication: which are include PAP, CHAP, EAP and PEAP protocols.

c. Group policy: which concern into network group policy.

The network authentication protocols work within complex and multiple algorithms in wide range of area in network authentication processes, many types of authentication and authorization processes developed and introduced until now. In many cases, the authentication processes are different and designed according to network types, for instance, the authentication processes in global systems for mobile GSM, satellite authentication protocols, computer networks wireless and wired authentication protocols [68].

### C.2. Open Systems Interconnection OSI

In order to understand and discuss the model of OSI by details, there are multi-function and subjects to answer in this regard that is normally not possible to be described in this report because of times consumer. But, general discussion and main functions of this model have illustrated in this part. As a general overview the Figure 4.2. shows seven layers of Open Systems Interconnection OSI, this model actually proposed by International Standard Organization ISO in 1977, in purpose of coordinating and managing of the network communication systems complex and trouble problems. This model breaks down the all the communication network problems into seven standard layers for data communication over any types of carrier network (Internet, Intranet, virtual communication, Local Area Network LAN, Wide Area Network WAN, MAN and etc.).

When two or more users communicate among or between each other, in fact, this standard model arranges, manages and solves the complex issues affiliated to connection criteria, however, in this model all the communication-related problems refers to a specific protocol which the protocols operating at different layers and different aims.

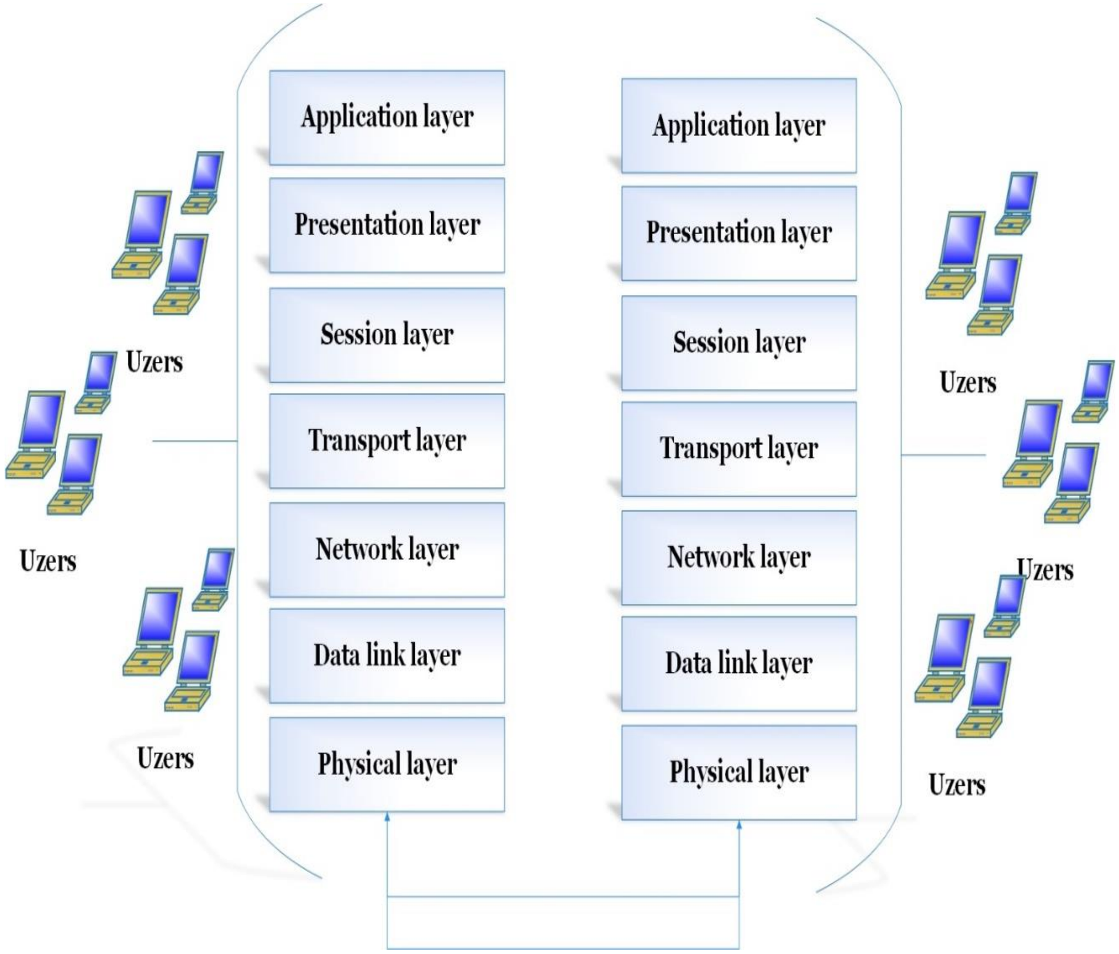


Figure 4.2. Seven layers of Open Systems Interconnect

In real network communication systems, this model is one of the most substantial models of networks, which supports and grantees connections among users, from physical layer up to application layer of this model multiple protocols involve to solve particular problem related to their own tasks. Orders of these layers are also important because in mutual communication of two users, the transactional data ordinary transfers steps by steps based on layer's protocol between them. The International Standard Organization offers multiple version of its products that support user's communication within the model of OSI, as also discussed in Afghanistan, they currently use ISO 2700 version, but MCIT attempts to upgrade and update this version to higher versions. In order to understand the fundamental functionalities of this model, here are as below the main functionalities of this layer along with modernization and communication has developed and presented into modern communication systems especially on computer network and data transmission, these functionalities are explained and overviewed generally.

### 1. Physical layer PL

To concern about this layer, it entangle with physical attributes of electrical and distinguish the raw bite of transmission or this layer engross with optical electromagnetic signaling approach like the alternative current voltage of electrons supposed to convey the electromagnetic signal and media types (physical cabling properties) as well as, the other media types which have physical involvements with coaxial cable, twisted pair and fiber optic, however, the other main responsibilities of this layer is impedance deterministic and the synchronization mediated between users for transferring the data over the network.

### 2. Data Link Layer DLL

This is the second layer of OSI model, which is resides over the physical layer and under the network layer, the main functionalities of this layer decomposed from other two different layer that is also called sub layer of data link layers similar to, the Media Access Control (MAC) and the Logical Link Control (LLC), as well as, this layer also provides the end-to-end data validity being transmitted over the network. Each of data link layer's sub layers has complex responsibilities.

### 3. Network Layer NL

The network layer is the third layer of OSI model that is generally responsible for managing logical addressing which is also called IP address and routing. In data communication, this layer is also called actual hardware layer because the actual hardware of the network being set up is involved in this layer of OSI model. For instance, practically the routers that are responsible for transmission of data, by mechanisms of defining routing table which is being defined in routers architecture (an especial computer used to build the network). In consideration to standard, this routing table contains a list of available destination address is being used for communications. This layer is also working with logical address of the sources (who sends the packets) and destinations (who receives the packets), as we know the IP addresses which are a unique address allocating for each user uniquely in goal of troubleshooting and more specifically for routing or transmission. The protocols such as TCP, UDP and Internet Protocol IP address are intervolved in this layer of Open Systems Interconnection OSI model.

### 4. Transport Layer TL

The is the fourth layer of OSI which are responsible for handling the transport functions (stability or instability data delivery from source to the destination), responsible for breaking sender's packets into smaller packets based on distinct protocol vice versa this layer in receiver side is responsible for opening the packets and decomposing them, in case if the packets loss or damage over the network this layer is responsible for resending them. However, Transmission Control protocol TCP segment sequencing, service address for specifying the requests on source and destination, and many other functionalities are the most common being implemented at this layer of OSI. Transmission Control Protocol TCP segment sequencing is used for ordering the broke down packets into destination layer which is called segmentation ordering. This protocol at this layer takes the packets segments and order them according to sender segments.

### 5. Session Layer SL

This layer resides under to presentation layer and above to transports layer where managing, and terminating connections between applications at each end of the communication are the most common responsibilities of session layer which is the fifth layer of Open Systems Interconnection OSI model. This layer also called port layer because for internet application each session is related to a specific port that is generally managing and arranging in this layer, however, from the other side, this layer is an interface between users and network.

### 6. Presentation Layer PL

This is the sixth layer of OSI model which is responsible for checking the data proper formats on source and destination, it happens when the presentation layer sends data this layer checks the format of transferred data and make sure that all the of the data are the incorrect format. In case, if the data are not in standard format then this layer changes them into correct format for transmission vice versa the destination layer is also checked and processes the same procedures.

Moreover, the other main tasks and responsibilities of this layer are encryption which is one of the key security feature in data communication, accrediting and recognizing the ASCII code, Unicode and Extended Binary Coded Decimal Interchange Code EBCDIC to assure that there is no interruption in data transport in both sender and receiver (Sources and Destination), as well as, another responsibility of this layer is squeezing and compression of data over the network in aims to decrease the network terrific and easily data transmission.

### 7. Application Layer AL

This layer is the last layer of Open Systems Interconnection OSI model that is involved in real data communication between source and destination, this layer is also can be called the real data communication layer.

In this layer the real data transfers to/from senders and receivers. The real data terrific is generating by application layer, there are many protocols such as HTTP, HTTPS, and

File Transfer Protocol FTP and also managing the users' requests are being supported by this layer of OSI model.

### C.3. Address Resolution Protocol ARP

In network connection and remote communication or session many types of protocols have defined and described by scholars and then implemented by trade or business enterprises, where on the most important and significant protocol is Address Resolution Protocol or shortly ARP. The Address Resolution Protocol ARP operates on the second layer of OSI model which is introduced in 1980 in purpose of allowing the network components and managing the physical address of networked devices. The specific definition and usage of this protocol which is taken from the mentioned references are "The address resolution protocol is a protocol used by the Internet Protocol IP, specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer" [69]. and this address are used "to convert the IP address to its corresponding physical network address for recognizing the source and destination addresses and allocation of the users" [70].

In today's communication systems in many technologies such as: Automatic Teller Machines ATM configuration under the network, Token rings which acts on Local Area Network on star topology of network continuously the token ring network topology operates on second layer (data link layer) of Open Systems Interconnection OSI model, Ethernet and Wi-Fi are used from address resolution protocol, there are many articles and journals concerned about this resolution protocol and its security problems and challenges. In our discussion this protocol is important because of the Media Access Control addresses, in strategy part of this reports some of the solutions for controlling and monitoring of the insider's attack have discussed. However, when the electrical devices try to be connected on network, first of all, this unique six byte or 48 bites must be cleared, otherwise, the devices will not be authenticated by network authenticator or it will not be a valid request. The complete authentication processes have shown on Figure 4.3. which is already taken from 23 footer reference.

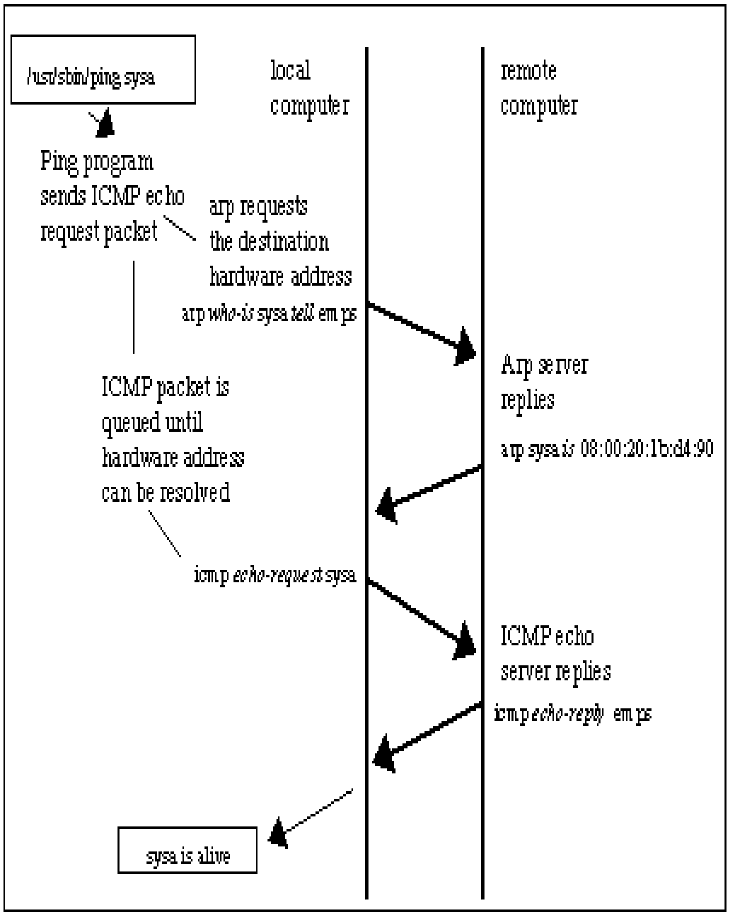

/usr/sbin/ping sysa
local computer
remote computer
Ping program sends ICMP echo request packet
arp requests the destination hardware address
arp *who-is* sysa *tell* emps
Arp server replies
arp sysa *is* 08:00:20:1b:d4:90
ICMP packet is queued until hardware address can be resolved
icmp *echo-request* sysa
ICMP echo server replies
icmp *echo-reply* emps
sysa is alive

Figure 4.3. Logic of ARP in real

# RESUME

Mr. Sayed Zakariya HABIB was born in 1987 at a beautiful and wonderful village in Afghanistan. He has completed his primary, secondary and high school at Abdul Gafoor-e-Sultani high school. After participating to a competitive exam in Afghanistan by the name of Kankur he successfully passed and enrolled to Kabul Polytechnic University KPU which is one of the top university in Afghanistan. After accomplishment of four academic years, he graduated from department of computer informatics engineering faculty of computer engineering in 2012. However, in 2014 he enrolled to department of cyber security, faculty of computer and information engineering at Sakarya University for doing his master degree and successfully finished in 2017.  Beside of his academic activities, he also worked more than four years in different fields such as; as application and database developer, as network engineer, as front end Value Added Service VAS and billing engineer at Mobile Telephone Network MTN which is an independent international telecommunication company.