Ministry of Higher Education

Kabul University

Faculty of Computer Science

Information Technology Department

Afghanistan CERT Challenges and Solutions

Thesis Supervisor: Assistant Professor Mohammad Tariq “Meeran” and Associate Professor Salim “Saay”

Thesis Author: Zeenat “Kohestani”

Year: 2014

APPROVALS

Supervisor: ____

Referee's Name:

i. ____

ii. ____

iii. ____

Chairman Department: _____________________________________

Dean of the faculty: _______________________________

Date: ____

Declaration

I hereby declare that the project entitled “Afghanistan CERT Challenges and Solutions” submitted for the bachelor degree in Computer Science is my original work and the project has not formed the basis for the award of any degree, fellowship or any other similar title.

Student name: Zeenat “Kohestani”

Student signature:

Date:

Acknowledgements

I am thankful to Almighty Allah who gave me the health and opportunity to complete this work. I am proud to be the follower of Prophet Muhammad (PBUH) who is ever an ember of guidance and knowledge for humanity.

I would like to say special thanks to respectable teachers (Assistant Professor Mohammad Tariq “Meeran” and Associate Professor Salim Saay) that they helped me for preparation of this document.

Each of our lecturers has kindly offered me a unique occasion to perform this work in his project group.

I would like to say thanks to Afghanistan CERT that kindly provides me most of information about AFCERT.

Finally, I would like to thank my family and my all lecturers of the department and Head of the department of Information Technology, for their guidance, friendly and encouraging attitude during my project.

Zeenat “Kohestani”

Abstract

Computer Emergency Response Team (CERT) is one of network security organizations that responds to major security incidents and analyzes product vulnerabilities. CERT works to manage changes relating to progressive intruder techniques and to the difficulty of detecting attacks and catching attackers.

Every country around the world has CERT and our country also has a CERT that created in 2009 and working and providing services and located in Ministry of communication and Information Technology.

The main goal of this thesis is to show which challenges Afghanistan Computer Emergency Response Team (AFCERT) is face to and which possible solutions are exist to help AFCERT to have more services and help our country in securing our networks.

These solutions that I recommend to Afghanistan Computer Emergency Response Team (AFCERT) are from comparing four countries CERTs those countries are India, Iran, Pakistan and China.

Hopefully this document will be a usefully document to Afghanistan Computer Emergency Response Team (AFCERT) and solutions will be useful to solve AFCERT challenges.

Contents

1 Introduction

Now days the Internet become one of the most powerful and widely available communications mediums on earth and our reliance on it is increasing day by day. Governments, organizations, banks, schools, universities conduct their day to day business over the Internet. With such widespread use of the Internet totally our daily life is relevant to the Internet.

Access to the Internet is easy and cheap but the systems attached to it lack a corresponding ease of administration. The Internet was not a secure environment because it did not need to be. Early on, networking involved connecting people and machines through communications media. The job of a networker was to get devices connected to improve people's ability to communicate information and ideas. The early users of the Internet did not spend much time thinking about whether or not their online activities presented a threat to the network or to their own data.

Today, the Internet is a very different network compared to its beginnings in the 1960s. The job of a network security professional includes ensuring that appropriate personnel are well-versed in network security tools, processes, techniques, protocols, and technologies. It is critical that network security professionals manage the constantly evolving threats to networks.

When in 1988 first Internet worm created by Robert Morris with 99 lines code and released 10% 0f Internet systems were brought to a halt.

Shortly after that a meeting was held to identify how to improve response to computer security incidents on the Internet.

The recommendations resulting from the meeting included to establishes a single point of contact for Internet security problem that trusted clearinghouse for securing information.

Finally, in response of recommendations the CERT Coordination Center (CERT/CC) and originally named Computer Emergency Response Team was formed to provide response to computer security incidents on the Internet.

CERT responds the major security incidents and analyzes product vulnerabilities and CERT works to manage changes relating to progressive intruder techniques and to the difficultly of detecting attacks and catching attackers.

CERT develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems to limit damage and to ensure continuity of services.

As in today’s world everything is based on information and the most critical thing for an organization is to secure its information and Afghanistan is also a country that is new in using telecommunication and information technology but now in Afghanistan also use of the Internet is widely and in government, organizations, schools, banks, universities and mostly people use the

Internet in their daily life.

Ministry of communications is planned to establish a center which will address the security issues of data over the digital networks inside and outside country and in 2009 they created AFCERT.

In this document we will discuss about challenges of AFCERT and how to solve these challenges.

1.1 Computer Emergency Response Team (CERT)

CERT is part of the U.S. federally funded Software Engineering Institute (SEI) at Carnegie Mellon University. CERT is chartered to work with the Internet community in detecting and resolving computer security incidents. The Morris Worm motivated the formation of CERT at the directive of the Defense Advanced Research Projects Agency (DARPA). The CERT Coordination Center (CERT/CC) focuses on coordinating communication among experts during security emergencies to help prevent future incidents. CERT responds to major security incidents and analyzes product vulnerabilities. CERT works to manage changes relating to progressive intruder techniques and to the difficulty of detecting attacks and catching attackers. CERT develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of services.

Computer emergency response teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT).
CERT focuses on five areas: software assurance, secure systems, organizational security, coordinated response, and education and training.

The name computer emergency response team is the historic designation for the first team (CERT-CC) at Carnegie Mellon University (CMU). The abbreviation CERT of the historic name was picked up by other teams around the world. Some teams took on the more specific name of CSIRT to point out the task of handling computer security incidents instead of other tech support work, and because CMU was threatening to take legal action against individuals or organizations who referred to any other team than CERT-CC as a CERT. After the turn of the century, CMU relaxed its position, and the terms CERT and CSIRT are now used interchangeably. (Ruefle, 2008)

1.2 History of Computer Emergency Response Team (CERT)

The initial CERTs were created by the efforts of various government agencies in the United States who implemented CERT structures in the late 1980's in response to a number of network incidents denying users of computing services for critical periods of time. In 1988, the Defense Advanced Research Projects Agency (DARPA) funded the CERT/CC (Computer Emergency Response Team/Coordination Center) to respond to computer security incidents related to the Internet network, concentrating mainly on UNIX2 operating systems .Similarly another government agency (Department of Energy- DOE) funded the CIAC (Computer Incident Advisory Capability) in 1989 to handle computer security incidents affecting DOE systems.

Today both "CERTs" have accumulated the experience of responding to many security incidents as well as issuing periodic "advisories": concerning system vulnerabilities and software defects which have come to their attention.

In the ensuing years other government and commercial organizations created CERTs and in 1990 the National Institute of Standards and Technology (NIST) co- operated with the CERT/CC, CIAC, the National Aeronautics and Space Administration (NASA) CERT, and other response teams, to set up a collaboration of those CERTs in existence (the majority being from North America) - the Forum of Incident Response and Security Teams (FIRST). (Georgia Killcrece, 2003)

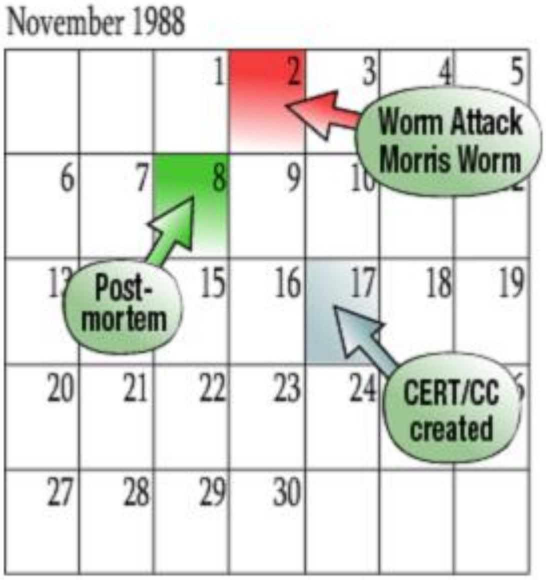

Figure 1 Timeline of Internet Worm Attack and Creation of CERT/CC

The purpose of the Forum is to provide a platform for CERTs to share their technical expertise and experiences of security incidents and thus further the development of a professional approach to computer security.

A final point, today FIRST is no longer an exclusive North American organization with CERTs from the Netherlands, United Kingdom, Australia, Germany and France becoming members or liaison members over the last few years.

CSIRTs are not all structured in the same manner; they do not all perform the same function or even have the same name. Every CSIRT is different, and these differences may include the CSIRT's

- Mission, goals, and objectives

- Constituency

- provided services (Moira J. West-Brown, April 2003)

1.3 Purpose of Computer Emergency Response Team (CERT)

The CERT CSIRT Development Team uses instead the term "incident handling" to describe the much broader activities that many CSIRTs perform in their day-to-day operations. Incident handling includes three functions: incident reporting, incident analysis, and incident response.

- Incident reporting involves receiving and reviewing incident reports and alerts.

- Incident analysis is the attempt to determine what has happened, what impact, threat or damage has resulted, and what recovery or mitigation steps should be followed.

- Incident response is the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop the incident from happening again.

We have also begun to see others in the CSIRT community use the term "incident handling" rather than "incident response" to describe the broader realm of CSIRT activities.

It is important to realize that incident handling is not just the application of technology to resolve computer security events. It is the development of a plan of action. It is the establishment of repeatable processes and methodologies for

- Notification and communication

- Collaboration and coordination

- Incident analysis and response (Georgia Killcrece, 2003)

1.4 Types of Computer Emergency Response Teams (CERTs)

CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs, such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), support an entire country. Other CSIRTS may provide support to a particular university such as Oxford, a commercial organization such as Boeing or SUN Microsystems, or a particular domain or IP range such as the Telia CERT Coordination Centre (TeliaCERTCC). There are also corporate teams and organizations that provide CSIRT services to clients for a fee, such as IBM Managed Security Services (IBM-MSS) or the debis Computer Emergency Response Team (dCERT).

CSIRTs can be categorized in many ways. One general way is to look at the main purpose, function, or services of the CSIRT, as shown in the following examples:

• Internal CSIRTs provide incident handling services to their parent organization, which could be a bank, a university, or a federal agency.

• Coordination centers coordinate and facilitate the handling of incidents across various CSIRTs, or for a particular country, state, research network, or other such entity. Usually coordination centers will have a broad scope and a diverse constituency.

• Analysis centers focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.

• Vendor teams located in software or hardware companies and handle reports concerning vulnerabilities in their products. They analyze the vulnerabilities, develop patches or workarounds, and disseminate this information to their clientele or to the broader public. They work with other CSIRTs, security experts, and researchers to track and respond to these vulnerabilities.

• Incident response providers provide incident handling services as a product to other organizations. They are sometimes referred to as managed security service providers (MSSPs).

(Georgia Killcrece, 2003)

These are some of the National CERTs:

No	Abbreviation	Name	Country
1	ALCIRT	National Security Computer Agency ALCIRT	Albania
2	DZ-CERT	Algerian Computer Emergency Response Team	Algeria
3	CERT AM	Computer Emergency Response Team Armenia	Armenia
4	CERT Australia	Computer Emergency Response Team Australia	Australia
5	CNCERT/CC	National Computer Emergency Response Team Coordination Center of China	China
6	CERT-IN	Indian Computer Emergency Response Team	India
7	CERTCC MAHER	Computer Emergency Response Team/Coordination Center	Iran
8	TR-CERT	Turkish Computer Emergency Response Team	Turkey
9	JPCERT/CC	Japan Computer Emergency Response Team	Japan
10	US-CERT	United States Computer Emergency Response Team	United States

Many countries have National CERT and to visit all of them visit website.[1]

2 Afghanistan Computer Emergency Response Team (AFCERT) 2

The ICT sector is very new in Afghanistan. In order to start the culture of using the new technologies and new methodologies; MoC has started the pilot phase of the E-Gov project in its offices; the project will re-engineer the process of the organization in order to implement e-administration and paperless office. Ministry of Communications is implemented a number of projects in the telecom sector which will enable Afghans to access information and communicate within and outside the country. The GCN (Government Communication Network) and DCN

[1] http://www.cert.org/incident-management/national-csirts/index.cfm

[2] Source : Ministry of Communication and Information Technology
Mr. Zamariali Wafa Director Information Security /CISO
Email : zamariali.wafa@mcit.gov.af

(District Communication Network) will provide an infrastructure, which connect all the government offices in Kabul and in provincial capitals enabling them to exchange information.

In today's world everything is based on information and the most critical thing for an organization to secure is its information. Ministry of Communications is planning to establish a center, which will address the security issues of the data over the digital networks inside and outside the country.

Establishment of Afghanistan Computer Emergency Response Team (AFCERT) is one of those projects.

New information and communications technologies (ICTs) are fostering profound changes throughout the world's social, political, legal and economic systems. For developing countries, ICTs have the potential to help reach key development goals as agreed upon in the United Nations Millennium Summit: reduced poverty, improved education and healthcare, enhanced empowerment, and greater protection of environmental resources. At the same time, the increasingly important role of ICTs in the broader process of globalization means that countries that do not tap into these technologies risk being left even farther behind. While domestic policy can help developing countries seize the advantages of ICTs, decisions made at the global level will increasingly affect these nations' ability to benefit from ICTs.

Information technology is transforming the economy and society, creating a completely new paradigm. Businesses are using telecommunications to speed up transactions, reduce costs, and expand their markets. Consumers are buying books, CDs, and clothing online.

Families are exchanging photos via e-mail. Students at all levels are taking courses via distance learning technologies. And telemedicine is making mental health services available in remote, underserved areas of the state.

It is clear that communication is crucial for the Government stability, national unity, conflict resolution, de-mobilization of old combatants and their re–integration in the society. The Ministry of Communication believes that communication and information technology play a significant and important role in the reconstruction and development of the country both from social as well as economical point of aspects. In fact, telecommunications is the key ingredient of economic - development.

There are several projects running by Ministry of Communications inside Afghanistan in order to increase the availability of cyber securities some of the main important projects which reflect the cyber securities are the following.

Ministry of Communications is implementing a number of projects in the telecom sector which will enable Afghans to access information and communicate within and outside the country. The GCN (Government Communication Network) and DCN (District Communication Network) will provide an infrastructure, which will connect all the government offices in Kabul and in provincial capitals enabling them to exchange information.

In today's world everything is based on information and the most critical thing for an organization to secure is its information. Ministry of Communications is planning to establish a center, which will address the security issues of the data over the digital networks inside and outside the country.

Establishment of AFCERT (Afghanistan Computer Emergency Response Team) is of a crucial importance for Afghanistan as other countries in Asia like Malaysia, China, Korea, and Indonesia etc.

AFCERT provides awareness, capacity building and cybercrime investigation to the government and private sector.

2.1 History of Afghanistan Computer Emergency Response Team (AFCERT)

According to the 2006 Annual Project Report of United Nations Development Program Afghanistan .The Information and Communication Technology (ICT) Capacity Building Project (Phase II) aims to assist the Government of Afghanistan to become part of the global information society. (Afghanistan, 01-Jan-2006 / 31-Dec-2006)

And .af Project is also part of the Information and Communication Technology (ICT) Capacity Building Project (Phase II).

Equipment purchased and installed for Afghanistan Computer Emergency Response Team (AFCERT), National Internet Registry Association (NIRA) and Internet Exchange Point (IXP), the whole .af project along with all its components were fully handed over to MoC.

The main intended outputs of Phase II includes the establishment and support to the National IC Council of Afghanistan (NICTCA), support to the modernization of the MoC, development of e-Governance policy and data center, support availability of secure internet access, advanced ICT training to produce a specialized cadre of Afghan men and women in the areas hardware/networking and database/software.

The .af country code top level domain name has been supported by UNDP/ICT Project since Jan 2003 and through this period it has been a sign of success for the ICT Project. The .af ccTLD (country code top level domain) is considered as one of the best managed country codes and during this period staff member of Ministry of Communications has been trained in technical as well as in administrative activities.

The full complement of hardware for all four components ([Afghanistan Computer Emergency Response Team (AFCERT), National Internet Registry of Afghanistan (NIRA), National Internet Exchange point of Afghanistan (NIXP)) of the project has been purchased during 1st quarter of 2006. Installation of this hardware has proceeded on schedule in the .af data enter at the MoC.

AFCERT – this security related project under .af was a critical step towards better governance of the Internet in Afghanistan.   The hardware for the project is ready; the project documentation has been completed and agreed upon by the MoC.   The last remaining task is for the MoC to hire the staff.

MCIT has focused on the establishment of physical ICT infrastructure in the country, since 2009 it is shifting its focus to the information layer. In order to bring in e-applications and make use of the already laid-down infrastructure it is quite important to have the related Cyber Security institutions, tools, regulations and infrastructure in place.

In this regard MCIT has taken the initiative to establish AfCERT. The Unit for AfCERT has been established, Staff hiring has started, ICT law has dedicated chapters for cyber-crimes, Joined the ITU-IMPACT Collaboration.

ITU has commitment to send two experts towards the end of 2009 to Kabul, to start drafting; Mechanism for the operation of the AfCERT needed SOPs for AfCERT, policies how AfCERT will interacts the Chief Security Officers in other ministries and organizations in Afghanistan of the Chief Security Officers essential documentation for affiliation of AfCERT with other international CERTs essential documentation which will clearly mention the focused areas for AfCERT to operate e.g. Spam, Intrusion Detection, Hacking etc. and training for the staff.

2.2 Purpose of Afghanistan Computer Emergency Response Team (AFCERT)

Since cyber threats are spreading day by day in order to fight against cyber-crimes, to make sure that the government and civilians' privacy is secure there is a need to establish the CERT team. This practice is being adopted all over the world.

As mentioned above that Ministry of Communications is establishing data networks throughout the country, which will be used by the government, private and as well public sector of the country. As the network will be expanded day by day and more users and more machines will be added to the network so it is important to have an entity which will take care of the following issues:

• Data over these networks will contain critical information, which will need protection from unwanted access.

• The organizations connected to the network will install machines on the network; it is important to double check whether the machines are type approved.

• Intrusions, virus, spam.

• Incidents related to hardware problem or miss-configurations.

•Handling international incidents.

•Illegal activities such as software piracy.

•Special requests from the Law Enforcement or the Government to do investigation.

•Intrusion

•Denial of Service (DOS)

•Spam

•Harassment

•Forgery

•Malware

•Hack Threat

•Destruction

AFCERT is created to detect the above mentioned issues and will make aware the member, registered organizations regarding the threat and will also help, recommend them how to overcome the issues.

2.3 Structure of Afghanistan Computer Emergency Response Team (AFCERT)

At the moment AFCERT has only one branch which is central office at ISSD, AFCERT don't have the mini CERTS in the country yet, but the whole government knows AFCERT's contact details.

At the moment there is more than 10 technical and professional staff at AFCERT and ITU-IMPACT is the main partner for our trainings and capacity building.

AFCERT operational 7 hours on day only and as the rule of government of Afghanistan there are two days officially off per week in Kabul and AFCERT don't have any operation in other holidays too.

AFCERT alerts organizations about major security incidents through official letters, emails and workshops and also AFCERT share security advisories to organizations through official letters, emails and workshops.

AFCERT doesn’t have any website to provide any information about current threats till now.

AFCERT protect sensitive data using some special encryptions method and they didn’t mention about those methods because of confidentiality of their organization.

AFCERT hire those employees will Bachelor and have certifications of Security+, CEH, CHFI, CISSP and at least two years’ work experience.

AFCERT does not provide support just for limited government it provides support for all Afghans and AFCERT prosecute hackers or problem makers based on evidences on court and court will make decision.

Through Interpol directorate AFCERT will trace and caught hackers from outside of country.

AFCERT has planned to make mini-CERTs, cooperate with educational institutions and as they said their website is under the construction.

3 Challenges of Afghanistan Computer Emergency Response Team (AFCERT)

3.1 Budget

Budget is of one basic challenges of AFCERT, as I had interview with administration of AFCERT the have plan to make mini-CERTs in each provinces and in every ministry but because they don’t have enough budget they are not able to make it and all round the world CERTs have 24/7 services but in our country AFCERT have 7 hours per day and it is also because they don’t have enough budget to hire employees to work 24/7.

3.2 ICT law of Afghanistan

As we know CERT is an organization that beside of awareness and providing information about threats and vulnerabilities of network and software CERT’s main service is to trace and catch hackers and problem makers and according ICT law we can catch they and countries court can give them punishment but other challenge that AFCERT is face it, that is ICT law of Afghanistan. ICT law draft is ready and the e-crime topic is covered by ICT law and Cyber law of Afghanistan but unfortunately ICT law of Afghanistan is under process on ministry of justice.

3.3 Prosecutions

In Afghanistan now we use computer and Internet in everything like our banking systems are computer base and we can access to our accounts from everywhere, the biggest announcement of exam I mean Kankor exam's result is online or computer base, online-shopping, and almost governmental and private organization exchange their sensitive data through the internet and all of them are computer base and if a hacker gain access to that data or change it so AFCERT should trace that hacker and catch him or her but for prosecute AFCERT should follow ICT law that unfortunately till now it is not available and for tracing and catching hackers and problem makers they use open source software like: ENCASE, BACKTRACK. These are not valid for other counties.

3.4 Cooperation among institutions

Afghanistan education is now in a better condition and they are many government and private Universities and institution that teach ICT, IT and computer science. If AFCERT will have cooperation with institutions or universities they can help them to awareness of new threats and vulnerabilities and can also help them for lunching some seminars, conferences and courses.

3.5 Education/Awareness

The main part of services of each CERT is to give education and awareness to member of CERT or public but AFCERT don't have any website for awareness and AFCERT is not so active in educate people or government or private organization. Now Computer and the Internet are widely used by Afghan people in their daily life, business, banking, education and almost every part of life but unfortunately they don't know at least basic ways to secure their connections and business etc.

And one thing else is that AFCERT is not one of the National CERT and it is not partner of First, or CERT to get update about current threats.

4 Solutions for Afghanistan Computer Emergency Response Team (AFCERT)

For having good solutions to AFCERT first of all I evaluated four countries CERT those countries are India, Iran, Pakistan and China they are neighbors of our country and somehow we have same culture and we are near geographically. AFCERT can work same like any of these countries CERT and three of them are national CERT without Pakistan CERT.

4.1 Computer Emergency Response Team (CERT) in India

[3]CERT-In (Indian Computer Emergency Response Team) is the National Incident Response Centre for major computer security incidents in its constituency i.e. Indian cyber community. CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents,
- Coordination of cyber incident response activates.
- Issue guiltiness, advisories, vulnerability notes and whitepaper relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

CERT-In is member of FIRST, APCERT and global research partner of APWG.

The primary role of CERT-In is to raise security awareness among Indian cyber community and provide technical assistance and advise them to help them recover from computer security incidents.

CERT-In provides technical advice to system Administrators and users to respond to computer security incidents.

It also identifies trends in intruder activity, works with other similar institutions and organizations to resolve major security issues and to the Indian cyber community.

The purpose of the CERT-IN is to become the nation's most trusted referral agency of the Indian Community for computer security incidents when they occur the CERT-In will also assist members of the cyber security in implementing proactive measure to reduce the risks of computer security incidents.

The Indian Computer Emergency Response Team (CERT-In) operate under the guidance and with authority delegated by the Department of Information Technology of Ministry of Communications & Information Technology , Government of India .

Mission of CERT-In is to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.

The Indian CERT's constituency is the Indian Cyber-community.

And CERT-In has some roles and functions that are explained below:

India CERT to provide single point of contact for reporting local problem assist the organizational constituency and general computing community in preventing and handling computer security incidents. To share information and lessons learned with CERT/CC, other CERTs, response teams, organizations and sites. Provide a 24/7 security service and response the incident.

CERT-In offers recovery procedures, artifact analysis and incident tracing, CERT-In issue security guidelines, advisories and timely advice and also do vulnerability analysis and response, risk analysis, security product evaluation and collaboration with vendors.

[3] www.cert-in.org.in

CERT-In is National Repository of India and a referral agency for cyber intrusions, CERT-In also profiling attackers, conduct training, research and development.
India CERT interacts with vendors and others at large to investigate and provide solutions for incidents.

The main functions of CERT-In are:
Reporting
CERT-In is a central point for reporting incidents and it is database of incidents.

Analysis
CERT-In do analysis of trends and patterns of intruder activity and develop preventive strategies for the whole constituency also in-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

Response
Incident response is a process devoted to restoring affected systems to operation and CERT-In sends out recommendations for recovery from and containment of damages caused by the incidents.
CERT-In helps the system Administrators take follow up action to prevent recurrence of similar incidents.

CERT-In have trainings and the objective is to create security awareness within the Government, public and critical sector organizations and communication and information infrastructure providers and to educate them in the area of Information Security with the latest security threats, needs and developments and deployment of techniques and tools in order to minimize security risk.
The Information Security training at CERT-In broadly covers the following:
Area/Topics:

- Systems and Network Security
- Application Security
- Wireless Network Security
- Security Attacks and Countermeasures
- Secure Coding
- Computer Forensics
- Information Security Policy & Procedures
-

Target Audience:

- Technical Decision Makers , CIOs ,CISOs
- Database , System and Network Administrators
- IT/Security Professional

And also CERT-In has website and provide many information through that we can know about vulnerabilities, trainings and can secure your PCs[4], this is URL of that website: http://www.cert-in.org.in

4.2 Computer Emergency Response Team (CERT) in Iran

Evaluation of CSIRT in Iran:
By entering the Internet in Iran since 1990s , day by day using the Internet become wide in Iran, after almost ten years since 2000 according to increase of the Internet in homes, organizations and government and beside widely increase of users attacks also increased, Network and computer security become valuable and finally in 2006 established CERTCC.

CERTCC MAHER (Iran Computer Emergency Response Team /Coordination Center) is National CSIRTs that is connected with CERT.org.

The Internet has immensely changed the pace of lives, even much more than industrial revolution. Cyberspace Security is the most important issue in the Internet, because numerous incidents are taking place every moment. Thus, according to the importance of incident handling and organizing Computer Security Incident Response Teams (CSIRT) in several countries around the Persian Gulf, it seemed essential to develop a similar center in our country. Therefore, establishment of a CSIRT center came into the agenda by Ministry of ICT. So, MAHER center was founded in order to handle and response the cyberspace incidents.
Scope
Governmental sector:

All of the organizations and governmental companies that work in the subset of Ministry of Information and Communication Technology (ICT)

- Private sector:

All of the companies that are authorized for their activities by Ministry of Information and Communication Technology

- Public sector :

All users may use the website information

Goals

- Create a single point in the Ministry of ICT to coordinate cyberspace incident handling activities
- Policy making, development and optimizing the methods of developing CSIRT teams
- Survey the security potentials in the country cyberspace and actualize them.
- Helping to create CSIRT teams in subsidiary organizations, companies and centers of ICT ministry in the first stage, and then helping to create them in other companies as well.

[4] http://www.cert-in.org.in/secureyourpc.in/SPC_colored_English/large/business_Ed.html

- Facilitate communication between groups and related organizations in order to share information related to the sanity of cyberspace
- Developing secure communication mechanisms for safe communication among all of teams
- Becoming a member of Asian and international CSIRT teams and creating international interactions

Structure
Organizational Structure of this center is as follow:

- Assessing and analyzing team
- Monitoring , data gathering and updating team
- Intrusion detection and incident response team
- Response coordination team
- Maintenance and supporting team

Roles and responsibilities
Cooperation with the national security organizations in order to assure the security of cyberspace and combat with cyber-crimes specifically

- Coordinating CSIRT teams within the ministry of ICT
- Interacting with other teams
- Exchanging experiences and analyzing incident responses
- Exchanging statistics and analysis of incidents
- Cooperating in continuous security assessment of cyberspace
- Transferring knowledge by holding training courses
- Periodic security assessment of member institutions
- Offering services in three levels: reactive services, preventive services ,assessing and auditing services
- Collaborating with other CSIRT groups in the ministry, regional and international zones
- Holding seminars and conferences in order to achieve the CSIRT's goals
- Presenting short-term and mid-term training courses to achieve the CSIRT goals
- Sending experts in order to exchange knowledge in the regional and international areas if needed
- Identifying and communicating with teams involved in producing, developing and improving CERT/CC
- Producing, updating and maintaining CERT/CC Portal in order to promote the public knowledge of security
- Gathering, analyzing, assessing and storing incident information in order to prevent future incidents

- Encouraging the related private and public sectors in order to register in CERTCC and providing secure communication services for the use of members and other users to access security information
- Formulating legislations and instructions to define communication methods between CSIRT teams
- Studying patterns and standards to identify the best methods of developing the CSIRT teams
- Evaluation and assessment of CSIRT teams in the ministry of ICT in order to optimize the teams' activities
- Collaborating with active teams to determine the roles and responsibilities of their sub-centers
- Cooperating in developing the organized CSIRT activities in the ministry of ICT
- Cooperating with relevant authorities to make and approve affective legislations, regulations and policies which affect the development of all CSIRT teams

the CERTCC MAHER provide other services like News, security reports , articles, protect your PC and also for awareness launch some congresses , seminars and courses and CERTCC MAHER has Website that provide may information about new current threats , vulnerabilities of soft wares and security reports and security advisory .

4.3 Computer Emergency Response Team (CERT) in China

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) was founded in September 2002. It is a non-governmental non-profit cyber security technical center and the key coordination team for China's cyber security emergency response community. As a national CERT, CNCERT strives to improve nation's cyber security posture, and protect critical infrastructure cyber security. CNCERT leads efforts to prevent, detect, warn and coordinate the cyber security threats and incidents, according to the guideline of "proactive prevention, timely detection, prompt response and maximized recovery".

CNCERT has branches and offices in 31 provinces, autonomous regions and municipalities across mainland China. As the key coordination organization of China's cyber security emergency response system, CNCERT organizes enterprises, schools, non-governmental groups and research institutes that are specialized in cyber security and coordinates ISPs, domain name registrars and other emergency response organizations in a joint effort to build the cyber security emergency response system of China and handle major cyber security incidents.

As an important non-governmental organization to assist in the cross-border handling of cyber security incidents, CNCERT actively carries out international cooperation in cyber security and is committed to establishing a mechanism of prompt response and coordinated handling for cross-border cyber security incidents. CNCERT is a member of the world-renowned Forum of Incident Response and Security Teams (FIRST) and one of the founders of Asia Pacific Computer Emergency Response Team (APCERT). As of 2013, CNCERT has established "CNCERT International Cooperation Partnership" with 127 organizations in 59 nations and regions.

Mission:

Incident Detection: Leveraging on the cyber security detecting platform, CNCERT performs proactive detection of security incidents for critical infrastructure. It also discovers cyber security threats and incidents by sharing data and information with domestic and foreign partners and by receiving cyber security incident reports from domestic and foreign customers through hotline, fax, email and website.

Early Warning: By making comprehensive analysis of big data and acquiring information from multiple channels, CNCERT can warn cyber security threats, report cyber security incidents and analysis cyber security posture. It provides customers with such services as information on cyber security situation and sharing of cyber security technology and information.

Emergency Response: If incidents of serious threat are proactively discovered or received, CNCERT will respond in a timely manner and actively coordinate the handling. Priorities include incidents that affect Internet operation security, affect a large scope of Internet users, and involve key government departments and critical infrastructure, cause major consequences users complaint, as well as all kinds of cyber security incidents reported by national emergency response organizations of foreign countries.

Security Evaluation: As a professional organization of cyber security evaluation, CNCERT provides security testing services for government departments, public institutions and enterprises guided by the principle of “supporting the regulatory, serving the society” and through scientific methods, standard procedures, impartial attitude, independent judgment and relative standards.

Incident Handling Procedures

Report: CNCERT has set up a 24*7 mechanism to accept the report of cyber security incidents. Both domestic and foreign users can report an incident to CNCERT in the following ways: website, email, hot line and fax.

Acceptance: Cyber security incidents undertaken by CNCERT mainly include the following types: malware, defacement, back door, phishing, vulnerability, information destruction, denial of service attack, abnormal domain, router hijacking, unauthorized access, spam, mixed cyber security incidents and other cyber security incidents.

Handling: After confirming that the incident is true by sufficient evidences, CNCERT will perform emergency handling based on the prompt response mechanism which has established with domestic and foreign ISPs, domain name registrars and cyber security service vendors.

Feedback: When each of the three steps above - report, acceptance and handling - is completed, CNCERT will provide feedback to the reporter, including receipt of the report, whether it is accepted and for what reason, and the handling results.

Services

Monitoring: Monitor and detect cyber-attacks on the basis network, the mobile internet, IDC, value-added business and some vital information systems, such as the online finance and securities. Currently, CNCERT is capable of detecting vulnerabilities, computer virus, such as Trojans and Botnets, defaced web-pages, malware-injected websites, DoS attacks, DNS hijacking, router hijacking, and phishing and so on.

Warning and Notification: Analyze and warn the cyber security threats, notify the incidents and analyze the macro-cyber-security trends based on the rich data sources and information acquired through multiple channels. And CNCERT also shoulders the responsibility of notifying the telecom industry of the cyber security according to the Notification Implementation Measures for Network Security Information which was promulgated in 2009 by the Ministry of Information Industry of China.

Incidents Handling: Handle the cyber-security incidents promptly depending on the efficient working mechanism with the carriers, domain registrars and security vendors as well as on the close cooperation mechanism with vital information departments and enforcements. As a significant member of FIRST and APCERT, two well-known cyber security cooperative organizations, CNCERT has also established cooperative mechanism on incident handling with several renowned cyber security organizations and the national CERTs across the globe. It receives cyber security reports form users home and abroad and handles the major emergencies in time.

Testing and Evaluation: As a professional organization in network and information security testing and evaluation, CNCERT delivers standard and fair relevant services with scientific methods and independent judgments, so as to support government administration and to serve the operational businesses. Being a vital member of China Communications Standards Association, CNCERT also engages in drawing up standards for communications network security and those for security protection of the telecom network and the internet.

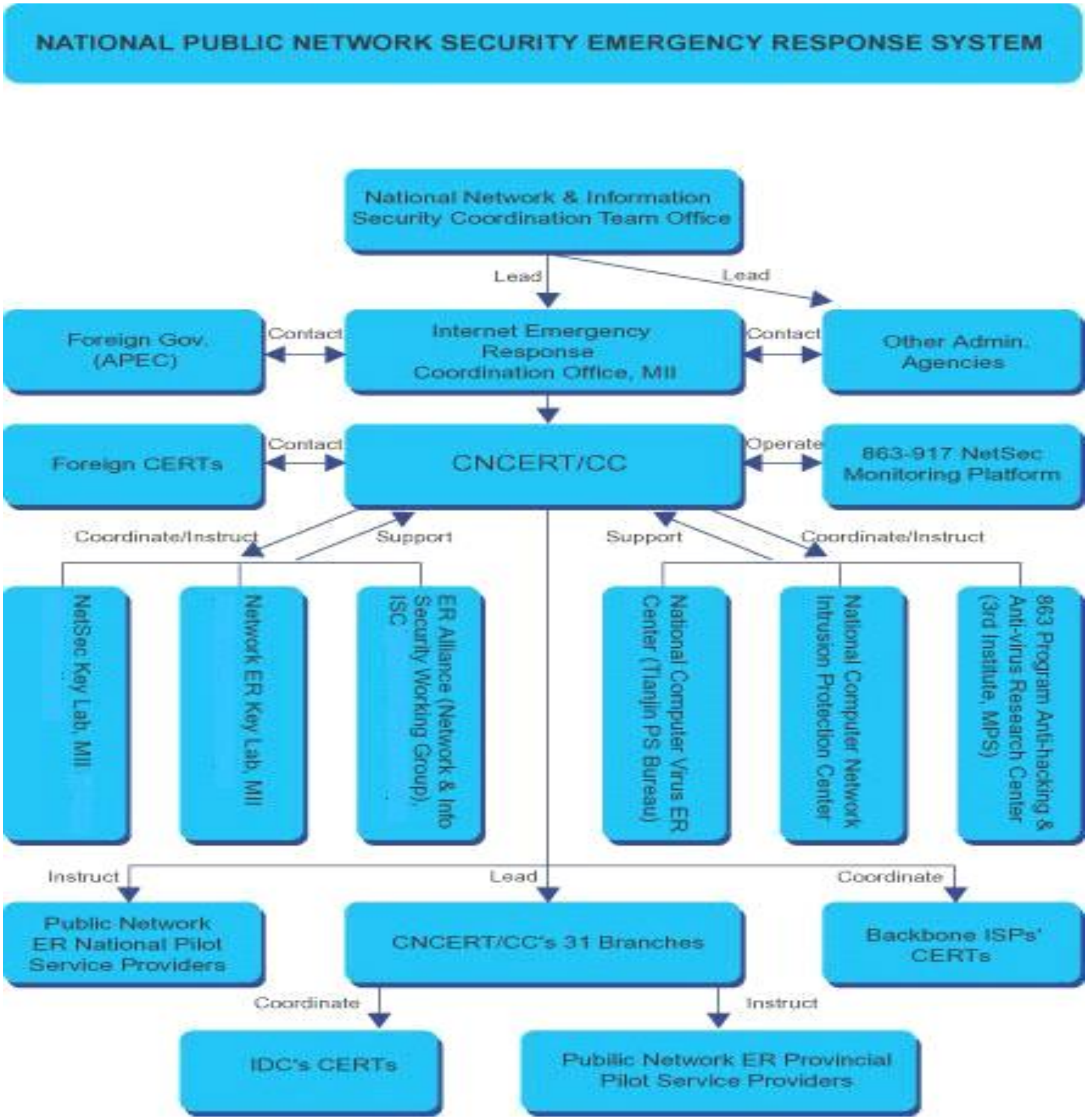
NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM
National Network & Information Security Coordination Team Office
Lead
Lead
Foreign Gov. (APEC)
Contact
Internet Emergency Response Coordination Office, MII
Contact
Other Admin. Agencies
Foreign CERTs
Contact
CNCERT/CC
Operate
863-917 NetSec Monitoring Platform
Coordinate/Instruct
Support
Support
Coordinate/Instruct
NetSec Key Lab, MII
Network ER Key Lab, MII
ER Alliance (Network & Info Security Working Group), ISC
National Computer Virus ER Center (Tianjin PS Bureau)
National Computer Network Intrusion Protection Center
863 Program Anti-hacking & Anti-virus Research Center (3rd Institute, MPS)
Instruct
Lead
Coordinate
Public Network ER National Pilot Service Providers
CNCERT/CC's 31 Branches
Backbone ISPs' CERTs
Coordinate
Instruct
IDC's CERTs
Pubilic Network ER Provincial Pilot Service Providers

Figure 2 Structure of CNCERT and communication with other CERTs.

CNCERT has a website and through that website provide weekly and Annual CNCERT issues and also provide news and events through that website.
You can report an Incident through website of CNCERT.
CNCERT is partner of FIRST and APCERT and also Anti Phishing Working Group (APWG).

4.4 Computer Emergency Response Team (CERT) in Pakistan

I evaluate two CERTs in Pakistan and their services first of all I want to explain both of CERTs services.

PakCERT (Pakistan Computer Emergency Response Team) is a member of Asia Pacific security Incident Response Coordination Working Group.

PakCERT security services were introduced to provide anyone the means to protect their valuable information assets by giving organizations & individuals' direct access to hackers and other IT professionals not usually available for hire.

The PakCERT protect the information assets of their clients through the use of education, technology and experience while maintaining the strictest levels of confidentiality in the industry.

PakCERT equipped with latest exploit codes and techniques the underground is using for years to compromise networks, PakCERT use the same techniques to harden network from such intruder attacks.

PakCERT mission is promoting cooperation amongst IT constituents for the effective prevention, detection and recovery from computer security incidents, providing a means for the communication of alert and advisory information on potential threats and emerging incident situations, promoting the sharing of computer security information, tools and techniques and providing professional security to harden networks from intruder attacks.

There are services that PakCERT provide:

- SECURITY ASSESSMENT & PENETRATION TESTING (SAPT) SERVICES (ETHICAL HACKING)

When any organization hire PakCERT to provide specialized, objective assessment of that organization's security vulnerabilities, that organization will get a cracker-jack team of IS consultants who are also IS researchers. That's because PakCERT believes that IS research must be linked to real-world IS problems, and real-world IS problems must influence what we research.

- ISO17799 COMPLIANCE

ISO17799 is actually a comprehensive set of controls comprising best practices in information security and at PakCERT they focus on the Security Audit Process to ensure business outcomes and for this they are internationally recognized generic information security standard.

- FORENSIC INVESTIGATION SERVICES

  By having this service PakCERT provides an extensive range of services in relation to the investigation and handling of computer related fraud, abuse and email misuse. Whether a computer is integral or incidental to your problem our experienced investigators can assist you from the initial fact finding right through to a successful prosecution or disciplinary action. Working closely with our clients, often under extreme secrecy, we have a proven track record of recovering vital evidence which could not have been found using conventional techniques.

- DEVELOPMENT & IMPLEMENTATION OF SECURITY POLICY FRAMEWORK

PakCERT understands the difficulties associated with developing a security policy and particularly with implementing and operating under new business rules. Fortunately, PakCERT's security policy frameworks provide standard solutions to typical environments thereby lowering the cost and complexity of policy deployment and business operations. PakCERT also understands the impact on cost, staff, and equipment introduced by new regulations.

- ON-DEMAND TRAINING

PakCERT currently provides on-site training on several information security (IS) topics. They provide training on these IS topics of value to your IT organization because they believe in the value of having all IT personnel trained on IS issues that are critical to keeping your business.

- SECURITY TOOLS & TUTORIALS ARCHIVE

Members of PakCERT get access to PackCERT's exclusive archive of security tools, tutorials and proof-of-concept exploits.

Security awareness public services are Advisories, alerts and security patches broadcast. Regular updates are made on the site and also sent to people who have subscribed to their mailing list, Security awareness through seminars and presentations in different IT events and Coordinate with ISPs, vendors and other CERTs to find security related solutions.

And beside of these services PakCERT provide defacement archive of hacked Pakistani websites and also resource center that give a source of information about CERT security checklists and guidelines , Microsoft Windows Security , Macintosh Security , Unix Security , Router Security and some Security Tools.

And PakCERT has a website and organizations can take membership of PakCert through that website and lots of information is available on that website.

Website: www.pakcert.org

The second CERT that I have evaluated from Pakistan is:

[5]*CERT Pakistan is a community project* promoted *by Tranchulas Ltd*.

CERT Pakistan is a non-profit organization dedicated to provide assistance in incident handling, response support and defense against cyber-attacks to Pakistani organizations.

The principle activities of CERT Pakistan are to monitor network threats and vulnerabilities, remain available for incident reports or new information regarding cyber security threats, and to respond to any security breaches in a timely manner. CERT also coordinates with relevant organizations and institutions to make sure our archives and information is up-to-date with the latest information security threats.

CERT Pakistan Vision: To be the most reliable and updated cyber security hub in Pakistan.

CERT Pakistan Mission: We believe in employing the latest information security techniques to build a safer and a more secure IT infrastructure not only for business, but also for safeguarding the national security in cyberspace.

Services of CERT Pakistan: CERT Pakistan offers a number of services to its members on a regular basis. These services are based on the type of security the member needs. From our Early Warning System to the 24/7 Incident Response Service, CERT Pakistan ensures that its members stay up-to-date with the latest in information security methods which makes it easier for them to act at the right time. These services provided by CERT Pakistan are based on a minimal fee.

The membership fee is based on monthly payments to CERT Pakistan.

For small size organizations (500 network users) monthly Rs.10000 , medium size organizations (1000 network users) monthly Rs. 16000 and large size organizations (2000 network users) monthly Rs. 18000.

Services List: CERT Pakistan offers a number of services to its members on a regular basis. The price of these services is included in the monthly membership fee. The services provided by CERT Pakistan include the following:

[5] Www.cert.org.pk

www.tranchulas.com

Security and Threat Updates: This service provides the members with the on-going information about different methods of security breaches, vulnerabilities in systems as well as their defense tactics. CERT Pakistan also provides the members with updates on the recent trends and events in cyber security around the world. This analysis would be done on a need basis i.e. when new events occur around the world, CERT Pakistan would update its members.

Early Warning System: The early warning system provides critical information about a direct threat or any information that requires the members' immediate attention. For any possible update like this, the members are advised to regularly check the contact number/email that they provided CERT Pakistan.

Security Archive Access: CERT Pakistan currently has an online archive which has articles and information about the threats, risk management, historical data and the work currently done on the security management. The members are given a username and password to access these archives at their own comfort.

Incident Response Service: This service is carried out by the team which is the first to respond to an incident that is reported to CERT Pakistan. It functions 24 /7 in order to minimize the response time in an event of a security breach. The team diagnoses the security threat and provides details on the nature of the breach. It also starts the recovery process and the members are also briefed about how to prevent such an incident from occurring in the future.

Conferences: CERT Pakistan arranges conferences on a need basis to update the members with the latest in information security news. The members would be given discounts on the fee of the conference and would also have the option of utilizing any speaking slot if they want.

CERT Pakistan is strictly a non-profit organization. The member subscriptions and the conference fees only cover the operational cost of the company.

CERT Pakistan also has a website that provides some general information and organizations can get membership to CERT Pakistan through that website and here is the URL of that website: http://www.cert.org.pk

4.5 Recommended solutions for AfCERT from mixture of all CERTs

According to these four countries CERTs and the main structure of a national CERT I recommend AFCERT some solutions.

1. All CERTs operate 24x7 because it is an computer security organization and just 7 hours per day is not enough for AFCERT and with hiring part time employees AFCERT can solve this problem and I recommend AFCERT to connect with computer science institutions and universities they have qualify students to introduce AFCERT for part time job.

2. All CERTs have official website and through that website provide information about threats and vulnerabilities and provide and recommend some feature to secure PCs and take report of threats and announce events, seminars and training courses. That website can help AFCERT to have interaction with members and makes easy their work.

3. Fortunately in Afghanistan Universities and Institutions promote very well especially in field of Computer Science if AFCERT will have cooperation to these sectors it will help them for education and awareness.

4. CNCERT (China National Computer Emergency Response Team) and CERT-In (Indian Computer Emergency Response Team) are good templates for AFCERT to work like that.

5. AFCERT make branches and offices in 34 provinces. As the key coordination organization of Afghanistan's cyber security emergency response system, AFCERT organizes enterprises, schools, non-governmental groups and research institutes that are specialized in cyber security and coordinates ISPs, domain name registrars and other emergency response organizations in a joint effort to build the cyber security emergency response system of Afghanistan and handle major cyber security incidents.

6. AFCERT should make itself a national CERT that have partnership with FIRST and CERT and APCERT. Here are stages to make a National CERT: (Killcrece, August 2004)

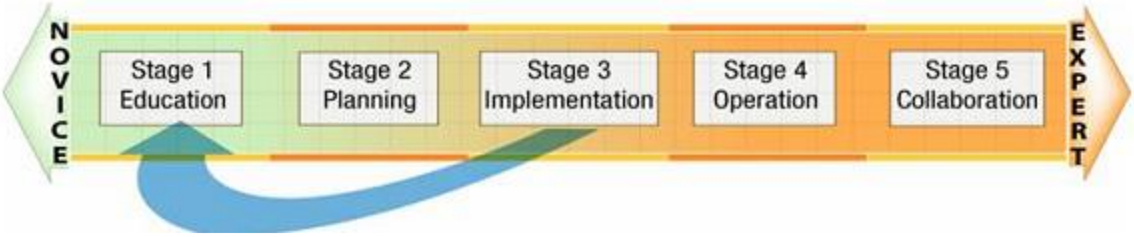

Figure 3 Stages of making National CERT.

Feature	AFCERT	China CERT	Iran CERT	India CERT	Pakistan CERT
National CERT	No	Yes	Yes	Yes	No
24*7 Services	No, Just 7 hours per day	Yes	Yes	Yes	Yes
Website	Under construction	www.cert.org.cn	www.certcc.ir	www.cert-in.org.in	www.cert.org.pk www.pakcert.org
Mini CERT	No	Yes	Yes	Yes	Yes
Services	Alerts organizations about major security incidents through official letters, emails and workshops and also AFCERT share security advisories. Aware people from security issues.	Monitoring, Warning and Notification, Incidents Handling, Testing and Evaluation,	Assessing and analyzing team, Monitoring, data gathering and updating team, Intrusion detection & incident response team, Response coordination team, Maintenance and supporting team	Provide single point of contact for reporting local problem assist the organizational constituency and general computing, offers recovery procedures, artifact analysis and incident tracing, profiling attackers, conduct training, research &developme	SECURITY ASSESSMENT & PENETRATION TESTING (SAPT) SERVICES (ETHICAL HACKING), ISO17799 COMPLIANCE, FORENSIC INVESTIGATION SERVICES, DEVELOPMENT & IMPLEMENTATION OF SECURITY POLICY FRAMEWORK, ON-DEMAND TRAINING, SECURITY TOOLS & TUTORIALS ARCHIVE

				nt	
Cooperation Partners		FIRST and APCERT and also Anti Phishing Working Group (APWG).	FIRST and APCERT	Partner of APWG	APCERT
Member -ship	ITU-IMPACT	FIRST, APCERT, CNCERT International Cooperation Partnership" with 127 organizations in 59 nations and regions.	CERT.org and it is a National CERT	CERT-In is member of FIRST, APCERT and global research	Asia Pacific security Incident Response Coordination Working Group.
Mission	Detect the security issues (Intrusions, virus, spam and etc.) and will make aware the member, registered organizations regarding the threat and will also help, recommend them how to overcome the issues.	Incident Detection, Emergency Response, Security Evaluation	Create a single point in the Ministry of ICT, Policy making, Survey the security potentials, Developing secure communication mechanisms, Becoming a member of Asian and international CSIRT	Profiling attackers, conduct training, research and development, Forecast and alerts of cyber security incidents, Emergency measures for handling cyber security incidents, Coordination of cyber incident response activates, Issue guiltiness, advisories, vulnerability	Promoting cooperation amongst IT constituents for the effective prevention, detection and recovery from computer security incidents, providing a means for the communication of alert and advisory information on potential threats and emerging incident situations, promoting the sharing of computer security information, tools and techniques and providing professional security to harden networks from intruder attacks.

				notes and whitepaper relating to information security practices, procedures, prevention, response and reporting of cyber incidents	
Incident Handling Procedures	Official letters emails and workshops and also AFCERT share security advisories to organizations through official letters, emails and workshops.	Report, Acceptance, Feedback	News, security reports, articles	Reporting, Analysis, Response	Report, Acceptance, Analysis, Response
Date of Establishment	2009	September 2002	2006	January 2004	.

5 Conclusions

This document is about AFCERT (Afghanistan Computer Emergency Response Team) Challenges and solutions.

First Section of this document is about CERT (Computer Emergency Response Team), History of Computer Emergency Response Team, Purpose of Computer Emergency Response Team and types of CERTs.
CERT is part of the U.S. federally funded Software Engineering Institute (SEI) at Carnegie Mellon University. CERT is chartered to work with the Internet community in detecting and resolving computer security incidents. The Morris Worm motivated the formation of CERT at the directive of the Defense Advanced Research Projects Agency (DARPA). The CERT Coordination Center (CERT/CC) focuses on coordinating communication among experts during security emergencies to help prevent future incidents. CERT responds to major security incidents and analyzes product vulnerabilities. CERT works to manage changes relating to progressive intruder techniques and to the difficulty of detecting attacks and catching attackers. CERT develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of services.

Computer emergency response teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT).

The initial CERTs were created by the efforts of various government agencies in the United States who implemented CERT structures in the late 1980's in response to a number of network incidents denying users of computing services for critical periods of time. In 1988, the Defense Advanced Research Projects Agency (DARPA) funded the CERT/CC (Computer Emergency Response Team/Coordination Center) to respond to computer security incidents related to the Internet network, concentrating mainly on UNIX2 operating system.

Second section is about AFCERT (Afghanistan Computer Emergency Response Team) and which kind of structure and services it has.
MCIT has focused on the establishment of physical ICT infrastructure in the country, since 2009 it is shifting its focus to the information layer. In order to bring in e-applications and make use of the already laid-down infrastructure it is quite important to have the related Cyber Security institutions, tools, regulations and infrastructure in place.

In this regard MCIT has taken the initiative to establish AfCERT. The Unit for AfCERT has been established, Staff hiring has started, ICT law has dedicated chapters for cyber-crimes, Joined the ITU-IMPACT Collaboration.

ITU has commitment to send two experts towards the end of 2009 to Kabul, to start drafting; Mechanism for the operation of the AfCERT needed SOPs for AfCERT, policies how AfCERT will interacts the Chief Security Officers in other ministries and organizations in Afghanistan of the Chief Security Officers essential documentation for affiliation of AfCERT with other international CERTs essential documentation which will clearly mention the focused areas for AfCERT to operate e.g. Spam, Intrusion Detection, Hacking etc. and training for the staff.

Third part of this document talking about Afghanistan Computer Emergency Response Team services that are limited and AFCERT is face to some challenges in this document I tried to mention those challenges.

Fourth part of this document is about solutions for AFCERT that I introduced some CERTs of our neighbor countries such as China, India, Iran and Pakistan that they are national CERT and have partnership with FIRST and APCERT and also Anti Phishing Working Group (APWG).

And working 24/7 and providing multiple services and can catch problem makers and attackers easily.

Finally, by mixture of all these CERTs I recommended some solutions to AFCERT and in the end with a table I compared AFCERT with other countries CERTs such as China, India, Iran and Pakistan.

I hope this document will be a useful document for AFCERT and some topics that I couldn’t cover it by this document I can provide those topics as future work those are How to make AFCERT as National CSIRT and making mini CERTs to 34 provinces of Afghanistan and connect them to Central AFCERT and How to make AFCERT member of FIRST and APCERT and also Anti Phishing Working Group (APWG).

CERT Acronyms and Names:

CERT- Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

CSIRC - Computer Security Incident Response Capability or Center

CIRC - Computer Incident Response Capability or Center

CIRT - Computer Incident Response Team

IHT - Incident Handling Team

IRC - Incident Response Center or Incident Response Capability

IRT - Incident Response Team

SERT - Security Emergency Response Team

SIRT - Security Incident Response Team

AFCERT- Afghanistan Computer Emergency Response Team

PakCERT -Pakistan Computer Emergency Response Team

CERT Pakistan - Computer Emergency Response Team Pakistan

CNCERT or CNCERT/CC -National Computer Network Emergency Response Technical Team/Coordination Center of China

CERT-In -Indian Computer Emergency Response Team

CERTCC MAHER- Iran Computer Emergency Response Team /Coordination Center

MoC – Ministry of Communication

E-Gov – Electronically Government

TeliaCERTCC - Telia CERT Coordination Centre

JPCERT/CC - Japan Computer Emergency Response Team Coordination Center

6 References

(Afghanistan, 01-Jan-2006 / 31-Dec-2006)

(Georgia Killcrece, 2003)

(Killcrece, August 2004)

(Moira J. West-Brown, April 2003)

(Ruefle, 2008)

7 Bibliography

Afghanistan, U. N. (01-Jan-2006 / 31-Dec-2006). *Information and Communications Technology (ICT) Project (Phase II)* . Kabul: UNDP Afghanistan.

Georgia Killcrece, K.-P. K. (2003). *State of the Practice of Computer Security Incident Response Teams (CSIRTs).* Pittsburgh : Carnegie Mellon University.

Killcrece, G. (August 2004). *Steps for Creating National CSIRTs.* Pittsburgh, USA: Software Engineering Institute Carnegie Mellon University .

Moira J. West-Brown, D. S.-P. (April 2003). *Handbook for Computer Security Incident Response Teams (CSIRTs)* . Pittsburgh: CMU/SEI.

Ruefle, G. K. (2008). Creating and Managing Computer Security Incident Response Teams(CSIRTs). Pittsburgh, Pennsylvania: Software Engineering Institute Carnegie Mellon.