ISBN-13: 9781511509992
ISBN-10: 1511509996

Recent Advances in Cybersecurity

By: Elsadig Saeid

Preface

The world had seen the fastest revolutions in the information and communication technology in the last two decades. Today, almost every aspects of human life are depending on the ubiquity cyberspace. Productivity, social networking, social development and movement, education and innovation, fighting a wear, marking product …etc, are just few of these facets of life that making use of the telecommunications connectivity and information technology. Inspite of all the benefits gained from this revolution; there are many inherited risks. As the world become very small, serious cybercrimes on communications and critical infrastructure goes behind the political and administrative boundaries (transnational). Moreover, the cybersecurity problems enlargement and development are appears to imitates the revolution in the communication and information technology.

This book aims to introduce the reader to the state of arts in the cybersecurity and critical information infrastructure protections. The first two chapters introduce the reader to the historical aspects of ICT development and a broad classification of cybersecurity problems. A chain course of actions to compete cybercrimes starting from introducing Chief Information security officer (CISO), planning, deploying technology tools, developing attribution methods, and developing legal framework are described in chapters three to six. Chapters seven, describes the cybersecurity problems inherited from using social networking systems and how to protect both family and child in the cyberspace. Parts of the celebrative efforts of the international community to secure the cyberspace are been described in chapter eight. Chapters nine through fifteen survey and describe individual countries experience and recent policies to toggle cybersecurity problem and maximally making use of the potential benefits brought by the cyberspace. Namely, these chapters survey Qatar, Australia, Malaysia, United States, Japan, United Kingdom, and the European Union. For each country, the national broadband plan, cybersecurity initiatives, Cybersecurity State, and non-governmental organizations established, child online protection efforts, and cybersecurity lows and legal frameworks enforced are been discussed.

This book, highlight the areas that will have the biggest impact on cybersecurity, thus, it can be considered as starting text for any one feel in shortage in his cybersecurity knowledge. In addition, it can be consider as policy manual for those seeking more progressive data protection.

TABLE OF CONTENTS

CHAPTER ONE 1

RECENT DEVELOPMENT IN COMMUNICATIONS AND INFORMATION TECHNOLOGY 1

Introduction 1
Historical overview of wired communications 4
Historical overview of wireless communications 5
The Development of Cellular System Communications 6
The development of Wireless Local Area Networks (WLANs) 8
Satellite Communications 8
Communications Network Components 11
The enlargement of Storage system 12
Data Center 13
Managing data centers 14
Data Replication 15
Data Backup 16
Layered Design approach and telecommunications standardization 16
Internet Growth and Development 16

CHAPTER TWO 19

RISKS ON INFORMATION AND COMMUNICATIONS SYSTEMS 19

Introduction 19
Classifications of Risks 19
Human-induced Risks 21
Some Example of Informatics and Communications Disasters 21
Submarine Cable link Disruption 21
Economical and Social Impacts 23
Estonia Cyber attacks on 2007 24
Early Response 25
Experiences learned 26
Problems Associated with Information and Communication Disasters 26

CHAPTER THREE 30

CHIEF INFORMATION SECURITY OFFICER (CISO) 30

Introduction 30
The general framework for the job 30
Technical Security 31
Information Security Management 32
Strategic Security 32
CISO Functions 32
CISO Career pathway 34

CHAPTER FOUR 38

PLANNING, DRAFTING AND BUILDING PRACTICAL AND LEGAL FRAMEWORKS 38

Introduction 38
Planning and Drafting the practical and legal framework 38
Human Factors 41
How to Control the Human Factors 42
Business Continuity 44
Disaster Recovery Plan 44

CHAPTER FIVE 46

TECHNOLOGIES AND TOOLS 46

Introduction 46
Technical tools for Information Protections 46
Firewall 46
Intrusion Detections 48
Anti-virus 49
Access Control 49
Authentication Systems 49
Encryptions 50
Attribution Methods 52
Security Models 53
System Assessment and testing standard 53

CHAPTER SIX 55

DIGITAL FORENSICS AND ACTING IN ACCORDANCE WITH THE RULES AND REGULATIONS 55

Introduction to Digital Forensics 55
Digital Forensic Tools 56
Legal Problem behind the process of digital Forensic and Collecting Evidence 57
Auditing 57
System auditing: Regulatory and compliance 60
Reporting 61

CHAPTER SEVEN 62

SOCIAL NETWORKS, FAMILY AND CHILD PROTECTION 62

introduction ..... **Error! Bookmark not defined.**
Social Networking Websites 62
General purpose social networking website 62
Social Networking for Education 63
Threats on some social networking sites 64
Legal Aspects 65
The negative uses of social networking system by total regimes and ideological groups 65
Child and Family Protection 66
Tools for Families Protection 68

CHAPTER EIGHT 73

INTERNATIONAL ORGANIZATIONS AND CYBERSECURITY 73

Introduction 73
The International Telecommunication Union (ITU) 73
ITU's Global Cyber-security Agenda (GCA) 74
ITU Cybersecurity Projects 77
International Multilateral Partnership Against Cyber Threats (IMPACT) 82
Global response centre 83
Policy and international Cooperation Centre 84
Training and Skills development 84
Security Assurance and Research 85
Forum of Incident Response and Security Teams (FIRST) 85
The main services provided by FIRST 86

CHAPTER NINE 87

QATAR EXPERIENCE 87

Current National Plans and Future Direction 87
Critical Sectors 88
Past and Present Initiatives and Policies 88
Organizational and institutional Overview 90
Early Warning 91
Child Online Protection (COP) 91
Laws and Legislations 92
Some Important web Resources 93

CHAPTER TEN 94

AUSTRALIAN EXPERIENCE 94

Current National Plan and Future Direction 94
Critical Sectors 95
Past and Present Initiatives and Policies 95
E-Security Law 97
Organizational and institutional Overview 97
Early Warning and Public Outreach 99
Child Online Protection (COP) 99
Laws and Legislations 102
Some Important web Resources 103

CHAPTER ELEVEN 105

MALAYSIAN EXPERIENCE 105

Current National Plan and Future Direction 105
Critical Sectors 105
Past and Present Initiatives and Policies 107
Cyber security conference 2005 108
Malaysian National Cyber-Security Policy 2007 108
Organizational and Institutional Overview 109
Early Warning and Public Outreach 109
Malaysian Computer Emergency Response Team 109
Cyber-Security Malaysia 110
Child Online Protection (COP) 112
Laws and Legislations 113
Some Important web Resources 113

CHAPTER TWELVE **115**

UNITED STATES EXPERIENCE **115**

Current National plan and future Directions 115
Critical Sectors 116
Past and Present Initiatives and Policies 117
Organizational and institutional Overview 119
Early Warning and Public Outreach 122
Child Online Protection (COP) 125
Laws and Legislations 127
Some Important web Resources 128

CHAPTER THIRTEEN **129**

JAPANESE EXPERIENCE **129**

Current Status and Future Directions 129
Critical Sectors 129
Past and Present Initiatives and Policies 130
Japan Cybersecurity Strategy *130*
The Basic Policy of Critical Information Infrastructure Protection *130*
Information Security Human Resource Development Program *131*
Management Standards for Information Security Measures for the Central Government Computer Systems *131*
Technical Standards for Information Security Measures for the Central Government Computer Systems *131*
International Strategy on Cybersecurity Cooperation J-initiative for Cybersecurity *131*
Information Security Outreach and Awareness Program *132*
Organizational and institutional Overview 132
Early Warning and Public Outreach 133
Child Online Protection (COP) 136
Laws and Legislations 138
Some important web resources 139

CHAPTER FOURTEEN **141**

UNITED KINGDOM EXPERIENCE **141**

Current Status and Future Directions 141
Critical Sectors 142
Past and Present Initiatives and Policies 142
Organizational and Institutional Overview 143
Early Warning and Public Outreach 145
Child Online Protection (COP) 146
Laws and Legislations 148
Some important web resources 149

CHAPTER FIFTEEN **150**

EUROPEAN UNION EXPERIENCE **150**

European Union national Plan 150
Identified Critical Sectors 151
Initiatives and Policies 151
Child Online Protection (COP) 153
Laws and Legislations 155
Some important web resources 156

REFERENCES **158**

LIST OF ABBREVIATIONS **171**

Chapter One

Recent development in Communications and Information Technology

Introduction

There is no doubt that the most important developments at the end of the twentieth century and the beginning of the twentieth century, is the acceleration of communications and information system development. Today information and communications technology is used in all aspect of human live. Before we entering deploy into the discussion of positive, negative, aspects of these systems, we are going to define both the main element of communication and information technology and the current state of arts in this field.

In 1988 Edward A. Lee and David G. Messerschmit wrote on their first edition of the book "Digital Communications " [1]

> "Why would voice and images be transmitted digitally? Doesn't digital transmission squander bandwidth? Doesn't it require more expensive hardware? After all, a voice-band data modem (for digital transmission over a telephone channel) costs ten times as much as a telephone and (in today's technology) is incapable of transmitting voice signals with quality comparable to an ordinary telephone. This sounds like a serious condemnation of digital transmission for analog signals, but for most applications, the advantages outweigh the disadvantages . . ."

In their introduction of the second edition of the same book published 1994[2], the authors obligated to revise the opening statement to the following….

> "Not so long ago, digital transmission of voice and video was considered wasteful of bandwidth ….was of concern. More recently, there has been a complete turnabout in thinking . . . In fact, today virtually all communication is either already digital, in the process of being converted to digital, or under consideration for conversion"

This complete turning about in the opening sentence of the book within short period (6 years) reflects the rapid development witnessed in this area in the last two decades. This development is due astonishing and rapid advance of scientific research in key areas that form the ribs and the important pillars of the communications and in-

formation revolution of the twentieth century. Figure 1.1 illustrates these key research areas.

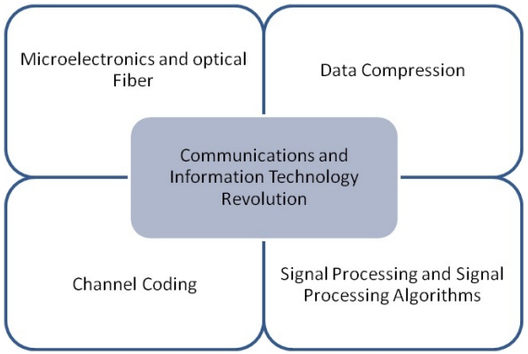


Figure 1.1: illustrates the main four pillars of information and communication Technology

In the last two decades, there was remarkable progress made in the data compression, which leads to a lot of bandwidth efficiency in communications systems, and reduction of the space required storing the data in the computing storage mediums. For example, in the television transmission: the satellite bandwidth required to transmit 32- analog TV channels two decades ago is been used today to transmit hundreds of digital TV channels. This advance in data compression also accompanied with massive development in the microelectronics and microprocessor engineering, which lead to enormous advances microprocessor computation and microelectronic device price cut down. The other factor, which also has a direct relationship to the development of microelectronics, is the advancement in the channel coding and digital signal processing. The progresses in these two areas lead to massive simplification of complex system design and practical design realization.

In fact, the technological advancement in these areas, did not lead to the ICT revolution of today, but had a significant impact in shaping our life in the twentieth century and the beginning of the twenty first century. These technologies are used in all fields of engineering, industrial, medical, and agricultural ...etc. Specifically we can mention a number of these areas are as follows:

- Medicine and biomedical engineering (diagnostic and therapeutic medicine);
- Industry (i.e. testing the quality of the picture and sound processing);
- Testing buildings and civil infrastructure assets using image processing and signal processing;
- Exploration and exploitation of natural resources and minerals using communications technology, control systems, signal and image processing;
- Security applications and crime prevention (i.e. streets and strategic place monitoring);
- Defense industry (i.e. accuracy correction, exploration by radar);
- Scientific research (measurements, control, computing, and analysis);
- Increase the efficiency of operation of industrial processes (i.e. optimum electricity power generation, transmission, distribution, and industrial process control);
- Measure and forecasting weather and early warning sensing (as in the cases of earthquakes and floods)
- Sophisticated quality tests and to identify the ingredients and active substances (i.e. using of Fourier Transform Infrared Spectroscopy (FTIR) analyzer);
- ... etc

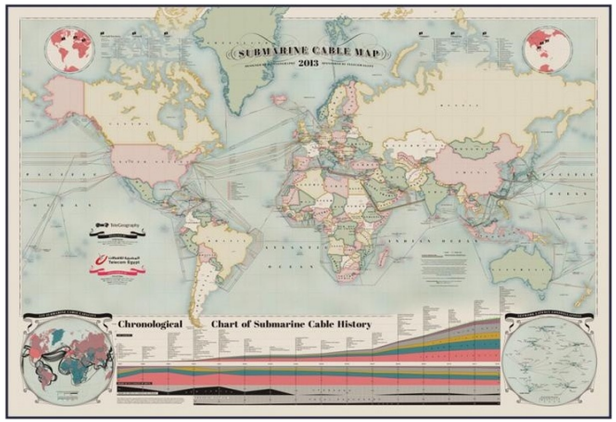
This time of the twenty-first century criminals, increasingly rely on the Internet and advanced information and communication technology (ICT) to further their criminal operations. These unlawful can easily leverage the ICT to carry out even traditional crimes such as distributing illicit drugs and sex trafficking. As well, they exploit the digital world to facilitate crimes that are often ICT technology driven, including identity theft, payment card fraud, and intellectual property theft. Cybercrimes have economic, public health, and national security implications, among others. Therefore, today we have two choose, either to work together to realize the potential of these technology and cybersecurity. On the other hand, we can succumb to narrow

interest and under fears the limit progress. Thus, today cybersecurity is not and end into itself: it is instead an overall individual, organizational, governmental, and international community obligations that all nations and people around the world must contribute their efforts willingly to ensure that the innovations in the area of cybercrime prevention is continue to improve the life of people.

In the next sections, we are going to build preliminary background on historical overview on the development of the ICT technology component and showing how we end up with ubiquity- networked and connected world.

Historical overview of wired communications

In March 1876, with 29 year old, Graham Bell was able to discover the telephone and established the foundation of the telephony networking[3]. Since then, this technology is widely used all over the world for all socioeconomic activities. Conventionally, telephone networking was using traditional Law impedance cable as transmission medium. In 1977, optical fiber is been used for data transmission at limited distances. Consequently, the manufacturing fabrications process is developed and fiber optic cables is been used for the first time for transoceanic communications in 1988. In this time United States is connected to Europe with 3150-mile cable with capacity up to 39000-voice channel[4, 5]. Since 1988, the upper capacity limit of the fiber optic cables approximately doubled each year. Recently in 2013 the maximum laboratory tested capacity is 1.05 Beta bits per second (Beta bits/sec) over one single mode fiber [6], which equivalent to 16x10^9 voice channel. Also during this time, the world has seen remarkable ubiquity connectivity using submarine cables. Figure 1.2, shows recent worldwide submarine cable map as per 2013.



Figures 1.2: Illustrates the latest picture of the transoceanic fiber optic submarine networking. (Source: TeleGeography, www.TeleGeography.com)

Historical overview of wireless communications

We can trace back starting day of the development of the wireless communication to 1895 when first time Marconi was able to send simple signal over a wireless channel. At the beginning of the twentieth century, a lot of socioeconomic factors were contributed to limits of the usage of wireless communication widely except for dedicated application (i.e. Military, and defense applications). At the ends of the second world wear, the American Scientist Cloude Shannon [7] published this excellent work on the capacity of the communications channel in 1948. This work sparks out a lot of research and development across a broad area of communications and signal processing. Consequently, channel coding for near space and deep space communications is been developed during sixties and seventies. The communications to the deep space enables research centers to send space vehicles far to discover what is around our world and communicate different information signals back. The object for near space communications is to enable people on the earth to communicate the information over a wide area. This goal is been achieved by satellite communication systems. Other areas of wireless communication which seen remarkable development in

the last two decades are the cellular communications and Wireless Local Area Networks(WLANs). In the next section, we are going to describe the development in these areas

The Development of Cellular System Communications

Unlike the usage of wireless mobile communication, which was developed at the beginning of the twentieth century, we can trace back the history of the cellular systems to the sixties and seventies of the last century when the concept cellular communications was developed at the Bell lab in the United States[8]. The main idea of the cellular communications is to divide the considered geographical area into small cells. Each set of mobile units within the cell coverage area is been connected to fixed base station unit located at the centre of each cell.

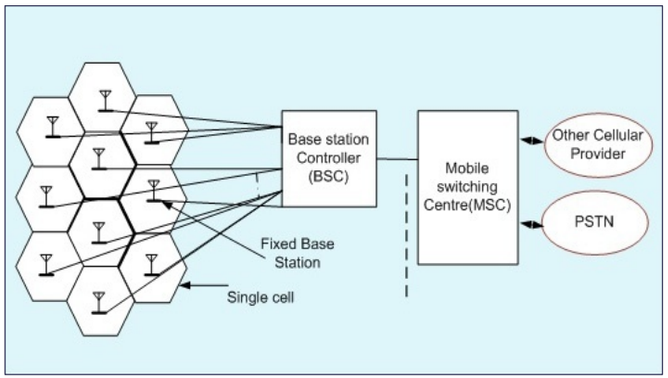


Figure 1.3: cellular System Network Architecture

In practice, the first generation cellular communications was developed in 1978. This system deployed in many developed countries around the world such as United States, Japan, and most of the European countries during the eighties of the last century. The most important services provided by this system are voice communications and locations determinations. At the end of the eighties and the beginning of the nineties the second generation of the cellular system id developed. This system makes use of the digital transmission technology to provide both better voice and SMS communication services[9]. The development of the microelectronics and the reduction of the price of the system component were the main factors that contributes to the wide spread of this system around the world in short period.

In 1997, the International Telecommunication Union (ITU) published the main requirement of what called the third generation cellular communication systems. The main service that required to be providing by this system are voice, SMS, and data transmission. Due to the economical crisis in south east Asia, and the largely slow down all over the world, system providers continuing the development of the second generation by upgrading the second generation to what is called 2.5 generation. In this system (GPRS, CDMA-1x) low data rate is transmitted by adapting packet switching over circuit switching. After the economical recovery, a lot of countries around the world were able to deploy the third true third generation system which provide relatively high data rate in addition to the conventional voice and SMS services. The special data communications components developed for the third generations are consequently developed and upgraded to 3.5 and 3.75 generations[10].

In 2008, the European 3GPP (Third Generation Partnership Project) group developed the main specifications of what is called Long Term Evolution (LTE) system, which are equivalent to the ITU specifications of the fourth generation cellular system. The main merits of this system are[11, 12] Providing high speed data rate;

- Reduces the transmission latency
- Increase the system capacity;
- Reduce the system architecture complexity;
- Making use of the IPv4/IPv6

These merits were achieved in the system design by making use of the Multiple Input Multiple Output (MIMO) and Orthogonal Frequency Division Multiple Access (OFDMA) technologies[13]. Today, in fact many countries around the world are already deployed the LTE or in the rollout process to deploy it soon. Table 1.1 summarizes the most important basic features of successive generations of cellular communication systems.

Table 1.1: Cellular systems subsequent Generations

Generation	Standards	Multiple Access	Service Supported
First Generation - 1978	Advanced Mobile Phone System (AMPS)	FDMA	Voice Service
Second Generation 1990	GSM, IS-95, IS-136	TDMA/ CDMA	Voice and SMS services
2.5th Generation	GSM-GPRS, CDMA-2000 1x	TDMA/ CDMA	Voice, SMS and Data services
Third Generation	WCDMA/CDMA-EVDO/UMTS	WCDMA	Voice, SMS and Data services
3.5th Generation	HSD-PA/HSDPA+/CDMA2000 1xEV-DO Revision A	WCDMA	Voice, SMS and High speed Data services
Fourth Generation	LTE/LTE advanced	OFDMA	Voice, SMS and High speed Data services

The development of Wireless Local Area Networks (WLANs)

In 1991, a group within the IEEE established to consider developing a wireless standard compatible with wired IEEE 802.3. This group is able to publish the IEEE 802.11 standard, which known globally as, Wi-Fi or wireless local area network standards in 1997. Today, the Wi-Fi technology is used to support the access network connectivity to integrate homes, public areas, schools, playgrounds, and universities open yards to the high speed core network[8]. Table 1.2; list the main types and characteristics of WLAN technology components and characteristics.

Table 1.2: Wireless local area network technology

Model/Standard	Peak Data Rate	Frequency
IEEE 802.11a	54Mb/s	5MHz
IEEE 802.11g	54Mb/s	2.4MHz
IEEE 802.11n	380Mb/s	2,4, 5MHz

Satellite Communications

We can assign the beginning of the idea of using Satellite links, to the paper, published in the journal of Wireless World by the British scientist Arthar Clark 1945, which was titled “Extra-terrestrial Relays” [14, 15]. After about twenty years from the emergence of this initial idea in this paper, the first space vehicle Synchronous Communication Satellite or Syncom-3 is lunched into space. As shown in the figure 1.4, this space segment was been operated by the National American Space Agency NASA in the geosynchronous earth orbit. The purpose of this geostationary satellite is to relay communications across the Pacific Ocean (location: above the equator at 180 degree East).

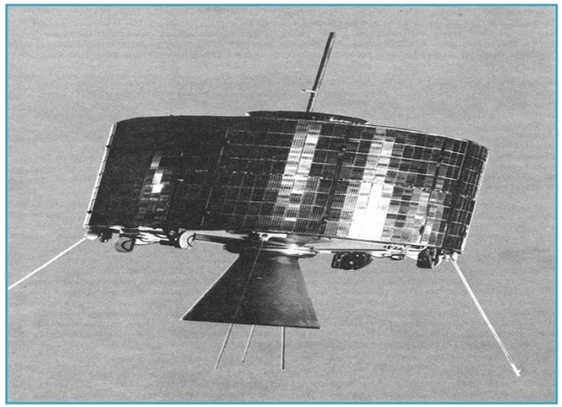


Figure 1.4: Syncom-3 Space Segment- 1964 -(Source NASA- http://nssdc.gsfc.nasa.gov)

Next, in April of the year 1965, Intelsat international organization launch it is first space segment Early Bird in the geostationary orbit at the 28 degree west. This satellite system is been used for telecommunication relaying transmission of telephony services across the Atlantic Ocean. Given the high cost of manufacturing and operating satellite system, in the early time regional, national, and international organizations are used to share the capital cost of building and operating satellite systems for both civil and military purposes. Table 1.3 includes the most important international organizations operating satellite communication systems.

Table 1.3: List of some important international satellite communications operators

National / International Organization	Operating Region
INTELSAT (1964-2001)	Operate 52 space segment in different part of the world to provide regional and transoceanic communication
Arabsat (1976-current)	Operate 5 satellite segment to cover Arab league countries and north Europe[16]
SES S.A	Operate 54 satellite space segment to have 99% coverage
Eutelsat	European group for commercial radio and TV broadcasting

The most important services provided by satellite systems are:

- Communications services to meet the requirements of civil applications, which includes both of the following:
    - Television and radio broadcasting service;
    - Voice communications (telephone);
    - Broadband services (data transfer);
    - Internet service;
- Military services;
- Early warning services;
- Air traffic management;
- Weather measurement and forecasting;
- Remote sensing;
- Global positioning system (location and time referencing);

Manufacturing, operating and facilitating satellite space segments to build large communication networks is astonishing and interesting fields of study, and that is difficult to describe in a small paragraph, therefore we recommend the reference [17] for readers eager to deepen their knowledge in this area..

Communications Network Components

Communications network is an integrated system to connect between the transmitter and receiver, through a set of elements (hardware and software components and connectors). These infrastructure components can be classified into three basic types as follows:

1. Telecommunication Transmission Network Elements: these elements constitute an infrastructure that connects between countries, states, different cities and the major sites within a single city. Within this type we have fiber optic transmitters and high-speed microwave link components (both ground and satellite components).
2. Access Network: This network enables the end user End-user access to the main sites and service (Central office, Interconnection and Switching office). Access network uses a different type of physical links such as regular telephone cables, fiber optic cables to homes (fiber-to-Home), etc.
3. Core Network, a network that connects and controls the Transmission network and the access network. Core network consists of the following elements:
    - Switching Elements
    - Interconnections elements
    - Data/Internet and messaging (Severs, Router and Switches)
    - Accounting and Control System
    - General value added service systems.
    - Data centre facilities

Hitherto, the capacity of the fiber optic components is increased or even doubled annually, thus there is no problem in the telecommunication transmission relative to the access network technology and solutions. Thus, today more the 90% of the research in this area is in the wireless network seeking solutions to develop the capacity of the access network (increase the bandwidth efficiency). The main tracks of research in this area are:

- Optimize the TCP/IP Protocol Layers (Cross Layer Design (CLD))
- Develop Corporative Networks.

- Making use of Multiple Input Multiple output (MIMO).
- Making use of Adaptive Modulation and Coding (AMC) and Multi-Carrier Modulation(MC) advantages

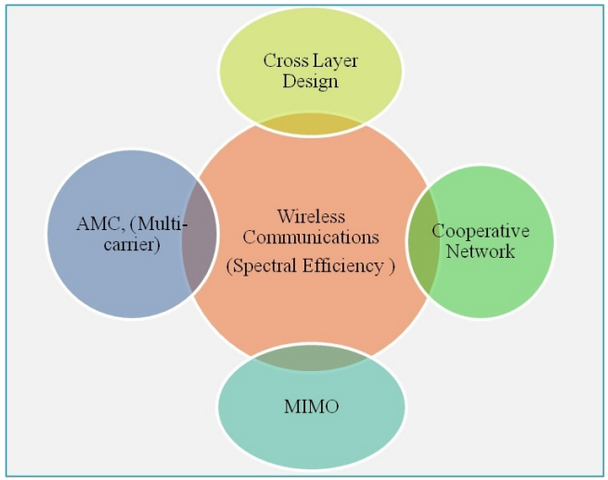


Figure 1.5: Illustrates the main research directions to improve the wireless spectral efficiency[18].

The enlargement of Storage system

From the information theory point of view, data transmission is similar data storage in the sense that in both operations the objective is reduces the redundancy and recovers the storied / transmitted data correctly. Today, with the sophisticated source and channel coding people are able to communicate high-speed data and storage large volume of data. We can list the set of storage technology as follows:

- Magnetic tapes
- Hard Disk
- Optical Storage
- Solid state Storage
- Storage Area Networks
- Optical Jukeboxes
- Disk Arrays
- …etc

Data Center

Data centres are special infrastructure facilities build to protect the data of the critical sectors. Selecting the building site and equipment for data centre is one of most difficult and critical Engineering task because it requires a lot of factor tradeoff ranging from the disaster recovery plan constraints of the size of an area of the business. In the US, the government regulations force large companies such as Microsoft, Intel... etc., to build multiple data centre facilities in different locations. Today, international companies such as Google use even distributed multiple data centers across the world as part of its disaster recovery plan. Using such high redundancy plan enabled the US government to recover from 11 September 2001 attack in short time without major losses.

The main requirements for the designing and securing data centres:

- Site selection (The building site should be in a safe area that is not subject to any natural and environmental hazards such as floods, earthquakes, or landslides).
- Utilities (the site should have good access the main utilities such as communications, power, water…etc)
- Building design (the designer should consider the risk management plan)
- Mechanical/Electrical systems design considerations (dual electrical service feeds, avoid ground loops in you power design, offer dual cooling and heating systems…etc).
- Facility Security / Monitoring (data centre should be equipped with multiple security systems, i.e. monitoring and access systems).

- Construction Monitoring (Monitoring and access control to your facility should start in the early stages of construction before the foundations)
- Electromagnetic Pulses (EMP)
- Cleaning (The data centre must be kept free of dust, dirt... etc.).
- Planning for the worst

Building and managing data centres are most expensive operations these days. Thus, today one of the most applied practices in many countries is that the government is going to build a large data centres to help small private sectors and public enterprise to handle risk management operations and disaster recovery plan in a cost effective way. The main business sectors that might be covered by the policy of business continuity and disaster recovery are as follows:

- Government and e-government
- e-commerce, banking and finance sectors;
- Banking system and related financial sectors
- Energy production and management sectors
- Information and communication technology sectors
- Public service sectors (Electricity, water, transportations)
- National security
- Education sectors
- Healthcare sectors
- …etc

Managing data centers

Managing large data centers is one of the most complex operations that require many advanced skills to turn about all the daily problems. To equip your IT personal with the required skill, the enterprise should plan and grand the necessary budget to fulfill this requirement. The most important and daily operations in data centers are as follows[19]:

- The following is a suggested list or items to monitor and provide notification to staff in the event of alarm intrusion
    - Fire detection
    - AC power failure
    - High/Low voltage alarm
    - Generator failure
    - UPS system failure
    - Temperature/humidity
    - Circuit breaker trips
    - Water leakage detection
    - Under floor water detection
- Recheck for the Electromagnetic Pulses (EMP) protection.
- Cleaning the site
- Evaluation and reviewing the disaster recovery plan

Data Replication

Data replication is one of the essential operations that can be used to maintain a real time identical copy of system transactions. As depicted in figure 1.6, the main server, which usually housed in the working area, can use the data replication mode of operation to keep the backup server, which usually housed in the remote data centre, synchronized in real time. If and for any reason, the main server goes down, the replications server will take over the control of the system for while until the main server turn up to synchronized again.

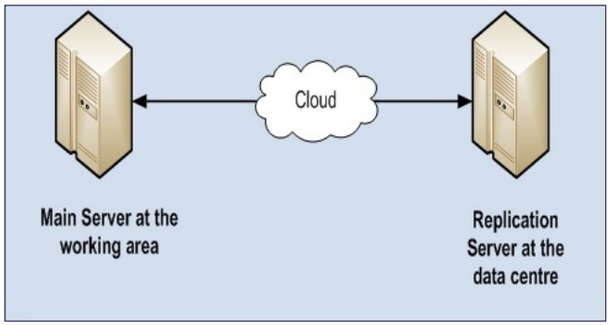


Figure1.6: Diagram depicting data replication process

Data Backup

Data backup is one of the most important routine operations that each self-governing sector should execute it as a part of their risk management plan. Practically, people need the backup copy of the data to restore the operating system full or partial damage from specific time reference points. Today there are different methods of backup; we can name here just a few such as:

- Full Backup
- Incremental Backup
- Differential Backup
- Reverse Delta Backup

According to the risk management and the sensitivity of the business, the system designer is going to select the economically and technically suitable data backup method and the optimum time to backup the data as well.

Layered Design approach and telecommunications standardization

One of the most important factors contributed to the revolution of the ICT technology is the layering and standardization of the system design. Today, equipments and even components from different venders interconnected and operate with any problems given that their interfaces are standards[20]. The most well known telecommunications standardization organizations are:

- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF) (Building the Internet Protocols).
- European Telecommunications Standards Institute (ETSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- American National Standards Institute (ANSI).

All over the world and in each country, there is regulation body for information and communication sectors. These regulating bodies from different countries are usually working together and with the international telecommunication union (ITU) to exchange information, knowledge, and developing working standards.

Internet Growth and Development

There a lot of disagreement on the starting time of the internet history, but I thank the best claiming argument is that connect the development of the fist digital computer system in 1950 and the starting of internet history. Since that time, progressively the technology is been evolved. In 1969 professor Leonard Kleinrock, exchange messages between the university California and Stanford Research Institute (SRI) using Arpanet network. In fact, during this time there are many experiments to send packets. In 1962, the PhD student Leonard Kleinrock submit this thesis titled "Message Delay In Communication Nets With Storage[21] ". This work setup the theoretical background for the packet switching and data communications. Due to many political restrictions and biased factors at this period, Arpanet is not widely used except at the US military and some educational and research institutes connected to the military.

In 1982, the TCP/IP protocol is standardized and strong trend appeared to use the internet services widely outside the ARPANET to include other institutes and to interconnecting the Computer Science Network (CSNET). Subsequently the American National Science Foundation (NSF) allows many research centers around the world to have access to the resources of the CSNET in 1986. Finally, the period from 1990 to 1995, many international organizations loudly call for widely use of the internet by public through the Internet Service Providers (ISPs). The main service provided by the internet can be summarized as follows:

- Mail services
- World wide web
- Video and VoIP calls
- Discussion forums
- Blogs and social networking
- Online shopping
- Education and research

Table1.4, list some of the main organizations that have significant contribution in the development of the internet. Also table 1.5, list some of the pioneer researcher and managers which their works significantly affecting the starting and enlargement of the internet networking.

Table1.4: Main national and international organizations contributed to the development of the internet

Organization	Web address	Contributions
Internet Research Task Force (IRTF).	http://irtf.org/	Research and development on long term related issues
Internet Engineering Task Force (IETF)	http://www.ietf.org/	Research and development/ Standardizations
Internet Assigned Numbers Authority (IANA)	http://www.iana.org/	management of address, root, and DNS
Internet Architecture Board (IAB)		Helping body to IETF
Internet society	http://www.internetsociety.org/	Active group dealing with daily problems of the internet

Table1.5: List of internet pioneers (contributing research, development, and managerial efforts)

Name	Contributions
Claude Shannon(1916-2001)	Father of the information theory
Vannevar Bush (1890-1974)	Stress the development of ARPANET Project
Paul Baran (1926-2011)	Developed the field of redundant distributed networks
Donald Davies (1924-2000)	Developed the idea of packet switching
J. C. R. Licklider (1915-1990)	Developed the concept of universal network
Douglas Engelbart (1925-3013)	Developed the concept of human–computer interaction
Bob Taylor	Developed the Ethernet and the Xerox Alto

Chapter Two

Risks on Information and communications systems

Introduction

Risk/ or hazard is defined as any expected horrific outcomes that associated with present or future operations. Risk is a part of all daily aspect of human life and it has to be considered in every engineering and planning operations. For the information and communications systems point of view, risk management denotes the process of understanding of all factors that can harmfully influence the function or operation of the system and develop the considered necessary plan to avoid the hazard or to reduce the consequence. In this chapter, we are going to make basic classification of risk on information and communication system, understand the economic and social effects, and list some practical examples of disasters on these systems.

Classifications of Risks

Generally, we can classify the disaster on information and communications system into two types: man-made disaster and natural disaster. Figure 2.1 points up the two types of adversities.

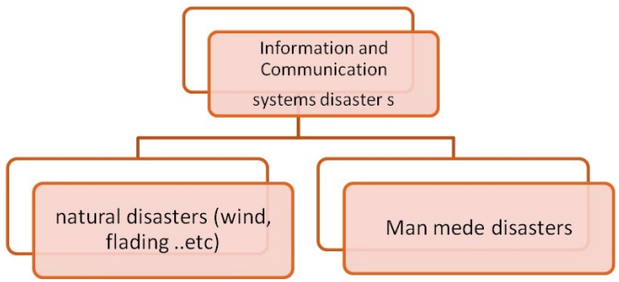


Figure 2.1: highlight the two types of adversity on communications and information systems.

Table 2.1: Examples on Some Risks that information and communication system may expose to it at any time.

disaster	description	Examples
Unauthorized access	Unintended access to classified information	-Lost of storage devices -Distribute secret information due to mistake -Unauthorized access to telecom network traffic
Natural disasters	wind, earthquake flooding	-Disruptions of submarine cable in 2011 in Japan (earthquake) -Large companies data center problem due to wind and flooding -Collapse on communication network in Tshwanchina in 2008 due to earthquake
Deployment of malicious applications (cyber-attack)	Using computer virus to intrude or destroy system/ data, stealing information, or modify the main function	-Attacking Iran nuclear using Stuxnet .[23] [22] Virus. – attacking social network in 2008 using Cyxymu program [24]. - Massive cyber Attack to Estonia in 2007. Attacking window based system in 2007 using Zotob program [25]. -attacking the safety system of nuclear station in 2003 [26] in USA -attacking Sony Pictures Entertainment 2014[27] -attacking Malaysia Airlines' website 2014 [28]
Jamming, interference , Power supply, Industrial Control Systems (ICS)	Using the interference tools to destroy the broadcasting to terrestrial or satellite TV	– Sending interference signal on restricted band. –Intentionally disconnect data center power supply. -Intentionally attack the power grid SACDA system.
System errors		-Systems error in the design, configurations, operations, and upgrade, Example: (US electricity, partial blackout in 2003) [29]
Communication link disconnections	Fiber optic cable disruption	-Fiber optic link disruption at the MEA region in 2008
Deceiving, Phishing, Identity theft, Cyber stalking, Cyber bullying, Online grooming	-Deceiving using websites -Deceiving using electronic messages	-Phishing Emails - Phishing Websites - Social Engineering Attack
Electronic Spying	Spying use special tools or through the telecommunications equipment	- Spying using special tools such as PRISM ،30] [31. -Spying through the telecommunication equipment -see the US problem reported on the references [34-32]

Human-induced Risks

In general, we can classify the risks that connected to human factors (state-sponsored and financially motivated attackers) as follows:

1. Risks connected to organized crime groups (attacking financial organizations).
2. Risks connected to state sponsor groups (crime connected to stealing secret information, research and development results, and important master plans).
3. Risk connected to political ideological groups (crime connected to critical infrastructures).

Some Example For Informatics and Communications Disasters

Risks are connected to future expected events that have some probability of occurrence. Thus, we have reasonable justifications to invest on planning for risk management and disaster recovery. Today risk management and disaster recovery plan is developed based detailed factors analysis such as business operations, probability of loss occurrence, expected loss, and many more. In this section to highlight the importance of these factors, we are going to discuss two types of cybersecurity risks: communication system disruption due to fiber optic cables connection disturbance and massive cyber-attack

Submarine Cable link Disruption

Today, one of the biggest disasters on communications systems is the fiber optic cable transnational link interruptions. Practical, these interruptions can result from natural disaster, surrounding environment or manmade operations. As we point out in the previous chapter that fiber, optics is heavily been used to carry huge data traffic between different countries, regions, and even different continents of the world. Thus

any interruption of fiber optic transoceanic link can result in sever effect on services based this communication link. Table 2.2 illustrates some of the important submarine cable interruption in 2008 in the Middle East region[36 ،35] .

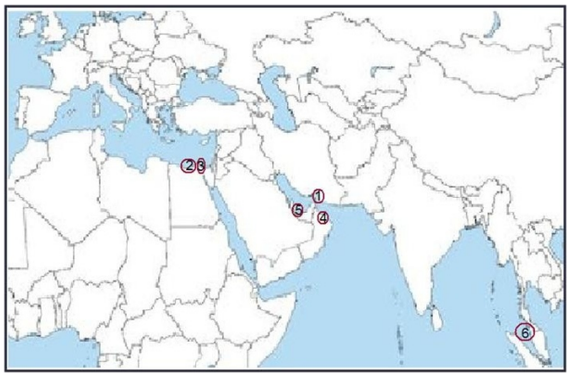


Figure 2.1: map shows the locations of submarine cable disjoints in 2008.

Table 2.2: main submarine link disruption in 2008 in the Middle East;

No	Disruption	Date
1	FALCON cable near Bandar Abbas, Iran	23 Jan
2	SEA-ME-WE-4 near Alexandria, Egypt	30 Jan
3	FLAG cable near Alexandria, Egypt	30 Jan
4	FALCON cable between Muscat and Dubai, UAE	1 Feb
5	DOHA-HALOUL between Qatar and UAE	3 Feb
6	SEA-ME-WE-4 near Penang, Malaysia	4 Feb

Table 2.3: list and explain the characteristic of the main optical fiber submarine cables[37]

Fiber link	length	Connected regions
Fiber-Optic Link Around the Globe (FLAG)	2800Km	Europe-America(FA-1), middle East-India, South East Asia-south Europe(FEA), north Asia
South East Asia–Middle East–Western Europe 4' (SEA-ME-WE 4)	18800Km	South East Asia–Middle East–Western Europe
South-East Asia - Middle East - Western Europe- 3 (SEA-ME-WE- 3)	39000Km	South East Asia–Middle East–Western Europe

Economical and Social Impacts

We do not find any study that estimates the impact of these series of link disturbances, but there is an overwhelming estimation of the loss of the international commercial operation on of billions US Dollars. This is because many international companies from US, UK, and other developed counties have active production sites in the affected region (Middle East, India, Pakistan) which depend heavily on the information and communication infrastructure. Furthermore, there is constant loss that can be calculated from the contribution of the internet and ICT sector in the overall GDP of these countries [39 ،38]. Table 2.4, summarize the estimated number of subscribers affected by these series of submarine cable disturbances in the Middle East in 2008 [37 ،36].

Table 2.4: Estimated Number of Subscribers Affected by the set of submarine cable link disturbances in 2008 in the Middle East

Country	Estimated number of subscriber affected
India	60,000,000
Pakistan	12,000,000
Egypt	6,000,000
Saudi Arabia	4,700,000
Iran	4,000,000
Emirates	1,700,000
Algeria	1,000,000
Sudan	1,000,000
Lebanon	400,000
Syria	300,000

Bahrain	-
Bangladesh	-
Maldives	-

Estonia Cyber attacks on 2007

Estonia is a country in the Baltic region of Northern Europe. It is bordered to the north by the Gulf of Finland, to the west by the Baltic Sea, to the south by Latvia and to the east by Lake Peipus and Russia. It becomes part of the European Union in 2004. Today Estonia considered one of the developed countries both economically and technologically.

The massive cyber-attacks on Estonia's critical infrastructures have been start on 27- April 2007 and continue for three weeks. During this time, and as indicated in the table 2.6, there were three batches of massive attacks on information and communications system, banking systems, railway stations, water management system, mass communications media, and food supply systems[41 ،40].

Table 2.6: explain the subsequent attack to Estonia in 2007

Type of attack	Date
Series of DDoS attacks to government main websites and internet service providers.	April 27/2007
Stealing and publishing the email address of parliament members, sending email to them, and halting the email services	April 30/2007
Tacking the main Government websites (using SQL injections)	May 3-9/2007

In general we found that this large scale cyber attack target both governmental and commercial Sectors and largely focus on the following Sectors[43 ،42]:

1. The government offices;
2. The parliament;
3. Ministries;
4. Daily newspapers;
5. State and private Radio and TV Broadcasting;
6. Government website;

Consequently, these chains of attacks are deeply affecting the telecommunications and information technology sectors, government sectors, and private commercial sector. In special cases, the attacks are even able to take over the control of some media and sending fraud messages using the name of the government. The following sectors are completely stopped or malfunctioning by the attacks [42]:

- The prime mister office and the parliament;
- Government ministries;
- Main political Parties websites;
- Three of the daily newspapers;
- Two banks;
- Internet service providers;
- Telecommunication companies;

In addition, we can summarize the technical harms on the telecommunication networks as follows:

- Routers / routing tables damaging;
- Routing Tables changed;
- DNS Servers overloaded;
- E-mail servers failure;

Early Response

To reduce the size of damage and negative economical impact of this cyber attack, the Estonian government took a lot of measures through the Estonian Computer Emergency Response Team (ECERT)(www.cert.ee/)[41 ،40] . The most important measures taken are as follows:

- Closing the entire affected website from the access from outside country;
- Stopping 99% of fraud communication's connection;
- Guide the attackers to attack damage website;
- Closely monitoring the internet with advanced and sophisticated tools;

- Blockade of Bots From Root Domain Name System(DNS) Servers;
- Ask for nearby countries internet service providers to put the attacks computers IP addresses on black list;
- Receive a lot of technical help from Italy, Spain, Germany and other EU countries;
- Estonian CERT leaves the website of the PM easy to be attack to avoid having the attacker search for other potential website;
- Attributer the attack to identify the attacker;
- Receiving high technical help from the NATO organization;
- As a result of this attack Estonian government calls for joint treaty for cybercrime prevention in 2008;

Experiences learned

There are many lessons learned from these massive organized cyber-attacks. Firstly, the collective response and the technical assistance from the different countries had the greatest role to guard the affected country and to recover the basic services in short period. Secondly, other countries and international organizations immediately modified their information security critical infrastructure protection policies [42] . For example, the EU immediately review and develop it is unified information policy to protect its member countries [44]. Also at the international organization level, the ITU develop it is global cybersecurity agenda (GCA) to support the greater global cybersecurity and protection. For more example, the reader can seek more lessons from reference [45]

Problems Associated with Information and Communication Disasters

At this moment of information age, cybersecurity, and critical infrastructure subject protection is on the most important strategic agenda of nearly every country. In this section, we are going to summarize the nature and the most important aspects of cybercrime and critical infrastructures attack.

The first fact about cybercrime is that it can go behind the country border (transnational). Secondly, it can deeply affect social, economical status and wellbeing of the country. Consequently, a lot of people look it as one of the threatening of the international peace and security [47 ،46 ،40]. Given all these facts, today there is no complete international legal framework that can be used by the international community to solve related arbitrations. For example for the case of on Estonia, the country is unable to use UN article 51(self defense) or article 4 from NATO treaty (collective defense) or even to call the UN security council under the UN article 41 [49 ،48] . So clearly the is legal scarcity and this problem should be solved in the near future by developing legal technology that can take into account the following aspects

- Determine the responsibility for the crime (individuals - organizations –groups, states, or backed groups by some countries)
- Save the rights of all parties.
- Determine the secondary responsibility , which includes the following aspects:
    - The responsibility of software companies that have left the door open to attack
    - Responsibility of the parties that contributed in one way or another to provide the right environment for cyber-attack (i.e. Failure of the state to fight against cybercrime groups within its borders or failure of the State to track the groups that are jamming satellite from within its territory).
    - Identify the responsibilities of Internet service providers
    - The responsibility of the system owner from which the attack has begun, if there is third party
- Support the trustiness between countries in this regard
- Identification of the technical, legal and coordination levels between States
- Alignment between personal freedom and the requirements of the investigation of the cybercrimes;

In addition to establishing legal framework, another important aspect that we have to consider is the development of technical solutions. By this technical solution, we do not mean just to solve simple daily problems, but development flexible and standard framework security protocol such as what is been applied by the ITU for cellular network security. Thus, the IETF should consider to developing a new version of

the DNS, IPv6, and BGP protocols that can support Practical and fast cybercrime attribution methods.

Chapter Three

Chief Information Security Officer (CISO)

Introduction

Chief Information Security Office (CISO) is newly established job within an organization after the fast revolution in information and communication technology. Today, every aspect to human life is depending heavily on the information and communication infrastructure. For example, in modern university, you can find thousand of computer and tens of servers connected together and connected the world through the internet. These computers and servers contain public, private, classified, confidential, and sensitive information. Thus, it is extremely necessary to introduce new job within the organization to manage the information security and to identify the best strategies to make maximum use of the newly developed information technology elements. These days, the CISO responsibilities are starting from information classifications, the levels of access to the information pulls, develop the security strategies, information security managements, and define and deploy information security technical tools. This chapter discusses the main responsibilities of the CISO and the CISO carrier pathway.

The general framework for the job

In any enterprise, the CISO is working toward achieving the following Goals:

- Confidentiality
- Availability
- Integrity

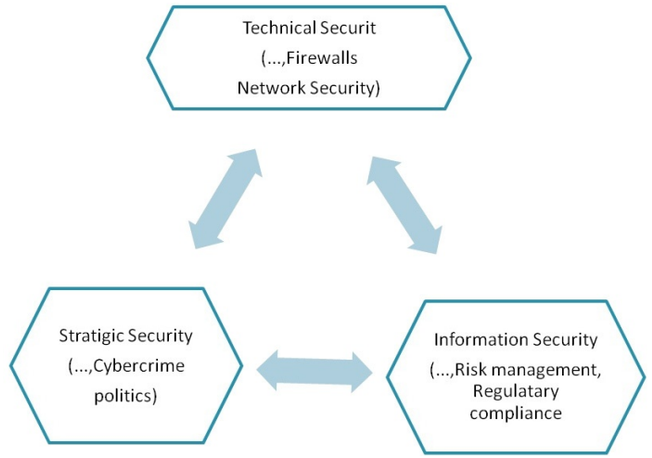


Figure 3.1: depicting the responsibilities of the CISO (the general responsibility framework for CISO to achieve his goal)

Technical Security

The most important and starting step for information security is that the CISO should persuade the top management team the organization to invest reasonable amount of the profit to deploy advanced technical tools for cybercrime prevention. Important subclass if these tools are as follows:

- System control tools
- Monitoring and access Control Tools
- Forensics and attributions tools

Important point that we have to highlight is that these tools must be developed continuously to meet the terms of the unremittingly and dynamic nature of the cyber crime techniques and tools. Another factor we have to consider is that we select CISO with live learning personality to make sure that every single element of the system is up to date.

Information Security Management

We denote by information security management all the management aspects connected to information security such as development and deployment of effective risk management plan, disaster recovery plan, and regulatory compliance. Today, different economical sectors require different information security aspects. For example in US healthcare sectors and educational sectors, have different information management aspects. Furthermore, healthcare sectors in Europe have different Regulatory Compliance than the same healthcare sector in US and vise versa.

Strategic Security

Strategic security management mean a deep understanding of the political dimension of cybercrime and how to cooperate with regional and international bodies for emergency response, intrusion detections policies advances, and laws and legislations harmonization. Furthermore, understanding these subjects will assist the CISO in the following subject matters:

- Security policy design
- Deployment of technology
- Human resources development
- Knowledge exchange and national/international cooperation

CISO Functions

Information security and critical infrastructure Protection is a unique process in the sense that form different economical activity we are going to have different objectives. For example, for universities have to keep the student and staff private data as well as the strategic research tracks, results, and the critical properties secure. In industrial sectors, the goal is to work for critical business assets, information systems, optimum operating conditions and continuity, and private information confidentiality. In both processes, the common steps are to secure the information system, main business critical elements, and strategic information. As shown in figure 3.1, which shows the general framework of the information security and management, the main tasks of CISO in each organization are as follows: firstly, he has to correctly setup system/organizations goals, develop and articulate the main policies, establish setup mechanisms, generate procedures and rules, and work for security awareness and training to maintain secure system. Given the fast development of information and communications technologies, an important external audit should been carried out with the goal of testing the compliance with regulation and policies as well as to give constructive and corrective input to the whole process.

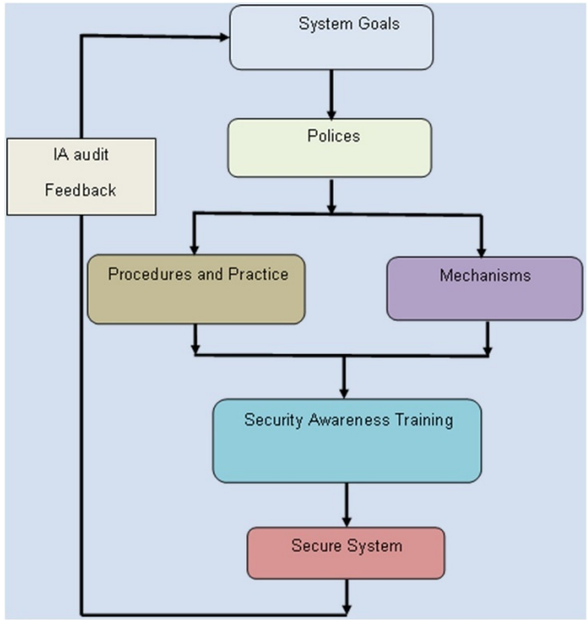


Figure 3.1: The general framework for information security management

As shown in figure 3.2, for any active process, we have to start with excellent planning which take into account all-important factors (Physical security, security technology and tools, business continuity, recovery plan, training and awareness, and external imposed regulations and rules). The second step is to go strictly after the developed plan and then in the third step we have to periodically evaluate and test the results to identify the weakness and introduce the necessary modifications.

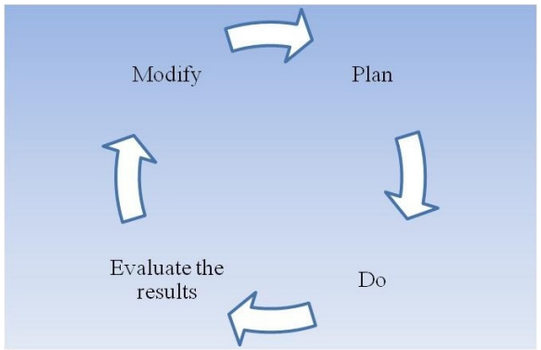


Figure: Shows the roadmap of information Security Policy improvement

CISO Career pathway

Principally, the CISO can originate from any academic background form science and Engineering given that he goes through advanced technical training to prepare and shape him to the job. Given the dynamic nature of information and communications technology (fast developing and growth), the CISO also must be intelligent person and have continuous learning attitude to rapidly understand the new themes in this quickly growing area. Furthermore today there are a lot of professional certificate that directly prepare the person to pursue specialized job in this field. Some examples of these professional certificates are:

1. Certified Information Systems Security Professional (CISSP): is a globally recognized standard of certification achievement that confirms an individual's knowledge in the field of information security. CISSPs are information assurance professionals who can define the architecture, design, management and/or controls that assure the security of business environments. To pass the CISSP exam, you have to study the following domains:
    - Access control
    - Telecommunication and Network Security
    - Information security governance and risk management
    - Software Development Security
    - Cryptography
    - Security Architecture and Design
    - Operations Security
    - Business Continuity and Disaster Recovery Planning
    - Legal، Regulations، Investigations and Compliance
    - Physical (Environmental) Security
2. Certification and Accreditation Professional (CAP): this professional certificate measures the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems. CAP examination tests the following Security aspects:
    - Risk Management Framework (RMF)
    - Categorization of Information Systems
    - Selection of Security Controls
    - Security Control Implementation
    - Security Control Assessment
    - Information System Authorization
    - Monitoring of Security Controls
3. Systems Security Certified Practitioner (SSCP): SSCP is an ideal starting point for a new career in infosec or to add another layer of security you need in your current IT career. The main topics covered by the SSCP exams are:
    - Access Controls.
    - Cryptography
    - Malicious Code and Activity
    - Monitoring and Analysis
    - Networks and communications
    - Risk, Response and Recovery.
    - Security Operations and Administration

4. Certified Cyber Forensic Professional (CCFP): CCFP certificate addresses more experienced cyber forensic professionals who already have the proficiency and perspective to apply effectively their cyber forensics expertise to a variety of challenges. The domain of CCFP study includes:
    - Legal and ethical principles
    - Investigations
    - Forensic science
    - Digital forensics
    - Application forensics
    - Hybrid and emerging technologies
5. Certified Secure Software Lifecycle Professional (CSSLP): CSSLP is an advanced certificate for everyone involved in the SDLC with at least four to five years of cumulative full-time work experience
6. HealthCare Information Security and Privacy Practitioner (HCISPP): is an advanced security professional certificate for healthcare practitioner which cover the following domains:
    - Healthcare Industry
    - Regulatory Environment
    - Privacy and Security in Health Care
    - Information Governance and Risk Management
    - Information Risk Assessment
    - Third Party Risk Management

Chapter Four

Planning, drafting and building practical and legal frameworks

Introduction

Managing information system and critical infrastructure are one of the most complicated Processes because it requires many stakeholders to work together and different managerial levels. The state should develop the legal framework that regulates the communications and information technology sectors. Independent organization should comply with government regulation and apply suitable internal policies and technologies that will provide the necessary protection at the institute level. This chapter will discuss the planning, drafting, and building practical legal framework for information security.

Planning and Drafting the practical and legal framework

Nowadays, there are enormous economical activities that depend heavily on the information and communications technologies. Thus, we have to admit that the process of developing a single security framework to answer the entire system requirements is extremely difficult task. Therefore, currently information system security professional and experts develop a general planning framework that can help policy developers to design any specific information security management for any organization. Figure 4.1; illustrate the steps and the structure of this framework

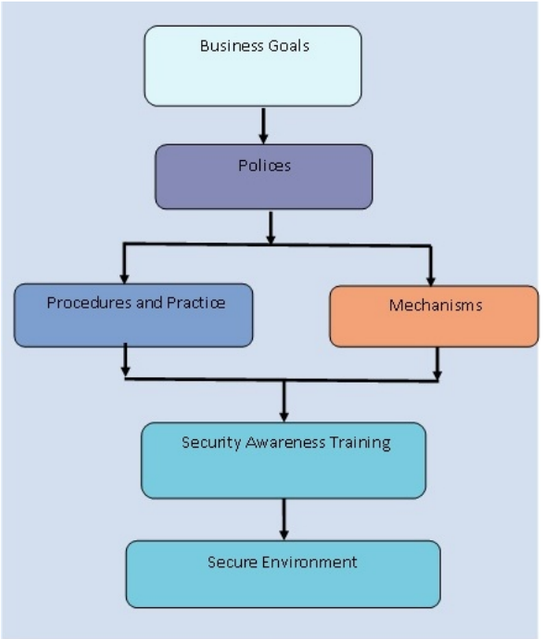


Figure 4.1: the general framework for information security management planning and development;

Based on the framework on figure 4.1: first, the developer should identify the main goal of the organization (Economic activities, outcome... etc), for example, the educational institutes have different goals than other government service organizations. Secondly, we have to develop the information security policies and consequently we have to identify the mechanism, procedures and practice tools. Finally, we have to develop the awareness and training plan that able to sustain the knowledge in cybersecurity area.

This is the general framework of information security planning. For those who are willing to go deeper than this point, I recommend to them to read the following

list of helping document and standards for information systems and telecommunications security:

- The publications of National Institute of Standard and Technology (www.NIST.gov) this website contains a lot of valuable material for planning and design of cybersecurity system. Important example of such materials are:
  - NIST-SP800-12,.[50] this document describe the planning procedure for information security (for US States enterprise)
  - NIST-SP800-13, this document describe the general principle of securing the Telecommunication Network Management[51]
  - NIST-SP800-30.[52] , this document summarize the main guidelines for the risk management
  - NIST-SP800-34, this sum up the main guidelines for the planning of business continuity .[53]
  - NIST-SP800-37, this document provides the main guidelines for risk management.[54]
  - NIST-SP800-5.[55] , this document provide the main information security guideline for government institutes and national/international organizations
  - NIST-SP800-39, this document articulates the main objectives and requirement for risk management.[56]
  - NIST-SP800-82 this document describe the procedures to protect industrial and SCADA System from cybercrime [57].
  - NIST-SP800-66 , this document Provide the main guidelines to protect health system in US HIPAA[58]
- The publications of the International Telecommunication Union (ITU) related to the issue of cybersecurity such as (E.408, E.409, X.805, X.1051)
- CISSP certificate related documents.
- EU documentations related to cybersecurity and critical infrastructure Protection such as (3GPP 33-Series, 3GPP2 S.S0086).
- Publications from industrial automation open networking associations. These documentation is important for those working in the industrial automations and information systems[59]
- American standard for electricity system protection for 2013[60].
- The publication of the American Cooperative Association for Internet Data Analysis [61].
- British Columbia Institute of Technology، Industrial Security Incident Database[62]
- ISO/IEC publications such as (27001:2005, 27002:2005, 27011:2008, 15408 (The Common Criteria))[63]

Partially the information system security and critical infrastructure protection process is intended to handle and control the humans factor, thus it inevitable to have awareness and engagement program within your information management plan.

Human Factors

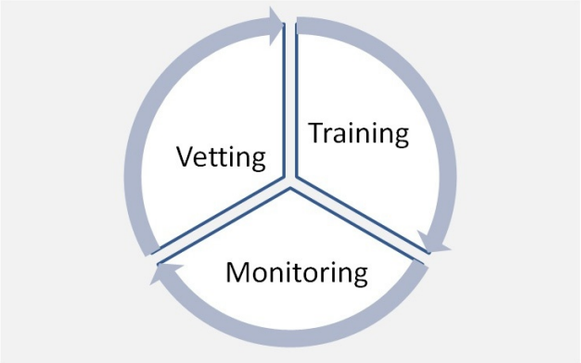
The human factor is the central element in the process information security, communications, and critical infrastructure protections[64]. Generally, we can distinguish two different of human factor effects:

1. External human factors(external to the system or organizations)
2. Internal human factor (internal to the system or organization)

It is extremely difficult to guess what an individual would do when he feel alone in the free open cyberspace. At this point, we have to think about the ethics and values as essential tools for protection. Officially, the best way to deal with the human factor is to develop rules, regulation, and legal framework that control every aspect of human information interaction.

How to Control the Human Factors

Technically, we can control the human factors by use one of the following tools as illustrated in the following diagram

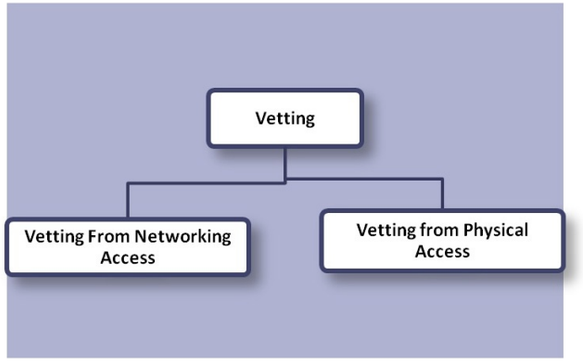


Training rise up the awareness of the employees about the importance of the data and how to professional manipulate the data [65] . For example the well-trained employee know where and how to use his official email, what kind of information that permitted to be sent and to what level to management, how to use the internet especially on websites that request private information. Generally, the proper training should cover the following aspects:

1. Defines type of risks, implications of each type of risk connects to cyber-attack.
2. Provide awareness on methods of cyber-attach and intrusions

Monitoring is another way to control the human factor. By monitoring, we can correctly ensure that our planned information security element is implemented correctly. For effective monitoring operation, we should connect the monitoring process to reword and punch rules,

Vetting people are one of the effective tools in information security, thus, in many countries, people used to call the information security unit the department of No. Generally, we can subdivide the vetting for access into two levels as illustrate in the following diagram.



We are going to introduce the technical tools used in the networks and at the system level to vetting people to have unauthorized access to valuable resources in a separate chapter. Before, deciding about access right for individuals and group to any resource, we have carried out professional classifications for the system resources. In practice the there are two methods of classifications:

1. Classification based on managerial/ administrative levels, which is appropriate for governmental and semi-governmental organizations. In this type of taxonomy, information is classified as follows:
    a. Sensitive information (i.e. financial, systems design, locations of critical sector)
    b. Strategic information (i.e. HR information, strategic decisions)
    c. Sensitive and strategic information(i.e. national security, data centers, financial information)
    d. Sensitive private information (personal information, personal financial)
2. Classifications of the industrial sectors which have just two categories:
    a. Sensitive and secret information related to the industrial operations
    b. Sensitive private information

Information classification at the end should make the information security management easier and effective in the organization. If you need a deep knowledge in this topic, you can consult the American standard NIST SP800-50 and resource of CIISP certificate.

Business Continuity

We mean by business continuity plan all the necessary arrangement that must been done to enable the resume partially or completely the continuity to the operation after specified and classified type of disaster. There [66]:. Examples of information and communications system disasters are:

- Thieving the data
- Demolished or lost/missed (11 September accident in US).
- Malfunction of critical industrial/ engineering operation (Iran nuclear reactor problem malfunctions due to virus).
- Denial of access or denial of services attack
- …etc

The central elements of the business continuity plan for information and communications systems are security, confidentiality, and availability. Other important factors that we have to consider in our plan are:

- Data centers safety.
- Continuity of the distributed system elements
- Safety of human resources, Communications Network, and power supply

Disaster Recovery Plan

Disaster recovery plan is defined as all sets of defensive rules/ steps that if applied correctly will make the plant operator respond effectively to the disaster and restart/resume the proper operation of the plant in short time [67] . The most important factors that we have to consider in the disaster recovery plan are that it should have reasonable cost, reasonable with the insurance value and act in accordance with the rules regulation of country hosting the economical activity. Moreover, the recovery plan should also convince the following plant controllers:

- Customers
- System auditors
- The regulators
- The employees
- Investors

When we prepare the disaster recovery plan, we have to consider the following factors:

- Timely Recovery of the critical operations
- Minimize the losses
- Meet the legal and regulatory requirement.

Chapter Five

TECHNOLOGIES AND TOOLS

Introduction

Using technical tools for critical infrastructure protections is an essential step to secure the communication and information system. Today, it is very important for information systems security management department to devote a considerable amount of it is budget to install and upgrade to up to date system security technical tools.

Technical tools for Information Protections

With the development of information era (Communication and information technology) and rapid growth of cybercrime all over the world, people from the early day start to develop intelligent technical tools to prevent and or /reduce systems' ability to be attacked. The following list represents the important technical tools used to prevent the system from a wide range of cybercrimes:

- Firewall
- Intrusion detections
- Antivirus
- Access controls
- Authentication systems
- Encryption
- Attribution methods

Firewall

Firewalls are one of the best technical solutions for networks and information system protections. Technically, there are two types of firewall system architecture: software based system or host based and software associated with dedicated hardware or network based systems. Figure 5.1shows the different types of firewalls.

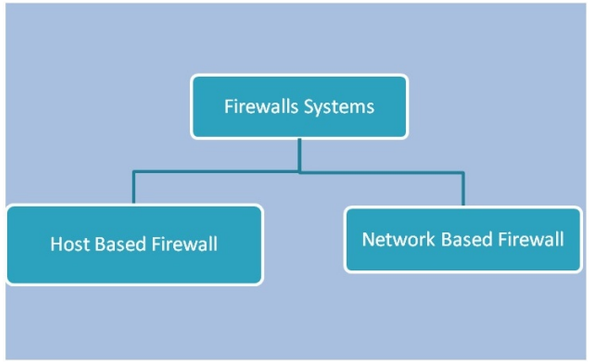


Figure 5.1: Classifications of firewall systems

As depicted in figure 5.2, network based firewalls are used to control packets transfer between two networks segments according to sets of selected rules [68]..

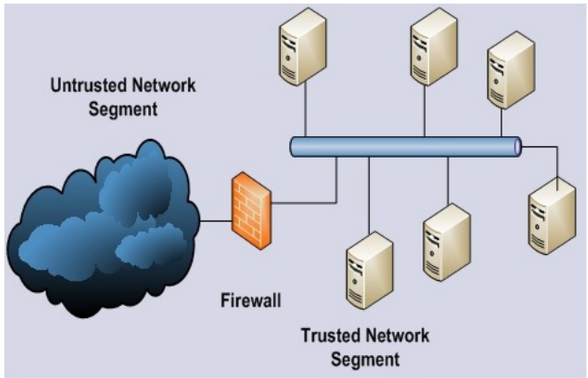


Figure 5.2: Network based firewall configuration

The first generation of the firewall devices was been deployed back in 1989. It was working on the three buttons down layers of the OSI system model (physical-data link, and network layers). Today with the great advances in communication technology, the third generation of firewall devices is working on all layers (Physical-to- application layer). At this moment, firewalls use the following criteria to classify and control the communicated messages (packets).

- Source and Destination IP address.
- Protocol Type (TCP/UDP).
- Destination TCP and UDP ports
- Source TCP and UDP ports
- The Interface Where the Packet Arrives
- The Interface Where the Packet is Destined

The most important open source Unix/Linux compatible software based firewall systems IPtable/IPchains, IP filter, PF packet Filter ،NPF, IPFW. In addition, there are other potential commercial system like Cyberoam, Eudemon، Microsoft's internet security and Acceleration (ISA) Server ،Nortel Networks Alteon Switched Firewall System.

Host based firewall is used for protecting the individual workstations form subclass of information security risks. Example of these systems is an Internet Connection Firewall (ICF—included with Windows XP and Windows Server 2003)

Intrusion Detections

Intrusion Detections Systems (IDS) are the classes of network protection systems that work inside the enterprise domain to detect intrusions from inside and outside the domain. The main principles for data analysis in IDS systems are[70 ،69] :

- Analysis of the system activities
- Analysis of system functions
- Observe and identify intrusion method
- Monitor user and system components, unusual activities and operation
- Observe and monitor user compliance with the internal system policy

The most important open source IDS packages are:

- Advanced Intrusion Detection Environment (AIDE)
- CARM-ng (Alert Correlation، Assessment and Reaction Module - Next Generation)
- Bro NIDS (Network based IDS)
- OSSEC HIDS system
- Prelude Hybrid IDS(work on network and distributed systems)
- Samhain system (Linux based system)
- Snort system (used to protect SCADA systems).[71]
- Suricata (developed by Open Information Security Foundation(OISF)) .[72]

In addition, some important and widely used commercial IDS systems are Network Intelligent Police (NIP), Cisco IDS 4250, and Cisco IDS.
IDS are working based on two scientific principles:

- Statistical anomaly-based IDS.[73]
- Signature-based IDS [74]

Anti-virus

A computer virus is a software component that developed with an intention to modify systems or data files and/or destroy, steal, and modify valuable information from the attacked / affected system. Antivirus systems are software packages that used to protect, remove/ recover or delete the effects of a wide range of viruses.

Access Control

The concept of Access control in information system security and critical infrastructure protection means simply applying selective control on the access operation at both system site (physical layer access control) and system resources (System Access Control).

Authentication Systems

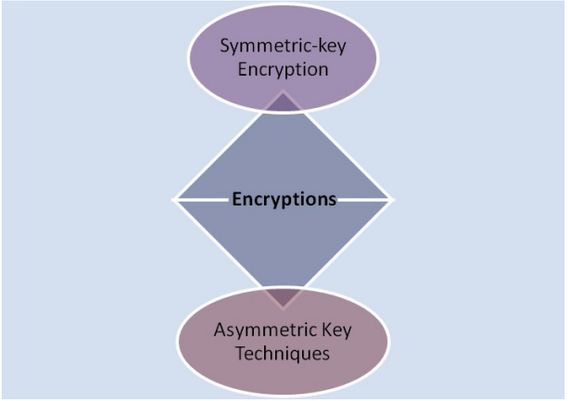
Authentication is an electronic Process that allows the computing machine recognizes and identify system user to give him permission to access to the system resources. Today, authentication systems are making use of different identification variable such as:

- Authentication based on variables that known to the user, such as Password, Personal Identification Number, and Special pattern
- Authentication using something owned by the user, such as -ATM smart card, mobile number
- Authentication based the biometric characteristic such as [75]
    - fingerprint recognition
    - face recognition
    - voice recognition
    - Keystroke recognition
    - Handwriting recognition
    - Finger and hand geometry
    - Retinal scan
    - Iris recognition

Today practically all system use multi- factor authentication technique to improve system security

Encryptions

Encryption is the process of coding the information with an objective of securing the data in the transmission process or storage. Encryption systems accomplish their task in two steps: first the transmitter Encrypt the data using an encryption algorithm, which transform a readable message into Encrypted or/ unreadable message. On the other hand, the receiver decrypts the message using a suitable decryption algorithm, which transform the encrypted message into simple decrypted messages. Between the Encryptor and the descriptor, the message holed secure in such way that any unauthorized user is unable to read the message or modify it without permission. Today, there are two classes of encryption algorithms: Symmetric key encryption and Asymmetric key encryption.



- Symmetric-key Encryption: in this type of encryption the same key used in the encryption process are going to be used in the decryption process. Some important Symmetric-key Encryption algorithms are:
    - Twofish algorithm
    - Serpent algorithm
    - Advanced Encryption Standard (AES) algorithm
    - Blowfish, CAST5 algorithm
- Unlike Symmetric-key Encryption in Asymmetric Key Techniques or Public-key Encryption techniques, different keys were used in encryption and decryptions. Some important Asymmetric-key Encryption algorithms are:
    - Diffie–Hellman Key Exchange
    - Digital Signature Standard (DSS)
    - Encryption using Elliptic Curve techniques
    - Paillier Cryptosystem
    - Password-authenticated key agreement
    - RSA
    - McEliece cryptosystem

- Merkle–Hellman knapsack cryptosystem

Some of the most widely used and important asymmetric-key Encryption applications are:

- GPG
- Internet Key Exchange
- ZRTP، A Secure VoIP Protocol
- Secure Socket Layer
- SILC
- SSH

Attribution Methods

Attribution of cybercrime means carry out both investigations the crime and assign it is responsibility to legally accountable and identified body. Attribution is an essential part of the legal frame of information and critical infrastructure security and protections[76].. Attribution operation is completely technical solutions that b depend heavily on the understanding to the system design, standard, and operating condition. Although it is outside of the scope of this book to discuss the technical details of this operation, we shall briefly summarize some examples from communication network attributions

Table 5.1: List and summarize the operating principles of some attribution methods

Attribution method	Description
Hash based IP traceback [77]	Router stores hash values of forwarded packets and try to trace back to the sources
Overlay network for IP Traceback [78]	Routers send all suspected packet to central Router for analysis to identify the source.
Ingress filtering[79]	In this method, Ingress router investigate all incoming packets
ICMP return to sender	Router send destination unreachable to and trace it back to the source
Hackback [79]	In this method router tracing back the source
Honeypots	This method depends on intelligent system the going to fall the attacker and intelligently identify it
Watermarking	In this method routers marks the packet to be able to trace back the source
Probabilistic packet marking	In this method some router sends the test packet back

Security Models

Information security model is the set of practical predefined rules that recommended to be applied for the information security of specific sectors. Today for a lot different economical activities, we have different information security model on the shelf so that we can apply it directly. Some of the most important information security models are:

- Access Control List (ACL)
- Bell–LaPadula Model
- Clark–Wilson
- Context-based access control
- Graham-Denning Model
- Lattice-Based Access Control (LBAC)
- Brewer and Nash model
- Capability-Based Security
- Multiple Levels of Security (MLS)
- Non-interference
- Role-Based Access Control (RBAC)

Generally, it is optional for the system designer to choose the perfect (best) security model to design and develop the information system security for specific applications.

System Assessment and testing standard

System assessment and testing standards required to be developed prepared by communications and information system protection, standardization, and regulatory body in each country. Table 5.2: List some of the widely used standards for information system and critical infrastructure protection.

Table 5.2: List some of the widely used system evaluation standard

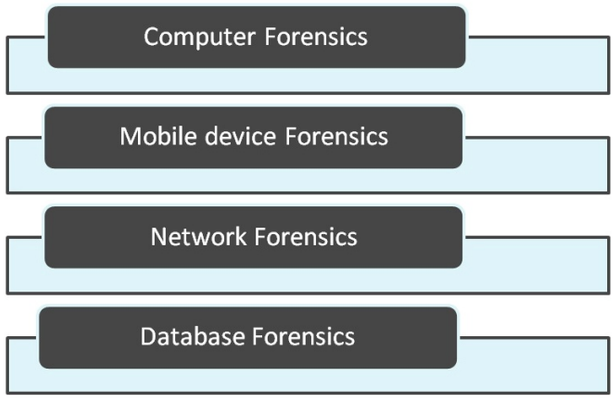
Standard	Country of Deployment
Trusted Computer System Evaluation Criteria (TCSEC)	United States
Information Technology Security Evaluation Criteria (ITSEC)	France, UK, Some EU Countries

Common Criteria or CC	International standard (ISO/IEC 15408)
Canadian Trusted Computer Product Evaluation Criteria	Canada

Chapter Six
Digital Forensics and Acting in Accordance with the Rules and Regulations

Introduction to Digital Forensics

Digital forensic evidence, also called Forensic Computing, is unlike most other forensic sciences because the nature of the material under examination is determined largely, by human cleverness. Rather than looking for traces of material deposited by physical or biological entities, which tend to develop and evolve slowly, we deal with fast developing technology crimes, which is updated, enhanced, and even created, at high rate[80]. Digital forensics is a new track that seeks to research and study all the technological aspects of collecting cybercrime evidence to be used further for attributions and pursuing legal procedures. Digital forensic is divided into the following study tracks[81]:



The main and most important operations in digital forensics are as follows:

- Seizure the source of the attack (normally this step requires officially authorized permission)

- Data acquisition
- Data analysis
- Attribution
- Reporting

Digital Forensic Tools

Practically, many open source tools (both software and integrated systems) can be used both for training and to investigate limited cases. Tables 6.1-to-6.3 list some of the types and classes of these tools.

Table 6.2: Computer Forensics tools

Forensic Tool	Operating System Supported
SANS Investigative Forensics Toolkit - SIFT	Ubuntu
Digital Forensics Framework	Windows / Linux
The Sleuth Kit	Unix-like/Windows
Open Computer Forensics Architecture	Linux
CAINE	Linux
Dumpzilla	Windows / Linux

Table 6.3: Memory Forensics Tools

Memory Forensics Tool	Combatable operating system
CMAT	Windows
Volatililty	Windows & Linux
Volatililty	Linux

Table 6.3: Network Forensics Tools

Network Forensics Tool	Combatable operating system
WireShark	Windows / Linux
NetworkMiner	Windows / Linux
Tcpflow	Windows / Linux
NetSleuth	Windows

Legal Problem behind the process of digital Forensic and Collecting Evidence

Today, many countries around the world suffering the lack of legal and legislative experience the area of cybersecurity, information, communications, and critical infrastructure protection. Thus, both legislative institutes and the cybercrime police departments in these countries are in need of advanced knowledge transfer and training to develop, practice cybercrime Laws, legislations, and investigate large-scale cybercrime. The most common challenges faced by under developed countries in the area of cybercrime and critical infrastructure Laws, legislation development, and crime investigation are:

- In a lot of cases the cybercrime incident(attack) is transnational which limits countries Law framework and investigation capabilities;
- Having a common agreement on haw to develop reliable and credible tools for digital forensic, cybercrime investigations, and cybercrime attribution; In US, there are some common standards to develop such tool you can refer to them at [82] ;
- Developing frameworks that defines when, where, and who can use these tools and under what circumstances. Because using these tools in wrong way can violate and go against the privacy of the individuals, groups and even organizations. The department of justice's in US develops some valuable regulation on how to use such tool. The reader can refer to these regulations at[83] .
- Training and development of human resource capacity (cybercrime police officers, Legislators, arbitrators, prosecutors, and lawyers) on how to handle cybercrimes;
- Developing the necessary Law technology (Laws and legislations suitable to the nature of cybercrimes);
- Laws and legal frameworks harmonization (harmonization of different countries Laws, legislations and even regulations);

Auditing

Auditing cybersecurity policies is an essential part the information, communication, and critical infrastructure protection. Auditing means critical examination and

checking the effectiveness of all component s of the information security management and critical infrastructure protection policies against standards and regulation frameworks and reporting finding and recommendations[84] . Figure 6.1 shows the follow chart of the audit process, which starts at the examination of the organization security goals and policies and end at providing constructive recommendation and advice as an input to the future development of the process.

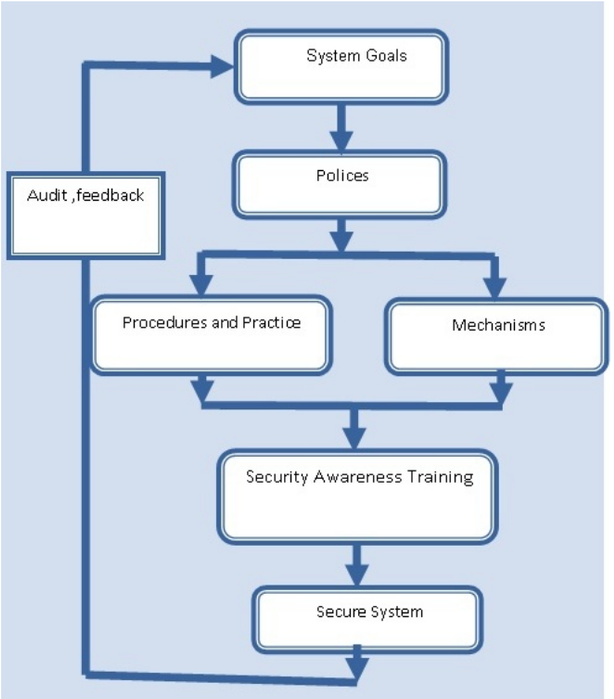


Figure 6.1: the general information security framework.

It very important for the audit operation to undergo through the following steps:

- Security risks which include the following steps
  - Testing the security of the communications and networking.
  - Testing and auditing the compliance with policies, regulations, and standards.
  - Testing the software security
  - Testing the effectiveness and robustness of the risk management and disaster recovery plan
- Controlling Over Data
- Adequacy of Backup and Off-site Storage

System audit start with massive collection of information from the system, construct the necessary analysis, carryout specialized tests and write the inclusive final report [86 ،85]. One of the most important technical tools used for system testing known as penetration test tools, which test the following system parameters and characteristics:

1. The chance of the system to be affected or intruded (penetration test).
2. Identify the sources of risks (for all operating conditions).
3. Calculate the cost dead for some well-known disasters.
4. Test the system technical security tools capabilities to resist against given types of attacks (intrusions).
5. Persuade the top-level management to invest on system security (developing the human resources and deployment of technical tools)

Table 6.4: list some of the well-known intuition detection tools that can be used for training and for limited practical

Table 6.4: Intrusion detection tools

Intrusion detection tools	System Version
System Administrator's Integrated Network Tool (SAINT)[87]	2002
Open Vulnerability Assessment System (OpenVAS)[88]	2013

Metasploit project[89]	2009
Pentoo Penetration Testing tool[90]	2013
BackBox[91]	2013
IT Health Check(ITHC)[92]	2010
Burp Proxy[93]	2013
Nessus Vulnerability Scanner[94]	2012
Ollydbg[95]	2012
Nmap[96]	2012

System auditing: Regulatory and compliance

Different countries have different rules and regulations for information system security and critical infrastructure protection. Thus, system-auditing operation must carry out in according the country rules, regulations and specific polices agreed and imposed by the owners. The most widely used standards for information system protections and audit are:

- Control Objectives for Information and Related Technology (COBIT)[97]: This standard is developed by (ISACA) in1996. A last version is COBIT 5, which published in 2012.
- ISO17799/BS7799:2000: This information security general standard is developed by International Standard Organization [99 ،98].
- Federal Information Security Management: this is an American governmental information security standard which strictly follow the information security Act of 2002.[100]
- NIST-SP800: This is a collection of standards define a set of the information security operation(intrusion detection, disaster recovery plan, technical security, etc…) in different economical activities [101].
- Using American national vulnerability database (http://nvd.nist.gov/)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Reporting

Auditing the information system is not the closing stages for information system protection. The best conclusion of high-quality auditing process is the inclusive report that addresses every aspect of information system and critical infrastructure protection. As shown in Figure 6.2, this conclusive report should go to the external bodies, executive management, and stakeholders inform them the status of the system. The most important points that most by address by any auditing report are as follows:

- Policies and regulations compliance
- The effectiveness of the risk management plan
- The effectiveness of the incident response management
- The effectiveness of training and capacity building plan
- Discrepancies found (according to the rule and regulations)
- The effectiveness of the Technical tools deployed
- The effectiveness of the information sharing and knowledge exchange

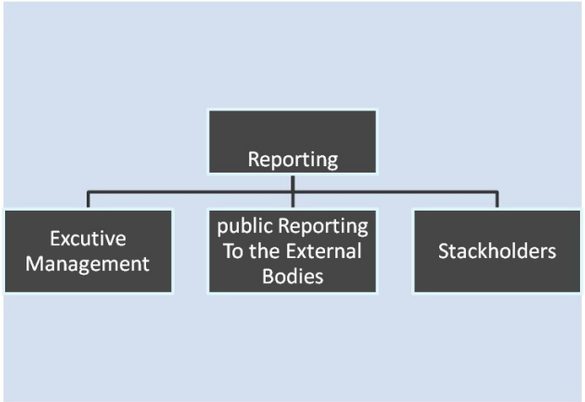


Figure 6.2: Report sharing relation

Chapter Seven

Social Networks, Family and Child Protection

Introduction

Social networking websites are a type of virtual community networking tools that has grown tremendously in popularity over the past few years. On these websites, people can easily network, develop relationships, and exchange views and ideas on different aspects of live (social, economical, political, science …etc). These tools are also expect to lead the change of the generations to come[102] .. Despite of all the benefits of the site, there are many associated risks behind using these tools.

Social Networking Websites

Social networks web sites can be classified into two types: General-purpose sites and special purpose sites as depicted in figure 7.1.

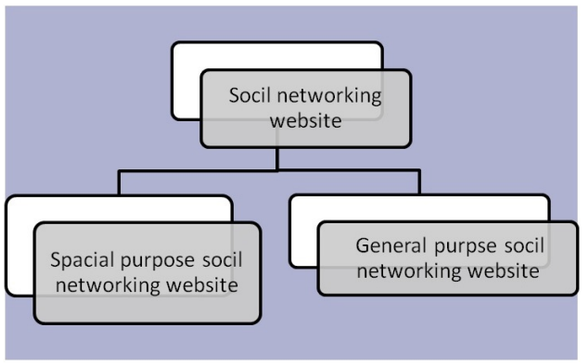


Figure 7.1: illustrates the general classification of social networking sites

General purpose social networking website

On this class of website/or tools people can network and communicate all social issue, build virtual relationships, exchange social and political ideas. Most common example from these classes of websites/ tools are:

- Facebook (www.facebook.com)
- Twitter (www.twitter.com)
- Linkedlin (www.linkedin.com)
- Myspace (www.myspace.com)
- Whatsapp (www.whatsapp.com) Mobile system
- Threema (https://threema.ch/e) Mobile system
- ....etc

Social Networking for Education

These classes of website were built to support the networking and exchanging of idea in special domain of live such as Education, Political …etc. Massive online education (MOOC) is one example of the classes of websites is dedicated to provide education. In these dedicated educational platform, students and educator exchanging information related to the subject of study. Just starting in 2011-2013, these websites are expected to change the way we educate and gaining special skills our live. Both the materials, and educators are of high quality and the enrollment of the student is elevated. At the begging of 2013. The American council of education announce the acceptance of the certificates issued by the institutes[103]. Table 7.1; list some of the important MOOC provider.

Table 7.1: List Important MOOC Providers

Provider/ web address	Universities/ number of courses Provided	Hosting country
Coursera, www.Courera.org	108 universities-621 course	United States
EDX, www.edx.org	32 universities	United States
Udacity, www.udacity.com	25 course	United States
Iversity, www.iversity.org	8 course	Germany
Open2study, www.open2study.com	15 universities	Australia
Schoo, http://schoo.jp/	-	Japan
Future learn	21 universities	United kingdom

http://futurelearn.com/		
Veduca, http://www.veduca.com.br	18 universities	Brazil

Threats on some social networking sites

Despites all the benefits of social networks, there are a lot of associated risk and potential cybercrime access. An example of these problems are as follows[105 ،104].

- People leave a lot of private data open on social networks, which open the door for negative usage.
- On special case, making a relationship on social media can lead to personal meeting, which bring many problems.
- Social website like facebook and twitter allow location identification of the user, which can leads to some potential traditional crime.
- Social sites like linkelin provide valuable employment history which may lead to potential source of traditional and high tech cybercrimes
- The educational materials provided by MOOC are also may not be appropriate for some people and regimes (example: the regime in North Korea may have an aversion to any material about democracy).
- It is possible for people from different cultural, traditional gender, background to network virtually in the cyberspace, which may also lead to a potential source of traditional and high tech cybercrimes
- The recommender systems on this website also can recommend to you someone that is not related to you and you may not know his behavior.
- There are also a lot of privacy and security concern on several applications working on social networking website and smart phones.
- Some users spend a lot of time on these websites, which negative to them, especially on their normal relationships and normal life activities.
- Today social networking web platform are used heavily in the act of wear. Thus may countries such as US, UK, and Israelis have led the way to establish and set up new social media army unit[106].

Legal Aspects

It is of great value for the life of people that the technology of the Law should be developed alongside with the development of information and communication technology and advancing in social networking. Given the recent advances in social networking, today there are tremendous needs to great expansion in criminal Law codes, cybercrime investigations and cybercrime attribution to meet the daily problems comes with the emerging technology.

The negative uses of social networking system by total regimes and ideological groups

In the recent past years, social networks were negatively used by some regimes and organization all over the world for different reasons. Important examples of these usages are as follows:

- In 2008, a person named Ahamed Mahair established a group and initiated a discussion on a political theme. In one week the group member increase up 70,000 and as a consequence of that, the security authority in the country traces him, seized him and prosecuted him
- In 2011 and 2012, Facebook play important role in Arab spring movement. There are many technical evidences that this tool also used by the regimes to seize the political opponent.
- Some countries use system called Pyramiden to monitor the discussion themes (providing detailed statistic on each topic) on the internet, then order their electronic military (Cyber Force) to reply to it.

- In some countries in extreme case, the authority blocks some social networking websites (For political reason).

To further deepen your knowledge on the issues related social networks table 7.2 lists some important recent studies.

Table 7.2: Important studies on some social networking themes

Reference	summary
Trust and privacy concern within social networking sites: a comparison of facebook and MySpace [104]	This study compares privacy on Facebook and Myspace
Social networking sites and our Live[102]	This study, conducted by a group of researchers to answer a lot of questions
MOOCs and the AI-Stanford like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses[103]	This study answers some questions related to the MOOC
How Edx plans to earn، and share، Revenue from Its free online courses[107]	This study answers the question related to the profit from MOOC services
What we're learning from online education[108]	
Social networking's good and bad impacts on kids[109]	
Social networking and security risks[110]	
Social networking statistics[111]	

Child and Family Protection

The Internet cyberspace offers remarkable benefits to adults and children, who can use the available online resources to improve school performance, expand learning, become familiar with other cultures, and maintain a network of colleagues around the world. There are many indication exists that children's effective use of the Internet leads to their academic success, and ultimately, professional accomplishment.

Nevertheless, for all the opportunities on the Internet to help children soar, personally and scholastically, many online dangers abound. Strangers, pretending to be someone else can communicate with child. Unsolicited email spam about websites with sexually explicit material can arrive in email inboxes. Requests for personal information for contests or surveys can be used in unauthorized ways to collect children private data. Cyber-bullying intimidating, frightening, or threatening texts or emails sent to children seems to be increasing. Moreover, countless easily accessed websites and chat rooms are filled with detailed information on extreme, offensive, bigoted, and violent activities. Protecting children on the cyberspace is an individual, community, government, and even an international comunity responsibility. Thus, everybody who cares about children must play a positive role in keeping them safe. Today all over the world parents, teachers, family, governments, organizations, and friends are all concerning the child protection in the cyberspace. Practically, different counties developed different approach for child online protection. These differences appeared due to the difference in religions, culture, values, and traditions of different communities and groups. In the last chapters, we are going to discuss examples of child online protection polices of different countries.

One notable solutions of guiding the children in the cyberspace is the using of the website navigation window as shown in an example of the Great Websites for Kids figure 7.2 (http://gws.ala.org). From this main webpage, child can navigate over 700 safe and valuable webpage. The web gate in Figure 7.3 also classify safe and valuable web page for child access. (http://www.kidsites.com)

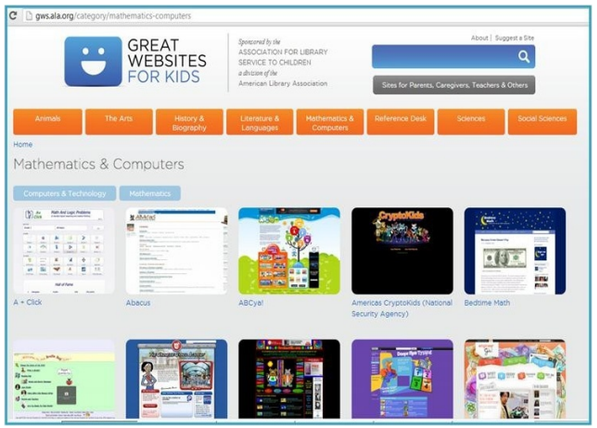


Figure 7.2: web gate for safe online cyberspace for children

(http://gws.ala.org)

Figure 7.3: Classified safe online WebPages (http://www.kidsites.com)

Tools for Families Protection

In addition to the accessible tools of awareness and guidance, which helps both children and Family member to stay away from Harmful web contents, there are many technical tools that can be used by families, educators, and schools to protect children on the internet. Table 7.3-7.7 list example of these tools:

Table 7.3: lists Some technical tools that help families to limit the time that children can spent on the internet[112] .

Tool Name	Operating systems supported	Web address of the Provider
CSWEB	Windows ME Windows NT Windows 2000 Windows XP Windows Vista	www.securitysoft.com
Safe Eyes Parental Control Program	Windows 98، Windows ME Windows 2000 Windows XP Windows NT	www.onlinesafetysite.com
Covenant Eyes Internet Accountability and Filtering Software	Macintosh OS X Windows Vista Windows ME	www.covenanteyes.com
	Windows NT، Windows 2000 Windows XP	
EyeTimer	Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.familysafemedia.com
KidZui	Macintosh OS X Windows Vista، Windows XP	www.kidzui.com
Family Protector	Macintosh OS X	www.intego.com/contentbarrier
McGruff SafeGuard	Windows XP Windows 2000 Windows Vista	www.GoMcGruff.com
Optenet PC	Windows 98، Windows ME Windows 2000 Windows XP	www.optenetpc.com
Net Nanny	Windows XP Windows 2000 Windows Vista	www.netnanny.com

Table 7.4: lists Some technical tools that help families to monitor their children on the internet[112]

Tool Name	Operating systems supported	The Web address of the Provider
McGruff SafeGuard	Windows NT Windows 2000 Windows XP Windows Vista	www.ParentsOnPatrol.org.
SafeEyes	Macintosh OS X Windows 98، Windows 2000 Windows XP	www.internetsafety.com
WebBlocker	Windows 95، Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.thewebblocker.com
Covenant Eyes Internet Accountability and Filtering Software	Macintosh OS X Windows Vista Windows ME Windows NT، Windows 2000	www.covenanteyes.com

	Windows XP	
Integrity Online/Everyware	Macintosh OS 9، Macintosh OS X Windows 95، Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.integrity.com
A+ Internet Filtering for Families،	Macintosh OS 9 Macintosh OS X Windows NT Windows ME Windows Vista Windows NT Windows XP Windows 2000 Linux OS-independent	www.hedgebuilders.com

Table 7.5: Lists Some technical tools that help block sexual contents on the internet[112]

Tool Name	Operating systems supported	The Web address of the Provider
PureSight online child Safety	Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP	www.icognito.com
ContentProtect	Windows 2000 Windows XP Windows Vista	www.contentwatch.com
KidZui	Macintosh OS X Windows Vista، Windows XP	www.kidzui.com
The Internet Filter IF-2K	Macintosh OS X Windows ME Windows NT، Windows 2000 Windows XP Linux	www.turnercom.com
Safe Access	Windows 2000 Windows XP Windows Vista	www.safeaccess.com
iProtectYou،	Windows 95، Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.softforyou.com

Table 7.6: Lists Some technical tools that vetting children from putting their private information on the internet[112]

Tool Name	Operating systems supported	The Web address of the Provider
CyberSieve	Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP	www.softforyou.com
Cyber Sentinel	Windows ME Windows NT Windows 2000 Windows Vista Windows XP	www.securitysoft.com
ContentProtect	Windows 2000 Windows XP Windows Vista	www.NetNanny.com
Integard	Windows Vista، Windows ME Windows 98، Windows 2000 Windows XP	http://en.kioskea.net
ModemLockDown	Windows XP Windows Vista	www.modemlockdown.com
SpectorPro	Windows 98، Windows ME Windows NT، Windows 2000 Windows XP	www.spectorsoft.com

Table 7.7: Lists some dedicated web browser for children [112]

Web Browser	Operating systems supported	The Web address of the Provider
MyWeb	Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP	www.myweb.com
SurfOnTheSafeside	Macintosh OS 9 Macintosh OS X	www.surfonthesafeside.com

	Windows 3.1 Windows 95 Windows 98 Windows ME Windows NT Windows 2000 Windows XP Linux OS-independent	
Awesome Library for Kids Browser	Macintosh OS 9 Macintosh OS X Windows 3.1 Windows 95 Windows 98، Windows ME Windows NT، Windows 2000 Windows XP Linux OS-independent	www.awesomelibrary.org
Aol Parental Controls	Windows Vista Windows 2000 Windows XP	parentalcontrols.aol.com
KidZui	Macintosh OS X Windows Vista، Windows XP	www.kidzui.com

Chapter Eight

International Organizations and Cybersecurity

Introduction

Given the importance of the international, cooperate efforts on cybersecurity issues; in this chapter, we are going to discuss the some efforts of the main international organizations working to develop the cyberspace security. Namely, we are going to mention the efforts of the International Telecommunications Union (ITU), International Multilateral Partnership Against Cyber Threats (IMPACT), and the Forum of Incident Response and Security Teams (FIRST)

The International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is an international organization that responsible to lead the regulation and development of the telecommunications at the international level. Based on his headquarter office in Geneva and the distributed regional offices all over the world the union work closely with other stockholders to coordinate the international efforts to connect the world. To carry out his mission, the union organized as follows:

- Secretary general office to carry out the administration tasks;
- Telecommunications development sector;
- Telecommunication standardization Sector;
- Radio communication sector;
- Regional offices for coordination the efforts and initiatives and provide advanced technical supports;

To properly compete or respond to cybercrimes, we have look at the issue of cybersecurity from the global prospective. This chapter summarizes the efforts of the ITU in the cybersecurity and critical infrastructure protection by discussing the IUT's global cybersecurity agenda and ITU-IMPACT shared duties.

ITU's Global Cyber-security Agenda (GCA)

To have secure communications and information system across the world, ITU announce what is called the Global Cyber-security Agenda (GCA) which built on the five basic working skeletons base as shown in figure 8.1

Figure 8.1: Points up ITU's Global cybersecurity Agenda

Legal Measures

On legal measures, ITU is working to help the member states to build their complete legal frameworks do deal effectively with cyber-security Legal difficulty. Given the goal for building global legal cybersecurity framework, ITU is contentiously support for Laws and legislation harmonization for different countries. Examples of these efforts are:

- Harmonization of ICT policies and legislation across the Caribbean (HIPCAR)[113].
- Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA) **.[114]**
- Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)[115]..

International Cooperation

In term of international cooperation, ITU is working jointly with the International Multilateral Partnership against Cyber Threats (Impact) to compete and quickly respond to cyber crime issue in the member states. In summary, ITU Impact is working to the following agenda to enhance the international cooperation for anti-cybercrime:

- Help the member states to establish Computer Incident Response Teams (CIRT)
- Evaluation and auditing for the member state national CIRT.
- Support the member states national and regional plan on child online Protection
- Support the member country initiatives for Laws and legislation harmonization (Law and legislations related to cyber security, cybercrime, and critical information infrastructure Protection).
- Support the member country access to the international resources related to cyber-security.

Capacity Building

ITU- Impact is continuously working to develop the human resources of the member countries in the area of cyber security through attractive advanced training exchange programs. The following points are the key strategic areas that ITU-impact a assist the me member states for capacity building[116] .

- Capacity building in information management;
- Building the technical experience;
- Support the research and development;

- Supporting the national level initiatives for building cyber-security Skills;
- Capacity building in the areas of Law, legislation and regulation;

Organizational Structure

On organizational structure, ITU –IMPACT are working on the road to strengthen the international cooperation between countries on cybersecurity themes and provide advanced technical support to developing countries to their information and critical infrastructure protection governing bodies. In this regards, ITU advice off member state to build the following organizations[117] .

1. A National Cybersecurity Council (NCC) to lead all cybersecurity organization and cybersecurity initiatives;
2. A National Cybersecurity Authority (NCA) , to implement the cybersecurity goals;
3. A National CERT and/or CSIRTs to act as focal point for incident response management;

Technical and Procedural Measures

On technical and procedural measures, ITU is continuously to identify the potential solution to the emerging cyber security problem by developing technical and procedural measures such as:

- Measures that enable threat detection;
- Measures that thwart cybercrime;
- Measures that enable business continuity;
- Measures that enable protection;

Based on these measures, ITU and IMPACT are working to develop technical potential solutions by [118]:

- Develop cybersecurity standards (ITU-T);
- Develop research and development initiatives (ITU-T study group 17);
- Coordinate the frequency conventions (ITU radio-communications);
- Response to incidents (Global Response Centre (GRC));

ITU Cybersecurity Projects

As of its commitment to the Global Cybersecurity Agenda, ITU continuously help member states to establish and improve their computer emergency response team (CERT) and other related projects.

In summary, ITU help the following countries to establish their national CERT

- Uganda
- Zambia
- Kenya
- Burkina Faso
- Burundi
- Jamaica
- Ghana
- Ivory Coast
- Tanzania
- Cybersecurity Innovation Centre for the Arab
- Least developed countries infrastructure protection program - project framework.

Table 8.1: lists the important ITU publications related to the cybersecurity subject

Publication	Contents Summary
The ITU National Cyber-security Strategy Guide[119]	This publication summarizes the ITU advice for cyber security at the state level
ITU-IMPACT Service Catalogue[120]	This publication summarizes the set of services provided by the ITU-Impact to each member state.
ITU-IMPACT Partnership Prospectus (ALERT) Applied Learning for Emergency Response Team [121].	This publication summarizes the ALERT services.

Cyber-security Guide for Developing Countries [122].	This publication summarizes the ITU cybersecurity guides for developing countries.
Understanding cybercrime: Phenomena، challenges and legal response[123]	This publication describes the cybercrimes and the legal response.
ITU/UNODC Cybercrime: The global challenge [124].	This publication summarizes the problems associated with cybercrimes
ITU National Cyber-security/CIIP Self-Assessment Tool [125]	This publication summarizes the step and tools for self-assessment.

Child Online Protection

Child online project is a part of ITU international agenda for cybersecurity (www.itu.int/cop). This project was proposed at the IUT council general summit in 2008 and approved by the secretary general, country members, and large international organizations. Table 8.2 list the main contributor for this project[126]:.

Table 8.2: The main contributors to the child online protection Project

Organization	Website
ITU	www.itu.int/cop
Children's Charities' Coalition on Internet Safety	www.chis.org.uk/
Child Helpline International	www.childhelplineinternational.org
ECPAT	www.ecpat.net
European Network and Information Security Agency	www.enisa.europa.eu
European Broadcasting Union	www.ebu.ch
European Commission Safer Internet Program	ec.europa.eu/saferinternet
European NGO Alliance for Child Safety Online	www.enacso.eu
Family Online Safety Institute	www.fosi.org
GSM Association	www.gsma.com
ikeepsafe	www.ikeepsafe.org
International Criminal Police Organization	www.interpol.int
International Centre for Missing& Exploited Children	www.icmec.org
optimal internet	www.optenet.com
Microsoft	www.microsoft.com
Telecom Italy	www.telecomitalia.com
Telecom Spain	www.telefonica.com
Save the Children	www.savethechildren.org
United Nations Children's Fund	www.unicef.org
United Nations Office on Drugs and Crime	
United Nations Interregional Crime and Justice Research Institute	www.unicri.it
United Nations Institute for Disarmament Research	www.unidir.org
Vodafone Group	www.vodafone.com

Child online protection Project objectives

1. Identify the risks and weakness for children in the cyber space.
2. Develop public awareness on all related issues connected to the problem of securing the child online.
3. Develop technical tools help to reduce the risk space.
4. Support Knowledge and information sharing

Figures 8.2- to-8.4, explain the ITU, governments, schools, families, and information and communication industrial sectors responsibilities to protect the child in the cyberspace.

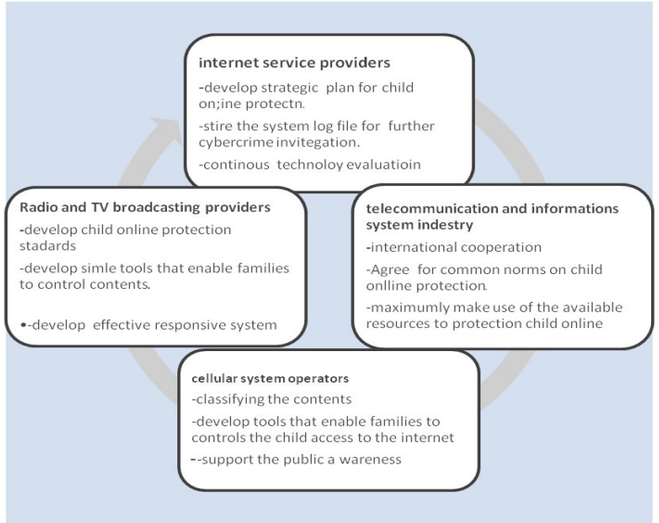


Figure 8.2: illustrates the ITU recommendations to the communication and information technology sectors to work for the child online protections.

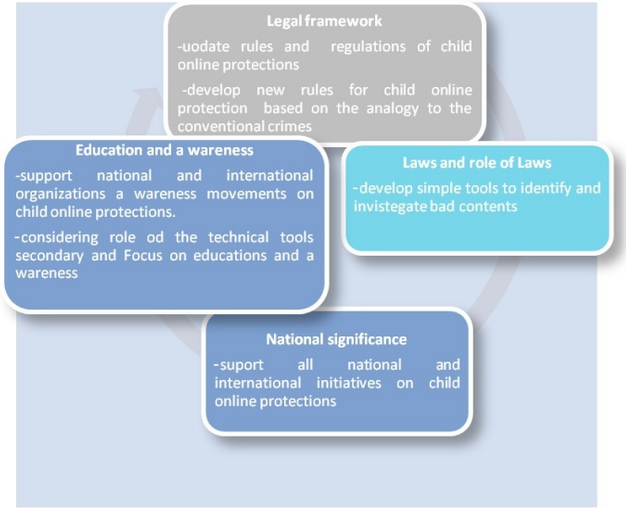
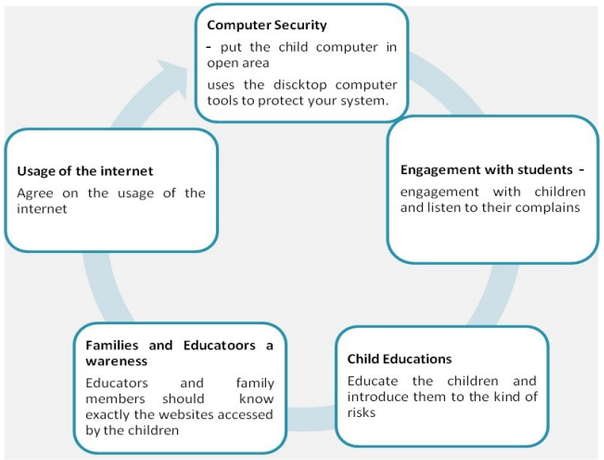


Figure 8.3: ITU recommendation on child online protection subject



Figures 8.4: ITU recommendation to the educators and families on the child online protection

International Multilateral Partnership Against Cyber Threats (IMPACT)

As part of the implementations of the Global Cyber-security Agenda (GCA), IUT signs an agreement with International Multilateral Partnership against Cyber Threats (IMPACT) in 2008. This agreement formally authorize IMPACT to carry on the implementation of the GCA from it is head office in Cyberjaya- Malaysia. From the 2011 Geneva World Summit of the Information Society (WSIS), IMPACT starts to coordinate the efforts and provides advanced technical supports to the 193 ITU member states to compete cybercrimes. Also today IMPACT provide technical support to the UN agencies and to the international organizations

The set of services provided by the IMPACT centre is illustrated in figure 8.5.

Figure 8.5: main service provided by the IMPACT Global response centre (GRC) centre

Global response centre

The Global response centre (GRC) is work to provide advanced technical supports to all member countries in emergency of communication and information systems. The GRC is work closely with leading industrial and research partners to gain advanced knowledge and experience. In addition, the GRC provide access to Electronically Secure Collaborative Application Platform for Experts (ESCAPE), which is unique application that enables information and knowledge sharing between experts around the world. Table 8.3, list the main service provided by the ESCAPE applications and the GRC.

Table 8.3: summarize the main services provided by the Global response centre (GRC)

Service Provided	Description/number
ESCAPE (Access to ESCAPE)	Access from one computer(one global IP address)
Ability to have Access to the Network Early Warning System (NEWS) and Data Visualization	✓

ESCAPE (Maximum number of ESCAPE portal accounts)	5
Ability to invite local experts to the IM-PACT expert Community	✓
Ability to escalate incidents to the IM-PACT expert Community	✓
Ability to upload malware for IMPACT analysis	✓
Ability to receive periodic security news	✓
Ability to receive periodic security reports (Generic)	✓
Ability to subscribe to ESCAPE's content	✓
Minimum number of Computer Security Incident Response Team members nominated	1

Policy and international Cooperation Centre

Within the GRC, the policy and international cooperation center is working toward achieving the following goals:

1. Support the international initiatives for cybercrimes and cybersecurity legal frames harmonization's.
2. Develop international awareness for cybersecurity and critical infrastructure protection.
3. Support the international initiatives in the area of child online protections.
4. Support the international cooperation and knowledge sharing.

Training and Skills development

The impact-training center is working in cooperation with international security solution providers to afford advanced technical, managerial, and training support to all ITU member states. Figure 8.6, illustrate the main training and capacity building areas provided by the ITU-impact-training program.

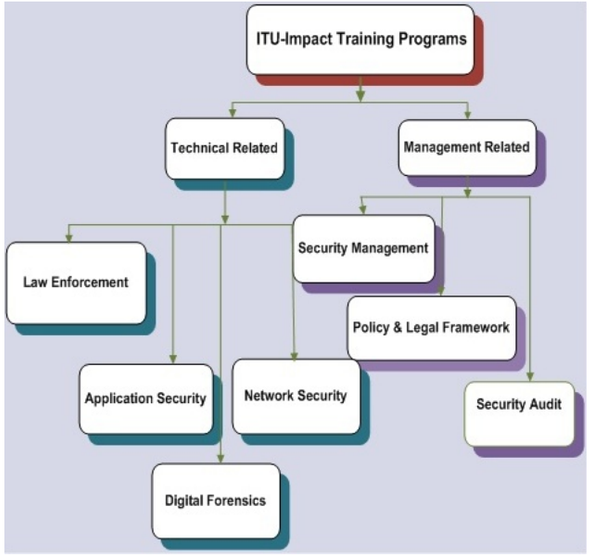


Figure 8.6: illustrate the training programs provided by the ITU-IMPACT

Security Assurance and Research

The security assurance and research center within the impact organization is working closely with some international information systems solutions providers to support the research and innovations in the area of cybersecurity and critical infrastructure protection.

Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams(FIRST), is established in 1990 to support the information exchange and cooperation on issues of mutual interest to the members for instance new vulnerabilities or a wide ranging attack on core system such as DNS servers or internet critical infrastructures[127]. This forum brings together a wide variety of security and incident response teams, including especially cybersecurity teams from the government, commercial, and academic sectors.

Thus, forum membership consists of teams from a wide variety of organizations, including educational, commercial, vendor, government, and military

Since 1990, FIRST members have resolved an almost continuous stream of security-related attacks and incidents, including handling ten thousands of security vulnerabilities affecting nearly millions of computers and networks all the way through the world connected by the emergent internet.

The main services provided by FIRST

Through its trusted communication and sharing environment, FIRST provide the following services it is members

- Access to best practice on how effectively responds to security incidents.
- Access to the and sharing of the best security tools
- Providing trusted and excellent communication and sharing environment
- Promote the global safe cyberspace
- Promote incident prevention
- Promote the knowledge update and CERT development.
- Access to up-to-date best practice documents
- Technical colloquia for security experts
- Some hands-on classes
- Organizing an Annual incident response conference
- Access Publications and web services
- Access to special interest groups

In addition to all these services, FIRST is also contribute with the ITU and ISO organization to develop a number of cybersecurity standards.

Chapter Nine

Qatar Experience

Current National Plans and Future Direction

Qatar is one of the richest states in the Middle East. In the recent years, there is a lot of development in all aspects of the life and economics. To become one of the excellent countries, the government in Qatar is working hard on the communications and information Technology sectors to increase the efficiency of the productions. The most important project in ICT sectors is the e-government, which is an integrated government cloud to provide the net of government services, the e-learning Patrol, the e-business, and Qatar National Broadband Network (QNBN), which is expected to be finished in 2015.

One of the most strategic project is Qatar is the Qatar Space project, which include lunching two space vehicles to provide More degree of freedom in communications transmission and broadcasting services. The space vehicle Soheel-1 was launched in September 2013 see figure 9.1, to provide the following services:

- Telecommunications networking;
- High Definition Television (HDTV) and Standard Definition Television (SDTV) Channels
- Internet networking

The space segment of soheel-1 is operating on the geostationary orbit at 25.5 East and will operate for 15 years lifetime to cover Arab state region and North Africa. Soheel-2, which plan to be in orbit in 2016 to fulfill the requirement of the country to the plan of 2022.

Figure 9.1: shows part of the launching process of the shell 1 satellite (source Aljazeera news broadcasting)

Critical Sectors

In Qatar, sectors are deemed as critical when their incapacitation or destruction would have a debilitating impact on the national security and social well-being of a nation. Taking into account this definition, the following sectors was defined as state critical infrastructures:

- Banking and finance
- Energy Facilities and Network
- Government
- ICT Sectors
- Healthcare
- Water
- Food
- Transportations
- Media
- Hazardous Materials

Past and Present Initiatives and Policies

Given the importance of the information security and critical infrastructure protection, the Qatar Supreme Council of Information & Communication Technology starts many initiatives to develop the process of communications and information system protections, the initiatives can be summarized as follows:

1. Establishment of Qatar Computer Emergency Response Team (Q-CERT) in 2005, figure 9.2, shows the main website of Q-CERT.
2. Publishing the National Information Assurance Policy v2 in 2014, which provides the necessary foundation and the relevant tools to enable the implementation of a full-fledged Information security management system within the organization[128]
3. Identification of critical information and communications infrastructures
4. Development of nationwide risk management plans.
5. Development of protection tools
6. Response to the emergency and providing technical helps.
7. Help critical sectors by providing advanced technical assistance and training.
8. Enabling knowledge sharing between private and state sectors
9. Enabling knowledge sharing between with the international and regional organizations and bodies

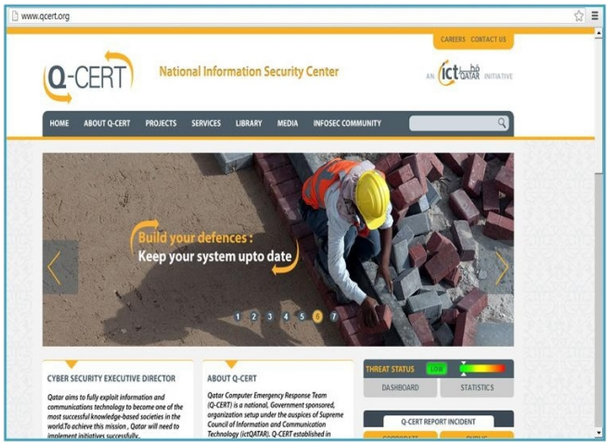


Figure 9.2: the main website of Q-CERT (www.qcert.org)

10. Development of security policy instructions for the Supervisory Control and Data Acquisition (SCADA) System to protect the industrial sectors.[129] The objective of the policy is to ensure the correct and secure operation of SCADA/DCS information processing facilities.

11. Development of the national Government Information Assurance Policy v1 [130]

12. Establishment of Qatar national satellite communications system to provide additional degree of independence

Organizational and institutional Overview

- Supreme Council of Information & Communication Technology: established in 2004 to carry out the management, regulate, protect, and introduces the main policies of the information's and communications sectors.

- Qatar Computer Emergency Response Team (Q-CERT): within the Supreme Council of Information & Communication Technology, QCERT is working to protect the critical infrastructures from cybercrime, introduce the general framework of cybersecurity, and provide advanced technical support to both state and private sectors. The cyber-security division directs efforts to:

1. Provide accurate and timely information on current and emerging information security threats and vulnerabilities
2. Respond to threats and vulnerabilities relevant to our constituencies
3. Promote the adoption of information security standards, processes, methods, best practices and tools
4. Build the local capacity and capability to manage cyber risks by providing specialized training and awareness

Early Warning

In Qatar, the computer emergency response team is working as a central point for information sharing between the state sectors and private sectors and the other international information computer emergency response teams. This team is also working for 24 hours to monitor the internet traffic and provide advanced technical support on emergency and cybersecurity incidents management.

Child Online Protection (COP)

On child online protection issues, the supreme council of information & communication technology is working closely with supreme council of educational to organize specialized workshops to lift up the public awareness on child online protections. On the other hand, also the supreme Council of information and communication technology is work closed with the supreme Council of the family and the ITU to develop educational materials for cybersecurity to introduce the educators about the basic of cybersecurity and make maximum use of the available web resources[131].

In general, we can summarize the efforts and initiatives of Qatar in child online protections in the following points:

1. Design and publish an interactive website to receive complaints and provide educational and supporting materials to increase the awareness on child online protections.
2. The supreme council of information & communication technology is working closely with educational institutes and organizations at the national level raise the awareness on child online protection.
3. The supreme council of information & communication technology is also working closely with the international organization that work to protect child in the cyberspace
4. The efforts of the child and woman society (part of Qatar foundation)
5. Safe space campaign effort, which aim to raise the awareness of the public(Teens, Educators, Parents) about the child online protection and how to have safe access to the internet [132]. The web page provides valuable resources, reports, and instructions on safe access to the internet.

Figure 9.3: Main web page of the child online protection web page, Safe Space (source: safespace.qa)

Laws and Legislations

- Electronic commerce and transactions law 2010[133][134] :
- Critical Information Infrastructure Protection Law, 2014

Some Important web Resources

Table 9.1: list the most important information security related web Resources

Organization name	Service provided	web address
Qatar computer emergency response team (Qcert).	Provide advanced technical support, constructive advice and Proposing good legislation practice	www.qcert.org
Supreme Council of Information & Communication Technology	Regulate the information and communication operations	www.ictqatar.qa
Safespace	Provide educational and awareness materials to help for child online protection	www.safespace.qa
Qatar E-learning Window	Provide related information and communication, educational and awareness materials	www.elearning.ictqatar.qa
Hokomi	Secure Government service window	portal.www.gov.qa

Chapter Ten

Australian Experience

Current National Plan and Future Direction

Australia is one of the truly developed countries where each aspect of life is heavily depending on information and communication technology. Given it is geographic location, area and connectivity requirements, Australian government builds high speed, and reliable Telecommunication Transmission Network across the country and reliable international transmission connectivity to other part of the world such as US, Japan, Middle East and South East Asia.

To upgrade its existing network to Australian government announce it National Broadband Network (NBN) project with total budget of 37 billion AU Dollar. The aim of this project is to connect 93% of the users with the Broadband network (fiber to home technology) by the year 2021. The project is also plan to connect remote areas with the 4th generation cellular communication service and to lunch two Next-Generations of KA-Band Satellites with 80Gbps for each unit to support the reliability, scalability, and the stability of it network during the critical times and disasters [135]

In 2009 the government establish the NBN Co to manage and implement the NBN project [136] . Figure 10.1, illustrates the main webpage of the NBN Co from which anyone can monitor its activities.

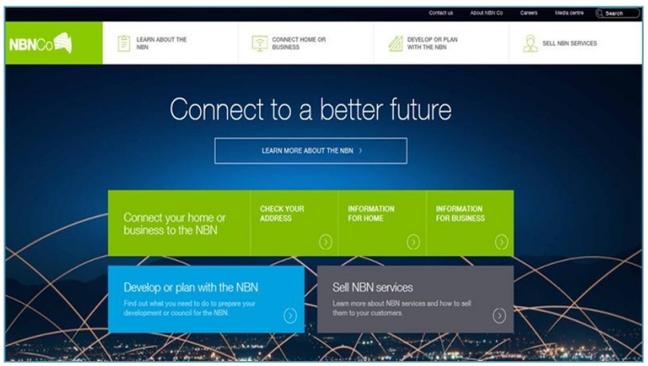


Figure 10.1: the main webpage of the national broadband network (NBN) (Source: http://www.nbnco.com.au/)

Critical Sectors

Australian governments define critical infrastructure as those physical facilities, supply chains, information technologies, and communication networks, which, if destroyed, degraded or rendered unavailable for an extended period, would significantly influence the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security. Thus, the government recognizes the importance of critical infrastructure, including those parts that provide essential services for everyday life (such as energy, food, water, transport, communications, health and banking and finance). A disruption to critical infrastructure could have a range of serious implications for business (including other critical infrastructure), In Australia the governmental assigned the responsibility of Protecting the critical infrastructure to the critical infrastructure advisory Council (CIAC) under the supervision of the Attorney-General's Department. The following sectors are being considered as critical infrastructure

- Telecommunications (Phone, Fax, Internet, cable, Satellites) and mass communications
- Energy(Oil & Gas Security)
- Banking and finance
- Food chain(Bulk Production, Storage, and Distribution)
- IT security
- Health system (Hospitals, Public Health, and Research and Development Laboratories)
- Mass gatherings
- Transport (Air Traffic Control, Roads, Sea, Rail, and Inter-modal)
- Water service (waste water, and waste management)

Past and Present Initiatives and Policies

The most recent initiative in Australia is the development of critical infrastructure resilience strategy (CIR) in 2010[137]. This Strategy describes the Australian

Government's approach to enhancing the resilience of the critical infrastructure to all hazards, which includes the following objectives:

1. Operate an successful business-government partnership with critical infrastructure owners and operators
2. Develop and encourage an organizational resilience body of knowledge and a common understanding of organizational resilience
3. Assist owners and operators of critical infrastructure to identify, analyze and administer cross-sectoral dependencies
4. Provide timely and high quality policy recommendation on issues relating to critical infrastructure resilience
5. Implement the Australian Government's cybersecurity Strategy to maintain a secure, resilient and trusted electronic operating environment, including for critical infrastructure owners and operators;
6. To support the critical infrastructure resilience programs delivered by the Australian government and Territories, as agreed and as appropriate;

Given that the majority of critical infrastructure in Australia is owned or operated by the private sector and the States and Territories, the Australian Government has a complex set of roles, responsibilities, and interests in CIR. The Australian Government is responsible to act as:

- An owner and operator of critical infrastructure
- The regulator of security in some industries (i.e. Aviation and maritime)
- The industry regulator in other sectors, but not necessary for the 'protection' of critical infrastructure from acts of terrorism
- Responsible for operating the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience, which provides national level forums for owners and operators of critical infrastructure to discuss critical infrastructure vulnerabilities with relevant government agencies
- The primary source of security threat assessments, and
- A source of research, scientific and technical advice relevant to the protection and resilience of critical infrastructure;

E-Security Law

The government of Australia announced the E-security Law in 2007 and devoted a large amount of resources to support information security initiatives across the country. In addition, the E-Security Policy and Coordination (ESPaC) body was established to work on the following objectives:

- Reduce the risk of the information and communications sectors
- Reduce the risk to the critical infrastructure
- Support the security of the end user (reduces phishing and massive attacks)

Organizational and institutional Overview

In Australian, the following organizations share the responsibility of information critical infrastructure protection:

- Attorney-General's Department: within the attorney general department, the information and critical infrastructure protection division is working to develop rules, regulations, and guidelines that contribute to the information system security and reduces the rate of cybercrimes. Also, this department manages the Trusted Information Sharing Network (TISN), and coordinates the critical infrastructure threat assessment briefing programs,
- Trusted Information Sharing Network for Critical Infrastructure Protection: this group was been established to support and sustain the information sharing process between the public and private sectors.
- E-Security Policy and Coordination Committee (ESPaC): This committee has members from the ministry of defense, national security, and communications Electronics commerce, cybercrime police, and the cabinet office. ESPaC is working under Attorney-General's office to rise up the public awareness, support the research and development

and coordinate the effort for information security and critical infrastructure protection

- Department of Broadband, Communications and the Digital Economy (DBCDE): is responsible for policy development, advice and program delivery across a range of activities including the National Broadband Network rollout, Australia's digital television switchover, initiatives that support development of the digital economy, telecommunications policy, media policy, cyber security and cyber safety, managing the radio frequency spectrum and postal policy. Under the CIR Strategy, this department is also responsible for:
    - The provision of portfolio specific policy advice on critical infrastructure related issues
    - The provision of secretariat support to the Communications Sector Group and the IT Security Expert Advisory Group, and
    - Drafting risk context statements and contributing to briefings under the threat assessment briefing
- Australian Federal Police (AFP): after circulation of the 2001cybercrime's Law the AFP establish the Australian High Tech Crime Centre [138] (AHTCC) to investigate the cyber-security crimes.
- Australian Security Intelligence Organization (ASIO) this government organization is responsible to collect intelligence information related to cyber crimes, do the necessary analysis, and provide the necessary advices to the other governmental bodies. Other duties also include:
    - The identification and prioritization of national critical infrastructure, including maintaining a database of national critical infrastructure
    - The preparation of vital and sectoral critical infrastructure threat assessments
    - The briefing of owners and operators of vital and sectoral critical infrastructure threat assessments, and
    - Protective security risk reviews for specified critical infrastructure.

Early Warning and Public Outreach

In Australia, there are two governmental organizations responsible to provide the services of early warning and intensifying the public awareness. These organizations are:

- Defense Signals Directorate (DSD): this directorate is responsible to handle Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS)
- Australian Computer Emergency Response Team (Aus-CERT): this team is established in the university of Queen land to provide advanced technical support and early warning services to both state and private sectors:
- Australian Cyber Security Centre (ASCS)

Child Online Protection (COP)

Given the importance of the child online protection, the Australian government build ups number of Laws and legislations for child protection on the cyberspace [139]. The responsibility of child protection is allocated the educators, family members, educational institutes, internet services providers, and Australian federal police. For example, the Australian federal police establish special unit for child protection is responsible for coordinates and investigate all cybercrimes related to the child. In addition, this unit coordinates with internet service providers to monitor the internet searching for illegal web contents according to the Australian Laws to carry on further active step against the hosting organization if it is in Australia or coordinate with international bodies if the content is hosted outside the country.

Australian federal police is also receiving the daily complaints from the public from the website shown in figure 10.2, and table 10.1 lists other importation organizations working on child online protection in Australia

On the other hand NetAlert ACMA Schools Outreach Program – which involve trainees to visit schools and community groups in every state and territory throughout Australia. The program provides parents and teachers with hands-on support and practical internet safety assistance, to help them ensure their children's or students' internet experience is a safe one. Recently this swapped by new Internet filtering technology named Net-Alarmed which levels the balance between safety and freedom. Figure 10.3; show the main webpage of this internet filtering. This internet-filtering stop put the following types:

- Pornography
- Violence
- Sex education
- Drug education
- Health information
- Gay and lesbian information
- Minority religious beliefs
- Terrorists
- Anti-Government sites
- YouTube and MySpace
- File Sharing

Table 10.1: list of organizations that receive daily complains on child online protection issues

Organization	Web address
Australian Federal Police	https://forms.afp.gov.au/online_forms/ocset_form
Thinkuknow	http://www.thinkuknow.org.au/
Virtual Global Taskforce	http://www.virtualglobaltaskforce.com/
Internet service providers	https://forms.afp.gov.au/online_forms/ocset_ispich_form.html
ACMA	http://www.acma.gov.au
NAPCAN	http://napcan.org.au/”’w

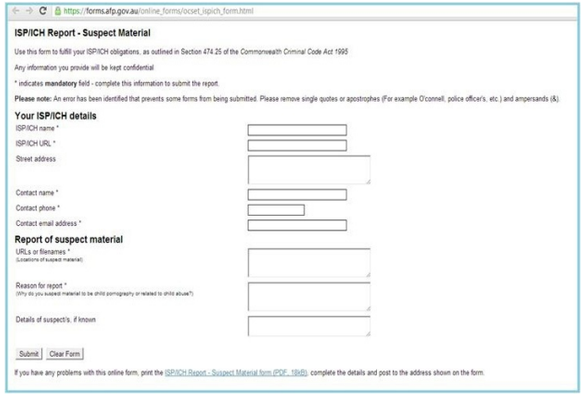


Figure 10.2: web frame designed by the internet providers to receive the public complains on child online protection

Figure 10.3: the main web page of the Net-alarmed (source: http://www.netalarmed.com/)

Furthermore, the government of Australia is working through the project of cybersmart figure 10.4 (http://www.cybersmart.gov.au), to provide valuable material to the schools, families, and educators to help them in child protection in the cyberspace.

Figure 10.4: the main webpage of the cybersmart organization (Source: http://www.cybersmart.gov.au)

Laws and Legislations

To develop the information and communications sectors the government of Australia legislate the following laws:

- Electronic Transactions Act (1999)/ Amendment Act 2011 [140] : The Act clearly states that a transaction under a law of the Commonwealth will not be invalid simply because it was conducted by the use of electronic communications. The Act allows any of the following requirements or permissions under Commonwealth law to be fulfilled in electronic form:
    - Giving information in writing
    - Providing a handwritten signature
    - Producing a document in material form, and
    - Recording or retaining information
- Cybercrime Act (2001): this Act gives federal law enforcement agencies the authority to investigate and prosecute groups who use the internet to plan and launch cyber-attacks (such as hacking, computer virus propagation, or denial-of-service attacks) that could seriously interfere with the functioning of the government, the financial sector, and industry[141].
- Spam Act (2003): this act was passed in 2003 as federal legislation by the Parliament of the Commonwealth of Australia. The purpose is to set up a method for the regulation of commercial e-mail and other types of commercial electronic messages. It restricts spam, especially e-mail spam and some types of cell phone spam, as well as e-mail address harvesting, however, there are broad exemptions. It is forced by the Australian Communications and Media Authority (ACMA)[142].
- Sexual Offences Against Children) Act 2010: the objective of this act is to protect children from sexual crimes.[143]
- Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011.[144]
- National Broadband Network act 2011: this act distress the freedom of information and the management of the broadband telecommunication network .[145]

Some Important web Resources

Table 9.1: list the most important information security related web Resources.

Organization name	Service provided	web address
Cyber-smart	Provide valuable advice on child online protection	www.cybersmart.gov.au
Stay Smart Online	Provide advanced technical advice on how to stay save online	www.staysmartonline.gov.au/

CERT	Provide advanced technical support and help on emergencies	www.cert.gov.au/
Cyber Security	Provide some basic security tools	www.dbcde.gov.au/online_safety_and_security/cyber_security
Cyber-safety plan	Provide child online protection materials	www.dbcde.gov.au/funding_and_programs/cybersafety_plan
The Easy Guide to Socializing Online	Provide valuable advice on how to be secure on social networking websites	www.dbcde.gov.au/easyguide
Online safety and security	Provide comprehensive description on government effort on information security	www.dbcde.gov.au/online_safety_and_security
OnSecure	Provide advanced technical support on recent issues.	www.onsecure.gov.au/
ScamWatch	Provide valuable advice on phishing	www.scamwatch.gov.au/
ThinkUKnow	Provide training material on child online protections	www.thinkuknow.org.au/
The Trusted Information Sharing Network	Act as Information Sharing Network hub	www.tisn.gov.au/Pages/default.aspx

Chapter Eleven
Malaysian Experience

Current National Plan and Future Direction

Malaysia is one of the fastest developing countries in the south East Asia. The government has an ambush plan for 2020 to become one of the best-developed countries. This plan incorporates an outstanding strategy to develop the information and communication sectors by:

1. Maximize the gain from the information and communication technology (developing the human resource capacity and using ICT in the industry)
2. Develop and bring up to date the communications systems infrastructure

To achieve the first goal the government works on the development of the human resources on all ICT related sectors (education, training, awareness campaigns) and decide to computerize all public and commercial services. Furthermore, the government increases the public confidence on ICT sectors by providing advanced technical support security and protection.

To develop the information and communication sector the government spend about 4billion US$ on what called High Speed Broad band (HSBB) Network project to upgrade the existing nationwide network to the second Generation fiber optic based network[146]. The objective of the project is to provide high-speed broadband access to the end user (about 100Mbps to the domestic user, 1Gbps to the small and middle enterprise customers)

On the other hand, the governments also work on to develop the satellite communication sector. Today the Malaysia East Asia Satellite (MEASAT) operating 5-space element in the geostationary orbit to provide wide range of service (TV and radio broadcasting, broadband internet). In addition, these elements can operate at the time of disasters as backup telecommunication transmission media

Critical Sectors

In Malaysia, Critical National Information Infrastructure (CNII) were defined in the CNII website as those assets (real and virtual), systems, and functions that are

vital to the nations that their incapacity or destruction would have a devastating impact on the following:

- National economic strength; confidence that the nation's key growth area can successfully compete in the global market while maintaining favorable standards of living;
- National image; projection of national image towards enhancing stature and sphere of influence;
- National defense and security; guarantee sovereignty and independence whilst maintaining internal security;
- Government capability to functions; maintain order to perform and deliver minimum essential public services.
- Public health and safety; delivering and managing optimal health care to the citizen.

Based on this definition, the following sectors are identified as National Critical infrastructure [147].

- National Defense & Security
- Banking & Finance
- Information & Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food & Agriculture

The Malaysian government is working through cybersecurity Malaysia (cybersecurity Malaysia) organization to coordinate the effort and support the information sharing between the different sectors. The CNII website shown in figure 11.1 is one of the common platforms for the information sharing for the purpose of information security and critical infrastructure protection. This website is also contain valuable information, recommendations and reports that can be used by the state sectors, private sectors, and public [148] .

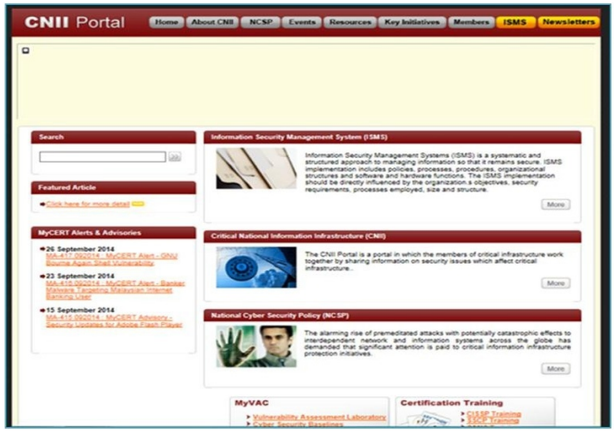


Figure11.1: the main webpage of the Critical National Information Infrastructure (CNII) (Source:cnii.cybersecurity.my)

Past and Present Initiatives and Policies

The Malaysian government announced National IT Agenda (NITA) in 1996 as a part of the nation's strategy to accomplish the requirement of the information era. This agenda contains general frameworks and timetables for all activities that need to be carried to develop the information and communications sectors. A part of these objectives was to increase the public confidence in using information and communication technology with the daily needs. Thus, providing information security becomes one of the essential needs to achieve the 2020 national plan to build information community.

Furthermore, and subsequently the National Information Technology Council (NITC) was established to support the public, private engagement to implement this agenda and to promote the E-Community, E-Public Services, and E-Economy concepts

Cyber security conference 2005

In 2005, a public-private-partnership driven conference is organized in the capital of Malaysia KL to gather cyber security industry experts and community to exchange ideas on security management, policy, and technology. Since then, this annual industry gathering is continuously organized by Cybersecurity Malaysia, the National cyber security specialist center under the purview of the Ministry of Science, Technology, and Innovation (MOSTI) to discuss the recent advances related to the following topics:

- Computer Emergency Response Teams
- Critical Infrastructure Protection
- Network and Application Security
- Security Management and Strategy
- Knowledge-Sharing

Malaysian National Cyber-Security Policy 2007

In 2007 Ministry of Science، Technology and Innovation (MOSTI) announced the national cyber security policy which aims at first place to address the risks to the Critical National Information Infrastructure (CNII).The Eight Policy Thrusts are as follows[149]:

- Effective Governance (Example: Promote effective cooperation between public and private sectors).
- Legislative & Regulatory Framework (establish, Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats).
- Cyber Security Technology Framework (Develop a national cyber security technology framework);
- Culture of security and Capacity Building (Develop, foster and maintain a national culture of security).
- Research & Development towards Self-Reliance (Formalize the coordination and prioritization of cyber security research and development activities).
- Cyber Security Emergency Readiness (develops and strengthens the national computer emergency response teams).
- Compliance and Enforcement (Standardize cyber security systems across all elements of the CNII)
- International Cooperation (Encourage active participation in all relevant international cyber security bodies, panels, and multi-national agencies)

Organizational and Institutional Overview

In Malaysia the main responsibilities of information security and critical infrastructure protection (policies development, regulation, cybercrime preventions and investigations… etc.) is assigned to the different organization as shown in table 11.1

Table 11.1: Summarize the responsibilities of the organization participated in information security and critical infrastructure protection in Malaysia

Responsible organization	Task
Communication and multimedia cooperation	Organizations/ regulation
Malaysian planning and modernization unit	Information security management in the public sectors
Cybercrime police department	Cybercrimes prevention, investigation
Ministry of Science، Technology and Innovation (MOSTI)	Cybersecurity policies development
Ministry of water and communications	Critical infrastructure Protections
Information Sharing Forum (ISF)	Public private information sharing and engagement

Early Warning and Public Outreach

In Malaysia, the following organizations are responsible to provide the technical support and rise up the public awareness of cybersecurity issues

Malaysian Computer Emergency Response Team

Malaysian Computer Emergency Response Team (MyCERT) is a government organization established in 1997. Since this time, this team has been considered as a reference technical support organization. The main objective of the MyCERT and be summarized as follows [150]

- Considered as a reference information security technical support as it is providing constructive support and advice to all government Sectors;
- Reports all attacks and incidents to the cabinets;
- Periodicals, publishing a report on recent advances on cybersecurity incidents, information security, and critical infrastructure attacking strategies.
- Provide and recommend best cybersecurity tools.
- Provide advanced training and awareness services to the public on information security and critical infrastructure protections.
- Receive and respond to the complaint related to the cybersecurity from the public, figure 11.2, shows the reporting main web page

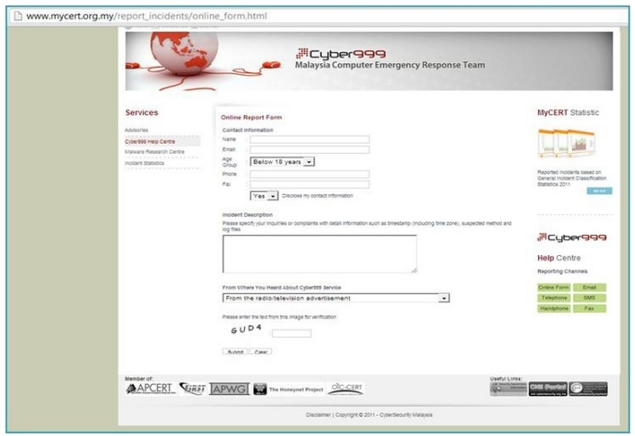


Figure 11.2: cybersecurity incident reporting main webpage (Source: www.mycert.org.my)

Cyber-Security Malaysia

In 2005, the government of Malaysia regulates the information security by adding additional responsibilities to the National ICT Security and Emergency Response Centre (NISER) and establishing the cybersecurity Malaysia organization under MOSTI to provide professional consultation and to act as trusted point for information sharing all government and private sectors in Malaysia [151]. Figure 11.3, show the main webpage for cybersecurity Malaysia that shows other information security partners. We can generalize the main services provided by cybersecurity Malaysia in the following points:

1. Research and development(cybersecurity incidents, instructions and attacking techniques)
2. Research and development in the fields of system auditing, reporting, cybercrime attribution and investigations, and computer forensic technology;
3. Periodically reviewing the cybersecurity policies, regulation, standards, coordinate with the international cybersecurity organization to know the latest updates in this area.
4. Develop the human capacity in this area.
5. Develop and manage the information system and critical infrastructure protestation Quality
6. Develop and regulate the professional certificates in cybersecurity

Figure 11.3: the main web page of the cybersecurity Malaysia (cyber-security Malaysia: www.cybersecurity.my)

Child Online Protection (COP)

Nationwide initiative was submitted in 2009 by the Malaysian communications and multimedia cooperation to protect child online. The main objective of the initiative is to support families to keep their children safe online. This initiative identified the follow risk point

- Cyber-bullying;
- Pornography;
- Violence;
- Racial abuse and hate;
- Online gaming & addiction;
- Online fraud & deception;

In response to this initiative, today in Malaysia many websites provide constructive advices to the families, educators, and schools on child safety online. An example of these websites is CyberSafe (www.cybersafe.my), figure 11.4 which contain a lot of valuable materials on child online protection [152].

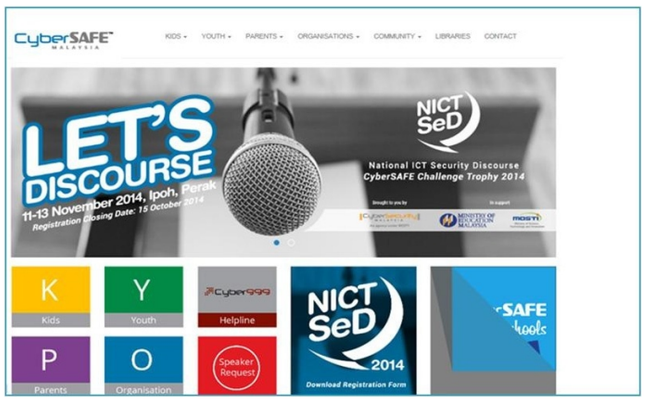


Figure: 11.4: illustrate the main webpage of Cyber safe (Source: www.cybersafe.my)

Laws and Legislations

From the early time of it is plan to develop the ICT technology, the Malaysian government starts to legislate laws and regulatory acts to provide a comprehensive legal framework to increase the public confidence in the ICT sector. The most important Laws related to the information, communications, and critical infrastructure protections are:

- Digital signature regulations 1998:[153]
- Malaysian Communications and Multimedia Commission Act (1998/2002): this Act seeks to provide a generic set of regulatory provisions based on generic definitions of market and service activities and services. The jurisdiction of this Act is restricted to networked services and activities only [154]
- Strategic Trade Act 2010: this document control over the export, transshipment, transit and brokering of strategic items, including arms and related material, and other activities that will or may facilitate the design, development and production of weapons of mass destruction and their delivery systems and to provide for other matters connected therewith, consistent with Malaysia's national security and international obligations[155].
- Postal Services Act 2012: this Act to provide for the licensing of postal services and the regulation of the postal services industry, and for incidental or connected matters[156]

Some Important web Resources

Table 11.2: list of important web address for information and critical information infrastructures

Organization name	Service provided	web address
Cybersecurity Malaysia	Provide advanced technical, education and awareness supports	www. cybersecurity.my

Malaysian computer emergency response team	Provide advanced technical support	www.mycert.org.my
Cyber Guru	Work as information security training center	www.cyberguru.my
Malaysian information security conference	Act as information sharing forum for the discussion of recent advances on cybersecurity	www.csm-ace.my
mytrustmark	Work as standing information security group	mytrustmark.cybersecurity.my
Critical National Information Infrastructure	Develop Laws and legislations	cnii.cybersecurity.my/main/about
cybersafe	Provide educations and training materials on child online protection	www.cybersafe.my

Chapter Twelve
United States Experience

Current National plan and future Directions

United States is the leading country in the world in information security and critical infrastructure protection. Although there is a large gap in the development of information and communications technologies between US and other countries, the US has constant ego to lead the world in this area. Thus each year, considerable amount of budget spent in research, development, and innovations in this area.

In 2010 and as a part of American Recovery and Reinvestment Act, the US government announced National Broadband Plan[157]. The six log term goals of this plan are as follows:

1. At least 100 million U.S. homes should have affordable access to actual download speeds of at least 100 megabits per second and actual upload speeds of at least 50 megabits per second.
2. The United States should lead the world in mobile innovation, with the fastest and most extensive wireless networks of any nation
3. Every American should have affordable access to robust broadband service, and the means and skills to subscribe if they so choose
4. Every American community should have affordable access to at least 1 gigabit per second broadband service to anchor institutions such as schools, hospitals, and government buildings
5. To ensure the safety of the American people, every first responder should have access to a nationwide, wireless, interoperable broadband public safety network
6. To ensure that America leads in the clean energy economy, every American should be able to use broadband to track and manage their real-time energy consumption

The US Federal Communication Commission (FCC), supervise the implementation of this plan by look up the statistics and indicators. Figure 12.1, show the main web page of the National Broadband Plan (Source: www.Broadband.gov)

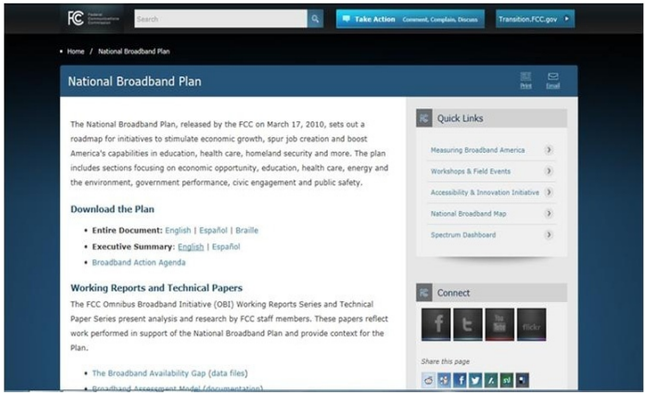


Figure 12.1: the main web page of the US National Broadband Plan (Source: www.Broadband.gov)

Critical Sectors

In the US, the Ministry of the Homeland Security in according to the Presidential Policy Directive 21 (PPD-21) defines critical infrastructures as "the infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being. based on this definition, the following Sectors are identified as State critical Infrastructures'[158] .

- Information Technology Sector
- Telecommunications sector
- Chemical Sector
- Commercial Facilities Sector
- Dams Sector
- Commercial Nuclear Reactors، Materials، and Waste Sector
- Government Facilities
- Transportation Systems Sector
- Emergency Service Sectors
- Postal and Shipping Services Sector
- Agriculture and Food sector
- Public Health and Healthcare Sectors
- Energy Sectors
- Banking and Finance Sectors
- Defence Industrial Base Sector
- Critical Manufacturing Sectors

Past and Present Initiatives and Policies

In US, People recognize the importance of critical information infrastructures protection since 1990. In the United States, any attack can have a major impact on the economy and national security of the country and the world. Given the proportion of this sensitivity, the federal government has introduced a number of initiatives, and has taken a series of preventive measures to protect the critical infrastructure of Informatics and Communications. These initiatives and measures have been summarized as follows:

- Establishment of the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1997(include both Government and private sectors members).[159]
- Presidential directive 62 and 63 on 1998 to protect critical infrastructure[160] .
- National Plan for Information [161] Systems Protection, 2000
- Homeland Security Executive Orders[162] and the establishment of the homeland security department in 2003
- Homeland Security Presidential Directive / HSPD-7[163] 2003 awarding the responsibility of the critical infrastructure protection to the homeland security department
- National strategy for homeland security 2002, Which includes the following points:
  - National Strategy to Secure Cyberspace[164]
  - Increase the national resistivity against cyber-attacks

- Reduce the loss by reducing the down time (when there is an attack)

- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.[165]
- National Strategy for Information-Sharing this strategy defines the information sharing protocol between different government sectors. This strategy updated in 2012 after the Wikileaks problem [166].
- Department of Defence Strategy for Operating in Cyberspace: this strategy is announced in 2011 to fulfill the following :[167]
  - Using the defence tools for information security
  - Search for new tools for information security
  - Cooperate and sharing knowledge
  - Building relations based on the information securities
  - Support innovation

- The national Strategy to Combat Transnational [168]Organized Crime: Addressing Converging Threats to National Security: this strategy is announced in 2011
- The International Strategy for Cyberspace: Prosperity، Security، and Openness in a Networked World: This strategy is announced in 2011 .[170 ،169]
- National Strategy for Trusted Identities in Cyberspace: this strategy is developed in 2011 to strengthen the information security and critical infrastructure protection [171]
- Safeguarding American Consumers & Families Privacy: the aim of this cybersecurity initiative is to protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties[172].
- Executive Order Promoting Private Sector Cybersecurity Information Sharing 2015: the aim of this executive order is to lay out a framework for expanded information sharing designed to help companies work jointly and work with the federal government, to quickly identify and protect against cyber threats.

Organizational and institutional Overview

At the beginning of information security and critical infrastructure protection era, the US government assigns the responsibility if critical infrastructure protection to government bodies in the ministry of commerce known as Critical Infrastructure Assurance Office (CIAO). This office was working closely with the Federal Bureau of Investigation (FBI) to investigate the cybercrimes and manage a cybersecurity incident response. With the development of information and communications sector and increasing of the rate of cyber-attacks, the government established the Department of Homeland Security (DHS) to protect the critical infrastructure with the help of the following organization:

1. National Office of Infrastructure Protection (OIP): this provide the following services:
   - Lead the operation/ plan of the critical infrastructure protection
   - Evaluate the risk management plans
   - Supervise the information sharing between different sectors
   - Collect the data and make the necessary analysis about risk
   - Establish international relations for information security and critical infrastructure protection.

2. Office for Cybersecurity and Communications (CS&C): this office coordinates between different on risk managements and cyber attack incidents handling. The main objective points are [173]:

- The telecommunication network should provide it is a service all time and under any condition.
- The national information security sector should work will all private and public sectors to protect the critical infrastructure
- Office of Emergency Communications (OEC): this office is working to develop an emergency communication system to make sure that the government order is coordinated at the emergency time.

3. US Department of State: the state department is working closely with the Defense department and foreign alliance to support all initiatives related to information security to reduce risk and vulnerability.
4. Congressional Focus: working as part of the homeland security committee to support the following directions:
    - Communication and critical information protection
    - Support the research initiatives related to information security and risk managements.
    - Making sure that all communication and information system can work at emergency time;
    - Supporting the national intelligence, information sharing, and risk management information
5. Government Accountability Office (GAO): This office generates periodic reports on cybersecurity incidents and the status of the country to compete cybercrime.
6. Defense Community group: This is work on developing strategic cybersecurity strategy for define and industrial defense systems.
7. Computer Crime and Intellectual Property Section : This section working within the department of justice's to articulate laws and legislations related to computer crime and intellectual properties.
8. Protected Critical Infrastructure Information Program (PCIIP) : the goal of this program is to boost information sharing in between private sectors
9. Information Sharing and Analysis Centers (ISACs): (figure 12.2, http://www.isaccouncil.org/memberisacs.html): on these information sharing centers, interrelated industrial group such as Microsoft, Intel, CA, Symantec, CSC, IBM, Oracle, eBay, EWA-IIT، Harris، Hewlett Packard, BAE Systems, IT, and VeriSign, In .are forming information sharing focal point to share risk information

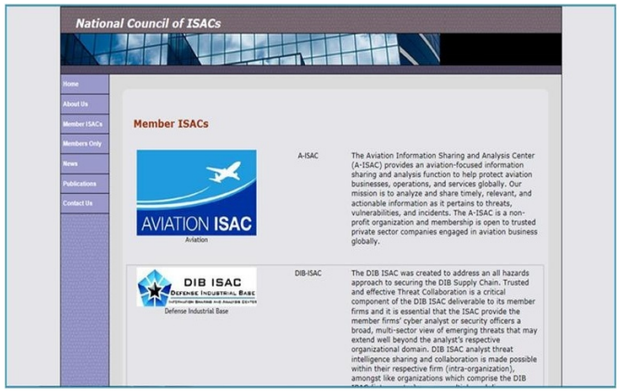


Figure12.2: the website for information sharing centers (Source: http://www.isaccouncil.org/memberisacs.html)

10. InfraGard office: this office coordinate between the private sectors and the FBI on research and development related to information security and critical infrastructure protection[174].
11. The office of National Cyber Security Alliance (NCSA): the purpose of this office is to gather industrial group and sectors in information sharing group to enable them to share valuable common information security and critical infrastructure practice and effective incident response handling techniques. Figure 12.3, shows the main web page of these groups(www.staysafeonline.org)

Figure 12. 3: National Cyber Security Alliance (NCSA) (www.staysafeonline.org)

Early Warning and Public Outreach

In United States, the following organizations are responsible to provide the technical support and rise up the public awareness of cybersecurity issues

1. CERT Coordination Center, Carnegie Mellon (http://www.cert.org/): this Centre is supported by the federal government to develop research and innovations and coordinate the efforts of CERT teams)
2. US Computer Emergency Response Team (US-CERT): established at the University Of Garage Mellon to prevent cybercrimes and provide advanced technical support and respond in emergencies;

Figure 12.4: The main Web page of the United States Computer Emergency Response Team (Source:www.us-cert.gov)

3. Federal Bureau of Investigation (FBI): FBI is responsible by the role of Law to investigate cybercrimes:
4. OnGuardOnline.gov (www.onguardonline.gov) this website is supported be research centers and large companies to raise the public awareness about protecting private data
5. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (http://ics-cert.us-cert.gov/): this center provides advanced technical support on cybersecurity of the industrial systems.

Figure 12.5: the main webpage of the OnGuardOnline (Source: www.onguardonline.gov/)

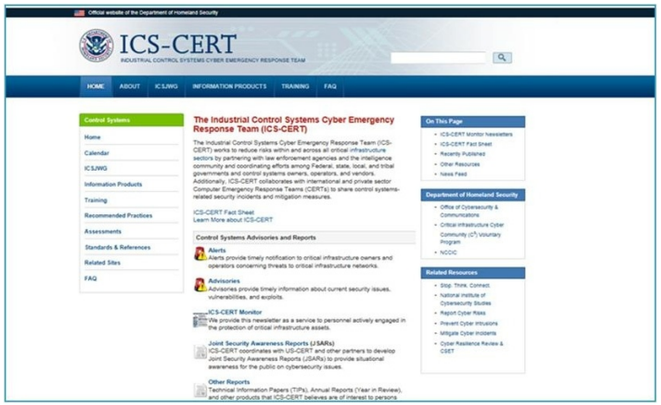


Figure 12.6: the main webpage of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (Source: http://ics-cert.us-cert.gov/)

6. The Defence Cyber Crime Center (DC3): figure 12.7 shows the main webpage (http://www.dtic.mil) this center has three labs

- Defence Computer Forensics Laboratory (DCFL): this lab responsibilities include investigation of cybercrimes and research and development.
- Defence Cyber Investigations Training Academy (DCITA): this academy provides advanced training in all aspects of cybersecurity
- Defence Cyber Crime Institute (DCCI): responsible to carry out advanced research and support the innovations.

Figure 12.7: the main webpage of the Defense Cyber Crime Center (DC3) (Source :www.dtic.mil)

Child Online Protection (COP)

The United States realize and recognize the importance of the child protections in the cyberspace from the early days. Thus, the government legislate may Laws in this regards:

- Children's Online Privacy Protection Act (1998): this act obligate websites to store child privacy data..[175]
- Children's Internet Protection Act(2000): this act obligate schools and public libraries to deploy technical security tools to control child navigation in the internet [176]
- Protecting Children in the 21st Century (2007): this act is complimentary to the 2000 child protection act which give further right to the educational institutes to control children in the cyberspace[178 ،177]

There are also many organizations that provide valuable material on the internet to increase the public awareness about risk online in the cyberspace; one of these important organizations is the National Center for missing and Exploited Children (http://www.missingkids.com/home) figure12.8, the main web page.

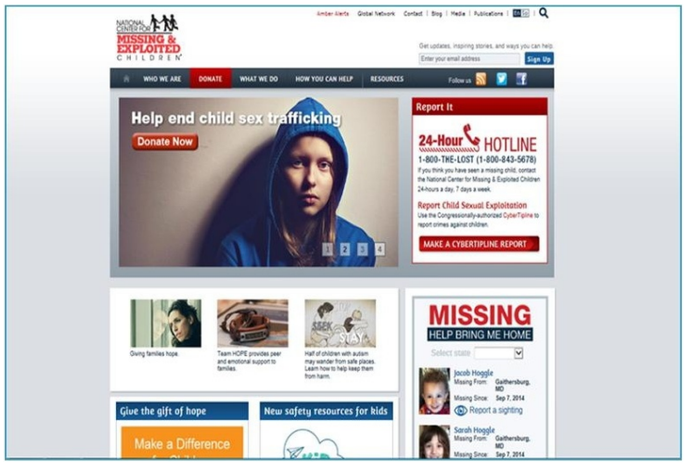


Figure 12.8 the main centre webpage of the National Center for missing and Exploited Children (Source: http://www.missingkids.com)

Laws and Legislations

Given the large influence of information and communications technology revolution to the daily life of people, from the early age of this great revolution US government realize and understand the importance of the regulation of this sector. Today, in the US, the most important Laws related to the information and communications sectors can be summarized as follows:

- Federal Advisory Committee Act (FACA) of 1972.[179] : this Law defines and regulates the information sharing between the government sectors.
- Computer Fraud and Abuse Act (CFAA) 1986:
- computer misuse act 1986 and modified in 1994 and 2007 respectively to accommodate new cybercrime [180].
- Executive Order 13010 to establish critical infrastructures protection [181].
- SA PATRIOT Act of 2001: this Law authorizes the FBI to investigate cybercrime, access private information if needed. Although there is a lot of problems associated with this Law, president Obama renew this Law in 2011 for 4 years .[183] [182]
- Executive Order 13228; EO 13228, 2001 to establish the department of Homeland Security s and Homeland Security council[184].
- Executive Order 13231 of October 16، 2001 to protect critical infrastructures based on information system.[185]
- Homeland Security Act 2002: this Law gives the right to the Homeland Security to access large amount of private data :
- Freedom of Information Act (FOIA): This Law exclude critical infrastructure operators form publishing [186].
- Terrorism Risk Insurance Act 2002 (modified and updated in 2005 and 2007 respectively) this Law identifying the amount of money can be paid back by the insurance company back to the user if there is an attack [187]
- Adam Walsh Child Protection and Safety Act 2007 [188].

Some Important web Resources

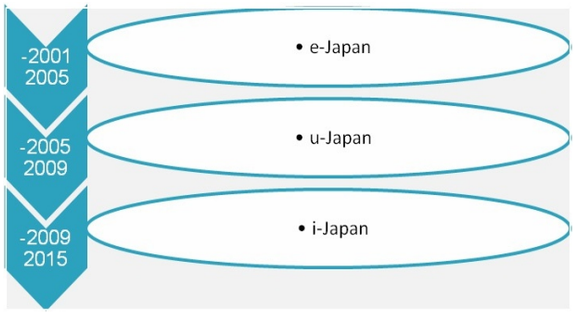
List 12.1: list of important web address related to the cyber security themes

Organization	Service Provided	Web address
Homeland Security	Coordinate the information and critical infrastructure protection	www.dhs.gov
US-cert	Provide advanced technical support	www.us-cert.gov
CERT Coordination Center	Coordinate the information and critical infrastructure protection	www.cert.org
onguardonline	Provide valuable guidance on information security	www.onguardonline.gov
Federal Bureau of Investigation (FBI)	Investigate cybercrime	www.fbi.gov
National Cyber Security Alliance	National Alliance on Cyber Security related themes	www.staysafeonline.org
Information Sharing and Analysis Centers (ISACs):	Act as information sharing points	www.isaccouncil.org

Chapter Thirteen
Japanese Experience

Current Status and Future Directions

Japan is the first county in the world that realized the force of the ICT for inducing national growth as indispensable for promoting economic growth and innovation, resolving social issues and for other purposes. Thus, it is one of the early countries in the world that plan for the concepts of Economic of knowledge and information community. In 2001, the Japanese government announce for the E-Japan Strategy which aim to develop upgrade the telecommunications network infrastructure [189]. By the end of the implementation of E-Japan Strategy, the government announces U-Japan Strategy, which aims to make use of information, and communications technology is all aspect of life[190] . in 2009 the government announce the i-Japan Strategy which aims to develop all e-government applications and make maximum use of the information and communications technology to develop the human resources, Healthcare system, and support the innovation[191]



Critical Sectors

In Japan, Critical Information Infrastructure (CII) is defined as the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted. If the function of the services is suspended, deteriorates, or becomes unavailable, it could have a significant impact on the national life and economic activities.

According to this definition, the Information Security Policy Council of Japan identifies the following sectors as CII[192][193]

- Information and communication services;
- Financial services
- Aviation services
- Railway services
- Electric power supply services
- Gas supply services
- Government and administrative services
- Medical services",
- Water services
- Logistics services
- Chemical industries",
- Credit card services"
- Petroleum industries

Past and Present Initiatives and Policies

Since 1998, to build what is called the information and communication community, the government of Japan introduces many initiatives, which can be summarized as follows:

Japan Cybersecurity Strategy

To realize safe cyberspace and to become world's most advanced IT nation, the information security policy council of Japan announced the cybersecurity strategy in order to make clear the necessity to widely promote measures related to cyberspace and approach of these measures as distinguished from efforts for assuring information security[194]

The Basic Policy of Critical Information Infrastructure Protection

The Information Security Policy Council announced the third edition of the Japanese Basic Policy of Critical Information Infrastructure Protection in 2014. This policy addresses the following points[193]:

- Maintenance and promotion of the safety principles
- Enhancement of information sharing system
- Enhancement of incident response capability
- Risk management
- Enhancement of the basis for CIIP

Information Security Human Resource Development Program

The Information Security Human Resource Development Program is developed in 2011 to examine the future direction of the human resource development policies for various information security issues described in the Information Security Strategy, Annual Plan, and HR Expert Committee Report[195]

Management Standards for Information Security Measures for the Central Government Computer Systems

The government of Japan announces standards for information security measures and compliance. Periodically, all government sectors evaluated and constructive advice will be provided according to the compliance to the government policies and regulations[196].

Technical Standards for Information Security Measures for the Central Government Computer Systems

The government of Japan announces the technical standards for information security measures and compliance. Periodically, all government sectors are technically evaluated and constructive advice will be provided according to the compliance by the government technical regulations[25]

International Strategy on Cybersecurity Cooperation J-initiative for Cybersecurity

This Strategy is based on the Japan Revitalization Strategy and the Cybersecurity Strategy, which were developed in June 2013, and summarizes the Japan's basic policy and its priority areas for global cooperation and mutual assistance in the field of cybersecurity [197]

Information Security Outreach and Awareness Program

Information Security Outreach and Awareness Program is developed to systematically organize outreach and awareness policies based on the Strategy and Annual Plan and execute more effectively under close collaboration of public and private sectors [198]

Organizational and institutional Overview

In 2005, the government of Japan set up two organizations under the cabinet secretariat to hold the responsibility of information security and critical infrastructure protection. These organizations are in charge of:

1. The Information Security Policy Council (ISPC) which is in charge of:
    - Developing and auditing the information security policies;
    - Evaluating the effectiveness of the information security systems;
    - Developing the information security, safety guidelines;
    - Recommending information security systems;
2. National Information Security Centre (NISC:[199] which is in charge of:
    - Planning and building strategies for government information systems;
    - Strengthen the security of the governmental systems;
    - Provide advanced technical support to the governmental organizations (at emergency);
    - Strengthen the security of all critical infrastructures;
    - Support the information-sharing (act as a focal point for information sharing);
    - Contribute to the development of the country's information security strategy and working with other organizations to build international relations;

Other important organizations are:

3. Ministry of Economy، Trade and Industry (METI): responsible to apply and monitor the cabinet policies related to the information security, e-commerce, e-government, and data protection. Also METI supports research and development and promote good information security policies to the private sectors
4. National Police Agency (NPA): within NPA, the High-Tech Crime Technology Division (HTCTD) or Cyber Forces is working to combat cyber crimes through the monitoring of the internet and telecommunications. In addition, the cyber-forces are also responsible to support the research and development, innovations, and collect data about the cybersecurity incidents, do the necessary analysis, and report the conclusions.
5. Ministry of Internal Affairs and Communications (MIC): This organization is responsible to develop the communications and information critical infrastructure.
6. Establishment of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR): this organization provides information sharing and analysis at CII operators, and organizations which serve as these functions
7. The establishment of CEPTOAR council: The council composed of representatives of each CEPTOAR, which carries out information sharing between CEPTOARs. This council is an independent body, not positioned under other agencies, including government organizations.
8. Japan Network Security Association (JNSA): This organization was established in 2000 to take the responsibility of the development of network security standards.

Early Warning and Public Outreach

In Japan, the following organizations are responsible to increase the public outreach and information security awareness:

- National Incident Response Team (NIRT): this team is established in 2002 under the cabinet secretariat to perform the following:
    - Understand the nature of cybercrime incident, collect important data, do some analysis, and forecast about the future.
    - Develop information security guidelines
    - Provide technical help on incident response.
    - Develop the knowledge capacity in this area.
- Japan Computer Emergency Response Team Coordination Center (JPCERT / CC) (http://www.jpcert.or.jp/english/) this center is established in 1992 to coordinate the information security task between all computer emergency response teams, telecommunication companies, technical solutions providers, and government sector. In addition, this center is responsible to coordinate internationally with other related centers.

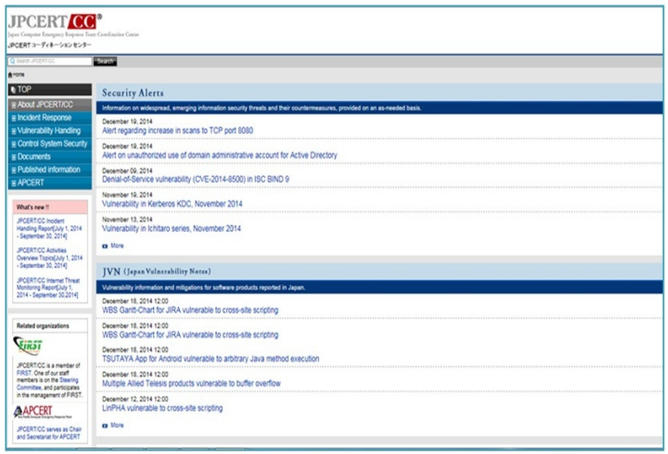


Figure 13.1: the main web page of the JPCERT / CC (Source: http://www.jpcert.or.jp/english/)

- Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/ APCERT): this team is established in 2003 to coordinate with computer emergency response teams in the pacific region.

Figure 13.2: the main website for the AP-CIRT / APCERT (Source: http://www.apcert.org/)

- Telecom Information Sharing and Analysis Center (www.telecom-isac.jp): this center is responsible to collect all the data related to cybercrime incidents, carry out the necessary analysis, and share out the important outcomes and results.
- Cyber Force: this team is working from the police department to monitor the internet and send early warning message to important sectors if there is any expected risk. Furthermore, this team also cries out some optional penetration test to identify the weakness and provide the necessary technical recommendations (http://www.npa.go.jp)

Figure13.3: Geographical locations of Japanese Cyber Force Bases (Source: http://www.npa.go.jp)

- @police website: @police is an Internet Security web Portal, whose purpose is to prevent high-tech crimes and cyber terrorism, and keep them from spreading, by quickly providing information gathered by the police on information security to Internet users, and increasing the public security awareness.

Child Online Protection (COP)

Japan is one of the first countries in the world that realize the importance of the child online protection. In 2009 it host the first strategic conference on this issue[200]. Generally, we can summarize the Japanese efforts on child online protection on the following

1. Act on Safe and Secure Internet Use Environment for the Youth (Act No. 79 of 2008)([201]
2. The implementation of E-net Caravan initiative (www.e-netcaravan.jp) figure13.4 : this initiative is led by the main telecommunication companies in Japan to lift up the awareness of the families, schools, educators about cybercrimes and the crime against child in the cyberspace
3. The implementation of the NTT docomo and Softbank Mobile initiative to provide special mobile with certain capabilities' to the to protect children in the cyberspace
4. Implementation of the Improving ICT Literacy at School program: the main objective of this program is to provide educational materials to the public to rise up the awareness of safe internet and child online protection
5. Establishment of the Mobile Content Evaluation and Monitoring Association (http://www.ema.or.jp/en/index.html): this group is working on child and family inline protection..[202]
6. Establishment of ROI (Internet-Rating Observation Institute) organization: POI is nongovernmental organization responsible to evaluate and classify the contents on the internet.
7. Establishment of Safer Internet of Japan group in 2009
8. Japan Internet Safety Promotion Association (JISPA)[203]

JISPA is a non-profit organization established on February 27, 2009 to link the various private-sector initiatives for the improvement of the Internet use environment. In this organization users, businesses, and educational institutions come together to carry out their activities on a larger scale and in a more effective manner. Within this organization there are five active research groups working in the following areas:

- Research & Study Working Group: this group intended to study internet's illegal and harmful information gives to youth. The group collects basic data and concludes out not only the positive side, but also possibility negative side effects brings.
  - Violence and bullying
  - Sexual behavior, sexual awareness
  - Suicide

- Dependent

- Anti-Child-Pornography working group: this research group intended to exchange and summarizes information about the international response against child pornography, and about the actual situation in Japan, and considers both legal and technical aspects of blocking and solving urgent problems.

- Community Site Working Group: this group is intended to search for a solution for the problems of youth in the use of the social game.

- Smartphone Working Group: This group is a collective of various stakeholders lead to measures to share the challenges in efforts to protect youth from the Smartphone.

- Social Game Working Group: This group search for solutions for the problems of young people in the use of the social game.

Figure 13.4: the main webpage of the E-net Caravan initiative (www.e-netcaravan.jp)

Laws and Legislations

- Unauthorized Computer Access Law -1999

- Act on Electronic Signatures and Certification Business (2000).

- The Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (Law No.144 of 2000): the purpose of this act is To promote measures for forming an advanced information and telecommunications network society expeditiously and intensively, in light of the urgency to adapt ourselves to the world's rapid and drastic changes in the socioeconomic structure caused by the utilization of information and telecommunications technology

- Act on Punishment of Activities Relating to Child Prostitution and Child Pornography، and the Protection of Children.[204] .

Some important web resources

Table 13.1: list of important web address for information and critical information infrastructures

Organization	Description	Web address
@police	Collect information related to cybercrime incident, doing research and development, and investigate cyber crimes	www.npa.go.jp
e-government management team	Inform the e-government related issues	www.e-gov.go.jp
National Information Security Policy Council	Development of information security policies	www.nisc.go.jp
Japan Computer emergency response team	Provide advanced technical support on information security and security incident handling	www.jpcert.or.jp
CERT for Asia pacific region	Provide advanced technical support on information security and security incident handling(for Asia pacific member countries)	www.apcert.org

Japanese Society for network security	Develop network security standards	www.jnsa.org/en/aboutus
Japanese Telecom – information sharing group	Support the information sharing between telecommunication, public and private sectors	www.telecom-isac.jp
Information sharing forum	Support the information sharing among information security experts	http://blog.jpcert.or.jp/

Chapter Fourteen
United Kingdom Experience

Current Status and Future Directions

UK is one of the most developed countries in the world in communications and information technology. To cope with fast development in the High-speed broadband communications, UK built and provides the main requirement of the telecommunications infrastructure to become a focal point for the most of the world submarine cables interconnecting the different parts of the world.

In 2009, the UK Department for Culture, Media and Sport and Department for Business Innovation and skills published an inclusive report (Digital Britain) which identify the basic needs to be done on information and communications technology sectors to meet the basic demands of the future Britain Plan/ vision [205]. The report describes the current state of the ICT and identifies the following points to be addressed with detailed timetable for future actions.

1. Modernizing and upgrading our wired, wireless and broadcasting infrastructure to sustain country position as a leading digital economy;
2. Providing a favorable climate for investment and innovation in digital content, applications and services;
3. Securing a range of high quality public service content, particularly in news;
4. Developing the nation's digital skills at all levels;
5. Securing universal access to broadband, increasing its take-up and using broadband to deliver more public services more effectively and more efficiently;

Digital Britain is an important document in such way that it give detailed point on how to achieve the future Britain vision [205]. In 2009, nationwide detailed plan to implement digital Britain developed with specific tables and time lines ended in 2015.

Critical Sectors

The UK‟ s national infrastructure is defined by the Government as: “those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends”. Based on this definition, the following sectors are defined as critical infrastructure.[207 ،206]:

- Communications Sectors;
- Emergency Services Sectors;
- Energy (Electricity، Natural Gas، Petroleum);
- Finance (Asset Management، Financial Facilities، Investment Banking، Markets، Retail Banking);
- Food (Produce، Import، Process، Distribute، Retail);
- Government and Public Services;
- Health (Health Care، Public Health);
- Transport (Air، Marine، Rail، Road);
- Water (Mains Water، Sewerage);

Past and Present Initiatives and Policies

For the protection of the critical infrastructure, the UK government distinguishes between two types of attacks: the physical attacks and the cyber-attacks, thus it develops. The main initiatives developed by the UK government are:

- National cybersecurity strategy (2003) this strategy was supported by the government cabinet. The main point in this strategy is to establish a central body for information security known as Central Sponsor for Information Assurance (CSIA) to accomplish the following:
  - Support the government to provide the public services through electronic windows
  - Support the national security of the UK by strengthen cybersecurity
  - Develop the economic by enabling the public to use the ICT tools
- Government Data Security initiative (2007): this initiative hand considered as an update to the National cybersecurity strategy.

Organizational and Institutional Overview

In UK, the responsibility of the protection of the critical infrastructure is assigned to the department of Homeland security with the helping of the following organizations

- The Centre for the Protection of National Infrastructure (CPNI): this centre is established in 2007 to protect critical infrastructure nationwide from tersest cyber-attacks (Figure 14.1 show the main web page of this centre). This centre is also support research and development, innovations and information sharing between cybersecurity research centers across UK and all over the world [206]:.

These organizations are strictly following up the recommendations of the centre.

- Cabinet office;
- Local government and public service gates;
- Department of commerce ;
- Department for Environment، Food and Rural Affairs;
- Department for Transport;
- Department of Health;
- Food Standards Agency;
- Finance;
- Emergency Services;
- Maritime and Coastguard Agency;
- The police;

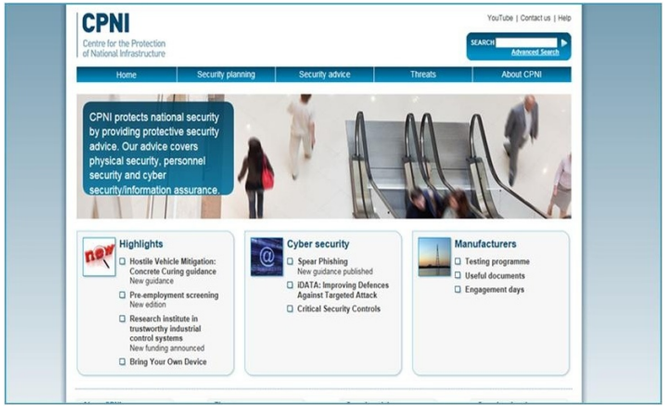


Figure 14.1: the main web page the Centre for the Protection of National Infrastructure (CPNI)-(source: www.cpni.gov.uk)

- Civil Contingencies Secretariat (CCS): the main purpose of this office is to support the government in the cybersecurity incident time and to provide advanced technical support on planning for risk management
- In addition, there are many private and nongovernmental organizations that share the responsibility and the information for cybersecurity with the government organization. Example of these organizations:
  - The Information Assurance Advisory Council;
  - British Computer Society;
  - National Computing Centre;
  - Internet Watch Foundation
  - Confederation of British Industry (CBI) (www.cbi.org.uk);
  - Institute of Information Security Professionals (IISP): (http://www.iisp.org);
  - European Information Society Group (EURIM) (http://www.eurim.org.uk/)(also Called The Information Society Alliance). This group is working closely with legislators and industrial partners to support the following information security directions:
    - Confidentiality
    - Information Protection
    - Monitoring
    - Awareness networks and skills
    - Securing the E-commerce
    - Identifies the points of weakness
    - Legal obligation

Early Warning and Public Outreach

In UK, the following organizations are responsible to increase the public outreach and information security awareness:

- Combined Security Incident Response Team (CSIRTUK): this group is responsible to help the private sectors in information security, risk management, and to provide advanced technical supports to enable these sectors to respond to cyber-attacks [208].
- GovCertUK (http://www.cesg.gov.uk) this group is responsible to help the government sectors in information security, risk management, and to provide advanced technical supports to enable these sectors to respond to cyber-attacks
- Ministry of Defense Computer Emergency Response Team (MODCERT): this team has distributed workplace around the country provides advanced technical help when it's needed and encourages the information sharing between the different sectors. Also, this team is responsible to coordinate the efforts of CSIRTUK and GovCertUK

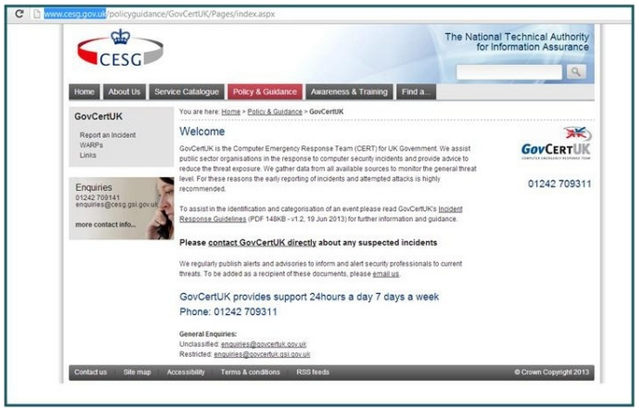


Figure 14.2: the main website of the Combined Security Incident Response Team (http://www.cesg.gov.uk)

- GetSafeOnline: as shown in figure 14.3, provide advanced technical knowledge on information security and safe use of the internet.

Figure 14.3: the main webpage of the GetSafeOnline (Source: https://www.getsafeonline.org/).

Child Online Protection (COP)

In 2006, UK government established the Child Exploitation and Online Protection Centre (CEOP) to respond to the critical online crimes against children. This center works in collaboration with other national and international organizations and high-level expert groups to combat cybercrime. Figure 14.4 shows the main web page that citizens can report an illegal web contents to the center to take further action

This center also supports the educational program known as ThinkUKnow (figure 14.5, the main webpage), which help and educate children of different ages to use the internet safely and how to deal with violent behavior and aggressions.

Figure 14.4: the main web page of the Child Exploitation and Online Protection Centre (CEOP)

Figure 14.5: the main webpage of the ThinkUKnow program (Source: http://www.thinkuknow.co.uk/)

There is another active group known as BeatBulling (figure 14.6). This group provides construction advice to educators, families, and children on how to deal with Bulling online.

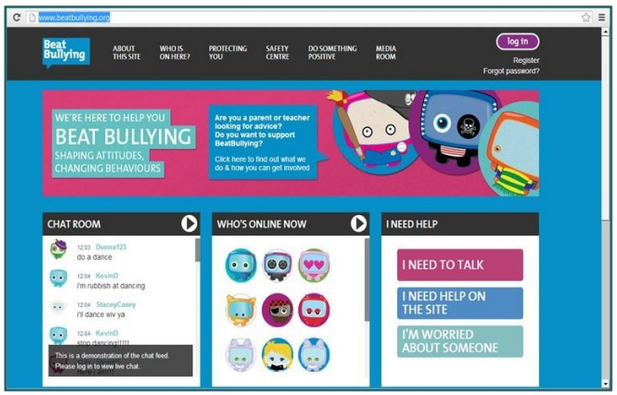


Figure 6.14: the main webpage of Bear Bullying group (Source: http://www.beatbullying.org/)

Laws and Legislations

Since the starting of the communication and information technology age, UK puts many Laws into practice to protect individual rights and state critical infrastructure. Examples of these lows are:

- Telecommunications (Fraud) Act 1997:
- Data Protection Act 1998:
- Electronic Communications Bill 2000:.[209] :
- Terrorism Act 2000:
- Police and Justice Act 2006:[210]
- 1996, Child Pornography Prevention Act.[211] :
- 2003, Sexual Offences Act.[212] :
- 2004,Children Act.

Some important web resources

Table 11.2: list of important web address for information and critical information infrastructures protections in the UK

Organization	Mission/Objective	Web address
Centre for the Protection of National Infrastructure	Critical infrastructure Protection	www.cpni.gov.uk/about/cni/
Combined Security Incident Reponse Team	Providing advanced technical supports	www.cesg.gov.uk
British Computer Society;	Training and HR development organization	www.bcs.org
National Computing Centre	Training and HR development organization	www.ncc.co.uk/
Internet Watch Foundation	Monitoring the internet	www.iwf.org.uk
Confederation of British Industry	Provide Technical support	www.cbi.org.uk
Institute of Information Security Professionals	Training and HR development organization	www.iisp.org
GetSafeOnline	Cyberspace protection organization	www.getsafeonline.org
saferinternet	EU group for cyber space protection	www.saferinternet.org
Child Exploitation and Online Protection Centre	Child protraction centre	ceop.police.uk
ThinkUKnow	Child online protection	www.thinkuknow.co.uk

Chapter Fifteen
European Union Experience

European Union national Plan

The European Union (EU) is one of the key international influential groups in the world today in terms of efforts and contributions in the field of research and development of communications systems and information Technology. In 2010, the EU announced the Digital Agenda for Europe for 2020, which aims to develop the following sectors:

- Create a new and stable broadband regulatory environment.
- New public digital service infrastructures through Connecting Europe Facility loans
- Launch Grand Coalition on Digital Skills and Jobs
- Propose EU cyber-security strategy and Directive
- Update EU's Copyright Framework
- Accelerate cloud computing through public sector buying power
- Launch new electronics industrial strategy

To achieve all these goals on time, The EU develops the breakdown plan which include the following

- The entire EU should be covered by broadband network by 2013.
- The entire EU to be covered by broadband above 30 Mbps by 2020
- Connect more than 50 % of the EU to subscribe to broadband above100 Mbps by 2020
- Have more than 50 % of the population to buy online by 2015
- Have more than 20 % of the population to buy online cross-border by 2015
- Have more than 33 % of SMEs to make online sales/purchases by 2015
- The difference between roaming and national tariffs to approach zero by 2015
- To increase regular internet usage from 60 % to 75 % by 2015, and from 41 % to 60 % among disadvantaged people.
- To halve the proportion of the population that has never used the internet from 30 % to 15 % by 2015
- Have more than 50 % of citizens to use e-Government by 2015, with more than half returning completed forms
- All key cross-border public services, to be agreed by Member States in 2011, to be available online by 2015
- To double the public investment in ICT R&D to € 11 bn by 2020
- To reduce energy used for lighting by 20% by 2020

Identified Critical Sectors

The protection of critical infrastructure, large IT facilities, and communication system of important topics that run the European research centers for a long period. The definition of critical infrastructure by the central administration of the Union as these physical assets and information systems and networks which, if damaged or stopped working for a short time, can make a devastating impact on health or public security or the economy of a Member State. Based on this definition has been the adoption of the following institutions as critical infrastructures

- Information and Communication Technologies (ICT)
- Water
- Food
- Health
- Financial System
- Civil Administration
- Transportation
- Chemical and Nuclear Industry
- Space Research

Initiatives and Policies

In EU, there is a common understanding on the importance of the information and communications systems and the critical infrastructure connected and depends on to these systems. Thus, from the early time the EU starts many initiatives and carryout

many researchers in this field to protect the assets. Some of these initiatives summarized as follows:

1. Green Paper on a European Program for CIP (EPCIP)[213] : this paper consecration on the following issues:
   - Defines the objective of information security
   - Set up the main principles
   - Develop the main framework
   - Defines the critical infrastructures
   - Defines the scope of the work at the national EU national levels
   - Define the responsibilities of the owner and the operator of the critical infrastructure
   - Identifying the role of the audit and evaluation operations on the safety of the critical infrastructure
2. Establishing the Critical Infrastructure Warning Information Network (CIWIN) (https://ciwin.europa.eu): this organizations is responsible to support and facilitate the information share on incident between the EU countries [214].
3. Establishing the European Network and Information Security Agency (ENISA): this agency provides advanced technical supports and training services to the computer emergency response teams of the member countries across Europe, Furthermore, also this agency support research and innovations and provide advanced technical support to the Industrial Control systems(SCADA)[215].
4. Establishing the Information Society Technologies (IST) FP6 and FP7, to support the research, development, and innovations
5. European Security Research Program (ESRP): the purpose of this program is to encourage research and development in information security.
6. Establishing the Critical Information Infrastructure Research Co-ordination (CI2RCO): the objective of this program is to coordinate and collectively support the research efforts across the EU member states
7. Establishing the EU Computer Emergency Response Team: this team works closely with all EU member states computer emergency response teams to coordinate the response and to reduce the negative effect of the cybercrime attacks, Figure 15.1: illustrates the main web page of the EU Computer Emergency Response Team
8. Establishing the European Cybercrime Centre (EC3) at Europol: The Centre working as a focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. Also this centre support member states and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with other international partners

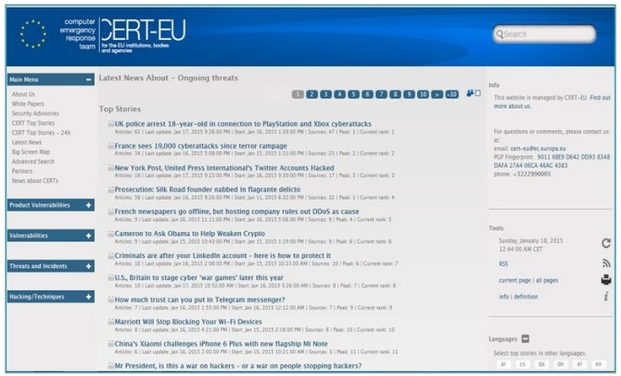


Figure 15.1: illustrates the main web page of the EU Computer Emergency Response Team

Child Online Protection (COP)

To protect children the cyberspace the European Union develop many initiatives to elevate the public awareness of the child protect in the internet[216].. The main objective of these initiatives is to inform and educate families, children, Educators, ICT industries, and legislators in the member countries about the potential risks in the cyberspace. In general, we can summarize the details of these initiatives in the following points:

1. Identify the potential risks in the cyber space.
2. Increase the public awareness on child online protection.

3. Develop tools to reduce the risks.
4. Support the information sharing between the member countries on child protection in the cyber space

To support the information sharing process between the member countries, EU builds main web page (figure 15.2, www.saferinternet.org) that enable everyone to navigate through it to the safe internet web page of the specific EU country

Figure 15.2: the main web page of the safer internet organization (Source: www.saferinternet.org)

The other more important initiatives include

1. Risktaking online behavior, empowerment through research and Training (ROBERT): This project intends to make online interaction safe for children and young people. This will be attained through learning from experiences of online abuse processes and factors that make young people vulnerable as well as those that offer protection. Perpetrators' strategies in relation to grooming of children online will also be explored along with developing an understanding of how abuse may develop in the online environment. Children and young people will be empowered in order for them to better protect themselves online.
2. The European NGO Alliance for Child Safety Online (eNACSO): based on the 1989 Convention on the Rights of the Child, the eNACSO initiative networked 27 children's rights NGOs from across the EU to work together to create a safer cyberspace environment for children. They aim to promote and support actions at national, European, and international level aimed at protecting children and promoting their rights in relation to the cyberspace new technologies.
3. EU Kids Online: EU Kids Online is a multinational research network seeks to enhance knowledge of European children's online opportunities, risks and safety. It uses multiple methods to map children's and parents' experience of the cyberspace, in dialogue with national and European policy stakeholders.
4. INHOPE: is an active and collaborative network of 51 hotlines in 45 countries worldwide Co- Co-funded by the European Union to deal with illegal content online. This network offers the public a way of anonymously reporting Internet material, including child sexual abuse material they suspect to be illegal. The Hotline ensure that the matter is investigated and if found to be illegal the information will be passed to the relevant Law Enforcement Agency and in many cases the ISP hosting the content
5. Youth Protection Roundtable Project[217]: this project is aimed to encourage a collaborative and cross-sector dialogue focusing on the optimal mix of effective technology-enhanced strategies on the one hand and education-based strategies on the other hand to enable youths - and responsible adults in the case of minors - for a safe and secure use of the Internet.

Laws and Legislations

Since its early time, the EU has developed many laws and regulating instruction to protect information systems and critical communications and other infrastructures. The most important ant notable Laws and legislations are:

- The Data Protection Directive (Act 1995): This Law concern the privacy when dealing with private information in the EU institutes. Recently another updated version of this Law with the name General Data Protection Regulation (GDPR) has been developed in 2012 with additional

chapters on social networking and cloud computing. This new law is expected to be practiced in 2014 [220-218].

- Directive on Electronic Signature[221](1999): this Law defines of aspects of using electronic signature in to and between EU countries .[222]
- Directive on Privacy Protection in the Electronic Communications Sectors2002: The objective of this Law is to protect the privacy when using the telecommunication system inside EU member countries. this Law is recently updated in 2009 [224 ،223].
- Treaty of Lisbon 2007: This treaty defines the principle and norms to build the EU community [225]
- The Directive on Data Retention 2006: this Law document obligate the telecommunications companies and service provider to store important data for some times to be used for investigation [227 ،226]
- Council Framework Decision on Attacks Against Information Systems 2005: this document defines the framework for legal coordinate between member countries on cyber security issues [228].
- Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography 2003: this framework defines the range of penalties for all crimes connected to child [229].
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse(2007).[230]
- Council Decision to Combat Child Pornography on the Internet(2000): this Law forbid the holding, and distribution of illegal contents in the or through the internet or any technical means [231].
- Convention on Cybercrime (2001)[232]

Some important web resources

Table 13.1: list of important web address for information and critical information infrastructures Protection in EU.

Organization	Objective/ mission	Web address
CIWIN	Information sharing between EU member states	www.ciwin.europa.eu/Pages
ENISA-EU	Provide advanced technical support on protection and cyber incident handling	www.enisa.europa.eu
CERT-EU	Coordinate between EU CERT teams	www.cert.europa.eu
Safer internet	Provide valuable materials on internet safety	www.saferinternet.org
Teach today	Train educators on child protection in the cyberspace	www.teachtoday.eu

References

[1] D. G. Messerschmitt and E. A. Lee, *Digital Communication*, 1 ed.: Kluwer Academic Publishing, 1988.

[2] E. A. Lee and D. G. Messerschmitt, *Digital Communications*, Second ed. Boston: Kluwer, 1994.

[3] A. J. Whitaker. Bell Telephone Memorial and Bell Homestead .

[4] J. M., *Optical Fiber Communications*. London: Printiace Hall International, 1985.

[5] D. Forney. (2005, 18 Aug, 2013). *6.451 Principles of Digital Communication II*. Available: http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-451-principles-of-digital-communication-ii-spring-2005

[6] optics. (2013, 18 Aug). *NEC and Corning achieve petabit optical transmission*. Available: http://optics.org/news/4/1/29

[7] c. shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal,*, vol. 27, pp. 379–423, July 1948.

[8] A. Goldsmith, *Wireless Communications*: Cambarge University Press, 2005.

[9] Rappaport, *Wireless Communications: Principles and Practice*: Dorling Kindersley, 2009.

[10] I. F. Akyildiz, D. M. Gutierrez-Estevez, and E. C. Reyes, "The evolution to 4G cellular systems: LTE-Advanced," *Physical Communication,* pp. 217-244, 2010.

[11] I. F. Akyildiz, D. M. Gutierrez-Estevez, and E. C. Reyes, "The evolution to 4G cellular systems: LTE-Advanced," *Physical Communication* vol. 3, pp. 217-244, 2010.

[12] Per Beming, L. Frid, G. Hall, P. Malm, T. Noren, M. Olsson, and G. Rune, "LTE-SAE architecture and performance," *Ericsson 98 Review,* vol. 3, pp. 98-104, 2007.

[13] Q. Li, G. Li, W. Lee, M.-i. Lee, D. Mazzarese, B .Clerckx, and Z. Li, "MIMO Techniques in WiMAX and LTE: A Feature Overview," *IEEE Communications Magazine,* vol. 48, pp. 86-92, 06 May 2010.

[14] A. C. Clarke. (Oct). *Extra-terrestrial relays*. Available: http://lakdiva.org/clarke/1945ww/1945ww_oct_305-308.html

[15] A. C. Clarke, "Extra-terrestrial relays," *Wireless World,* pp. 305-308, October 1945.

[16] arabsat. (Oct). *Arab satellite communications organization*. Available: http://www.arabsat.com/pages/Default.aspx

[17] D. Doddy, *Satellite Communications*, 3 ed.: McCrow-Hill, 2001.

[18] E. Saeid, "Precoder Design Based On inter-antenna Leakage Minimization for MU-MIMO," PhD, Electrical and Electronic Engineering, Universiti Technology Petronas, Tronoh, Malaysia, 2013.

[19] SANS_Institute. (2002, Requirements for the Design of a Secure Data Center. Available: http://www.sans.org/reading-room/whitepapers/recovery/requirements-design-secure-data-center-561

[20] V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Communications,* pp. 3-11, Feb 2005.

[21] L. Kleinrock, "Message Delay In Communication Nets With Storage," PhD, Electrical Engineering, MIT, 1962.

[22] G. Putic. (2013, Sept). *Stuxnet: An Effective Cyberwar Weapon*. Available: http://www.voanews.com/content/stuxnet-an-effective-cyberwar-weapon/1691311.html

[23] R. McMillan. (2010, Sept). *Siemens: Stuxnet worm hit industrial systems*. Available: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

[24] K. Hart. (2008, Aug). *Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar*. Available: http://msl1.mit.edu/furdlog/docs/washpost/2008-08-14_washpost_russia_georgia_cyberwar.pdf

[25] C. S. I. Operations. (2005, Aug). *Zotob Worm Information*. Available: http://www.cisco.com/web/about/security/intelligence/zotob-worm.html

[26] K. Poulsen. (2003, Aug). *Slammer worm crashed Ohio nuke plant network*. Available: http://www.securityfocus.com/news/6767

[27] c. w. t. s. s. b. For Sony Pictures CEO. (2015, 31 Jan). *For Sony Pictures CEO, cyberattack won't set studio back*. Available: http://www.reuters.com/article/2015/01/09/us-northkorea-cyberattack-sony-idUSKBN0KI02420150109

[28] W. Cummings. (2015, Jan). *Cyber Caliphate hacks Malaysia Airlines website*. Available: http://www.usatoday.com/story/tech/2015/01/25/malaysia-airlines-hack/22332867/

[29] D. Verton. (2003, Sept). *Software failure cited in August blackout investigation*. Available: http://www.computerworld.com/s/article/87400/Software_failure_cited_in_August_blackout_investigation

[30] D. castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," ed: The information technology & innovation foundation, 2013.

[31] US_Government, "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," D. o. n. intelligence, Ed., ed. Washington DC: Director of national intelligence, 2013.

[32] E. Messmer. (2013, Nov). *Don't trust the NSA? China-based Huawei says, 'Trust us*. Available: http://www.computerworld.com/s/article/9243335/Don_t_trust_the_NSA_China_based_Huawei_says_Trust_us_

[33] J. Snyder. (2013, Nov). *The Huawei security risk: Factors to consider before buying Chinese IT*. Available: http://searchsecurity.techtarget.com/feature/The-Huawei-security-risk-Factors-to-consider-before-buying-Chinese-IT

[34] B. Carlson. (2012, Nov). *Why is US Congress afraid of Chinese telecommunications giant Huawei*. Available: http://www.globalpost.com/dispatch/news/regions/asia-pacific/china/121009/huawei-ZTE-investigation-US-congress

[35] E. Zmijewski. (2008, Aug). *Mediterranean Cable Break*. Available: http://www.renesys.com/2008/01/mediterranean-cable-break/

[36] M. S. Media. (2008). *Mid East Communication Cables Cut, Companies Lose, Win Internet Providers*. Available: http://www.mathaba.net/news/?x=581059
[37] R. Drake. (2008, Aug). *The Submarine Cables – A Complete Guide to the 2008 Internet Outage*. Available: http://randomdrake.com/2008/02/12/the-submarine-cables-a-complete-guide-to-the-2008-internet-outage/
[38] R. S. a. c. Christof Gerlach, "Economic Impact of Submarine Cable Disruptions," APEC Policy Support Unit, Bangkok, Thailand2012.
[39] J. Oates. (2008, Aug). *Submarine cable cut torpedoes Middle East access*. Available: http://www.theregister.co.uk/2008/01/30/india_mideast_lose_internet/
[40] S. J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law,* vol. 27, pp. 1-60, 2009.
[41] J. Davis. (2007, Aug). *Hackers Take Down the Most Wired Country in Europe*. Available: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
[42] S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Stephen Herzog,* vol. 4, pp. 49-60, 2011.
[43] M. W. C. Ashmore, "Impact of Alleged Russian Cyber Attacks," S. o. A. M. Studies, Ed., ed. Kansas: U.S. Army 2009.
[44] H. o. l. E. U. Committee, "Protecting Europe against large-scale cyber-attacks," London2009.
[45] E. Tikk, K. Kaska, and L. Vihul, "International cyber incidents: legal considerations," Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn Estonia2010.
[46] S. Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense," *The yale journal of international law,* vol. 38, pp. 179-215, 2013.
[47] H. lobel, "The Law of War Implications of the Private Sector's Role in Cyber Conflict," *Texas international law journal,* vol. 47, pp. 618-640, 2012.
[48] M. C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Low Studies,* vol. 89, pp. 109-122, 2013.
[49] M. C. Waxman, "Comperhensive Ligal Approch for Cyber Security," PhD, Low, University of Tartu, 2011.
[50] B. Guttman and E. A .Roback, *An Introduction to Computer Security: The NIST Handbook*: NIST, 1995.
[51] J. Kimmins, C. Dinkel, and D. Walters, "Telecommunications Security Guidelines for Telecommunications Management Network NIST Special Publication 800-13," U. S. D. O. Commerce, Ed., ed. Gaithersburg,: U.S. DEPARTMENT OF Commerce, 1995.
[52] G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*. Gaithersburg: U.S. DEPARTMENT OF COMMERCE, 2002.
[53] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency Planning Guide for Federal Information Systems," NIST Special Publication 800-34 Rev. 1May 2010.
[54] N.-J. t. force, *Guide for Applying the Risk Management Framework to Federal Information Systems*: U.S. Department of Commerce, 2010.
[55] NIST, *Recommended Security Controls for Federal Information Systems and Organizations* U.S. Department of Commerce 2009.
[56] NIST, *Managing Information Security Risk Organization, Mission, and Information System View*: U.S. Department of Commerce 2011.
[57] S. Carlos M. Gutierrez. (2007, Guide to Industrial Control Systems Security, Second Public Draft, NIST Special Publication. Available: http://industryconsulting.org/pdfFiles/NIST%20Draft-SP800-82.pdf
[58] M. Scholl, K .Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg. (2008, 2013). An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule *NIST Special Publication 800-66*. Available : http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
[59] Industrial_Automation_Open_Networking_Association. (2006). *IAONA Handbook Network Security*. Available: http://www.vpi-initiative.com/download/IAONA-Security-Guide-15-draft.pdf
[60] US_Government. (2013, Aug). *Version 5 Critical Infrastructure Protection Reliability Standards*. Available: http://www.ferc.gov/whats-new/comm-meet/2013/041813/E-7.pdf
[61] US_Government. (Aug). *Cooperative Association for Internet Data Analysis*. Available: http://www.caida.org/home/
[62] I. S. I. D. British Columbia Institute of Technology. (Aug). *Industrial Security Incident Database*. Available: http://www.securityincidents.net/index.php/About/
[63] C. Rajmohan, G. Subramanya, and N. Sharma (2012) .Telecommunication Networks: Security Management. *White Paper* .
[64] X. R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social Engineering: The Neglected Human Factor for Information Security Management," *Information Resources Management Journal,* vol. 1 ‹8Sept 2011.
[65] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems,* pp. 106-125, 2009.
[66] T. w. Bank, "World Bank Group Strategy for Information and Communication Technology," ed: World Bank Group 2012.
[67] N. Mayer, P. Heymans, and R. Matulevičius. (Aug). *Design of a Modelling Language for Information System Security Risk Management* Available: http://www.nmayer.eu/publis/RCIS07-CR_NMA-PHE-RMA.pdf
[68] D. Hucaby, D. Garneau, and A. Sequeira, *CCNP Security firewall 642-618 Official Cert Guide*. Indianapolis: Cisco Press, 2012.
[69] K. S. P. Mell, "Guide to Intrusion Detection and Prevention Systems," vol. NIST Special Publication 800 ‹94-U. S. D. o. Commerce, Ed., ed: National Institute of Standards and Technology, 2007.
[70] R. U. Rehman, *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID* Prentice Hall, 2001.
[71] P. Weaver. (Aug). *SNORT IDS for SCADA Systems*. Available: http://www.snort.org/assets/114/Snort_RH5_SCADA.pdf
[72] O. I. S. Foundation. (2010, 2013). *Suricata (software)*. Available: http://www.openinfosecfoundation.org/index.php/download-suricata

[73] V. Jyothsna, V. V. R. Prasad, and K. M. Prasad, "A Review of Anomaly based Intrusion Detection Systems," *International Journal of Computer Applications,* vol. 28, pp. 26-35, Aug 2011.
[74] M. Uddin, K. Khowaja, and A. A. Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents " *International Journal of Network Security & Its Applications,* vol. 2, pp. 129-141, Oct 2010.
[75] F. F. I. E. Council. (Aug). *Authentication in an Internet Banking Environment*. Available: http://www.ffiec.gov/pdf/authentication_guidance.pdf
[76] S. McGee, R. V. Sabett, and A. Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law,* vol. 8, 2013.
[77] H. Burch and B. Cheswick" ‹Tracing Anonymous Packets to Their Approximate Source," in *Proceedings of the 14th Systems Administration Conference*, New Orleans, Louisiana, 2000.
[78] Jeffrey Hunker, Bob Hutchinson, and J. Margulies. (2008, Jan). Role and Challenges for Sufficient Cyber-Attack Attribution .
[79] D. A. Wheeler, "Techniques for Cyber Attack Attribution," I. f. d. analyses, Ed., ed. Alexandria, Virginia: IDA, 2003.
[80] E. Casey, *Handbook of Digital Forensics and Investigation*: Elsevier Academic Press, 2010.
[81] A. M .Marshall, *Digital Forensics Digital Evidence in Criminal Investigation*: JohnWiley & Sons, Ltd, 2008.
[82] NIST, " Computer Forensics Tool Testing Project Handbook," U. D. o. Comerce, Ed., ed: US . Department of Comerce, 2012.
[83] J. Ashcroft, D. J. Daniels, and S. V. Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," U. S. D. o. Justice, Ed., ed: U.S. Department of Justice, 2001.
[84] M. Damianides, "Sarbanes–Oxley and it Governance: New Guidance on it Control and Compliance," *Information systems Management,* pp. 77-85, 2005.
[85] R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799 " *The Info rmation Management Journal* pp. 60-66, Aug 2005.
[86] J. N. Ezingeard, McFadzean, E., & Birchall ‹D, "A model of information assurance benefits," *EDPACS,* pp. 1-16, 2005.
[87] SAINT. (20 Aug). *SAINT is a Vulnerability Assessment Tool*. Available: http://www.saintcorporation.com/
[88] OpenVAS. (20 Aug). *Open Vulnerability Assessment System (OpenVAS)*. Available: http://www.openvas.org/
[89] Metasploit. (20 Aug). *Metasploit Project*. Available: http://www.metasploit.com/
[90] Pentoo. (20 Aug). *Pentoo Penetration Testing tool*. Available: http://www.pentoo.ch/
[91] Blackbox. (20 Aug). *BackBox Penetration Testing tool*. Available: http://www.backbox.org/
[92] VMware. (20 Aug). *IT Health Check (ITHC)*. Available: http://www.vmware.com/company/acquisitions/ithc.html
[93] Burp. (Aug). *Burp Proxy*. Available: http://portswigger.net/burp/proxy.html
[94] T. N. Security. *Nessus Vulnerability Scanner*. Available: http://www.tenable.com/products/nessus
[95] OllyDbg. *OllyDbg Pen-test*. Available: http://www.ollydbg.de/
[96] Nmap. (Aug). *Nmap Pen-Test*. Available: http://nmap.org/
[97] ISACA. (20 Aug). *Control Objectives for Information and Related Technology*. Available: http://www.isaca.org/COBIT/Pages/default.aspx
[98] S. Direct. (20 Aug). *ISO 27002 - The Information Security Standard*. Available: WWW.STANDARDSDIRECT.ORG
[99] M. J. Kenning, "Security management standard — ISO 17799/BS 7799," *BT Technol J,* vol. 19, pp. 132-136, 2001.
[100] NIST. *Federal Information Security Management Act of 2002*. Available: http://csrc.nist.gov/groups/SMA/fisma/index.html
[101] NIST. *NIST-SP800*. Available: http://csrc.nist.gov/publications/PubsSPs.html
[102] K. N. Hampton, L. Sessions!Goulet, L. Rainie, and K. Purcell, "Social networking sites and our lives," Pew Internet ProjectJune 16 2011.
[103] C. O. Rodriguez. (2012, 19 Aug). *MOOCs and the AI-Stanford like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses* .
[104] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in *Thirteenth Americas Conference on Information Systems*, 2007.
[105] M. Pagani, C. F. Hofacker, and R. E. Goldsmith, "The Influence of Personality on Active and Passive Use of Social Networking Sites," *Psychology & Marketing,* p. 441456, May 2011.
[106] N. Hines. (2015). *Keyboard Warriors: British Army Joins the Twitter Wars*. Available: http://www.thedailybeast.com/articles/2015/01/31/keyboard-warriors-uk-army-to-set-up-social-media-unit.html
[107] S. Kolowich. (2013, 19 Aug). *How EdX Plans to Earn, and Share, Revenue From Its Free Online Courses*. Available: http://chronicle.com/article/How-EdX-Plans-to-Earn-and/137433/
[108] D. Koller. (2012). *What we're learning from online education*. Available: http://www.ted.com/talks/daphne_koller_what_we_re_learning_from_online_education.html
[109] S. N. s. G. a. B .I. o. Kids. (2011, 19 Aug). *Social Networking's Good and Bad Impacts on Kids*. Available: http://www.apa.org/news/press/releases/2011/08/social-kids.aspx
[110] B. Dinerman, "Social networking and security risks," *GFI White Paper,* 2011.
[111] S. Browser Media, MacWorld. (2012, 19 Aug). *Social Networking Statistics*. Available: http://www.statisticbrain.com/social-networking-statistics/
[112] G. N. Wise. (Aug). *Keeping children safe on the Internet is everyone's job*. Available: http://kids.getnetwise.org/safetyguide/
[113] ITU. (2012, Aug). *Establishment of Harmonized Policies for the ICT Market in the ACP Countries*. Available: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf
[114] ITU. (2012, Aug). *Support for harmonization of the ICT Policies in Sub-Saharan Africa*. Available: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/hipssa/Pages/default.aspx
[115] ITU. (2009, Aug). *Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)*.

Available: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx
[116] ITU. (Aug). *Capacity Building*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/cap-build.html
[117] ITU. (Aug). *Organizational Structures*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/org-struc.html
[118] ITU. (2009, Aug). *Technical and Procedural Measures*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/tech-proced.html
[119] I. T. Union, "The ITU National Cybersecurity strategy guide," ed, 2011.
[120] ITU-IMPACT, "ITU-IMPACT Service Catalogue ", I. T. Union, Ed., ed, 2011-2012.
[121] ITU-IMPACT. (2011, Aug). *ITU-IMPACT Partnership Prospectus (ALERT) Applied Learning for Emergency Response Team*. Available: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/ALERT.pdf
[122] ITU. (2009, Aug). *Cybersecurity Guide for Developing Countries*. Available: http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
[123] ITU. (2012, Aug). *Understanding cybercrime: Phenomena, challenges and legal response* Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[124] UNODC/ITU. (Aug). *ITU/UNODC Cybercrime:The global challenge* . Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf
[125] ITU. (2009, Aug). *ITU National Cybersecurity/CIIP Self-Assessment Tool*. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf
[126] I. T .Union. (2010, Child Online Protection. Available: http://www.ictliteracy.info/rf.pdf/COP-Child_Online_Protection.pdf
[127] I. FIRST.org. (1995, 30). *FIRST is the global Forum for Incident Response and Security Teams*. Available: https://www.first.org/
[128] MICT, "National Information Assurance Policy v2," Q. ICT, Ed., ed. Qatar: Ministry of Information and Communications Technology, 2014.
[129] Q. ICT, "Controls for the Security of Critical Industrial Automation and Control Systems Guidelines," ed: ICT Qatar, 2012.
[130] S. C. o. I. a. C. T. (ictQATAR), "Government Information Assurance Policy," ed: Qatar Supreme Council of Information and Communication Technology (ictQATAR) 2012.
[131] H. Al-Jaber. (2012, Aug). *Protecting Qatar's Children in Cyberspace* . Available: http://www.ictqatar.qa/en/news-events/news/protecting-qatars-children-cyberspace
[132] Q. ICT. (2012, Aug). *Cyber safety awareness*. Available: http://www.ictqatar.qa/en/program/cyber-safety-awareness
[133] Q. Government, "Electronic Commerce and Transactions Law," ed. Doha: ICT-QATAR, 2010.
[134] Q. Government, "The Bylaw Regulating the Work of Certification Service Providers," ed. Doha, Qatar: ICT-qatar, 2010.
[135] M. Bingemann. (2010, Nov). *Satellite operators shortlisted for national broadband network* Available: http://www.theaustralian.com.au/technology/satellite-operated-shortlisted-for-national-broadband-network/story-e6frgakx-1225873722807
[136] N. _Co. (2009, Aug). *NBN CO*. Available: http://www.nbnco.com.au/
[137] A. government, "Critical infrastructure resilience strategy," ed. Austrlia: Ausrlian government, 2010.
[138] A. F. P. (AFP). (July). *Australian High Tech Crime Centre*. Available: http://www.afp.gov.au/policing/cybercrime.aspx
[139] P. Holzer and A. Lamont, "Australian child protection legislation," *Australian Institute of family studies,* 14 Oct 2009.
[140] I. L. Wikia. (Jan). *Electronic Transactions Act 1999*. Available: http://itlaw.wikia.com/wiki/Electronic_Transactions_Act_1999
[141] a. government. (Jan). *CYBERCRIME ACT 2* 001Available: http://www.austlii.edu.au/cgi-bin/download.cgi/cgi-bin/download.cgi/download/au/legis/cth/consol_act/ca2001112.txt
[142] A. Government. (4). *Other Telecommunications Privacy Issues: Spam Act* Available: http://www.alrc.gov.au/publications/7320%.Other%20Telecommunications%20Privacy%20Issues/spam-act
[143] Austrilan_government. (2010, Aug). *Sexual Offences Against Children) Act 2010*. Available: http://www.comlaw.gov.au/Details/C2010A00042
[144] Austrilan_government. (2011, Aug). *Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2011*. Available: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4456
[145] Herald_Sun_News. (2011, Nov). *NBN bills finally pass lower house*. Available: http://www.heraldsun.com.au/archive/news/nbn-bills-finally-pass-lower-house/story-fn7x8me2-1226029602261
[146] B. H. Lee. (Sept). *TM HSBB: The Journey and the anticipatxion*. Available: http://www-mura.ist.osaka-u.ac.jp/ondm2010/pdf/ws2.3-pdf
[147] C. S. Malaysia. (2013, 27 Aug). *Critical National Information Infrastructure*. Available: http://cnii.cybersecurity.my/main/about.html
[148] C. malaysia. (Aug). *Critical National Information Infrastructure*. Available: http://cnii.cybersecurity.my/main/index.html
[149] T. a. I. Ministry of Science, "National Cyber Security," ed. Malaysia: Ministry of Science, Technology and Inovation, 2007.
[150] MyCert. (Aug). *Malaysian computer Emergency Response Team*. Available: http://www.mycert.org.my/en/
[151] C. Malaysia. (Aug). *CyberSecurity Malaysia*. Available: www.cybersecurity.my(
[152] CyberSafe-Malaysia. (Aug). *CyberSafe malysia*. Available: www.cybersafe.my
[153] M. Goverment. (Aug). *Digital signature (amendment) act 2001 ACT*. Available: http://www.skmm.gov.my/Legal/Acts/DIGITAL-SIGNATURE-ACT-1997-REPRINT-2002/DIGITAL-SIGNATURE-REGULATIONS-1998.aspx
[154] M. Govenment. (Aug). *Malaysian Communications and Multimedia Commission act*. Available: http://www.skmm.gov.my/Legal/Acts.aspx
[155] Malaysian_govenment. (2010, Aug). *Strategic trade act 2010 (STA) [act 708]*. Available: http://www.skmm.gov.my/Legal/Acts/Strategic-Trade-Act-(STA)-Act-708.aspx

[156] Malaysian_govenment. (2012, Aug). *Postal services act 2012 act 741*. Available: http://www.skmm.gov.my/Legal/Acts/Postal-Services-Act-2012-Act-741.aspx
[157] A. F. C. Commission, "america's plan executive summary," F. C. Commission, Ed., ed, 2009.
[158] H. security. (27 Aug). *Critical Infrastructure Sectors*. Available: http://www.dhs.gov/critical-infrastructure-sectors
[159] P. s. C. o. C. I. Protection, "Critical Foundations Protecting America's Infrastructures," 13 Oct 1977.
[160] J. D. Moteff, "Critical Infrastructures: Background, Policy, and Implementation," *Congressional Research Service,* 11 July 20.11
[161] *National Plan for Information Systems Protection Version 1.0 An Invitation to a Dialogue*, 2000.
[162] U. G. P. Office, "Homeland security act of 2002," U. S. G. P. Office, Ed., ed, 2002, pp. 2135 - 2321.
[163] W. Paper, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," ed: ISAC Council, 2004.
[164] U. Government, "National Strategy to Secure Cyberspace," ed. Washington: The White House, 2003.
[165] U. Government, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," ed. Washington: the white house washington, 2003.
[166] U. Government, "Natinal Strategy For Information Sharingand Safegarding," ed. Washginton: The WhiteHouse, 2012.
[167] US_Government. (2011 ،Aug 2013). Department of defense strategy for operating in cyberspace. Available: http://www.defense.gov/news/d20110714cyber.pdf
[168] US_Government. (2011, Strategy to combat transnational organized crime. Available: http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf
[169] K. M. Finklea and C. A. Theohary, "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement," Congressional Research Service2013.
[170] US_Government. (2011, Aug .(*International l strategy for cyberspace*. Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[171] US_Government. (2011, Aug). *National Strategy for Trusted Identities in Cyberspace (NSTIC or Strategy)*. Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[172] A. Holpuch. (2014, 12 Jan 2015). *Obama outlines new cybersecurity initiatives to protect consumers* Available: http://www.theguardian.com/us-news/2015/jan/12/obama-cybersecurity-initiatives-student-data-consumers
[173] U. H. Security. (Aug). *Office of Cybersecurity and Communications*. Available: http://www.dhs.gov/office-cybersecurity-and-communications
[174] InfraGard. (Aug). *Learn More About InfraGard*. Available: https://www.infragard.org/FsafFT%2525252BDEUrq3EOQ9lsoJSt5VO98yZFD0ua36j7dev8%2525253D%21
[175] Cybertelecom. (Aug). *the Children's Online Privacy Protection Act (COPPA)*. Available: http://www.cybertelecom.org/privacy/coppa.htm
[176] U. F. C .Commission. (Aug). *Children's Internet Protection Act*. Available: http://www.fcc.gov/guides/childrens-internet-protection-act
[177] N. Willard. (2012, Aug). *Protecting Children in the 21st Century*. Available: http://www.districtadministration.com/article/protecting-children-21st-century
[178] Congress. (2007, Aug). *S. 49 (110th): Protecting Children in the 21st Century Act*. Available: http://www.gpo.gov/fdsys/pkg/BILLS-110s49is/pdf/BILLS-110s49is.pdf
[179] W. R. Ginsberg, "Federal Advisory Committees: An Overview " *Congressional Research Service,* 2009.
[180] I. L. Treatise. (28 Aug). *Computer Fraud and Abuse Act*. Available: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA(
[181] *EXECUTIVE ORDER EO 13010 CRITICAL INFRASTRUCTURE PROTECTION*.1996 ،
[182] US_Government. (2001, Sept). *USA Patriot Act of 2001*. Available: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
[183] FoxNews. (2011, Sept). *Obama Signs Last-Minute Patriot Act Extension*. Available: http://www.foxnews.com/politics/2011/05/27/senate-clearing-way-extend-patriot-act/%7Cdate
[184] US_Government. (2001, Sept). *Executive Order 13228 of October 8, 2001:Establishing the Office of Homeland Security and the Homeland Security Council*. Available: https://www.fas.org/irp/offdocs/eo/eo-13228.htm
[185] US_Government. (2001, Sept). *Executive Order 13231 of October 16, 2001 Critical Infrastructure Protection in the Information Age*. Available: https://www.fas.org/irp/offdocs/eo/eo-13231.htm
[186] US_Government. (Sept). *The Freedom of Information Act (FOIA)*. Available: http://www.foia.gov/
[187] March, "2013 Terrorism risk insurance report," 2013.
[188] U. Government, "Adam Walsh Child Protection and Safety Act," ed: US Government.
[189] Japan_Government. (2001, Aug). *e-Japan Strategy*. Available: http://www.kantei.go.jp/foreign/it/network/0122full_e.html
[190] Japan_Government. (2005, Aug). *U-japan*. Available: http://www.soumu.go.jp/menu_seisaku/ict/u-japan_en/
[191] J. G. of. (2009, Nov). *i-Japan Strategy 2015*. Available : http://www.kantei.go.jp/foreign/policy/it/i-JapanStrategy2015_full.pdf
[192] G. o. Japan, "The Second Action Plan on Information Security Measures for Critical Infrastructures ", T. I. S. P. Council, Ed., ed, 2009.
[193] J. I. S. P. Council, "The Basic Policy of Critical Information Infrastructure Protection," I. S. P. Council, Ed., 3rd ed. Japan, 2014.
[194] J. i. s. p. council, "Cybersecurity Strategy"," i. s. p. council, Ed., ed. Japan: information security policy council, 2013.
[195] J. I. S. P. Council, "Information Security Human Resource Development Program," ed: Information Security Policy Council, 2011.

[196] J. I. S. P. Council, "Management Standards for Information Security Measures for the Central Government Computer Systems," ed. Japan: Information Security Policy Council, 2012.
[197] J. I. S. P. Council, "International Strategy on Cybersecurity Cooperation j-initiative for Cybersecurity," ed. Japan: Information Security Policy Council, 2013.
[198] J. I. S. P. Council, "Information Security Outreach and Awareness Program," ed: Information Security Policy Council, 2011.
[199] G. o. Japan. (2013, Sept). *National Information Security Centre*. Available: www.nisc.go.jp
[200] ITU. (2009, Aug). *ITU/MIC Strategic Dialogue on Safer Internet Environment for Children*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/cop/meetings/june-tokyo/programme.html
[201] T. a. I. G. o. J. Ministry of Internal Affairs and Communications Ministry of Economy. (2009, Aug). *Workshop on Initiatives in Promoting Safer Internet Environment for Children*. Available: http://www.oecd.org/sti/ieconomy/43511802.pdf
[202] EMA. (Aug). *Mobile Content Evaluation and Monitoring Association*. Available: http://www.ema.or.jp/en/member_list_en.html
[203] JISPA. (Aug). *Japan Internet Safety Promotion Association*. Available: http://good-net.jp/english/
[204] G. o. Japan. (Sept). *Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children* Available: http://www.asianlii.org/jp/legis/laws/aopoartcpacpatpoc1999an52om2619991176/
[205] UK_Goverment, "Digital Britain," Department for Culture, Media and Sport and Department for Business, Innovation and Skills2009.
[206] U. Government. (29 Aug). *Centre for the Protection of the National Inferstructure* Available: http://www.cpni.gov.uk/about/cni/
[207] C. Office, "A Summary of the: Sector Resilience Plans for Critical Infrastructure 2010 / 2011," ed. London: Cabinet Office, 2011.
[208] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA, 2003.
[209] U. _goverment. (2000, Sept). *Electronic Communications Act 2000*. Available: http://www.legislation.gov.uk/ukpga/2000/7/contents
[210] U. government. (2006, Sept). *Police and Justice Act 2006*. Available: http://www.legislation.gov.uk/ukpga/2006/48/contents
[211] C. P. P. Act. (2001, Aug). *Governing pornography and child pornography on the Internet: The UK Approach*. Available: http://www.cyber-rights.org/documents/us_article.pdf
[212] U. government. (2003, Sept). *Sexual Offences Act 2003*. Available: http://www.legislation.gov.uk/ukpga/2003/42/contents
[213] C. o. t. e. communities, "Green paper on a european programme for critical infrastructure protection ", ed. Brussels: EU, 2005.
[214] E. States. (Sept). *Critical Infrastructure Warning Information Network*. Available: https://ciwin.europa.eu/Pages/Home.aspx
[215] E. States. (Sept). *European Network and Information Security Agency (ENISA)*. Available: www.enisa.europa.eu
[216] E. union. (2012, Sept). *The Protection of Childre n Online*. Available: http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf
[217] E. Commission, "Title," unpublished.|
[218] D. P. Commissionor. (Aug). *EU Directive 95/46/EC - The Data Protection Directive*. Available: http://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm
[219] E. Union, "Directive 95/46/Ec of the European Parliment and the council of 24 october 1995," *official Journal of European communities,* 1995.
[220] E. commission, "Proposal for a regulation of the european parliament and of the council," Brussels25 Jan 2012.
[221] "Directive 1999/93/EC of the european parliament and of the council of 13 December 1999 on a Community framework for electronic signatures," *Official Journal of the European Communities,* 2000.
[222] Europa. (Aug). *Community framework for electronic signatures*. Available: http://europa.eu/legislation_summaries/information_society/other_policies/l24121_18en.htm
[223] E. Union, "Directive 2009/136/ec of the european parliament and of the council of 25 November 2009," *Official Journal of the European Union,* 2009.
[224] EUROPA. (Aug). *Data protection in the electronic communications sector*. Available: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm#amendingact
[225] E. Union. (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community CIG 14/07* Available : http://www.consilium.europa.eu/uedocs/cmsUpload/cg00014.en07.pdf
[226] e. union, "Directive 2006/24/EC of the european parliament and of the council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications ervices or of public communications networks and amending Directive 2002/58/EC," *Official Journal of the European Union,* 2006.
[227] L. Feiler. (2008, Aug). *The Data Retention Directive*. Available: http://rechtsprobleme.at/doks/feiler-DataRetentionDirective.pdf
[228] E. Union, "COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005 on attacks against information systems," *Official Journal of the European Union,* 2005.
[229] E. union. (2003, Aug). *Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography* Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:HTML
[230] C. o. Europe. (2007, Aug). *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Available: http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

[231] E. Union, "Council decision of 29 May 2000 to combat child pornography on the Internet "،*Official Journal of the European Communities,* 2000.
[232] E. Commission. (2001, Jan). *Convention on Cybercrime*. Available: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

List of Abbreviations

ACL	Access Control List
Aus-CERT	Australian Computer Emergency Response Team (Aus-CERT)
AES	Advanced Encryption Standard
AFP	Australian Federal Police
AHTCC	Australian High Tech Crime Centre
AIDE	Advanced Intrusion Detection Environment
AMC	Adaptive Modulation and Coding
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
AP-CIRT/ APCERT	Asia Pacific Computer Incident (Emergency) Response Team
ASIO	Australian Security Intelligence Organization
CAP	Certification and Accreditation Professional
CCFP	Certified Cyber-Forensic Professional
CDMA	Code Division Multiple Access
CEOP	Child Exploitation and Online Protection Centre
CIAO	Critical Infrastructure Assurance Office
CI2RCO	Critical Information Infrastructure Research Co-ordination
CIRT	Computer Incident Response Team
CISO	Chief Information Security Office
CISSP	Professional Certified Information Systems Security
CIWIN	Critical Infrastructure Warning Information Network

CLD	Cross Layer Design
COBIT	Control Objectives for Information and Related Technology
COP	Child Online Protection
CPNI	Centre for the Protection of National Infrastructure
CSNET	Computer Science Network
CSSLP	Professional Certified Secure Software Lifecycle
DCCI	Defense Cyber Crime Institute
DCFL	Defense Computer Forensics Laboratory
DCITA	Defense Cyber Investigations Training Academy
DNS	Domain Name System
DSD	Defence Signals Directorate
DSS	Digital Signature Standard
ECERT	Estonian Computer Emergency Response Team
EGPRS	Enhanced General Packet Radio System
ENISA	European Network and Information Security Agency
ESCAPE	Electronically Secure Collaborative Application Platform for Experts
ESPaC	E-Security Policy and Coordination
ESRP	European Security Research Program
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FLAG	Fiber-Optic Link Around the Globe
GCA	Global Cyber-security Agenda (GCA)
GPRS	General Packet Radio System
GRC	Global Response Centre
HCISPP	HealthCare Information Security and Privacy Practitioner
HDTV	High Definition Television
HIPAA	Health Insurance Portability and Accountability
HIPCAR	Harmonization of ICT policies and legislation across the Caribbean
HIPSSA	Harmonization of the ICT Policies in Sub-Sahara Africa
HSBB	High Speed Broad band
HSDPA	High Speed Data Packet Access
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICB4PAC	
ICMP	Internet Control Message Protocal
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communication Technology
IDS	Intrusion Detections Systems
IEEE	Institute of Electrical And Electronic Engineering
IETF	Internet Engineering Task Force
IMPACT	International Multilateral Partnership Against Cyber Threats
INTELSAT	International Telecommunication Satellite
IRTF	Internet Research Task Force
ISACs	Information Sharing and Analysis Centers
ISP	Internet Service Providers
ISPC	The Information Security Policy Council
ITSEC	Information Technology Security Evaluation Criteria

ITU	International Telecommunication Union
JNSA	Japan Network Security Association
JPCERT / CC	Japan Computer Emergency Response Team Coordination Center
LAN	Local Area Network
LABAC	Lattice-Based Access Control
LTE	Long Term Evolution
My-CERT	Malaysian Computer Emergency Response Team
MEASAT	Malaysia East Asia Satellite
METI	and Industry (METI)، Trade،Ministry of Economy
MIMO	Multiple Input Multiple Output
MLS	Multiple Levels of Security
MODCERT	Ministry of Defense Computer Emergency Response Team
MOSTI	Technology and Innovation ،Ministry Of Science
NATO	North Atlantic Treaty Organization
NBN	National Broadband Network
NEWS	Network Early Warning System
NIRT	National Incident Response Team
NISC	National Information Security Centre
NIP	Network Intelligent Police
NIST	National Institute of Standard and Technology
NSF	National Science Foundation
OFDMA	Orthogonal Frequency Division Multiple Access
OISF	Open Information Security Foundation
PCCIP	Presidential Commission on Critical Infrastructure Protection
Q-CERT	Qatar Computer Emergency Response Team
QNBN	Qatar National Broadband Network
RBC	Role-Based Access Control
SCADA	Supervisory Control and Data Acquisition
SEA-ME-WE-4	South-East Asia - Middle East - Western Europe- 3
SEA-ME-WE-4	South East Asia–Middle East–Western Europe 4
SDTV	Standard Definition Television
SRI	Stanford Research Institute
SSCP	Systems Security Certified Practitioner
SynCom	synchronous Communication satellite
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDMA	Time Division Multiple Access
TISN	Trusted Information Sharing Network
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network
WSIS	World Summit of the Information Society

Proof

Printed By Createspace

Digital Proofer