Security strategies to overcome cyber measures, factors and barriers

Jawad Hussain Awan[1], Shahzad Memon[2], Rahat Ali Khan[3] ,Abdul Qudoos Noonari[4], Zahoor Hussain[5] and Muhammad Usman[6]

[1,2,3,4,5]*Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan*.

[6]*Department of Computer Software Engineering, UET Peshawar Mardan Campus , Pakistan*.

Abstract: Cyber challenge is an emerging issue in cyber protection situation in order to provide training education. In the stages of the technology development and production of portable and computing campaigns of civilization, cyber control which is suitable and a progressively major approach in the accomplishment of national defense. Breaching of information is an ordinary event because of mutually growing business and also broadcast the information security legislation globally. Whereas, numerous privacy controllers exist and the leading standard has to respond on reported cyber activities. More, this paper overview the current emerging issues, barriers, threats, attacks and research directions in the field of cyber and information security to defend and protect their information resources adjacent to cyber-crimes. Therefore, Interruptive cyber measures are classified into five classes which are foundation campaign for malicious actors as they can interrupt a targeted network and the classification of these interruptive cyber measures enables to contrast events either existing in same class or different classes. More, this paper elaborates six basic prominent factors and barriers which are most effective factors for organizations, business and governments. At last, cyber security strategies, cyber risks and key areas of few countries (Such as: Germany, UK,USA) have been illustrated in Section security strategies for cyberspace to achieve future goals, also aware the researchers, strategy makers, scientists, technologists and organizations to develop new tools, approaches, techniques to dealt with above mentioned barriers.

Keywords: *Security, Strategies, Cyber Measures, Factors, Barriers.*

1. Introduction

Leakage of information and disclosures of memory are major threats to the protection of recently designed operating systems. Although the major attempt put them at risk to sophisticated and targeted cyber intrusion for protected important cyber systems. These days, the majority of systems offer network services and use a permanent software stack which comprised of system software, web servers, catalog, and a virtualization film. Whilst network security operations hold their own rank of particular inspection, a failure to present network inspection in provisions of conventional military operations which produced various difficulties in scheduling and implementation. Whereas numerous data protection regulators are available as well as the leading standard counters reactively on detected events. Reactive response is functional for cleaning out targeted infringes and improves the study in active cyber protection, which uses game-altering essentials such as difficulty. Regrettably, the level and outcome of cyber-threats has enlarged extensively day-on-day even with different defense approaches are developed and set up. It is obvious that end-users take part in an important function inside the information security area, as they are regularly the principal goal and the key control which follows events [1].

Information and Security professionals are no more with assurance condition that, their vital systems cannot be contravened. Therefore, it is of vital importance to frequently and repetitively analysis and polish their proficiency. Cyber challenges trainings and several existing training tools improve the realistic skill to mitigate a cyber-attack for security professionals[2]. Furthermore, the new and innovative approach needs to be introduced to reduce the surface of attack. From the literature, it is highlighted that various researchers propose gloom techniques, such as hiding IP addresses or make them anonymous and some created dynamic addressing but these have not been successfully implemented yet. This paper overviews diverse perceptions to the discovery of an innovative key, which integrates appropriate investigation into active protection in order to adapt dynamic transform [3]. Usually, the greater part of cyber-attacks next to cyber systems has been performed in modern technical behavior and targeting upon the Information Technology system. Though, the landscape of security incidents has changed dramatically over the last few years as attackers have increased their focus and involvement with end users. Phishing, Spam, and Ransom ware are most targeted attacks in the perspective of cyber-attack which are continually employed to target confidential information of end-users and one third organizations worried about the privacy of their employee's sensitive information [4].This is additional appropriate while researcher, user and technologists take into concern the vulnerabilities, processing and storage of virtualized assets which exist in cloud based infrastructures.

The transparency is prominence in virtualized resources which is valuable besides increases the threat of information leakage. The threat of secret information leakage has been increased more as divergences of concern subsist among businesses running on the similar cloud which lifts a necessitate for novel modernization in cloud infrastructures and reduce the possibility of confidential information breach [5]. Further, this paper is divided into eight sections. section I discusses about the introduction, aims and objectives is discussed in section II, literature review

Corresponding Author Email: jawad.awan@scholars.usindh.edu.pk[1]

illustrated in section III, classes of interruptive cyber measures interrupt disrupt are discussed in section IV, Prominent Factors and Barriers are discussed in section V, Security Strategies for Cyberspace is proposed in Section VI, and conclusion is discussed in section VII.

2. Aims and Objectives

The main goal of this research is to highlight emerging issues, barriers, factors which creates challenges for the services offered either by government or business organization. This paper will also helpful for researchers, policy makers to aware existing security strategies, policies discussed in this paper.

3. Related work

Information and cyber security is an emerging field which needs innovative and novel approaches, techniques and practices to deal with modern cyber-attacks, cyber terrorism activities, threats to critical infrastructures and social sites. Easy access of Internet service increased the ratio of end-user as well as increased the protection factor [6]. From collected literature that reliability, accessibility or confidentially attack, protection, flexibility of the nation's cyber resources and government services is an immense challenge for governmental organizations. Stolen of national IDs, Dyre banking malware and phishing campaign are most popular incidents in cyber age. Cyber threat interruption, defense breaches of networks are general cause's of complex problems in these days [7]. eGovernment security threats, services and challenges along with their security measures and stipulation of cyber services and information via social sites, email have been discussed. Moreover, this is common routine and noticed that information age needs trust, familiar rules and digital division crisis, which affect the operation of an eGovernment services. From this paper [8], it is found that various emerging wearable and sensor technologies offer proficient and consistent services.

Further WBAN (Wireless Body Area Network) security and protocol issues are challenging directions which are also under research. Moreover, Inherent complexities create challenging environment to understand supply chains and vulnerabilities as well as provide cyber-criminal chance to conceal malicious incorporation inside individual module of operational systems, commercial constitution, and sharing networks. Thus, an analytics framework is proposed and recommended in [9], and which decreases the complication in the identification and mitigation of Supply Chain Resources. In [10], a novel model is discussed for the development and economy of architectural design, services, driving force for true and fast-track development which provide true principal in the emerging countries of Arab Peninsula, Asian and African growing regions. Up to 2016, 120 million people were part of this growing market share and trade. Furthermore, it is necessary to protect isolation in STOA (Science and Technology Options Assessment) which requires to be modernized to acquire function of the most recent technological progress. Freemium model is commonly used in cloud computing users are facilitated to use basic services free of cost. Existing information security rules do not match with current modes of data transfer used in various cyber services which attract cyber-criminals. Customers, users and citizens of eGovernment needs more control and have to secure their confidential information and incentives do not ensure disclosure by default but ensure the privacy by design which results standard system. At last, it is noticed that security and privacy are necessary for a reliable internet or cyber service. Mostly in the perspective of disclosure about surveillance of internet, whose confidentiality is at risk? Accessibility can be challenging, with the threat of stable loss of information, either attacks by malicious web users or physical disasters. Presently, security approaches or practice is released to hack regular user's data. The EU supports simple and easier systems to be secure from hacker's attempt [11]. Cyber-crime activities, network protection and data create composite problems that grow into the domain of national policy and security [12].

4. Classes of Interruptive Cyber Measures

According to [13] interruptive cyber measures can be classified into five classes which are foundation tactics for malicious actors as they can interrupt a targeted network. Message manipulation, exterior service interruption, interior communication interruption, information Attack and tools attack are interruptive cyber measure classes which are illustrated in Fig. 1 and discussed as below sub sections:

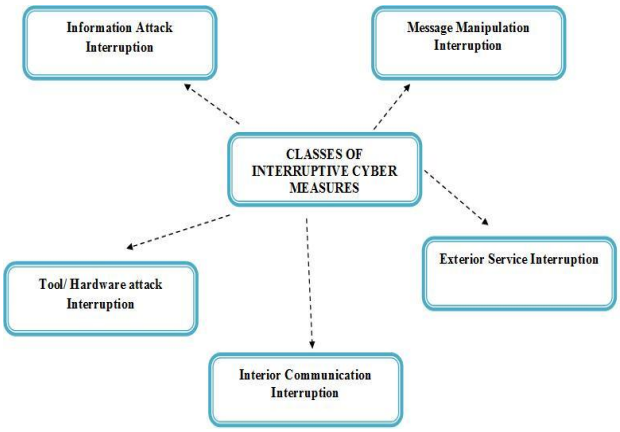

Figure.1 Classes of Interruptive Cyber Measures

A. Message Manipulation

Hijacking of a user's confidential information such as passwords is interrupting the social media of an organization. Various procedures are known as cyber-attacks, those carried out by the negotiation of a user having social media website account. In this way, the distinctiveness of a message manipulation action demonstrates that activist has account authentication information which is main source of communication and its access is exterior to a victim's business network; critical systems have no spoil; and victim can simply remediate by using reset password service with the help of service provider organization [14].

Hijacking of user accounts is insignificant only with social media user accounts which are targeted not with their computers. Because of this, these interruptive actions have small scope as compared to other interruptive events. The interval of this event is directly related to the reset password

service of social media involving hijacked social media credentials. The duration of message manipulation is resolved in a very small time span (either minutes or hours).

B. Exterior Service Interruption

Interruption of exterior operations is carried out via a distributed denial of service (DDOS) attack or website defacement. External overflow of requests to a website server is also a familiar type of interruptive event, it has ability as requested along with the aim of devastating. The outcome is a failure to tackle genuine requests, foremost to an error for the client. This interruptive event identified as a DDoS attack which happens hundreds time in a day and athwart a variety of business companies around the globe. The extent of an exterior DDoS is normally outwardly where the activist remains away from the network of organization. DDoS are single-node targets which are the outer web presence of organization's computer infrastructure. The activists create a sequence of botnet requests and expect to devastate the capability of the target to deal the traffic of user information or content[15]. If thriving, the activist thwarts supplementary genuine users to visit the website.

The scale of DDoS events changes and depends on the significance of the organization's operations existing on websites. For example, a large furniture manufacturer company whose website purchasing webpage is not being display for 20 hours, whereas this type of event may create disturbance to retailer who relies on online purchases. The interval of exterior DDoS interruption events depends on the complexity of the invader and also varies from minutes to weeks[16]. The immense bulk of DDoS actions are tonic by filtration technique of IP addresses, which are drawn in in the attack, thus the operations of an organization's web server are interrupted and the ability of the attacker quickly reduced. Whereas in average case, the majority attacks last only 17 hours and unsettling apparent facing network peripherals, the rising capacity of bandwidth bother against the data centers that indicate a disturbing tendency [17].

C. Interior Communication Interruption:

Interruption of inner operations through is carried by Denial of Service (DoS) of a network. So, thwarting workforce from the access of their email accounts and other necessary files form network, those files can increase the yield of an organization, efficiency, and probably intimidate enduring the shares of market for goods and their services. When an activist got access to inner systems and denies client or user between their computers and corporate systems in that case operations can rapidly stop the operation. The aim of an activist is to interrupt the large number of services of business organization network or user's computer system. That effect can be enabled to attack the network devices through execution of that attack[18]. Internal communications interruption event includes the following characteristics:

Activists control inner authorized access of network to access the services such as Email, numerous computers can be delivered ineffective, as critical services are unreachable and assailant is capable to exclude system supervisors from the infrastructure of network, foremost to major hindrance in reconstituting regular procedures. Hefty organizations integrate control systems for stock or manufacturing systems, where the shutdown of production caused by denying computers from communication with one another. Another effect escorts to huge number of inner computers which do not allow the access of essential business systems by accessing cyber services. The interval of inner interruption of service events have a tendency to last longer than exterior DDoS events. Often, the user credentials are changed, keep off Information Technology (IT) personnel and creating difficulty for the system administrator to salvage control and recover. This type of interruptive event can take time to recover fully in days, weeks, and months in rare cases.

D. Information attack

Interruption of inner operations is also carried via interior multipoint deletion handling of user data, encryption and annihilation of core systems. An attack is targeted to control or annihilate entire data or connected computer systems in an attempt to enduringly upset the operations of an organization and it is fourth type of interruptive event. An activist controls the infrastructure of network to transfer the malicious code among the network of connected computers to concurrently alter, remove the files, corrupt the operating systems of computers, adjust the firmware and try to annihilate peripherals. Information attack events consist of following characteristics.

Attackers control interior authorization of network access to annihilate data and core systems which have not just denying access; the interval of interruptive event is time taking as much as a network administrator needs to recover data and substitute hardware. The extent of a data attack varies from one computer to other end node connected in a network. Attacker controls encryption to claim compensation from user to return data by deploying disruptive payload once. Which known as ransom ware and used with intention of opportunity rather than as element of a conscious operation. Though, activists control profound entrance in a targeted network to thrust malicious piece of code to a large number of computers and subsequently synchronize effecting to obtain maximum cause.

The interval of a data removal attack is noticeable by major interruptions in revisit to usual procedures. An encoded storage device is difficult to recover, and the critical effects to the primary firmware which can entail major upgrading of equipment. The effect is to shove recovery further than an only some days to months.

E. Hardware/ Tool Attack:

Interruptions of interior operations are done by annihilating physically or halt the potential control of equipment, access to critical infrastructure such as electric power. Unauthorized access of network destroys physical equipment between the virtual and physical globe as well as highlights an exposure to the essential systems which can sustain present life. This kind of criminal activity requires a deep knowledge about the system and its network having major resources and control systems. Hardware attack events consist of following characteristics:

Cyber criminals control the interior access of networks as they modify control systems, the production of products

C

have sustainable effect when impact to physical equipment happens, trends changes the outcome impact to be long, physical equipment requires replacement as well as primary network infrastructure need changes.

Hardware attack's spoil transfers from business network to the corporal environment. The extent of this event is more limited as compared to internal communications interruption and smaller quantity of central network nodes is impacted. When interruption of the German steel mill taken place, the physical connected to the network was impacted rather than the disruption of business network.

The scale of hardware attack incident is directly associated to the productive capability and significance of equipment damaged or obstructed. For example, when large power generators affect the intensity of power generation at grid is impactful than the disruption to a control system that is limited in offices. Whereas an interior communications interruption and information attack incident causes the outcome of production because of oblique effect of denying access while equipment attack event annihilates directly the production factor.

The interval of an equipment attack event has longer target as compare to other interruptive attacks, while physical equipment is delivered permanent. Replacement of special physical equipment is time taken process which may take months to years otherwise simple physical equipment is easily replaced. The classification of these events enables to contrast events either existing in same class or different classes. Every interruptive event can be identified by characteristic of different strategies and procedures applied by cyber criminals or activists of a target network.

5. Prominent factors and Barriers

In this section, level of protection, Insufficient market preparation for CIIP (Critical Information Infrastructure Protection), Interest level of government on CII (Critical Information Infrastructure), Sharing of cyber-security information, Sharing of cyber-security information, insurance sector and encouragement by government are prominent factors and barriers which have been shown in Fig. 2 and discussed as under [19].

A. Level of protection

Mostly companies require high level of security for the protection of their CII investments is so much costly. Many countries such as: South Africa, the government setting a budget that does not include funds for the cyber security protection of the country.

B. Insufficient market preparation for CIIP

Most of the organizations and the government require the scientific awareness and proficiency as they defend CII [20]. Nowadays, it has been analyzed that educational institutes set 40% marks to pass a candidate in technical subjects. Such as: Mathematics, Computer Science. This type of strategies and rules does not produce mathematical and technical understanding strong amongst the youth in the computer science and engineering fields at university level.

C

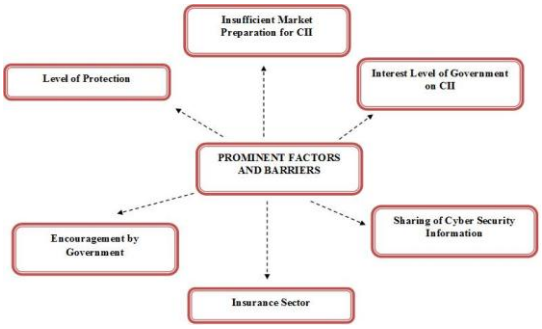

Figure.2 Prominent factors and Barriers

C. Interest level of government on CII

Pakistan lacks the cyber laws and regulations to cope with the variation taken place by CII. It has been reviewed by MIT committee [21], [22] that The Pakistan requires cyber-criminal law. Electronic Transaction Ordinance is the just recommended for the guideline to deal with issues about cyber security. Furthermore, it is said that the country lacks an officially or recognized tool for national public and private organizations which should be implemented internationally recognized standards.

In cyber age, cyber-security of country is obsolete which is entirely ineffective and unrelated [7]. When we want to search for Pakistan's National Cyber-Security Policy or laws, the only two documents existing which states "Electronic Crime/Cyber Bill 2015" [6], which is presented twice in National Assembly of Pakistan for recommendation but it is under review till now. Though this has consequently changed. When the public has not any access to a recognized, contend and approved document then it becomes difficult for common people to support the government official and private organizations to accomplish CII cyber security objectives.

D. Sharing of cyber-security information

Currently, the government is not taking strong steps to share information among business organization about the security of CII and it should be defined that which information is shared. The government arranges seminars, workshops, publishing reports, which facilitates public and private organizations to deal with a situation when cyber threat is targeted and which procedures recommended to overcome on those threats. The government needs to be setup a protected and confidential scheme of sharing cyber protection information as well as private organization must share information, knowledge and expertise about the cyber threats, barriers, challenges and its security. In this way, an enhanced and protected CII environment will be created in short time period.

E. The insurance sector

The insurance sector of the country has to design and implement policies and risk assessments as well as assess CII security of an organization. Higher secured and protected organization should give tax benefits as they can invest that amount in securing their CII [23]. A motivational and friendly scheme should be designed and implemented between both the government and the insurance sector to achieve their future in collaboration. New motivational and encouraging programme should be set up for owners and business organization officials as they invest to achieve requested protection of CII

Table 1. Cyber security strategies, risk and key areas

COUNTRY	CYBER SECURITY STRATEGY	SECURITY OF CYBER RISKS	KEY AREAS
Australia	ACCC [30] (Australian Competition and Consumer Commission) AFP [31] (Australian Federal Police) ASIC [32] (Australian Securities and Investment Commission) HTCO[33] (High tech Crime Operations) ACORN[34] (Australian Cybercrime Online Reporting Network)	Surveillance and foreign intrusion, Explosion of weapons, State-based divergence and, cyber terrorism and aggressive extremism	Investigation of cyber-crimes, threats and scams (concerned with financial services) Enhance global collaboration, promote reliance and assurance in cyberspace athwart the region and international standards among multi-stakeholder processes in cyberspace
Germany	National Cyber Security Council [35], National Cyber Response Centre [36]and External Cyber security policy[37]	Cyber damage, Cyber surveillance Critical Infrastructure, and Cyber threats/attacks	Defensive and protective procedures against IT incident providing offensive strategy, international engagement, improving law enforcement, and training cyber personnel
Japan	Japan Cyber security Strategy[38] and Cyberspace, Information Security Policy Council[39]	overseas, cyber-attacks and critical infrastructures	Develop cyber flexibility; promote global associations, execute a risk-based technique, provide cyber defense to systems, Ministry of Defense and Self Defense Force
UK	NCSP [40][41], CPNI (Centre for the protection of national infrastructure)[42], NaCTSO (National Risk Register and National Counter Terrorism Security Office	Hostile attacks and cyber-crime	Gather intelligence, Sponsor policies, and Protect from criminals. .
USA	NSTIC (National Strategy for Trusted Identities in Cyberspace)[44] CPR (Cyber security policy review)[45], CNCI (Comprehensive National Cyber security Initiative) [46], NCIRP(National Cyber Incident Response Plan) [47]	State sponsor hackers, global cyber association, botnet, and Cyber terrorists.	Defend from Cyber-attack and malicious cyber actors. Gathering action required to secure access for sharing. Construct capabilities; promote international standards and associations.
India	National Cyber Security Policy (NCSP), National Cyber Security Strategy, policy and Roadmap, CERT-IN [45]Information Security	Terrorism, cyber threats, cyber-crimes, Protection of cyber services	Protection for cyber security training for law enforcement agencies Investigation of cybercrime
Pakistan	Section 293 of the Criminal Code[7][43] [44] PISA R3C [45]	Child Pornography, Terrorism, cyber threats, cyber-crimes, Protection of cyber services and critical infrastructure	Protection and awareness about cyber security Enhance technical skills and utilize resources Investigation of cybercrime

F. Encouragement by government

The government of Pakistan and other governments around the globe require promoting and influencing companies and organizations to share perceptive information and offer help whenever required or requested for the protection of CII. Reliance is one of the essential barriers that contribute lack of information sharing for cyber-security of CII because of this organization are tentative to share information amongst participants although the sharing of this information will be beneficial for the cyber- society. Cultural, official and rigid necessities are also barriers to information sharing. Responsibility and contractual commitment of organizations are also identified as barriers in information sharing to CII [24]. The government of Pakistan should start to work collaboratively with companies and organizations in these aspects and setup and negotiate a mechanism to overcome on these barriers consecutively achieve strong cyber security protection for CII.

6. Security Strategies for Cyberspace

The UN Institute for Disarmament Research has issued a latest study and identified that nearly 50 states have developed various cyber capabilities, few of them for cyber warfare [25]. It is also identified that cyber capabilities vary extensively with USCYBERCOM, which illustrates one of the leading cyber-defense agency in the globe is emerging US Army US Navy, US Air and US Marine Corps, Force into a joined command. In the year of 2015 [26], U.S. Department of Defense (DOD) strategy draws on combined cyber domain from the three missions. Provide protection to the DOD networks, organizations, and information; to guard the U.S. homeland and its public

interests from cyber-attacks; and to offer incorporated cyber capabilities to sustain military actions and emergency campaign.

Furthermore, cyber security defense strategies of few countries has been discussed and illustrated to achieve following goals[27], [28]:

- Set up cyber-crime and protection policies and competence
- Increasing cyber flexibility
- Collecting cyber intelligence and taking action against criminals as defined under predefined international cyber law
- Offering training programme to cyber personnel and cyber military
- Increasing global unions in cyber environment
- To establish policies, strategies for international cyberspace.

Cyber security strategies, security of cyber risks, and the key areas of the few countries has been discussed in following Table I[29].

6. Conclusion

This paper overview the current emerging issues, barriers, threats, attacks and research directions in the field of cyber and information security. More, existing operation systems along with their working, complexities, and services have been discussed in literature review section. Message manipulation, exterior service interruption, interior communication interruption, information attack and tools attack are basic interruptive cyber measure classes which are foundation tactics for malicious actors as they can interrupt a targeted network and the classification of these interruptive cyber measures enables to contrast events either existing in same class or different classes.

Every interruptive event is identified via the activity of cyber criminals or activists. Level of protection, Insufficient market preparation for CIIP, interest level of government on CII, sharing of cyber-security information, level of importance placed on CIIP by government, sharing of cyber-security information, insurance sector and encouragement by government are prominent factors and barriers which are most effective factors for organizations, business and governments. At last, cyber security strategies, cyber risks and key areas of few countries (Such as: Australia, Germany, Japan, UK, USA, India, Pakistan) have been illustrated in Section security strategies for cyberspace to achieve future goals and aware the researchers, strategy makers, scientists, technologists and organizations to develop new tools, approaches, techniques to dealt with above mentioned barriers. Furthermore, some aggressive groups of security have to be introduced to develop novel techniques, tools and strategies to overcome vulnerabilities, attacks to infiltrate an inadequately protected system networks and interrupt.

Rerefences

[1] K. R. Choo, "The cyber threat landscape : Challenges and future research directions," *Comput. Secur.*, vol. 30, no. 8, pp. 719–731, 2011.

C

[2] Ivan Burke and R.P. van Heerden, "Automating Cyber Offensive Operations for Cyber Challenges," in *11th International Conference on Cyber Warfare and Security*, 2016, no. March, pp. 65–73.

[3] Jim Chen and Gilliam Duvall, "Proceedings of The 11th International Conference on Cyber Warfare and Security," in *On Dynamic Cyber Defense and its Improvement*, 2016, pp. 74–80.

[4] N. Clarke, F. Li, S. Furnell, I. Stengel, and and G. Ganis, "Proceedings of The 11th International Conference on Cyber Warfare and Security," in *Information Security and Practice: The User's Perspective*, 2016, pp. 81–89.

[5] M. Dlamini, J. Eloff, and and M. Eloff, "Proceedings of The 11th International Conference on Cyber Warfare and Security," in *Industrial Espionage: Corporate Data Continues to Leak*, 2016, pp. 89–97.

[6] J. Awan and S. Memon, "Threats of Cyber Security and Challenges for Pakistan," in *11th International Conference on Cyber Warfare and Security: ICCWS - 2016, Boston USA*, 2016, p. 425.

[7] J. H. Awan, S. Memon, M. Shah, and F. H. Awan, "eGovernment Services Security and Challenges in Pakistan," in *SAI Computing*, 2016, pp. 1082–1085.

[8] J. H. Awan, S. A. Memon, N. A. Memon, R. Shah, Z. Bhutto, and R. A. Bhatti, "Conceptual Model for WWBAN (Wearable Wireless Body Area Network)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 377–381, 2017.

[9] N. Edwards, G. Kao, J. Hamlet, J. Bailon, and and S. Liptak, "Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security," in *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 2016, pp. 98–106.

[10] Marios Panagiotis Efthymiopoulos, "Cyber Security in Smart City of Dubai," in *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 2016, pp. 107–118.

[11] S. Foresight, T. O. Assessment, E. Parliament, E. Union, T. European, T. Eu, M. Translation, T. Stoa, G. Systems, C. C. Services, and S. N. Websites, "Security of the Internet , including e-Government , cloud computing and social networks," 2014.

[12] J. A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," no. December, pp. 1–12, 2002.

[13] C. Harry, "A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact," in *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 2016, pp. 172–179.

[14] T. Islam and D. Manivannan, "A Classification and Characterization of Security Threats in Cloud Computing," no. September, pp. 1–20, 2016.

[15] N. Choucri and C. Jackson, "Perspectives on Cybersecurity: A Collaborative Study," 2016.

[16] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016.

[17] Akamai, "QUARTERLY SECURITY REPORTS," 2016. [Online]. Available: https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp. [Accessed: 15-Jul-2016].

[18] A. D. Maynard, "Navigating the fourth industrial revolution," *Nat. Nanotechnol.*, vol. 10, no. 12, pp. 1005–1006, 2015.

[19] F. Mohideen, "The Cyber-Security State of our Nation: A Critique of South Africas Stance on Cyber-Security in Respect of the Protection of Critical Information Infrastructure," in *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 2016, p. 235.

[20] J. Perry, "Are there any indians left in Colombia? The indigenista movement from 1940 to 1950," *AIBR. Rev. Antropol. Iberoam.*, vol. 11, no. 03, pp. 363–381, 2016.

[21] B. Hoekman and A. Mattoo, "Trade in Services and Economic Development," *Growth (Lakeland)*, no. September, 2007.

[22] A. M. (eds.), *Free and Open Source Software (FOSS) and other Alternative License Models: A Comparative Analysis*, 1st ed. Springer International Publishing, 2016.

[23] K. P. Ambachtsheer, "THE FUTURE OF PENSION MANAGEMENT," no. May, pp. 1–19, 2016.

[24] NDIA, "Cyber Division." [Online]. Available: http://www.ndia.org/Divisions/Divisions/Cyber/Pages/default.aspx. [Accessed: 25-Jun-2016].

[25] Unidir, "The Cyber Index - International Security Trends and Realities," p. 153, 2013.

[26] D. R. Tobergte and S. Curtis, "DOD Strategy for Operating in Cyberspace," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[27] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Comput. Secur.*, vol. 60, pp. 154–176, 2016.

[28] N. Choucri, S. Madnick, and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Inf. Technol. Dev.*, vol. 20, no. 2, pp. 96–121, 2014.

[29] V. Greiman, "Cyberwarfare: From the Trenches to the Clouds," in *11th International Conference on Cyber Warfare and Security: ICCWS2016*, 2016, p. 156.

[30] ACCC, "Australian Competition and Consumer Commission," 2016. [Online]. Available: https://www.accc.gov.au/. [Accessed: 10-Jul-2016].

[31] APF, "Australian Federal Police," 2016. [Online]. Available: https://www.afp.gov.au/. [Accessed: 22-Jul-2016].

[32] ASIC, "ASIC Home | ASIC - Australian Securities and Investments Commission," 2016. [Online]. Available: http://asic.gov.au/. [Accessed: 12-Jun-2016].

[33] High Tech Crime, "High tech crime | Australian Federal Police," 2016. [Online]. Available: https://www.afp.gov.au/what-we-do/crime-types/cybercrime/high-tech-crime. [Accessed: 25-Apr-2016].

[34] ACORN, "ACORN | Australian Cybercrime Online Reporting Network," 2016. [Online]. Available: https://www.acorn.gov.au/. [Accessed: 24-May-2016].

[35] *Restricted Cyber Security Strategy for Germany*. 2016.

[36] NRCCC, "National Response Centre For Cyber Crime," 2016. [Online]. Available: http://www.nr3c.gov.pk/. [Accessed: 18-Jun-2016].

[37] EEAS, "European Union - EEAS (European External Action Service) | EU International Cyberspace Policy," 2013. [Online]. Available: http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm. [Accessed: 18-Apr-2016].

[38] "Cyber Security Strategy: The Government of Japan," 2015.

[39] NCI, "National center of Incident readiness and Strategy for Cybersecurity," 2015. [Online]. Available: http://www.nisc.go.jp/eng/.

[40] S. Gilmour, "Policing Crime and Terrorism in Cyberspace: An Overview," *Eur. Rev. Organised Crime*, vol. 1, no. 1, pp. 143–159, 2014.

[41] OCSIA, "Office of Cyber Security and Information Assurance - GOV.UK." [Online]. Available: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance. [Accessed: 22-Mar-2016].

[42] G. Ateniese, *Critical Infrastructure Protection : Threats , Attacks and Countermeasures*, no. March. La Sapienza, 2014.

[43] NCT, "National Counter Terrorism Security Office - GOV.UK," 2016. [Online]. Available: https://www.gov.uk/government/organisations/national-counter-terrorism-security-office.

[44] NST, "National Strategy for Trusted Identities in Cyberspace," 2016. [Online]. Available: http://www.nist.gov/nstic/.

[45] "Cyberspace policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure."

[46] CN CSI, "The Comprehensive National Cybersecurity Initiative | The White House," 2016. [Online]. Available: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[47] A. V.-K. Pernik, Jesse Wojtkowiak, "CCDCOE."

[48] J. De Lange, R. Von Solms, and M. Gerber, "Better Information Security Management in Municipalities," in *Conference Proceedings*, 2015, pp. 978–1.

[49] PakCert, "PakCert." [Online]. Available: http://pakcert.pk/. [Accessed: 08-Aug-2016].

[50] "Cyberwellness Profile Islamic Republic of Pakistan."

[51] S. A. Memon and J. H. Awan, "Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan," in *Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense*, 2017, pp. 50–61.

About authors

Jawad Hussain Awan is a member of IFIP WG 9.10 - ICT Uses in Peace and War. He is PhD Research Fellow, in Institute of Information and Communication Technology at University of Sindh, Pakistan. He completed his MPhil in CTP (Cyber Terrorism Prevention) framework for national Identification Databases. His research interests are Cyber security, Information Security, e-Governance, e-Democracy, Security challenges in Information Systems and Wireless Body Area Networks. He published his research in

C

several national and international research journals. Mr. Awan attended and presented his research in national and international conferences. He is also Microsoft Certified Professional in Web Programming.

Dr. Shahzad Memon is a member of IEEE. He is working as an Associate Professor, in Institute of Information and Communication Technology at University of Sindh, Pakistan. He completed his doctorate in Livens issues with fingerprint sensors technology from Brunel University, London, UK. His research interests are fingerprint Sensors, multimodal biometrics, Cyber security, Micro and Nanosensors for security applications, Simulation of Micro and Nano-systems, Security challenges in Information Systems. He published his research in several national and international research journals. Dr. Memon attended and presented his research in national and international conferences. He is also member of Institution of Engineering and Technology UK, and IAENG, USA

Rahat Ali Khan is a Research Assistant and PhD Research Student, in Institute of Information and Communication Technology at University of Sindh, Pakistan. His research interests are Wireless Body Area Networks and Sensors.

Abdul Qudoos Noonari is an MPhil Research Student, in Institute of Information and Communication Technology at University of Sindh, Pakistan. His research interests are Cyber security, Information Security.

Zahoor Hussain is a PhD Research Student, in Institute of Information and Communication Technology at University of Sindh, Pakistan. His research interests are Smart Energy Management, Smart Metering System, and Smart Grid.

Dr. Muhammad Usman is an Assistant Professor, in Department of Computer Software Engineering, UET Peshawar, Mardan Campus, Pakistan. His research interests are energy efficiency and security in next generation networks, wireless sensor networks and cognitive radios.

C