I. J. Computer Network and Information Security, **2019, 1, 62-69**
Published Online January 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.01.06

Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan

Qamar Atta Ul Haq
Computer Science Department, ISP University 9-KM Bosan Roads, Multan Pakistan +92-61-111-786-477
PAKISTAN
E-mail: qamarattaulhaq@gmail.com

Received: 11 July 2018; Accepted: 14 November 2018; Published: 08 January 2019

***Abstract*—**This research report analyses the plebeian interest and tension hostility between privacy and cyber security in Pakistan. I explore the areas threaten by hackers in means of ATM card hacks and social data sniffing. It explores the challenges for Cyber security belongs to privacy and data protection.

Index Terms—Cyber security, cyber jihad, hacking aggression, Intrusion detection system and intrusion prevention systems, Intellectual property, Computer security, Cyber terrorism, Security risks, Encryption, Hacking Vulnerability.

I. INTRODUCTION

The process or steps are adopted to protect the system against the criminal malefactor or unauthorized access and the use of data of military, industrial and business is called cyber security. A criminal way and activity that is adopted by a person and a group through the use of computer and internet called cyber crime. Cyber issue is pulling everyone's attention of World Wide [1].

Charles Babbage was the professor of the Cambridge University in 1837 build the mechanical, modern computer called "Analytical Engine" and that work is surprisingly more than 100 years of future work, it was an astonishing moment of his work. The united State military give the official approval in 1943 to first computer called ENIAC (Electronic Numerical Integrator and Computer). The ENIAC possess the very large requirements as a collection of the 18,000 of the vacuum tubes which designed to give the computation power of 100,000 amounts of pulses in per second, which speed 300,000 more and faster than human power of processing the information. The prediction of the Gordon more in 1965 that the amount of transistors on a computer chip will be double in every year. The first Hackers friendly tool that is OSINT (Open Source Intelligent) and it was web enabled [1]. The cyberspace (Communication over a linked billion of computers via the internet) was firstly occur in 2011.Hacker is the expert person, that expertise in computer system, the hacker used that knowledge to access the data in unauthorized and illegal way. The research group of UK (United Kingdom) IWM (information warfare monitor) in 2009 tells the existence of the "Ghost Net" that is a collection of compromised 1000 computers in more than 103 countries, that infected and victimize the world wide countries [1, 4, 19].

Mafia Boy in 2001 from the Montreal is a student of 15 years age created the DOS (Denial of Services) attack on the online web based companies that result a financial damage of $1000000 dollars. Syrian air force defense system in 20017 sudden disabled by the cyber-attack. The first worm introduced in 1949 by the John von a mathematician during proposing the "self-replicating automata" and that will remain in experimental stage [2].

The annual cost of the global cybercrime is predicted that it can be extended approximate from 3$ TD (Trillion Dollars) till 2015 to 6$ in 2021. The cyber security industry and market in 2015 spending the $75 billion Dollars which is extended and grow to an unbeatable record in history in 2018 that is $101 billions of dollars and the prediction about the cyber security cost that is growing to $170 billion dollars in 2020. The European countries, making the directives used to protect the information in systems from threats, EGDPR (European General Data Protection Regulations and the Second directive are NIS (Network Information Security). Pakistan is currently focusing the national when Pakistan army facing a threat from terrorists as well as international cyber security threats coming from the China and India it is a strategic war for the survival of Pakistan [2, 13, 21].

Pakistan facing two wars, one against with the terrorists and second with the issues of cyber security. The services of internet available since from 1990 in Pakistan. Pakistan population is 200,813,818 in 2018, which is 2.97% of the total world population. Pakistan have 6th position in the list of the country by population, and population density is 250 per km2 and 39.6% of the population is urban. Pakistan population 200,813,818 and from that there is 44.3424 million of internet users in Pakistan and also there is mobile subscribers adding 1million a month, approximate 16.5 million users browse and use internet from there mobiles while others are broadband subscribers. In Pakistan 80% smart phones found less than price of the $100 [2, 6, 7, 8].

ICT (Information and Communication Technology) fastest developing industry in Pakistan. , Corresponding to the report of ITU (International Telecommunication

Union), In 2001 almost 1.3% of population was using internet and by the end of 2006 that the estimated figure was increased 6.7% of population, till the end of 2012 this figure increases to 20million. While ISPAK (Internet Service Provider Association of Pakistan) said that in 2012 the figure is about 10million [3]. Separate from these reports IT THINK TAMKS asserted that the figure should be crossed 30million.3G and 4G available in Pakistan from April 14, 2014.The Government of Pakistan earned from 3G and 4G from auction is about $930 million and $210 million. According to PTA (Pakistan Telecommunication Authority) annual report 2018 shows that 50 million cellular subscribers, 56 million 3G/4G subscribers, 3 million basic telephony subscribers and 58 million broadband subscribers [3, 7, 16, 20].

A. Identifying The Security Back Holes And Laps In Pakistan Institutions

Russian and Chinese hackers are involved in trying for breaching the Pakistani bank's security by obtaining the people ATM card information on the Darknet or a dark website. According to my Research 2000000 ATM card information were sold on a Darknet and the price of per ATM card information that is sold is $150. I am suggesting the 20000 Pakistani banks to improve security systems that is used for international transaction through ATM cards or any other medium. Improve Monitoring system for employee that is involved in dealing to sale ATM card information on a dark website

II. Literature Riew

There are 50 countries who introduced their strategies for cyberspace and for cyber security. The most vital infrastructure about protection towards the cyber security, there are 25 countries who introduced and show the policies of cyber security, United States of America, Algeria, United Kingdom, Australia, Switzerland, Brazil, Sweden, Canada, Spain, Estonia, Singapore, Finland, Russia, France, Poland, Germany, New Zealand, Hungary, Norway, India, Netherlands, Italy, Malaysia, Japan.

The cyber security and the probability appraisal cyber security threats to the Distributed control system (DCS), supervisory control and data acquisition (SCADA) networks and Industrial Control Systems (ICS) introducing organizational and Government groups

1. CSP (Cyber Secure Pakistan)
2. NUST (National University of Sciences & Technology)
3. CERTs (Computer Emergency Response Teams)
4. EAS (Enterprise Application Systems)
5. EMS (Energy Management Systems)
6. ISO/IEC 17799 (Information Security Management)
7. PCSRF (Process Control Securities Requirements Forum)
8. SPP-ICS (System Protection Profile for Industrial Control Systems)
9. ISA-TR99.00.01-2004 (Security Technologies of Manufacturing and Control Systems)
10. NIAC (The National Infrastructure Advisory Council)
11. NCS (The National Communication System)
12. NCSD (National Cyber Security Division)
13. CSSP (Control Systems Security Program)
14. ISA (Instrumentation, Systems, and Automation Society)
15. NIST (National Institute for Science and Technology)
16. NERC (The North American Electrical Reliability Council)
17. US CERT (The United States Computer Emergency Readiness Team's)
18. ISACs (Information Sharing and Analysis Centers)
19. CND (The Computer Network Defense)
20. CSIS (Center for Strategic and International Studies)
21. CERT/CC (Coordination Center)
22. NIST (National Institute for Standards and Technology)
23. IDS (Intrusion Detection System)
24. CIC (Created by the Cyber Innovating Center)
25. NICERC (The National Integrated Cyber Educating Research Center)
26. PTA (Pakistan Telecommunication Authority)

III. Types of Cyber Criminals and Attacks

Cyber criminals are those people (programmers) who use their expertise and skills to commit a crime on internet and stole someone information or any other sensitive data for the purpose of blackmailing and for money called cyber criminals. Usually this are programmers who used their skills in illegal activities we know that is a crime [4].

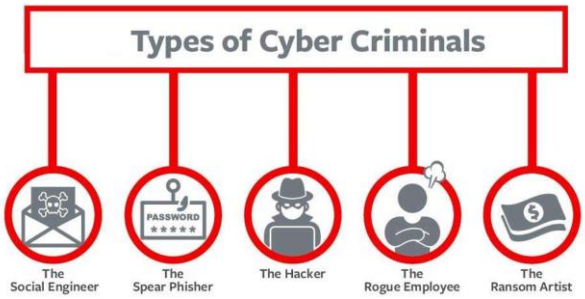

Fig.1. Types of Cyber Criminals [4, 19]

Cyber-attack is any kind of abhorrent actions that is taken by the cyber-criminal on computer through internet to stole and get someone sensitive information and data for illegal purpose. Cyber criminals adopt different methods and way so that they can force any of computer user to attract towards bait and catch in a trap. There are following some types of a programmers possible attacks through the internet on a computer.

Fig.2. Types of Cyber-Attacks [4, 19, 14, 9]

While the Governments of Pakistan emphases on terrorism war NAP (National Action Plan), at that time another threat feels to be appearing as purview of visible horizon that is cyber security. Today modern life depends on the online services and online shopping because we are intellectual that is the reason of information and personal data at risk of stealing our personal information and data from hacking and others related to the unauthorized access, that major issue confronting the Pakistan. Since our cell phones and computers are victims of more than 8 countries, whose intelligence agencies are interfering in our personal life and the aggression of hacking and for money increasing day by day and we are enduring suffering from that situation, now Pakistan focusing the cyber security to protect the rights and personal data from stealing someone.

The first spam email brought in 1978, when it was transmitted to the ARPANET (Advanced Research Project Agency Network). The UK police caught the student as he hacked FBI email in 2005 and some documents of NATO are hacked in Afghanistan and "Mafia Boy" attacks on DOS (Daniel of Services).In 2000 Swedish NORDEA bank victim and about $100000 was stolen.

Cavelty in 2010 prepared annotations about the triune or multiple interlacing preaching about the domain or field of cyber security. Cyber is affix predicating the cyber space and pertains to the ECN (Electronic Communication Networks) virtual realism by oxford in 2014. Cyberspace destined and contrived as an IE (Information Environment) by Friedman in 2013. The present-day cyber security standard is FIRST the Forum of Incident Response Security Teams and IEEE Institute of Electrical and Electronics Engineering and NIST National Institute of Standers and Technology and the ICANN The internet Corporation for Assigned Names and Numbers.

HAIMS and CHITTESTER works result that to reduce the effects of cyber-attacks. HONEY POTS amuse the attacker from attaining the vital system information. CORDESMAN works on cyber threats. KLIMBURG works on cybercrime. MCHUGH examining the dealings of treble speed of networks. KING ET, he inquire about the cyber threats. LOPEZ suggest the security services about smart grid. WHITMAN and MATTORD works on information protection. MARTIN and RICE their works about cyber domineering. MILLER trying to secure the system. NELSON and NASH trying amending to control system. NISSENBAUM improving the cyber security schemes. ANSS describe and handle cyber-attacks. DHILLON who introduced the idea of data security. ERIKSSON who stops penetration of information. ARQUILLA introduced the transmutation of war into cyber war. CLARKE give the concept of cyber warfare.

Pakistan, now starts working about cyber security because Pakistan facing two wars one about terrorism and second to protect, secure and protect their people privacy, data and information from accessing outside the country intelligence agencies and the most enemy threat facing Pakistan from India one from India interfering Karachi and Baluchistan matters to split the Pakistan and second accessing the digital data from American and India and others countries intelligence agencies. For that purpose Pakistan increases his security policy and starting awareness to the people through the seminars and through universities.

1. PIPS (Pakistan Institute of Parliamentary Services)
2. PISA (Pakistan Information Security Association)
3. NSA (National Security Agency)
4. Senator Mushahid Hussain particularly elaborate the cyber security threats.
5. PKCERT (National Emergency Team)
6. NAP consist the cyber security
7. Cyber security taskforce
8. According to SAARC Pakistan should have to be initiate the steps against cyber security
9. PECO

NSA gives report to Pakistan about the security gaps in Pakistan and digital data may stole from the terrorists and use for the terrorism activity. On the behalf of the NSA report Pakistan senate defense committee and PIPS AND PISA take charge on the consequence of opposing Pakistan through cyber security on July8, 2013.Now that time, Pakistan first time take stand to oppose the cyber threats belong to Pakistan. Pakistan information security association hire the experts from NUST, LUMS, RIPHA University and the internet providers.

The defense committee organized the seminar in which parliamentarian are invited for awareness and introduced the seven points of the plan related to the cyber security and threats by committee chairman M.Hussain Sayed

1. M\O defence
2. HEC
3. LUMS
4. NUST
5. PISA
6. CSTF
7. Ministries law
8. Ministries interior
9. Foreign affairs
10. FIA
11. NAB

IV. CYBER CRIME

In **November 2018** due to a cyber-attack 624 customers of different 22 banks are losing their money which is 11.7 million. A legal report from the FIA is that the data of 19,865 ATM cards were sold on a dark web. The action of using computers and networks as an instrument for the interest of illegal criminal activity. Cyber-crime in tensest threats are knocking the doors of Pakistan but regrettably grapevine Pakistan laws are calm and waiting for execution. ICT seventh exposition and admitted CONNECT exhibition Karachi and reported approximate 200 cases of hacking and blackmailing in 2012. Pakistan facing the following crimes

1. Physical detrimental a computer system
2. Fiscal crimes
3. Logic dud
4. Cyber smut
5. Virus and worms assail
6. Email burlesquing
7. DSN
8. Cyber calumniation
9. Salami assail
10. Cyber haunting
11. Information diddling
12. Unsanctioned accession to computer systems and networks
13. Online hazarding
14. Password smashing
15. Blackmailing for stealing electronic information

The situation of cybercrime in Pakistan is very dangerous but still there is no strict laws. In 2011 approximate 25 instances will occurs and registered with concerning to cybercrime. Facebook profile and account information stealing through hacking as the intention of blackmailing for some benefits and unreal Facebook accounts of girls is used to necessitate for retaliation because from the girls side family had refused the marriage offering, but still there is no cyber laws in Pakistan.

In 2015 Pakistan originate steps to secure Pakistan from the cybercrime and threats of cyber security related issues with the team or organization of PSA and Ultra Spectra (pvt). April8, 2015 the conference asserted organized coordinated with the coaction of NUST-SEECS and more than fifty fence-sitters means stakeholders on call and this conference become leading Asian consequence for all fence-sitters admitting Government, data protection professed means professionals, data security enterprisers, telecommunication sector security steering plus administrators, trusting sector and information technology sector to contribution perceptivity into the most recent demonstrated creations and concepts. The schedule discussion for cyber security of Pakistan is to search as entirely the interior or internal and extraneous or international community of interests admitting ICANN, APNIC, Internet social club, Google, territorial CERTs, world-wide investigators on the issue to arrive and contribution of their undergoes as substantially. The canonic intention and causative posterior this conference is too conscious the people of Pakistan about the cybercrime and cyber terrorism, for that purpose cyber invulnerable Pakistan comprising a chain of building training, workplaces, cognizance sittings, contenders, keynote oratory, panel conversation, security discussion by illustrious internal and external industry professionals. Proficient awareness sittings and holding the succeeding training sittings, CHFI (Computer Hacking Forensic Investigation), mobile diligence incursion testing, contrary engineering malevolent program, Linux origin instruments workplace by Pakistan, system protection workplace through ICANN and APNIC. LEA workplace in Pakistan, kid security through the internet society.

Cyber-crime arises quickly in Pakistan. Concording to the cyber-crime wing (CCU), furcate of FIA Federal Investigation Agency, exclusively events and exclusively are notifiable and reported in the unit, in 2007 cyber-crime related events reported to CCU is 62 and in 2008 the events rapidly increases to 287 and after passing laws from the parliament of Pakistan the ration of cyber-crimes were deteriorated from 2009 117 events and 2010 and half exclusively 73. Later on the ratio increases again and rapidly from the previous and antecedently ration of events that is 2011 to 2012 is 411 events , 2013 is 290,2014 320 with tiny blackmailing,2015 is about 345, in the start of 2016 there were 89 till march events are reported to FIA.[7, 8]

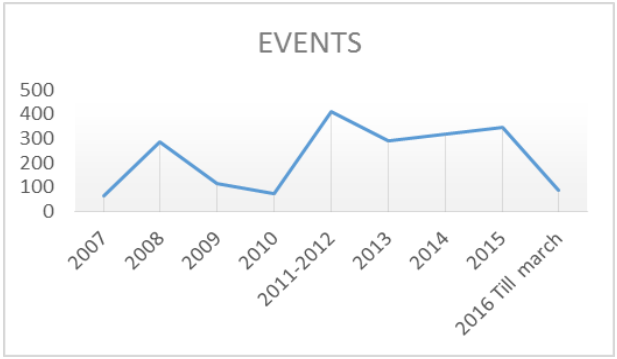

Fig.3. Hackers Attack in Pakistan

Edward Snowden a brave man scrupulous to disclose, reveal and fetched out how the USAs NSA National Security Agency spotting on majority countries in the world. Such spotting evidently constituted by USAs political, economic and combatant or military international vantage. The fifth nearly and most spotted on country is India, straight a lot than Russia and China. Conceiving the India is the USAs momentous collaborator, spotting on the India that is infract of trust for USA, therefor USA spotting all the countries except India. Iran in the crowning list 14 billion sets up of the USA intelligence and administrative unit, the second number of Pakistan is came approximate 13.5 billion, the third number of the Jordan is about 12.7 billion, in fourth position Egypt comes estimated figure is 7.6 billion and

the fifth number come of the be loving country of USAs India approximate is 6.3 billion.

Cyber-crime as well intromit directing viruses on distinct systems, sending calumniation contents. Pakistan committee of the cyber-crime is following features can be

1. Computer territory direct approaches attacking to the others computer systems
2. Computer districted used as a tool to confide imposter and the banned hazarding or gaming
3. Computer are used as a supportive for storage felonious and purloining of data or information.

V. CYBER LAWS IN PAKISTAN

Cyber laws or the inferior conversationally and national laws of Pakistan is a consideration that capsulate the effectual consequences associated to the manipulation and the use of communicatory, relations and the disseminative expressions of electronic network entropy gimmicks or devices and engineering's. The following Pakistan cyber laws for criminals

1. ETA The Electronic Transaction Act (1996).
2. ETO The Electronic Transaction Ordinance (2002)
3. PACCA Perspective analysis of Cyber-crime act (2006)
4. EFTA The Electronic Funds Transfer Act (2007)
5. PECOP The Prevention of Electronic Crime Ordinance Pakistan (2007)
6. PECOA Prevention of Electronic Crime Ordinance Act (2008)
7. PCCCOA Prevention and Control Cyber Crime Ordinance act (2009)
8. FTOA The Fair and Trial Ordinance Act (2012)
9. PECOA Prevention of E Crimes ordinance Act (2013)
10. PPOA Protection of Pakistan Ordinance Act (2014)
11. EDPCCOA The Electronic Documents and Prevention of Cyber Crime Ordinance Act (2014)
12. PECOA Prevention of Electronic Crimes Ordinance Act (2015)
13. AECOA Amendment Electronic Crimes Ordinance Act (2016)

There are five primary points of 2016 cyber-crime act is the following

a. First, it is a crime or illegal activity to transmit or send a messages or pictures to any persons e-mail address.
b. Second, the constabulary and the police force, Federal investigation agency and any other agency will not necessitate the inquiry endorsement and warrant to search.
c. Subordinate incision or section 17 and 18 political critique and the political manifestation should be criminalized and illegitimate.
d. Subordinate incision or section 31, Government can Barricade and take accession to some internet site online or current informant.
e. Subordinate incision or section 26, ISP'S, eateries, promenades, buildings, offices airports and the bus stations anyplace with the internet adroitness should be required to accommodate and hold information and data for three months.

Table 1. Cyber-crime Punishments in Pakistan [7, 8]

Crime	***Immurement/imprisonment***	***Penalization/penalty***
Data damage	3	3-Lac
Criminal data access	3	3-Lac
Criminal access	3	3-Lac
System damage	3	3-Lac
Electronic forgery	7	7-Lac
Electronic fraud	7	7-Lac
Misuse of devices	3	3-Lac
Unauthorized access to code	3	3-Lac
Malicious code	5	5-Lac
Defamation	5	5-Lac
Cyber stalking	3	3-Lac
Cyber spamming	6-months	50,000
Spoofing	3	3-Lac
Pornography	10	10-Lac
Cyber terrorism	life	10-million

VI. CONSCIOUSNESS CURRICULUM

Pakistan organizing the awareness seminar for their people and the main purpose to aware the people of government and private sectors to secure their information and important personal data.

Table 2. Cyber-crime Conferences in Pakistan [7, 8, 9]

ISSUES/CONSEQUENCES	Involvement
Cyber Security Conference 2015 in Multan	many
Lecture about superior menace of Cyber offenses and Cyber Terrorism	80
Cyber Security and protection disputes and suffices answer (intervening Level Management)	200
Cyber Security and protection disputes and suffices answer (grayer or old Level Management)	85
predilection about Cyber offenses (secondary Level Management)	40
Equal crusades and exploits to fighting Banking associated Cyber offenses and currency Laundering (precedential administrators of Banking Sector)	200
Cyber Security and protection disputes and suffices answer (at Karachi)	200
Cyber Security and protection disputes and suffices solutions (at Lahore)	20
Litigating or Processing of beginning Cyber offense event and case by NR3C	30
Satisfactory standard Efforts to fighting ISP's associated and corresponding to the Cyber Crimes	20
Cyber offenses or crime For SIG, at FIA Academy and pedantic	200
Cyber offenses challenges situation and Solution at Islamabad	200
Entropy or information Security and Cyber offenses at Islamabad	250
Information protection security and Cyber offenses at Islamabad	200
Conference on Cyber Security at Karachi	300
One day workshop on Cyber Security and protection Challenges and disputes & Solutions	52
Lecture on the origination of Introduction to Cyber Crimes	60 Trainee and beginner Judges of Punjab
Training and educating Polices of Agency officers in the area or field of Digital Evidence and manifest Islamabad, Peshawar, Lahore, Karachi, Quetta and Muzafrabad	35
Lecture about the Cyber Security and protection to beginner and trainee NAB Officers	35
One day conference on the Cyber Security and protection	37
Lecture about the data and Information Security demonstrating in NAB	60
Lecture on the data and Information Security delivering in NAB	50
Four Days conditioning or Training Workshop for subordinate training ASPs at federal Police Academy	45

VII. Pakistan Struggling and Exertion Against the Cyber War

PISA Pakistan Information Security Association, the CSP Cyber Secure Pakistan, Pakistan interior ministry and defense ministry, ICANN, APNIC and the Engineering school of NUST is SEECS (School of Electrical Engineering and Computer Science) working collaborating and cooperating to each other for technical awareness and the cyber security of Pakistan, all of these working unitedly and organizing seminars training sessions and workshops and for technical awareness is follows [10]

DNSSEC (Domain Name and System securities) workshops, Mobile applications and Penetration and incursion testing training sessions, REM (Reverse Engineering Malware) workshops, LINUX supported public and open Source tools, Computer hacking forensic or practical investigation and probe, Women centric cyber security and protection seminar, Child online security and protection workshop and ceremony cyber secure Pakistan 2015. In 2018 a hope to protect the information may take government steps

VIII. Suggested Security Tools by Professionals

According to the APSCC (Asia Pacific Satellite Communication Council more than 9 billion records are lost or stole per year [9]

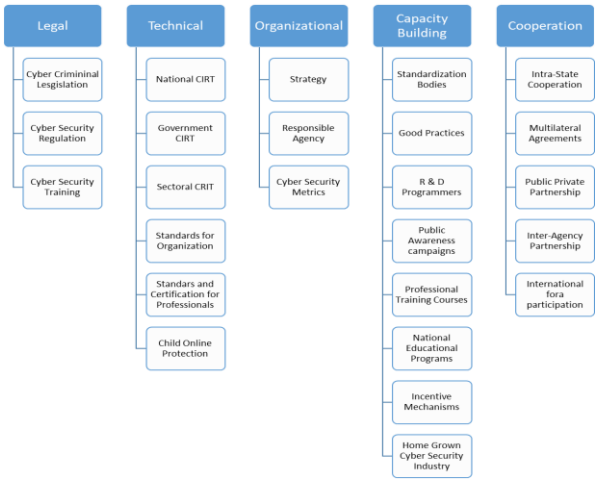

Fig.4. Technical Awareness [10, 13, 21]

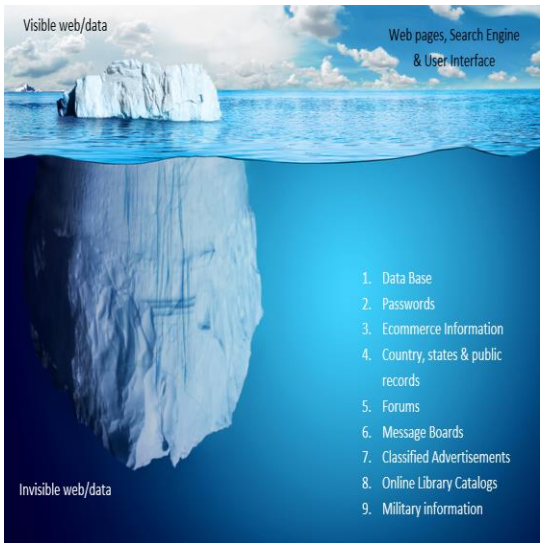

Fig.5. PSCC Report [9, 11, 10]

1. Sysinternals and Windows Godmode suggested by the RON WOERNER the director of cyber security studies at Bellevue University.
2. Microsoft EMET suggested by the YIER JIN the assistant professor of computer sciences and EE (Electrical Engineering) at the University of Central Florida.
3. Secure@source, Q-Radar, ArcSighr and Splunk suggested by the JEEF NORTHROP the CTO at international association of secrecy or privacy professionals and experts.
4. Insider thread protection suggested by the MIKE PAPAY the VP and CISO at Northrop Grumman.
5. Privileged identity management suggested by the ANDRAS CSER the security analyst and expert at Forrester.
6. Patch management suggested by the GARY HAYSLIP the Deputy Director for CISO in the city of San Diego.
7. Blue box suggested by the DR.JOHN D. JOHNSON the global security strategian and security architect and designer for John Deere.
8. Endpoint detection and response suggested by the NEIL MACDONALD the VP and distinguish or discern analyst at the Gartner.
9. Fire Eye suggested by the RANDY MARCHANY the information technology security lab director and the security officer in the Virginia.
10. Advanced security analytics suggested by the JOHNA TILL JOHNSON the CEO at Nemertes Research.

IX. Conclusion

This article has presented and confronted inspection or review of the scientific literature about the cyber security, protections, awareness and consciousness, security disruptions and laps, cyber security situations, cyber-crimes, cyber laws and punishments, cyber terrorism and for cyber security suggested security tools by professionals in Pakistan. For this purpose and determination 42 articles were read, collective and gregarious, compactly and succinctly delineate or describe.

References

[1] Seminar, “Security in Cyber Space: Implications and Challenges,” Center for International Strategic Studies (CISS), Islamabad Marriot Hotel, September 30, 2014.

[2] Deibert, Ron. Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Prepared for the Canadian Defense & Foreign Affairs Institute, August 2012.

[3] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen, Nowlan, William Perdue, Julia Spiegel; “The Law of Cyber Attack”; Forthcoming in the California Law Review, 2012.

[4] WSIS Thematic Meeting on Cyber security Geneva, 10 June 2005 A Comparative Analysis Cyber security Initiative Worldwide Page 3-4.

[5] The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure.” (Canongia & Mandarino, 2014).

[6] Dr. Sadiq Ali Khan Department of Computer Science National University of Computer and Emerging Sciences FAST.

[7] FIA, NAB, SEECS, PISA, CSP and NUST researches documents.

[8] APSCC. (2018, 11 10). step1.php. Retrieved from online.fpsc.gov.pk:online.fpsc.gov.pk/fpsc/gr/step1.php

[9] Brahima Sanou (Director, T. D. (2017). Global Cybersecurity Index (GCI). Global Cybersecurity Index (GCI), 65.

[10] J. Blackburn and G. Waters. Optimising Australia’s Response to the Cyber Challenge. Kokoda Foundation, 2011.

[11] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang. Securityaware optimization for ubiquitous computing systems with SEAT graph approach. J. of Computer and Syst. Sci., 79(5):518–529, 2013.

[12] M. Gallaher, A. Link, and B. Rowe. Cyber Security: Economic Strategies and Public Policy Alternatives. Edward Elgar Publishing, 2008.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58(11):2715–2729, 2013.

[14] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials, 14(4):998–1010, 2012.

[15] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1–11, 2011.

[16] M. Qiu, H. Su, M. Chen, Z. Ming, and L. Yang. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Communications Magazine, 50(5):142–149, 2012.

[17] F. Hu, M. Qiu, J. Li, T. Grant, D. Taylor, and S. McCaleb et al. A review on cloud computing: Design challenges in architecture and security. J. of Computing and Info. Tech., 19(1):25–55, 2011.

[18] F. Liu, H. Lo, L. Chen, and W. Lee. Comprehensive security integrated model and ontology within cloud computing. J. of Internet Technology, 14(6):935–946, 2013.

[19] N. Rani, A. Satyanarayana, and P. Bhaskaran. Coastal vulnerability assessment studies over india: a review. Natural Hazards, 77(1):405– 428, 2015.

[20] K. Gai, M. Qiu, L. Tao, and Y. Zhu. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Security and Communication Networks, pages 1–10, 2015.

Authors’ Profiles

Qamar atta ul haq was born on Nov 9, 1993 in Multan .He completed his Higher Secondary School and college from the hometown Multan. He completed his graduation degree from the Institute of Southern Punjab Multan Pakistan and then he

completed his master degree from ISP Multan and got Gold medal for his work. After that he goes to the IUB University for MSCS with the specialization in Artificial Intelligence and carry on his research to facilitate the Nation from his research and work.

How to cite this paper: Qamar Atta Ul Haq,"Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.1, pp.62-69, 2019.DOI: 10.5815/ijcnis.2019.01.06

