HIGHER EDUCATION AND CYBERCRIME IN QUAID-i-AZAM UNIVERSITY,ISLAMABAD, PAKISTAN

ومن يُؤت الحكمة
فقد اُوتی خیرًا کثیرًا

QUAID-I-AZAM UNIVERSITY
ISLAMABAD

AMINA AKMAL

Department of Sociology

Quaid-i-Azam University,Islamabad

2017

HIGHER EDUCATION AND CYBERCRIME IN QUAID-i-AZAM UNIVERSITY,ISLAMABAD, PAKISTAN

ومن یُؤت الحکمة
فقد اُوتی خیرًا کثیرًا

QUAID-I-AZAM UNIVERSITY
ISLAMABAD

"Thesis submitted to the Department of Sociology, Quaid-i-AzamUniversity, Islamabad, for the partial fulfilment of the degree of Master of Science in Sociology".

AminaAkmal

Department Of Sociology

Quaid-i-Azam University, Islamabad

Quaid-i-Azam University, Islamabad
(Department of Sociology)

FINAL APPROVAL OF THESIS

This is to certify that we have read the thesis submitted by Ms. Amina Akmal , it is our judgment that this thesis is of sufficient standard to warrant its acceptance by the Quaid-i-Azam University, Islamabad for the award of the Degree of "M.Sc in Sociology ".

Committee

1. Dr. Muhammad Zaman
   Supervisor

2. Dr. Mazhar Hussain Bhutta
   External Examiner

3. Dr. Sadia Saeed
   Chairperson Dept. of Sociology

Sadia Saeed

Acknowledgement

All praise belongs to Allah who is most merciful and most beneficent and also have utmost respect for His Holy Prophet (P.B.U.H) who made us capable to recognize the creator. I would like to thank Almighty Allah who gave me the courage and showed me the path and provided me spirit to complete my academic goal. I feel highly honored to express my heartiest gratitude for my supervisor, Dr. Muhammad Zaman for his skilled guidance and full moral support. He is always there to guide me in there special way. I am also obliged to my respected teacher Mr.Farhan Ahmad Fiaz, Mr.Sarfraz Khan, Dr.Sadia Saeed for their kind attention that enriched me with the knowledge of sociology. I am highly thankful to my parents and family for supporting in every sphere of life. Without their support, it would not have been possible to achieve my aims. May God bless them in the entire world! Finally, I am thankful to all those friends who have helped me in my research. I am happy that my all the respondents cooperated with me during my research work.

Amina Akmal

ABSTRACT

Higher education conveys vast consequence and it has a definitive in human capital development. It has most significant part for the economic enablement of a country because it is the way to get from those who are foreign, learn skills from them and use them in their own country for prosperity. As we compare Pakistan with other countries of the world, the condition of cybercrime in relation to higher education, acts are not less to the mark among those countries that are in cybercrime index. The less availability of employment in Pakistan has increasing trend of cybercrime. Therefore, the quantitative study was conducted in Quaid-i-Azam University Islamabad. The sample size was of 120 respondents and tool used for data collection was the structured questionnaire. In order to analyze the data, the researcher used SPSS version 16.0. According to the current study, higher education does not meet the demands of common people that lead them to cybercrime in order to meet their demands of common life. The significance level was less than 0.05. That is why, alternative hypothesis was accepted and null hypothesis was rejected. The researcher concluded that higher education of some people paves the way for cybercrime. Less opportunities of market for the workers leads to involve in criminals activities. While the trends of having lavish life style is also the cause of joining criminal activities.

Table of Contents

Chapter No. 1 1

INTRODUCTION 1

1.1 Cybercrime is Threat to Business 3

1.2 Advanced Education of Technology and Cybercrime 3

1.3 Statement of the Problem 4

1.4 Objectives of the Study 4

1.5 Significance of the Study 4

Chapter No. 2 6

REVIEW OF LITERATURE 6

2.1 Higher Education and Cybercrime in Developed Countries 7

2.2 Higher Education and Cyber Crime in Under Developed Countries 11

2.3 Higher Education and Cybercrime in South Asia 12

2.4 Higher Education and Cybercrime in Pakistan 13

2.5 Assumptions 14

Chapter No. 3 16

THEORETICAL FRAMEWORK 16

3.1 Routine Activity Theory 17

3.2 Higher Education and Cybercrime 17

3.2.1 Application of Theory 18

3.3 Routine Activity Theory and Cybercrime 19

3.4 Propositions 20

3.5 Hypothesis 20

3.5.1 Null Hypothesis 20

3.5.2 Alternative Hypothesis 20

Chapter No. 4 21

CONCEPTUALIZATION AND OPERATIONALIZATION 21

4.1 Conceptualization 22

4.1.1 Higher Education 22

4.1.2 Cybercrime 23
4.2 Operationalization 24
4.2.1 Higher Education 24
4.2.2 Cybercrime 25
Chapter No. 5 26
RESEARCH METHODOLOGY 26
5.1 Research Design 27
5.2 Universe of Study 27
5.3 Unit of Analysis 27
5.4 Sample Size 27
5.5 Tools for Data Collection 27
5.6 Tools for Data Analysis 28
5.7 Techniques for Data Analysis 28
5.8 Pretesting 28
5.9 Ethical Concern 28
5.10 Opportunities and Limitations of the Study 28
Chapter No. 6 29
RESULTS 29
Chapter No.7 53
DISCUSSION AND CONCLUSION 53
7.1 Discussion 54
7.2 Conclusion 56
REFERENCES 58
ANNEXURES 62

List of Tables

Table No 6.1 Respondets Gender 30
Table No 6.2 Respondents Age 30
Table No 6.3 Respondents Education.. 31
Table No 6.4 Family Pattern.. 31
Table No 6.5 Occupation of the Respondents 32
Table No 6.6 Marital Status.. 32
Table No 6.7 Higher Education and Advanced Technology.. 33
Table No 6.8 Technical Education and Higher Education 33
Table No 6.9 Expectations and Future.. 34
Table No 6.10 Highly Educated and Harm Society.. 35
Table No 6.11 Study Courses and Commit Cybercrime 35
Table No 6.12 Acquiring Specialization Without Education 36
Table No 6.13 Opportunities for Work Experience.. 37
Table No 6.14 Educational Liberty and Free of Speech.. 37
Table No 6.15 Higher Education and Unethical Behavior.. 38
Table No 6.16 Students Read Syllabus Only if Something Goes Wrong....... 39
Table No 6.17 Role of Educated People Against Cybercrime Fight.. 40
Table no 6.18 Knowledge About Cyber Security.. 40
Table No 6.19 Victim of Cybercrime 41
Table No 6.20 News About People Being Harassed Online 41
Table No 6.21 Cybercrime and Social Life 42
Table No 6.22 Guidance Government Officials and Cyber Security Risks ... 42
Table No 6.23 Cyber Security Professionals and Cyber Threats 43
Table No 6.24 Cyber Threats for Organizations.. 44
Table No 6.25 Cybercrime and State-Sponsored Hacking.. 44
Table No 6.26 Conflate Higher Education with Ability.. 45
Table No 6.27 Cyber Attacks Against Government Networks 45
Table No 6.28 Unit to Deal with Cybercrimes Incident Response.. 46

Table No 6.29 Cybercrime Courts 47

Table No 6.30 Theft of Email Id.......... 47

Table No 6.31 Computer Hacking 48

Table No 6.32 Online Malicious Code 48

Table No 6.33 Interception of Computer Data 49

Table No 6.34 Internet Pornography 49

Table No 6.35 Damage to Computer Systems or Data 49

Table No 6.36 Information Developmental Cybercrime 50

Tabel No.6.37 Higher Education and Cybercrime 51

Table No 6.38 Chi - Square Test 51

List of Figures

3.1 Routine Activity Theory and Cybercrime..........19

Chapter No. 1
INTRODUCTION

Cybercrime is a crime related to the computer that is why it thought that only higly educated can be involved in cyber crimes as it is not like other armed crimes. A higly trained person in internet and computer knowledge can hack a system. Brenner (1973:379) stated that growth of industry, increase in the economy and rise in urbanization has also increased the rates of crimes. So the rates of the crimes are higher in the urbanized cities. There are some factors which may influence crimes as inflation, income inequality, low standard of education and poverty. Unemployment is also a main factor that is involved in cybercrimes.When youth, able to do work but fail to find any job orwork, gets upset then many disturbances can occurs. This defeat often leads to leave or weak the social bonding of the young man. There is lot of chances the involvement of same guys in the easy way earning money which can leads them to some odd or may into cybercrime activity. They observed twenty-first century trenditions of similar tricks and the same is going on with other customary wrongdoings, for example, robbery, blackmailing and provocation.

Yorke (2010:19-20) stated that individuals around the world profited somehow from the wing of the internet and the openings it has given. Regardless of whether through mainstream long range interpersonal communication destinations like Facebook, the growth in online trade evidently representing more than eight percent of retail deals in Britain alone or the coming of web based managing an account, the web is currently a crucial piece of regular daily existence in vast parts of the world. The uses of the internet are broad. Data and communication advancements help run our vehicle frameworks, vitality and asset supplies, and modern working frameworks. However, with developing reliance comes more noteworthy powerlessness and hazard from deceitful people who wish to bring about damage, or look for money related or individual increase, through their activities. In spite of the fact, familiarity with these dangers is expanding, a great part of the present civil argument is accumulated at the approach or military level. How then can culture overall be educated and arranged to meet this danger and how might it be urged to be a piece of a far reaching arrangement.

1.1 Cybercrime is Threat to Business

Yorke (2010:20-21) revealed that the variety and nature of dangers from the internet, and their potential damage; has caught the consideration of strategy producers, government officials and the media. In the internet, individuals know how totake steps with comparativefreedom, below the shelter of namelessness. Dangers can come similarly from states, fanatic or fear gatherings, singular programmers, and sorted out hoodlums - among others - who can use control unbalanced to the exertion or resources required in the physical world. It was mentioned in the article, the National Security Strategy expressed that 'administration, the private area and natives are under supported digital attacks today, from both threatening states and offenders.' It recorded such assaults as a top need 'Level One' danger to national security and reserved simply over $1 billion (£650 million) to counter it; over $240 million (£150 million) more than already expected. Dependence on the internet is just responsible to increment while the limit of governments and industry to tolerate and bear the hazard reduces. Advancing more prominent mindfulness and individual obligation is essential not only for its own particular purpose but rather as a component of managing a significantly more extensive risk.

1.2 Advanced Education of Technology and Cybercrime

Pool (2013:299) stated thatwith the fast movement in communication innovation, there had been a development in personal computers related assaults gone for both the equipment and programming of nations personal computer frameworks. Some of these assaults are private performers working for their own particular objectives, yet different attacks are submitted by countries trying to adventure shortcomings in their foes 9 personal computer innovation frameworks. In spite of more successive events of these digital assaults, the universal group still cannot seem to embrace a system to represent the guidelines countries are to follow in this new field of fighting. This remark revealed the historical backdrop of digital fighting and the modem digital weapon countries and private performers are using in this new combat zone. This remark then shows the current lawful structure government acquiring outfitted clashes and its appropriateness to digital fighting. Additionally examined inside this remark is the means by which digital secret activities could assume a part in molding global law. This remark covers proposed thoughts identifying with what structure could administer digital fighting and what that system could substantively.

1.3 Statement of the Problem

Higher education and cybercrime is used as a subject of scientific studies; and much concentration have been given to their impact on society. Less educated people mostly are unaware about the cybercrime. Often it is associated with the highly skilled or educated people. This study is intended to focus on the question: does higher education and cybercrime are associated with each other?

1.4 Objectives of the Study

1. To highlight the main causes of the frequently occurring of cybercrime at Quaid-i-AzamUniversityIslamabad in different shapes.
2. To explore the impact of higher education on cybercrime in educational premises.

1.5 Significance of the Study

This study has both hypothetical and concrete consequence. Although a number of studies conducted on cybercrime and their impact on development and environment, this is the first sociological analysis of cybercrime. In this way, this current research provides theoretical knowledge on higher education and cybercrime and their consequences in academic and working areas.

Secondly, this research has a practical significance for other universities and institutes. The institute can thus be able to recognize the root causes of cybercrime and its negative consequences for society. Apart from the local community, the local arbitration system can also acquire knowledge in order to address one of the main issues which undermine development and deteriorate the society further.

Chapter No. 2

REVIEW OF LITERATURE

2.1 Higher Education and Cybercrime in Developed Countries

Saban, McGivern and Saykiewicz (2002:30) stated that in the past, cyber experts regularly make and plan for future cyber activities, some times they even used to bought ideas from other experts in order to improve their skills in particular field of cybercrime. In any case, with the current evolution in innovation, criminals at no time in the future essential to leave home to straight their tricks. A gathering of "telephone experts" entered the personal computer frameworks of Sprint, Equifax and even the National Crime Information Center is used in this regard. These people downloaded many calling card numbers, which were sold to Canada, who passed them on to Ohio (City of Cleveland). Those numbers sophisticated toward someone else in Switzerland, and in the end wound up in the hands of organized crimes branches in Italy.

Wilczenski and Coomey (2006:327) stated that cyber directing can take few steps, including helpful programming and web based advising adjustment to few hypothetical methodologies, behavioral, psychological, instructive, and psycho dynamic among them. The improvement of internet cafe take into account immediatly, online contact amongst advisor and customer. Counselling and discussion through the online work is a method for achieving inaccessible zones to guide administrations and additionally, upgrade correspondence among experts. Today, school guides regularly take part in online communication with associates, students and guardians. Mechanical advances are changing regular directing practices in schools while displaying new moral difficulties.

Lane (1984:347-349) stated that in the middle of 1600s and 1700s, few countries started to set up new colleges and universities in zones that had practically zero involvement with academic culture and advanced education. Such a reorientation of the advanced education arrangement moving far from extending the conventional associations and towards institutional development was especially evident in the Baltic states. The Danish model centered upon maintained college focuses, which would be altogether different from the built up organizations, highlighting interdisciplinary and viable significance. The Finnish model was more arranged towards a national development of scholastic culture, presenting customary associations where there had been none. The Norwegian model included both components; from one perspective building up a conventional college in Trondheim and on the other leaving upon institutional advancement making the arrangement of local universities. The strategy procedure in Sweden that brought advanced education into the undeveloped ranges of Norrland was may be the most obvious case of institutional legitimization. The approach took around twenty years actualize and investigation of the closures, means and results of the arrangement may expand our comprehension of the rationale of advanced education change.

Mora (1997:233-240) concluded that the investigation completly granted to reach a few determinations with certainty. As a matter of first importance, it showed that the level of democratization and interest in higher education of various financial gatherings is noteworthy. Regardless of the change in value, less special gatherings are still underrepresented in the higher education population. On the off chance that we consider the word related status of the family, it can be determined that those families whose principle householders are non-talented laborers or farming specialists are definitely underrepresented in the higher academic education. Families with an administrator or expert principle householder are exceedingly spoken. This outcome is totally with the accordance that the families with fundamental householder has low instruction levels and the most under-represented in advanced education. Low educational levels and low gifted employments for the guardians are related with low levels to higher education for their kids. In spite of the fact, that our information does not allow us to investigate the access to various sort of studies from different sources. There is confirmation of self-enrollment in Spain. Offspring of best appraised word related levels take after an indistinguishable track from their folks evaluated word related levels take after an indistinguishable track from their folks. At the point when family pay per family unit part is considered, the portrayal in advanced education is to some degree uniform in all bury intervene and upper salary chooses, while youngsters from families in the last 30 for every penny are underrepresented in advanced education populace. Low family salaries and guardians' low training levels diminish door is open for youngsters to enter advanced education.

Wilczenski and Coomey (2006:330) stated that moral concerns reached out to the nature of separate instruction projects and reachable to them. It is not clear how well an in vivo (crime specialised course) course means separation instructions organize. Brenner (1973:385-391) detailed meta-investigation of the relative separation learning writing in the course of recent decades. The outcomes proposed that unusual utilization of separate training beat their classroom partners on different educational completion results while synchronous applications perform all the more inadequately. A result look into base is expected to think about graduate - level separation learning with conventional in-class courses in fields, for example school advising, which requires that understudies create solid relational abilities and clinical judgment. Although advantageous and disadvantage, remove learning conveys with it a few weaknesses. The relational progression amongst educated people and understudies are distinctive in face to confront than separation instruction set tings. Understudies may have less chance to make inquiries in the light of fact. The coordination of associating on the web are more troublesome, considering difficulties. For example, the planning of inquiries, writing speed, coordination of numerous inquiries, and the need to keep the exchange streaming. Understudy to-understudy cooperation, albeit conceivable is restricted by a similar arrangement of calculated blocks. Galeotti (2013:32) stated that likewise, understudies may scold their correspondence since it is recorded or might be unseemly in connected dialogue since it is depersonalized. Access to the innovation expected to bolster remove knowledge stands a critical thought on behalf of morally capable preparation, to an extent this makes sense. According to the Hyman (2013:18) Cybercrime Report, 556 million of people in the world face cybercrime attacks each year, but this is often the result of ignorance of people. Proper protections would have prevented the risk. Outside the simple issue of having the right defenses, there is a broader and much more problematic question. To what extent the security of Internet compromised by a dangerous grouping of criminals and states (Hyman 2013:18).

Satapathy (2000:1059-1061) stated that it was likewise unbelievable if programmer could be connected to these digital vandals of a month ago. Satapathy (2000:1059) mentioned Programmer alludes to a man who utilizes his aptitude with personal computers to attempt to increase unapproved access to Personal Computers documents or systems. In that sense, the digital vandals being referred to did not hack or pick up passage into the Personal Computers at the sites influenced or trade off any data at these destinations.

Satapathy (2000:1060) stated that these attacks were the most authentic in the chronological background of web which not just actually blackout these fundamental sites for fairly a long time as well made a genuine abrasion in user trust in the web based business itself. In the event that these advanced sites could not prevent digital attacks on themselves, how were they going to make sure person delicate basics and charge card data of consumers. Such incidents were also frustrating to e-organizations, a significant lot of whom nowadays rely on upon the net for time basic buy of data sources. The US government considered attacks imperative and upbraided the same as "vindictive disturbance of honest to goodness business". Satapathy (2000:1061) mentioned that the US lawyer general, Janet Reno, immediately reported a Fedral Bureau Intelligence. examination, while her agent Eric

Holder undermined jail sentences of five to 10 years and fines of US $ Dollar at least 250,000 for the offenders. Later on, president Clinton himself called a crisis summit of web administrators, personal computer security specialists and US government authorities on February 15, entice to discover answers for issues raised by these web strikes. There are reports that the FBI, as well as the US Secret Services and the Pentagon are attempting to flush out the guilty parties with the assistance of personal computer security specialists. Be that as it may, clearly the pursuit is difficult.

2.2 Higher Education and Cyber Crime in Under Developed Countries

Cassim (2011:123) explained that cybercrime is thriving on the African continent. The increase in broadband access had resulted in an increase in internet users. Thus, Africa had become a safe heaven for online fraudsters. African countries are worried with burning issues such as poverty, the Aids disaster, the fuel crisis, political instability, cultural instability and traditional crimes, such as murder, rape and theft. As a result, the fight against cybercrime is layer behind. The lack of Information technology knowledge by the criminals and the deficiency of appropriate legal frameworks to treaty with cybercrime at general and provincial levels have compounded the harms.

Strydom and Fouire (1999:155) presented an authentic outline of the advancement of higher education look into in South Africa by concentrating on past accomplishments and conditions and present and future difficulties. An effort is rolled out to call attention to the improvements in both the unique circumstance and worldview of advanced education examines. The policy maker represent how examine concentrations and strategies were formed by the political plan of the old South Africa, and highlight the issues which advanced education as now and later on should address as a major aspect of the change procedure of advanced education, as well as of South African culture in general.

2.3 Higher Education and Cybercrime in South Asia

Enginner et al.(2010:4-5) explained that educators and understudies' associations, grass-roots gatherings, scholastic and social activists from 16 unique states speaking to the All India Forum for Right to Education are profoundly upset at the arrangements of systemic withdrawal of the State from higher (counting proficient) instruction being sought after heartlessly by the focal government. These strategies are plainly intended to build the pace of privatization and commercialization of advanced education, bringing about fast increment in the cost alongside fall in the nature of training. At the base of such approaches is the disturbing choice of the legislature to make instruction at all levels, including school training, a trade-capable item and, accordingly, a wellspring of benefit. At any rate on account of advanced education, these strategy measures appear to be an outcome of the offer made by the administration in the General Agreement on Trade in Services (GATS) to bring advanced education under the World Trade Organization (WTO) administration as trade-able services in order to raise up their level in every stander that make people able to have skills in every aspect in respective field.

O'Neil (2001:28-31) stated that mechanical developments make it harder to catch criminals or spies is not new. The appearance of the phone additionally constrained law requirement to reevaluate its investigative devices. Fighting expert uncover an extraordinary arrangement about how the administration sees the difficulties to law requirement in the Digital Age. Modern psychological oppressors may bring down the country's electrical framework. So, new security measures are vital. The country's phone framework is going advanced. So, real modifications must be made to guarantee law implementations proceeded with capacity to wiretap crooks and spies. Disavowal of administration assaults against Internet organizations must be anticipated. So, the extent of existing personal computer violations must be extended to cover harms, created by failure of business. Another administration device whose application to the digital age has raised concerns is the pen-enrol; a gadget used to record the numbers dialed to start a phone discussion. Catching the real discussion requires a warrant in view of a high evidentiary appearing. Getting the number dialed requires just the administration's accreditation that the number is pertinent to a continuous criminal examination. Revisions made in 1986 (O'Neil 2001:30) to the pen enroll law have been deciphered by the administration to stretch out pen enlist requests to email messages. Since there is no all-around characterized parallel between a phone number and an email address, applying pen enlist requests to email has raised worries about the constantly broadening extent of government interruption into Internet correspondences.

2.4 Higher Education and Cybercrime in Pakistan

Rasool (2015:21-34) stated that cybercrime hazards in Pakistan is a growing phenomenon. Improper management and restrictions in respect to cyber security may increase more problems and trials for Pakistan. In the parallel approach, it is not safeguarding its digital websites. In this way, Pakistan is misplacing its national groundwork powers. In Pakistan, cybercrime has been growing into the organizations of banking, education along with army and administration zones. However, Pakistan failed to keep secure its official bounds. The foremost zones of Pakistan are facing cyber illegal contact difficulties. Pakistan has still not established advanced schemes to certify its safety from cyber dangers. Now, the private data of a common person or government is not safe, so it come to be a general danger for Pakistan. Although for this serious problem, laws had previously approved but not operated. Cyber bill had approved by the parliament but government and other stakeholders were not considering this issue. The banking sectors of Pakistan providing facilities of online banking but their systems fail to secure their clients' accounts. In banking regions ATM scams have come to be are very common. Hackers install skimmer devices in ATM machines and they hack card details, money and other personal information of the peoples from their accounts. Some banks of Pakistan suffered cyber assaults and they misplaced enormous amount of currency, like Alied Bank of Pakistan, network was hacked many times.

Cyber conflict is much complicated than the traditional pressures within Pakistan and India. Pakistan is not compensating full consideration to the field of technology, however India financing much more in this field in the sense to generate more severe dares regarding cyber warfare. Israel also provides services to India against Pakistan. That is why Indian hackers control to Pakistani hackers in breach the safe borders of cyber barriers.

According to Memon and Awan (2017:2) Pakistan has an inhabitants of 182.1 million, and youth underneath the age of 25, 63% of the overall population. From this young community, more than 80% are internet users, and the mainstream of them are "netzians." Youth has the ability to transfer their country into the next level of political and commercial liberation, if it can essentially organized. The young educated students are working in different fields for human rights, labor rights, media, science and technology. All these fields are vital for the asset and establishment of the country. Young people are new leaders and use cyber process in elections for fair results, which is highly acceptable by the young population of Pakistan.

2.5 Assumptions

1. Higher education is a way towards success and earn money.

2. Cybercrime is mind game crime commit by technical person who has bookish knowledge as well as pragmatic.

3. People who are not highly educated are also doing such acts in technical way.

4. Cybercrime is used as passion to attract other people to fall in their web of victim.

Chapter No. 3

THEORETICAL FRAMEWORK

3.1 Routine Activity Theory

Routine activity theory developed by Marcus Felson additional studied by Madero-Hernandez and Fisher (2012:13-27) stated that three principles involved in committing crime. These principles are:inspired criminal, a suitable target and nonappearance of an expert guardian. The factors that cause a particular target attractive are situation and crime specific.

The systematic meeting point of the routine activities takes a macro-level analysis and highlights macro shifts in the patterns of sufferer and criminal activities. It emphases on particular criminal actions and offender judgements. Routine activity theory is based on the supposition that crime can be committed by anyone that has the chance. The theory moreover stated that sufferers are specified varieties on whether to be targets mostly by not placing themselves in circumstances where a crime can be committed against them.

3.2 Higher Education and Cybercrime

The theoretical approach on higher education and cybercrime is a genuine problem of the modern society. Higher education is not the problem but by this the crime happens especially that is the root issue of current situation, which causes heave loss to our society both morally and economically. Per this theoretical perspective cybercrime happen on the basis of motivation and this type of motivation offender acquire while learning through education. It is true illiterate people do not know how to use computer and how to run any software, so it is directly linked with education, so Higher the education higher the motivation and higher the skills of cybercrime. Cybercrime can be stopped by education, imparting it in right manners, and technology would use against it. There is one hurdle that can only be removed by higher education and use of skills in right way. Unemployment is one of the main hurdle that compel people to commit such type of crimes, highly qualified people when get no any job on their standard level they chose this way to earn easy money.

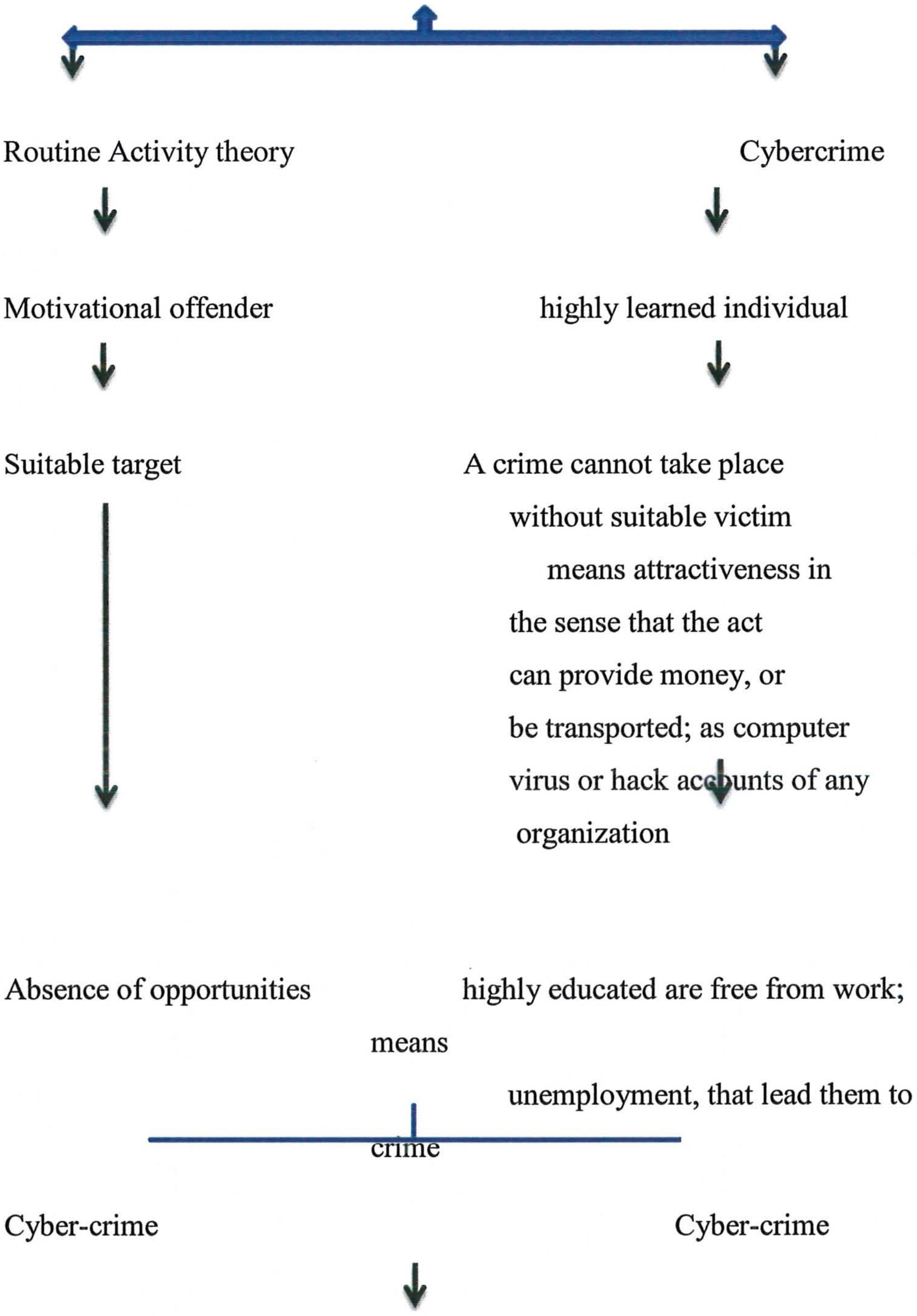
Wholly it is that higher education causes the cybercrime in one aspect or another.

3.2.1 Application of Theory

Quaid-i-AzamUniversity was one of the peaceful area of the Islamabad, everyone used to work and study without any tension. This area is regarded as the educational hub area of the Islamabad and this area is developed for study purpose. In this institution online work has been done by online computer system, such as students are connected through internet. In very early days they worked peaceful and no anyone try to interfere in others' work. In that time people were educated regarding online system. As time passes people become educated in this way they became employed in industries and banks and in other sectors. Day by day the ratio of higher educated become increase. The rising ratio effect negatively, in sense jobs becomes short and highly educated individuals inclined to other side in order to fill the earning gap that is cybercrime. In this way routine activity theory can be applied on higher education and cybercrime.

In current situation rising ratio of population with higher education and multi-skills are the cause of cybercrime and this context their education serves them as guidance by which they commit cybercrime. Cybercrime in the sense the hacking of the bank accounts and enter in the privacy of industry such as stealing the designs of new variety and then they sell to other companies by which respective or victim company suffers a heavy loss. In this way higher education causes cybercrime.

3.3 Routine Activity Theory and Cybercrime



Routine Activity theory

Motivational offender

Suitable target

Absence of opportunities

Cyber-crime

Cybercrime

highly learned individual

A crime cannot take place
without suitable victim
means attractiveness in
the sense that the act
can provide money, or
be transported; as computer
virus or hack accounts of any
organization

highly educated are free from work;
means
unemployment, that lead them to
crime

Cyber-crime

To find out the gap that how higher education cause cyber-crime.

Figure 3.1 Routine Activity Theory

Above figure Figure 3.1 showed that any work which you intent to do can be occurred when any force compelled you or motivate you. The researcher applied it on cybercrime in that way that cybercrime is a crime which is motivated by learning, it may be from education or experiences. On second step theory states that whenever any offenders intend to commit crime he set target and that fit his criteria. The researcher applied it on crime cannot take place without suitable victim means attractiveness in the sense that the act can provide money, or be transported; as computer virus or hack accounts of any organization. At last step theory states that absence of opportunities paves the way for people to commit cybercrime. It means workless people indulge to commit cybercrime to earn easy money.

3.4 Propositions

1) In urban areas day by day cyber-crime getting its roots tight, that creates unrest in the society.
2) Highly educated people are paying more attention to learn skills of cyber-crime that is alarming for the future of upcoming generation.

3.5 Hypothesis

Higher education cause cybercrime.

3.5.1 Null Hypothesis

H_o: Highly educated and skills persons are not involved in cybercrime.

3.5.2 Alternative Hypothesis

H_1: Highly educated and skills persons are involved in cybercrime.

Chapter No. 4

CONCEPTUALIZATION AND OPERATIONALIZATION

4.1 Conceptualization

Conceptualization is one of the main parts of quantitative and qualitative social research. It is a systematic process in which researcher shape the important concept and variable research with the help of authentic and research based literature. In this research the researcher has opted two variables one is higher education and second one is cybercrime. These concepts are conceptualized here.

4.1.1 Higher Education

"In higher education educators seem to take the ideals described above seriously and practically and to teach and relate to children accordingly, instead of rationalizing and convincing them- selves ex post facto that existing practices are consistent with such ideals" (Walberg and Thomas 1972:198).

According to the view Walberg and Thomas higher education is something where educators try to impart theoretical as well as practical education to the learners respectively.

Kaufman (1968:415) stated that "In Higher education, we are attempting to meet needs: needs of society, needs of learners, and needs of educators to be responsive to requirements placed upon us by those we strive and serve".

Further the higher education elaborated by Kaufman he explained higher education in broader sense that it is as a tool to meet the essential needs of society, society as a aspect those who are learners within society and these are the responsibilities of those who serve in this regard.

According to Thompson (1992:52) "Higher Education is crucial for your personal happiness and for your qualifiedsatisfaction . We trust that the best possible training for a fruitful future is a rich and satisfying experience in your higher education itself".

In the definition of Thompson that higher education is the ingredient of happiness in the sense of professional satisfaction, and he adds that higher education is the step to the successful future.

Higher education is the name through this one learn the things at advance level for him demands. Higher education at some level serves the role to help offender and make him skilful.

4.1.2 Cybercrime

Different authors defined cybercrime differently. According to Cassim (2011:123) "Cybercrime or 'computer crime' seems to have no precise definition. On the one hand, a computer may become the object of a crime when theft of a computer hardware or software occurs". Above definition of cybercrime is defined as it is linked with computer system, by computer these types of crimes take place it sometimes in the shape of hardware and sometimes in the shape of software.

Unlike this definition, Ploom (2003:576) addressed shortcomings and defining cybercrime in "the wording of the necessary elements of computer crimes in the Penal Code, suggests possibilities for interpreting some of the elements of such crimes and proposes solutions to problems encountered or to be countered in practices". The author argues that huge harmas a fundamental component of personal computers damage is unjustified, as on Estonia's promotion to the digital wrongdoing tradition, this reservation was not made. The spread of personal computer infections may happen by inaction, how to characterize the evacuation of a code, secret word or whatever other defensive means as an essential component of such an offense as personal computer hacking and whether personal computer tramping is culpable under the Penal Code. Examining the arrangements with respect to personal computer related extortion; the creator contends that there is no reference to the illicitness of the demonstration. Furthermore, the creator looks at whether salary not got and non-exclusive harm qualify as harm brought on by digital wrongdoing.

According to Gordon and Ford (2006:13) "Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes)". The overhead definition define that cybercrime is something that consist of many things as doing illegal actions as hacking the accounts of others and online money laundering etc.

The comprised definitionsof cybercrime is that it is act that harm property of the victim, offender select the particulecase and attract some centre of attraction, in this concern knowledge plays important role to find information from multiple sources.

4.2 Operationalization

The process of defining by which the researcher gives their own observation based perceptions about the variables. The researcher clearly justifies and identifies the concepts of the existing situation which used in present study.

4.2.1 Higher Education

All scholars have defined higher education accordingly, but the researcher conducted current study in Quaid-i-Azam university, Islamabad. The area selected for research has high ratio of higher educated people. Many of the people pay their full emphasis on higher education in order to manage status quo in society in every aspect. According to the area the definition fits as higher education is the form of happiness by learning new and advance things, by these people become happy and this happiness guarantees them success in the way where they go. After higher education they become well prepared to search their earning sources.

4.2.2 Cybercrime

The research was based on students and on their area based perception that how the cybercrime is happening in their respective areas, the mood of it varies area to area, the researcher had depicted it by explaining in these terms. The area which was selected for research is also dense in population and the portion of the youth is slightly higher than others. So the other people of the society have the perception higher educated people are there. The youth is the younger part of the sector who are highly educated, which is in search of work and do not find any suitable work. In order to fill their earning gap they always try to find way to earn easy money. The people of this area are highly expert in using computer based applications. Their skills are the source to indulge them to commit cybercrime, because cybercrime is the source to earn money in different shapes.

Chapter No. 5

RESEARCH METHODOLOGY

5.1 Research Design

The design of this research is quantitative in nature. The nature of the quantitative research is easy to describe the data gathered from respondents. The researcher used survey method and data was collected through structured questionnaire.

5.2 Universe of Study

This researchwasconducted in the Quaid-i-Azam University, Islamabad. The data collected from the people who have some knowledge regarding the cybercrime. This area was chosen by the researcher because the researcher is the student of the this university and some of the cases were found in this regard, so the researcher select this area for current research.

5.3 Unit of Analysis

The target population of the research was respondents of the area of Quaid-i-Azam University, especially the people from the age of 18 to 30 who were studying in MS.c, MPhil and PhD.

5.4 Sample Size

It was difficult for the researcher to collect the data from whole population. In this research, the researcher chose 120 respondents for the purpose of sampling from the area of university.

5.5 Tools for Data Collection

The most used technique to gather data is survey. This method is found to be the most appropriate for the data collection. The researcher used a structured, close ended questionnaire. The questionnaire was made in English language.

5.6 Tools for Data Analysis

The statical package for social sciences (SPSS) was usedfor data analysis. The researcher used this scientific approach the real and to the point result after the process of some statistical tests.

5.7 Techniques for Data Analysis

The researcher used descriptive and inferential statistics. Percentages, frequencies, and chi-square tests checked the relativity and relation of the data.

5.8 Pretesting

The researcher took (20) twenty respondents in order to pretest the questionnaire. The respondents were taken in a way that they were also belonging to the area of the research.

5.9 Ethical Concern

The maintenance of ethical concerns is important. When the researcher was conducting the research, she asked the questions in way that people feel friendly to respond. Any of the respondents was not gone under any sort of puzzlement and ignominy. It was the due responsibility of the researcher to maintain all the information of the respondents.

5.10 Opportunities and Limitations of the Study

The researcher studied the area well before starting the research and she was having well knowledge about the area. So it was an easy opportunity for her to answer the questions as respondents were easily available.

Chapter No. 6
RESULTS

In this part the researcher has given the inclusive summary of the section features and interpretations. Different tables are constructed and brief interpretations of each table have been given. The percentages and frequencies are mentioned in tables. First of all researcher provided the table of demographic information of the respondent.

Table No 6.1 Respondets Gender

Sex of the respondent	Frequency	Percent
Male	81	67.5
Female	39	32.5
Total	120	100.0

Table No 6.1 showed that majority of the respondentswere male because it was handy for researcher to collect the data from male respondents of the society for being a easy access or availability of them. While a proportion of female respondents was also in the data collection. It is because most of the cybercrime reports are against male that is why male respondents were regarded as essential.

Table No 6.2 Respondents Age

Age of the respondent	Frequency	Percent
18-22	34	28.3
23 -28	79	65.8
29 or above	7	5.8
Total	120	100.0

Table No 6.2 describe that majority of the respondent were aged from the group of 23-28 because the higher educated people fall under this category now a days cybercrime rate mostly exist in young generation so the percentage of this group is high.

Table No 6.3 Respondents Education

Education of the respondent	Frequency	Percent
Bachelor	21	17.5
Masters	50	41.7
M.phl	23	19.2
P.hd	17	14.2
any other	9	7.5
Total	120	100.0

Table No 6.3 revealed that most of the respondents were Masters with a frequency and percentage of 50 and 41.7 percent accordingly. 19.2 percent of the respondents were M.PHIL, 17.5 percent of the respondents were Bachelor degree holder, 14.2 of the respondents were P.HD and 7.5 respondents are others. This ratio is high because expert people are involed in cybercrime they are highly learned due to this, in case they do not meet the criteria of their deserving job they become involved in crime to meet their ends.

Table No 6.4 Family Pattern

Family pattern of the respondent	Frequency	Percent
Joint family system	35	29.2
Nuclear	69	57.5
Extended	16	13.3
Total	120	100.0

Table No 6.4 showed that majority of the respondents belonged to nuclear family type with the frequency and percentage of 69 and 57.5 percent accordingly. The current universe is not so much tradition to have multiple system of family structure. Family pattern matters because large family face large problrms so it was the need to get multiple family pattern for current study.

Table No 6.5 Occupation of the Respondents

Occupation of the respondent	Frequency	Percent
Employed	18	15.0
Unemployed	29	24.2
Student	71	59.2
Business	2	1.7
Total	120	100.0

Table No 6.5 described that majority of the respondents was students with the frequency and percentage of 71 and 59.2 percent. Unemployed respondents are with the frequency of 29 and 24.2 percent. Data mostly collected from unemployed and students because the researcher used to get factual information so he tried to collect the maximum data from unemployed and students respondents to understand the core of the issue of the problem.

Table No 6.6 Marital Status

Marital status	Frequency	Present
Single	80	66.7
Married	33	27.5
Divorced	2	1.7
Widowed	1	.8
Separated	4	3.3
Total	120	100.0

Table No 6.6 illustrated that majority of the respondents were single and not married yet because the age group that was selected for data collection was young and teen age group to know about the higher education and cybercrime.

Table No 6.7 Higher Education and Technology

Higher education meets the demand of advanced technology	Frequency	Present
Strongly agree	31	25.8
Agree	75	62.5
Somewhat agree	13	10.8
Disagree	1	.8
Total	120	100.0

Table No 6.7 describe that majority of the respondents were agree with the frequency and percentage of 75 and 62.5 percent that they think higher education meets the demand of advanced technology. With the frequency of 31 and 25.8 percent of the respondents were strongly agree, 13 and 10.8 percent of the respondents were somewhat agree, and only 1 respondent was disagree that higher education not meets the demand of advanced technology. The overall data in the table indicates that higher education is meeting the demand of technology and it is this higher education which is providing the base for cyber crime. It is because the the educated youth have the capacity to use technology in different ways.

Table No 6.8 Technical Education Fit into the Aims of Higher Education

Technical education fit into the aims of higher education	Frequency	Present
Strongly agree	40	33.3
Agree	62	51.7
Somewhat agree	14	11.7
Disagree	4	3.3
Total	120	100.0

Table No 6.8 elaborate that majority of the respondents were agreed with the frequency and percentage of 62 and 51.7 percent that the technical education fit into the aims of higher education, Or 40 and 33.3 percent of the respondents were strongly agreed, and with the frequency of 14 and 11.7 percent of the respondents were agreed somewhat, 4 and 3.3 percent of the respondents were disagreed that they do not think that the technical education fit into the aims of higher education. Students, having the technical education, lead to the introduction of a modern world. They have overcome the different problems regarding the basic needs of life. They have invented all the such things which have provided a man a great level of easement.

Table No 6.9 Expectation About Higher Educated Student as Product of Future

The existence of expectation about the higher educated student as product of future	Frequency	Percent
Strongly agree	62	51.7
Agree	45	37.5
Somewhat agree	13	10.8
Disagree	0	0
Do not know	0	0
Total	120	100.0

Table No 6.9 point out that majority of the respondents were strongly agreed with the frequency of 62 and 51.7 percent think that higher educated students are as product by future. 45 and 37.5 percent of the respondents were agreed or with the frequency of 13 and 10.8 percent of the respondents are somewhat agreed with educated student as product by future. Because people are keen to live the life in the better way. Education is necessary for providing a standard life style.

Table No 6.10 Highly Educated People do not Harm Society

Highly educated people do not harm society	Frequency	Percent
Strongly agree	50	41.7
Agree	52	43.3
Somewhat agree	14	11.7
Disagree	4	3.3
Total	120	100.0

Table No 6.10 figure out that majority of the respondents were agree with the frequency of 52 and 43.3 percent think that highly educated people do not harm for the society. The respondents with the frequency of 50 and 41.7 percent were strongly agree or 14 and 11.7 percent of the people were agree somewhat with this thing. With the frequency of 4 and 3.3 percent of the respondents were disagree that they don't think so. Ehducated people are well aware of ethics and morality. Education have fed them with positive nature. They have well polished minds and positive thoughts,so they can be beneficial but not harmful for the society.

Table No 6.11 Study Courses Included Anything which Causes to Commit Cybercrime

Study courses included anything which causes to commit cybercrime	Frequency	Present
Strongly agree	37	30.8
Agree	62	51.7
Somewhat agree	18	15.0
Disagree	0	0
Do not know	3	2.5
Total	120	100.0

Table 6.11 shows that majority of the respondents were agree with the frequency of 62 and 51.7 percent that they think the specialized courses of study within the program included anything which causes a person to commit cybercrime. With the frequency of 37 and 30.8 percent of the respondents were strongly agree or 18 and 15.0 percent respondents were agree somewhat and with the frequency of 3 and 2.5 percent of the respondents have no knowledge about this.Students ,concerned with the fields of computer science, are involved in bank robberies by shifting money from one account to another. They can do so without any weapons and arms. Higher studies of computer science lead them to earn money in the most easy way without any hardwork.

Table No 6.12 Acquiring specialization without education

Acquiring specialization without education	Frequency	Present
Strongly agree	37	30.8
Agree	47	39.2
Somewhat agree	25	20.8
Disagree	10	8.3
Don’t know	1	.8
Total	120	100.0

Table No 6.12 illustrates that majority of the respondents were agreed with the frequency of 47 and 39.2 percent that they think without higher education people have specialization on their own by daily experiences. 30.8 respondents replied they are strongly agree or 20.8 percent respondents are agree somewhat and with the frequency of 190 and 8.3 percent respondents were disagree with this and .8 percent respondents do not have knowledge about this question. People have acquired skills in the other fields like to sew the clothes, cooking and other works. Education is not necessary for these fields. They have learned these specialities from their own single teachers.

Table No 6.13 Opportunities for Work Experience

Opportunities for work experience	Frequency	Present
Strongly agree	59	49.2
Agree	25	20.8
Somewhat agree	8	6.7
Disagree	27	22.5
Do not know	1	.8
Total	120	100.0

Table No 6.13 reveals that majority of the respondents were strongly agreed with the frequency of 59 and 49.2 percent that they think opportunities are available to gain work experience. 20.8 percent respondents were agreed and 6.7 respondent were agreed somewhat, 22.5 percent of the respondents were disagree that they do not think so and only with the frequency of 1 and .8 percent of the respondents were don't know about this question. People can gain experience in any field without any hurdle. Vast majority of professional fields are found in Pakistan.

Table No 6.14 Educational Liberty and Free of Speech

Educational liberty extends beyond the regular restictions of free speech	Frequency	Present
Strongly agree	20	16.7
Agree	50	41.7
Somewhat agree	21	17.5
Disagree	27	22.5
Do not know	2	1.7
Total	120	100.0

Table No 6.14 shows that with the frequency of 50 and 41.7 of the respondents contracted to agree that they believe academic freedom extends beyond the normal boundaries of free speech and for that matter decorum. Whereas 16.7 percent of the respondents are strongly agree with the frequency of 20, and 17.5 percent of the respondents are agree somewhat. With the frequency of 27 and 22.5 percent of the respondents disagreed that they don't think so and 1.7 percent of the respondents have notan idea about this belief. As growing phenomena of capitalization spreads in underdeveloping states, it also came with the characterstics of educational liberty.

Table No 6.15 Higher Education Guides People About Unethical Thing that Harms the Society

Higher education guides people in term of any unethical thing that cause society damage	Frequency	Present
Strongly agree	29	24.2
Agree	60	50.0
Somewhat agree	15	12.5
Disagree	16	13.3
Total	120	100.0

Table No 6.15 describe that those people who think that higher education guides people in term of any unethical thing that cause society damage are agree with the frequency of 60 and 50.0 percent because education guide us in both terms ethical or unethical things. 24.2 percent of the respondents were strongly agree and 12.5 percent replied they agree somewhat or with the frequency of 16 and 13.3 percent of the respondents were disagree that education do not guide peoples for that things which is cause for society damage. Higher education gives a good level of fine sense to a man. They have great perceptions about the things that can damage a society. They make the people aware of unethical things. They direct the people to avoid the unethical things.

Table No 6.16 Students Read Syllabus Only if Something Goes Wrong

Students never read syllabus until something goes wrong	**Frequency**	**Present**
Strongly agree	13	10.8
Agree	41	34.2
Somewhat agree	29	24.2
Disagree	21	17.5
Do not know	16	13.3
Total	120	100.0

Table No 6. 16 explains that majority of the peoples were agree with the frequency of 41 and 34.2 that they agree students never read their syllabus until something goes wrong. Or 10.8 percent of the peoples are strongly agreed and 24.2 percent respondents replied they agree somewhat that students never read their syllabus, 17.5 percent of the respondents disagree with this question and with the frequency of 16 and 13.3 of the respondents don't have any idea about this. Different students have different level of interest regarding their studies. Diligent students pay proper attentions to their studies. On the other hand , careless students play negligence and do not study syllabus until something goes wrong.

Table No 6.17 spell out that those people who think highly educated people are playing the role of the intelligence in the fight of cybercrime are agree with the frequency of 55 and 45.8 percent of the respondents. 40.0 percent of the respondents replied to strongly agree and 14.0 percent of the people were agree somewhat with this idea.7 that makes .2 percent disagree with the statement while 0 percent do not know about the statement. Common educated people do not know know the meaning of cybercrime even. Highly educated people can assist in the prevention of cybercrime.

Table No 6.17 Role of Educated People Against Cybercrime Fight

Role of educated people against cybercrime fight	Frequency	Present
Strongly agree	48	40.0
Agree	55	45.8
Somewhat agree	10	14.0
Disagree	7	.2
Do not know	0	0
Total	120	100.0

Table no 6.18 Knowledge About Cyber Security

Everyone already know about cyber security	Frequency	Present
Strongly agree	34	28.3
Agree	50	41.7
Somewhat agree	24	20.0
Disagree	11	9.2
Do not know	1	.8
Total	120	100.0

Table No 6.18 elaborate that majority of the respondents were agree with the frequency of 50 and 41.7 that everyone already know about cyber security. Or with the frequency of 34 and 28.3 percent of the respondents were strongly agreed and 20.0 percent of the people were agreed somewhat and 9.2 percent of the people were replied that they disagreed, everyone don't have the knowledge about cyber security. Everyone knows about cyber security but no one consider it important to take preciocautions.

Table No 6.19 Victim of Cybercrime

Victim of cybercrime	Frequency	Present
Strongly agree	30	25.0
Agree	44	36.7
Somewhat agree	33	27.5
Disagree	12	10.0
Do not know	1	.8
Total	120	100.0

Table No 6.19 represent that majority of the peoples agreed with the frequency of 44 and 36.7 that they heard of someone who has been a victim of cybercrime. 25.0 percent of the respondents were strongly agree and 27.5 percent of the respondents were agreed somewhat or with the frequency of 12 and 10.0 percent of the respondents replied that they disagree whereas .8 percent of the respondents do not know about this question. Common people , having the bank accounts, and reknown banks are very common victims of cyber crimes. People, commting the bank robbery through cyber crime, transfer the money from one account to another. A student's data regarding the high level research is also a subject of cyber crime.

Table No 6.20 News About People Being Harassed Online

News about people being harassed online	Frequency	Present
Strongly agree	19	15.8
Agree	42	35.0
Somewhat agree	25	20.8
Disagree	29	24.2
Do not know	5	4.2
Total	120	100.0

Table No 6.21 discloses that with the frequency of 42 and 35.0 percent of the respondents were agree that they have many time seen in the news about people being harassed online, or 15.8 percent of the peoples were strongly agree and 20.8 percent of the respondents were agree somewhat regarding news about online harassed.24.2 percent of the peoples were disagree and 4.2 of the respondents were don't know about this question. Facebook is in very common use now-a-days. Harassment is mostly done through facebook. People do the harassment by taunting and giving bad comments.

Table No 6.21 Cybercrime Impact on Social Life

Cybercrime impact on social life	Frequency	Present
Strongly agree	44	36.7
Agree	43	35.8
Disagree	29	24.2
Do not know	4	3.3
Total	120	100.0

Table No 6.21 put forth that majority of the respondents were agree with the frequency of 43 and 35.8 percent that cybercrime impact on social life. 36.7 percent of the respondents contracted to a strongly agree that cybercrime has impacts on social life and 24.2 percent of the respondents replied disagree or 3.3 percent of the people were not know about the statement. It impacts the individual who gone through the incident of cybercrime, it effects the life of individual socialy and psychologicaly.

Table No 6.22 expose to view that majority of the respondents were strongly agree with the 28.3 percent of the peoples that there is general guidance for helping government officials understand cyber security risks and key actions. 25.0 percent of the respondents were agree and 21.7 percent are agree somewhat regarding general guidance and 25.0 percent of the respondents were disagreed with this question. While 6 percent that makes 1.7 percent were do not know. New advanced hacking techniques are introducing day by day. For this reason government officials should also up to date regarding cybercrime security risks, which is not fulfilled by government as required.

Table No 6.22 Guidance Government Officials and Cyber Security Risks

Guidance for helping government officials understand cyber security risks	**Frequency**	**Present**
Strongly agree	34	28.3
Agree	30	25.0
Somewhat agree	20	20.0
Disagree	30	25.0
Do not know	6	1.7
Total	120	100.0

Table No 6.23 Cyber Security Professionals and Cyber Threats

Cyber security professionals are enough to secure networks against cyber threats	**Frequency**	**Present**
Strongly agree	24	20.0
Agree	50	41.7
Somewhat agree	32	26.7
Disagree	8	6.7
Do not know	6	5.0
Total	120	100.0

Table No 6.23 pictorate that those people who think that qualified cyber security professionals are enough to secure networks and data against cyber threats are agree with the frequency of 50 and 41.7 percent. 20.0 percent of the peoples were strongly agree and 26.7 percent of the respondent replied agree somewhat or 6.7 percent of the peoples were disagree and 5.0 percent of the respondents were do not have any idea regarding cyber threats. There are enough seats in every country for security puposes either its cyber or armed.

Table No 6.24 Cyber Threats for Organizations

Cyber threats for private businesses and government organizations	Frequency	Present
Strongly agree	20	16.7
Agree	44	36.7
Somewhat agree	28	23.3
Disagree	26	21.7
Do not know	2	1.7
Total	120	100.0

Table No 6.24 exemplify that majority of the respondents were agreed with the frequency of 44 and 36.7 percent of the peoples that they think economical concerning cyber threats for private businesses and government organizations are happening through this act. 16.7 percent of the peoples were strongly agree and 23.3 percent of the peoples agree somewhat or 21.7 respondents replied disagree to this question and 1.7 percent of the respondent do not have any idea. In this era hackers are much advanced in cybercrime that they can hack any organization either governmental or private.

Table No 6.25 Cybercrime and State-Sponsored Hacking

Cybercrime and state-sponsored hacking	Frequency	Present
Strongly agree	30	25.0
Agree	60	50.0
Somewhat agree	21	17.5
Disagree	7	5.8
Do not know	2	1.7
Total	120	100.0

Table No 6.25 demonstrate that with the frequency of 60 and 50.0 percent of the peoples were agree that it exist a marked distinction between cybercrime and state-sponsored hacking. 25.0 percent of the peoples were strongly agree with the distinction and 17.5 percent of the respondents were agree somewhat or 5.8 percent are disagree and .8 percent of the respondents have no idea about this distinction. Sometime states involved in criminal activities for political purposes.

Table No 6.26 Conflate Higher Education with Ability

Conflate higher education with ability	Frequency	Present
Strongly agree	52	43.3
Agree	44	36.7
Somewhat agree	22	18.3
Disagree	2	1.7
Total	120	100.0

Table No 6.26 decorate the results about those peoples who agree with the frequency of 32 and 26.7 of the total respondents that we can conflate higher education with ability. 56.7 of the respondents were agree and 16.7 of the respondents replied to somewhat agree with this question. Everyone has its unique abilities and higher education only polished them.

Table No 6.27 Cyber Attacks Against Government Networks

Cyber attacks against a government network	Frequency	Present
Strongly agree	44	36.7
Agree	52	43.3
Somewhat agree	22	18.3
Disagree	2	1.7
Total	120	100.0

Table No 6.27 highlights that 43.3 percent of the peoples were agree that they think there is possibilities that cyber attacks against a government network in coming time. With the frequency of 44 and 36.7 percent of the peoples replied to strongly agree and 18.3 percent of the peoples were agree somewhat or 1.7 percent of the respondents totally disagree with cyber-attacks. A recent activity of cybercrime from India shown the cyber threats to the security.

Table No 6.28 Unit to Deal with Cybercrimes Incident Response

Established a unit charged with dealing cybercrimes incident response	Frequency	Present
Strongly agree	21	17.5
Agree	56	46.7
Somewhat agree	28	23.3
Disagree	10	8.3
Do not know	5	4.2
Total	120	100.0

Table NO 6.28 depicts that majority of the respondents with the frequency of 56 and 46.7 were agree that country identified created or established a unit charged with dealing cybercrimes incident response. 17.5 percent of the respondents are strongly agree with this question and 23.3 percent of the people were agree somewhat, 8.3 percent of the respondents were disagree and 4.2 percent people were do not know about this idea. Every country established certain units for serving the publical issues. Pakistan also has aunit to deal with the cybercrimes incidents.

Table No 6.29 exhibit that majority of the respondents were agree with the frequency of 44 and 36.7 percent that specific courts for the trials of cybercrimes is in their knowledge. Rather the 18.3% of the respondents were strongly agree and 34.2% of the peoples were agree somewhat with this knowledge, whereas 8.3 percent of the peoples were disagree and 2.5 percent of the respondents were do not know about the question. Pakistan is also enriched in cyber hackers. So, In 2015, Pakistan developed cybercrime courts for the purpose of identifiying and control over cyber criminals.

Table No 6.29 Cybercrime Courts

Courts for the trial of cybercrime	Frequency	Present
Strongly agree	22	18.3
Agree	44	36.7
Somewhat agree	41	34.2
Disagree	10	8.3
Do not know	3	2.5
Total	120	100.0

Table No 6.30 Theft of Email Id

Online identity theft	Frequency	Percent
Occur frequently	35	29.2
Occur infrequently	38	31.7
Have not occurred	47	39.2
Total	120	100.0

Table No 6.30 indicates the results about online identity theft, with the frequency of 47 and 39.2 percent of the peoples said it has not occurred or 31.7 percent of the respondents replied it occur frequently, 29.2 percent respondents answered occur frequently online identity theft. Online theft of identity is common and hackers can easily hacked accounts.

Table No 6.31 put on views of the respondents about hacking, majority of the respondents said it occur infrequently with the frequency of 59 and 49.2 percent of the respondents. 27.5 percent of the respondents replied that have not occurred and 23.3 percent peoples answered it occur frequently. Computer hacking is very common and can be easily hacked by the hackers.

Table No 6.31 Computer Hacking

Hacking in computer	Frequency	Percent
Occur frequently	28	23.3
Occur infrequently	59	49.2
Have not occurred	33	27.5
Total	120	100.0

Table No 6.32 Online Malicious Code

Online malicious code	Frequency	Percent
Occur frequently	68	56.7
Occur infrequently	19	15.8
Have not occurred	33	27.5
Total	120	100.0

Table No 6.32 showed that majority of the peoples said malicious code occur frequently with the 56.7 percent of the respondents, whereas 27.5 percent of the peoples replied it have not occurred and 15.8 percent of the peoples said it occur infrequently. Online malicious code is a growing phenomenon in which maleware viruses sent to the other's computers to interrupt or hack their system.

Table No 6.33 spell out that majority of the respondents with the frequency of 61 and 50.8 percent of the peoples said illegal interception of computer data occur frequently, 23.3 percent of the respondents said it have not occurred, whereas 25.8 percent of the respondents said it occur infrequently. Hackers easily intercept the data of other's computers which is very in all over the world.

Table No 6.33 Interception of Computer Data

Interception of computer data	Frequency	Percent
Occur frequently	61	50.8
Occur infrequently	31	25.8
Have not occurred	28	23.3
Total	120	100.0

Table No 6.34 Internet Pornography

Internet pornography	Frequency	Percent
Occur frequently	43	35.8
Occur infrequently	50	41.7
Have not occurred	27	22.5
Total	120	100.0

Table No 6.34 showed that majority of the respondents said online trafficking in internet pornography occur with the frequency of 50 and 41.7 percent. 35.8 percent of the peoples argue that it occurs frequently or 22.5 percent of the respondents said online trafficking in internet pornography have not occurred. One of the worse side of internet is pornography. Hackers can easily use this in for their benefits and to blackmail others. Now a days it changed its shape into a profitable business.

Table No 6.35 Damage to Computer Systems or Data

Damage to computer system or data	Frequency	Percent
Occur frequently	36	30.0
Occur infrequently	33	27.5
Have not occurred	51	42.5
Total	120	100.0

Table No 6.35 elaborates that majority of the respondents answered have not occurred intentional damaged to computer system or data with the frequency of 51 and 42.5percent of the respondents, whereas 27.5 percent of the peoples said it occur infrequently and 30.0 percent of the respondents said it occur frequently. Cybercrime is the biggest threat to computer system. Data can be hacked from any country, any region and any organization.

Table No 6.36 Information on Developmental Activities in Cybercrime

Information on development activities in respect of cybercrime	Frequency	Percept
Occur frequently	11	9.2
Occur infrequently	48	40.0
Have not occurred	60	50.0
Total	120	100.0

Table No 6.36 spell out that majority of the respondents answered have not occurred with the frequency of 60 and 50.0 that our country don't provide information on development activities in veneration of cybercrime, 40.0 present of the respondents said it occur infrequently or 9.2 present of the respondents replied that it occur frequently. Pakistan is underdeveloped country which has lack of resources to being updated in developmental activities of cybercrime.

The below Table No 6.37 highlighted that mainstream of the respondents were agreed with the hypothetical statement that highly educated people do not harm society .It meant that higher educated peoples are working for welfare in the society. This result shows that highly educated know technology in positive sense and use it in positive sense that is why highly educate people are no harmful for society they spread awareness among the peoples of the community. It further showed the positive relation between welfare and by advance technology in the era of science.

Tabel No.6.37 Higher Education and Cyber Crime

Higher education meets the demand of advanced technology	Do you think highly educated people do not harm society?				
	Strongly agree	Agree	Somewhat agree	Disagree	Total
Strongly agree	15	12	3	1	31
Agree	30	33	9	3	75
Somewhat agree	5	7	1	0	13
Disagree	0	0	1	0	1
Total	50	52	14	4	120

Table No 6.38 Chi - Square test

	Value	Df	Asymp. Sig.(2-sided)
Pearson chi-square	9.304[a]	9	.410
Likelihood ratio	6.454	9	.694
Linear-by-linear association	.643	1	.423
N of valid cases	120		

The Pearson Chi-Square Value in the above table is 9.304a, Degree of Freedom is 9 and the Asymp. Sig is .410. It was significant because the value was higher than 0.05. So, the alternate hypothesis was accepted and the null hypothesis was not accepted. The rejection of null hypothesis shows that highly educated peoples are not harmful for society and get full advantage from technology in positive sense.

Chapter No.7

DISCUSSION AND CONCLUSION

7.1 Discussion

Patterns of cybercrime vary crime to crime. In the same category, the patterns are also similar to some extent but in other category they become totally different with respect to time, place, target and nature of crime. The patterns of hacking, money theft from accounts, stealing, and so on, are totally different with one another. The findings of this research showed that the problem such as cybercrime because of unemployment, and unemployment arises owing to inconsistency in types and forms of governments, lack or market labor opportunities, limited private sector and corruption. All these factors creates this vary issue of cybercrimes. While in all social institutions fails to hold the grip because these institutions also faced with same problems. To enhance the opportunities for labor market policies must be reviewed. Youth involves in cybercrimes activities by the attraction of the life style or pattern of already existing members of cyber criminalist. In this regard firm grip of law and regulation can survive the portion of youth from criminal activities. While on the other hand education ministry may change its policy towards the various programs, in contact of skills with programs also can make able the youth to have education as well as skills with it, that at least prevent our youth to commit such crimes and make them able to earn handsome money.

Lane (1984:347-349) stated that the 1600s and the 1700s, a few countries started to set up new colleges and universities in zones that had practically zero involvement with academic culture and advanced education. Such as reorientation of the advanced education arrangement moving far from extending the conventional associations and towards institutional development was especially evident in the Baltic states. The anish model centered upon purported college focuses, which would be altogether different from the built .up organizations, accentuating interdisciplinary and viable significance. The Finnish model was more arranged towards a territorial expansion of scholastic culture, presenting customary associations where there had been none. The

Norwegian model included both components; from one perspective building up a conventional college in Trondheim and on the other leaving upon institutional advancement in and in addition making the arrangement of local universities. The strategy procedure in Sweden that brought advanced education into the immature ranges of Norway was maybe the most obvious case of institutional legitimization; the approach took around twenty years actualize and an investigation of the closures, means and results of the arrangement may expand our comprehension of the rationale of advanced education change. Madero-Hernandez and Fisher in (2012:13-27) stated that highly learned people are expert to find easy means to do cybercrime. In this process their academic knowledge properly operated, it was because their skills were not used in the field where it was required. Their unemployment indulged their mind to commit cybercrime.

All in all, cybercrime is thought to be a danger in Pakistan, especially for young students in educational institute because it kills talent, when students are attracted by variety of things they become slight part of education. This is on account of; the young people in addressed could be controlled to undermine the conditions of cybercrime. In contradiction of this substance, there is the necessity by administration at all stages, general collection and diverse associates to leave on immoral occupation formation to yield these young people tainted the avenues. Subsequently, Pakistani pioneers ought to endeavor to advance great administration keeping in mind the end goal to cause youth strengthening, work and financial improvement in various point. Along these lines, in view of the discoveries of the paper it along these lines prescribed that, Pakistani Government need to assume its sacred part by making empowering financial and political environment including the arrangement of framework to make mechanical atmosphere venture inviting. Additionally a bundle of arranged venture ought to be set up, which will hugely prepare the youth with valuable exchange and entrepreneurial abilities in Automobile, Agricultural creation and preparing, coordinated science center and data innovation among others. These things can keep away our student or educated ones from cybercrime shadow.

7.2 Conclusion

Circumstance influences the individual explicitly, especially the circumstance in which the researcher dressed and found out about the diverse qualities of life and nature of family and settings of companions influences stoutly to any criminal in which he grew up. However, few people got the wrongdoing normally. It is anecdotal to resemble their privately-run company. Indeed, even that each part has his own illicit action and which they as often as possible obliging it as their redundant work. Higher education and crimes often relates on many angles in social settings. To test this hypothesis the researcher tested the area on hypothetically depending upon the data. The results showed that majority of people agreed that some educated people play vital role in this regard but most highly educated are not involve in this act, only average people indulge in such attractive things and become culprit. A big proportion was also in the favor of that highly educated know technology in positive sense and use it in positive sense that is why highly educate people are no harmful for society they spread awareness among the people of the community. While, without higher education people have specialization on their own by daily experiences. It means that without higher education people have specialization by their own in this regard. It means people learn while working under the supervision of highly educated people learners get mastery over it then he or she start doing cybercrime to earn easy money. According to the current findings, the significance level was less than 0.05 that is why alternative hypothesis was accepted and null hypothesis was rejected. The researcher concluded that higher education of some people paves the way for cybercrime. Less opportunities of market for the workers leads to involve in criminals activities. While the trends of having lavish life style is also the cause of joining criminal activities.

REFERENCES

Brenner, Susan W. 1973. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." *The Journal of Criminal Law and Criminology* 97(2):379-391.

Cassim, Fawzia. 2011. "Addressing the Growing Specter of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and other Regional Role Player." *The Comparative and International Law Journal of Southern Africa* 44(1):123-138.

Enginner, Mehar. G Haragopal, Madhu Parsad, Sunil, Keder Nath Pandey, Parabhakar Arade and Anil Sadgopal. 2010. "Higher Education." *Economics and Political Weekly* 45(37):4-5.

Galeotti, Mark. 2013. "The Cyber Menace." *The World Today* 68 (7):32-35.

Gordon, Sarah and Richard Ford. 2006. "On the Definition and Calassification of Cybercrime." *Springer-verlag France* 2:13-14.

Hyman, Paul. 2013. "Cybercrime: Its Serious, But Exactly How Serious?." *Communications of the ACM* 56(3):18-20.

Kaufman, Roger A. 1968. "A system Approach to Education Derivation and Definition." *AV Communication Review* 16(4):415-425.

Lane, Jan-Erik. 1984. "Higher Education Regionalization." *Higher Education* 13(4):347-349.

Madero-Hernandez, Arelys and Bonnie S. Fisher. 2012. "Routine Activity

Theory." *The Oxford Handbook of Criminological Theory Edited by Francis T.Cullen and Pamela Wilcox* :13-27.

Memon, Shazad and Jawad Hussain Awan. 2017. "Transformation Towards Cyber Democracy: A Study On Contemporary Policies, Practice and Adoption Challenges for Pakistan." *Springer International Publishing* 1-8.

Mora, Jose-Gines. 1997. "Equity in Spanish Higher Education." *Higher Education* 3(33):233-249.

O'Neil, Michael. 2001. "Cyber Crime Dilemma: Is Possible to Gurantee Both Security and Privacy?." The *Brookings Reviews* 19(1):28-31.

Pool, Philip. 2013. "War of the Cyber World: The Law of Cyber Warfare." *American Bar Association* 47(2):299-320.

Ploom, Tristan. 2003. "Definition of Cyber-Crime." *Juridica* 576-578.

Rasool, Sadia. 2015. "Cyber Security Threats in Pakistan: Causes Challenges and way Forward." *International Scientific Online Journal* 21-34.

Saban, Kenneth A. Elaine McGivern and Jan Napoleon Saykiewicz. 2002. "A critical Look at the Impact of Cybercrime on Consumer Internet Behavior." *Journal of Marketing Theory and Practice* 10(2):29-37. Computer Mediated Marketing.

Satapathy, C. 2000. "Impact of Cyber Vandalism on the Internet."

Economics and Political Weekly 35(13):1059-1061.

Strydom, A. H and Magda Fourie. 1999. "Higher Education Research In South Africa: Achievements, Conditions and New Challenges." *Higher Education* 38(2):155-167.

Thompson, Keith. 1992. "Quality Control in Higher Education." *British Journal of Educational Studies* 40(1):51-56.

Walberg, Herbert J and Susan Christie Thomas. 1972. "Open Education: An Operational Definition and Validation in Great Britain and United States." *American Educational Research Journal* 9(2):197-208.

Wilczenski, Felicia Land and Susan M. Coomey. 2006. "Cyber Communication: Finding its Place in School Counseling Practices, Education and Professional Development." *Professional School Counselin* 9(4):327-331.

Yorke, Claire. 2010. "Cyber security and Society." *The World Today* 66(12):19-21.

ANNEXURES

Higher Education and Cybercrime in Quaid-i-Azam University, Islamabad, Pakistan

AminaAkmal

Dear worthy-respect respondent, I am AminaAkmal, a student, doing M.sc in sociology, in Quaid-i-Azam University Islamabad. This is questionnaire I am going to making you fill this, so that I request the favor of your filling this questionnaire, it is requested you to fill it by reading it clearly. And your honorable cooperation and in providing unbiased response is highly commendable and will be prove meaningful in order to achieve trustworthy results of this research. My topic of research is "Higher Education and Cybercrime in Quaid-i-AzamUniversiy, Islamabad, Pakistan." The data collected, shall be used for academic purpose only and will be kept secret.

Questionnaire ID ------------------------

Demographic profile:

Gender:

Male 2) Female

Age of the respondent

18 to 22 b) 23 to 28 c) 29-35 b) any other__

Educational qualification

Bachelor b) Masters c)M.phl d) P.hd e) any other

Family types

Joint family system (b) Nuclear `(c) extended d) any other

Occupation of the respondent

Employed b) Unemployed c) student d) Business e)Retired

Marital Status

Single b) Married c) Divorced d) Widowed e) separated

Education

Do you think higher education meets the demand of advanced technology?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you think the technical education fit into the aims of higher education?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you think highly educated people do not harm society?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

The existence of the expectation about the higher educated student as product by future?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you think the specialized courses of study within the program included anything which causes you to commit cybercrime?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you think without higher education people have specialization on their own by daily experiences?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you think opportunities are available to gain work experience?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Why do some believe educational liberty extends beyond the regular restrictions of free speech and, for that matter, dignity?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you think higher education guides people in term of any unethical thing that cause society damage?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you agree students never read the syllabus until something goes wrong?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you agree we can conflate higher education with ability?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you think highly educated people are playing the role of the intelligence in the fight to the cybercrime?

Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Cyber Crime

Do you agree everyone already know about cyber security?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Have you heard of someone who has been a victim of a cybercrime?

Strongly agreeb) Agree c) Somewhat agree d)disagree e) Don't know

Have you seen anything on the news about people being harassed online in this respect?

a) Strongly agree b) Agree c) Somewhat agree d) Disagree e) Don't know

Do you agree that cybercrime impact on social life?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you agree that there is general guidance for helping government officials understand cyber security risks and key action steps?

a) Strongly agree b) Agree c) Somewhat agree d) disagree
e) don't know

Do you agree the qualified cyber security professionals are enough to secure networks and data against cyber threats?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you think only economical concerning cyber threats for private businesses and government organizations are happening through this act?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you agree it exist a marked distinction between cybercrime and state-sponsored hacking?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you think it is possible a major cyber-attack against a government network or a critical infrastructure in the coming time?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

Do you agree that your country identified, created, or established a unit or entity specifically charged with dealing cyber-crimes incident response?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know

This is in your knowledge that your country identified, created, or established a specific court for the trials of cybercrimes?

a) Strongly agree b) Agree c) Somewhat agree d) disagree e) don't know