International Journal of
Technology and Systems
(IJTS)

CYBERCRIME: THEORETICAL DETERMINANTS, CRIMINAL POLICIES, PREVENTION & CONTROL MECHANISMS

Khalifa Nasser K A Al-Dosari

IPRJB
INTERNATIONAL PEER REVIEWED JOURNAL AND BOOK PUBLISHING

International Journal of Technology and Systems
ISSN 2518-881X (online)
Vol.5, Issue 1, No.3. pp 34-63, 2020

www.iprjb.org

CYBERCRIME: THEORETICAL DETERMINANTS, CRIMINAL POLICIES, PREVENTION & CONTROL MECHANISMS

Khalifa Nasser K A Al-Dosari
Post Graduate Student (PhD): Brunel University London
Corresponding Author Email: khalifaaldosari@hotmail.com

Abstract

Purpose: The research aimed to explore the theoretical determinants of cybercrime in Qatar and assess how it can be prevented and minimised.

Methodology: This was done using the mixed method research design through the survey strategy and semi-structured interviews with experts in the field of cybercrime in Qatar. Having adopted a mixed-method research methodology, the study had a target population of 200 participants for questionnaire survey, while expert interview had a target population of 11 experts. All these participants were purposively sampled in pursuit of engaging respondents who had knowledge, experience and expertise in cybercrime, such as IT experts and professionals working on cyber security solutions, Lawyers, police officers working in cybercrime department in Qatar, and lawyers who had dealt with cybercrime. The results of the survey were quantified using the Likert scale and analysed quantitatively by the factor analysis, and frequency tables. The results of the interviews were analysed qualitatively.

Findings: The results of the survey revealed that the most typical types of cybercrime in Qatar include website hacking, email cyberattacks, and online banking cyberattacks. The predominant motive for cybercrime in the country is monetary gains. However, the findings from the logistic regression analysis reveal that different types of cybercrime are associated with different determinants, and online banking crimes are predominantly driven by monetary gains. Moreover, the findings from IT experts interviewed revealed various measures can be adopted as control measures of cybercrime activities and hazards, such as development of stronger networks by commercial companies to protect their cyber assets and use of up-to-date protective software that detect and ensures complete data security.

Unique contribution to theory, practice and policy: Further, the findings, in relation to the effective methods and mechanisms for preventing cybercrime, suggest that it can be reduced through the spread of awareness among people and companies and through the adoption of preventive control mechanisms. Further, the study recommends that governments should formulate and implement legislations aimed at enhancing stringent measures of combating and dealing with cybercrime in convergence with international standards and practices. Besides, companies should adopt technological cybersecurity solutions to enhance effective protection of intellectual property, intrusion, and malicious damage of data as well as other cyber-related crimes.

Keywords: *Cybercrime, Criminal Policies, Prevention Mechanism, Cybercrime Control, Cybercrime Determinants.*

1.0 INTRODUCTION

Cybercrime refers to crimes that are committed on the internet through the use of computer as a target victim or a tool of committing the crime.1 Moreover, cybercrime has been described as a wide range of internet-based offences in the form of various activities such as, hacking computer systems and data, computer-related fraud and forgery, such as phishing, content offences, such as disseminating child pornography, as well as dissemination of pirated content, such as copyright offences.2 Up until 2014, there was no legal document that would regulate cybercrime and persecute cyber criminals in Qatar. Currently, there are only 13 articles making prescriptions for cases of cybercrime in Qatar. The current legislation does not have specific remedies for types of cybercrime. Moreover, even the existing legislation have been described as being too lenient on culprits of cybercrime, with the most cited case of leniency being the punishment prescribed for cybercriminal activities that does not exceed 10 years imprisonment or fine of $137,000.3 Besides, there research shows that there is insufficient reporting of cybercrime in Qatar, contributing to a lack of sufficient accurate and reliable data on cybercrime available from public sources.4 This has necessitated prevalence of internet-based crimes, such as human and drug trafficking with facilitation of cyberspace and illegal money laundering through the financial system using cyber space.5 Therefore, this research undertook primary data collection to attain the information from experts in the field of cybercrime towards policy formulation for the prevention and control of cybercrime in Qatar.

Research Rationale

On 5 June 2017, Qatar faced one of the severest diplomatic crises in its modern history, when the Gulf Cooperation Council (GCC) countries, led by Saudi Arabia, accused Qatar of supporting Iran and the Muslim Brotherhood and even financing terrorism. This led to a surge in cybercrime aimed at hacking Qatari websites and emails.[6] Currently, Qatar has made improvements in its financial system, making it fully compliant with international

[1] Wanyana, Racheal Rose. "Cybercrime in Uganda, an analysis of the Legal Framework." (2019).

[2] United Nations Office on Drugs and Crime, "Transnational organized crime threat assessment." TOCTA Report (2010), PP. 217-232. < https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_draft_2603_lores.pdf> Accessed 29 August 2020.

[3] Tabassum, Aliya, Mohammad Saleh Mustafa, and Sumaya Ali Al Maadeed. "The need for a global response against cybercrime: Qatar as a case study." In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6. IEEE, 2018.

[4] Naheem, Mohammed Ahmad. "Legal analysis of Qatar's anti-money laundering and combating terrorist financing legislation and regulation amidst the summer 2017 GCC crisis." *Journal of Money Laundering Control* (2020).

[5] Tabassum, Aliya, Mohammad Saleh Mustafa, and Sumaya Ali Al Maadeed. "The need for a global response against cybercrime: Qatar as a case study." In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6. IEEE, 2018.

[6] Ibid, 34

regulations, such as the Financial Action Task Force (FATF) that has been significant regulatory progress in preventing terrorist financing and anti-money laundering (ALM).[7] However, the risk of cybersecurity remains high in the country, with little practical scientific measures being put into actions towards resolving this security threat. Therefore, it is imperative to assess the main determinants of cybercrime and also propose effective measures that can be implemented to reduce or even eliminate cybercrime in Qatar.

Aim & Objectives

1. To assess the main determinants of cybercrime In Qatar.
2. To analyse the most common types of cybercrime committed in Qatar.
3. To evaluate potential control mechanisms for preventing cybercrime in Qatar.
4. To make recommendations for criminal policies that can prevent and minimise the extent of cybercrime in Qatar.

Research Questions

1. What factors contribute to the emergence and growth of cybercrime in Qatar?
2. What types of cybercrime prevail in Qatar?
3. How is it possible to prevent cybercrime in Qatar?
4. What control mechanisms are currently employed and can be employed in the future to prevent cybercrime in the country?

2.0 LITERATURE REVIEW

Conceptual Framework & Theories

Popular cybercrime include; phishing, malware, DoS and DDoS attacks, Trojans, MitM attacks, identity theft, cyber fraud, key and screen loggers, cyber bullying, cyber laundering, worms, and sniffers.8 Previous researchers tended to present the concepts underlying cybercrime as a taxonomy (Brar, Harmandeep Singh and Gulshan Kumar, 20189) or ontology (Barn, Ravinder and Balbir, 201610).11 A predominant number of

[7] Ibid, 16

[8] Okutan, Ayşe. "A Framework for Cyber Crime Investigation." *Procedia Computer Science* 158 (2019): 287-294.

[9] Brar, Harmandeep Singh, and Gulshan Kumar. "Cybercrimes: A proposed taxonomy and challenges." *Journal of Computer Networks and Communications* 2018 (2018).

[10] Barn, Ravinder, and Balbir Barn. "An ontological representation of a taxonomy for cybercrime." (2016).

classifications are taxonomies.12 The main determinants of cybercrime include the penetration of broadband internet, the development of technologies, geopolitical conflicts, income gap, and racial as well as ethnic conflicts. Cybercrime has both financial and non-financial effects on targets.13 Determinants of cybercrime and preventive mechanisms can be explored using a conceptual framework based on the Fraud Triangle below

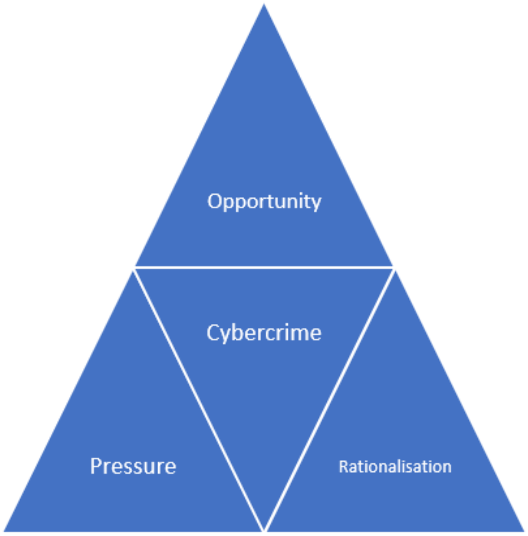


Figure 1: Fraud Triangle

The Pressure segment deals with determinants of cybercrime represented by variables such as political tensions, religious tensions, and potential monetary gains. The Opportunity segment deals with the technological capabilities and skills of cyber criminals. Based on these factors, effective control and preventive mechanisms can be developed. Lastly, the Rationalisation segment describes the main arguments used by cyber criminals to justify their actions.

The Routine Activity Theory (RAT) is a macro theory that explains the occurrence of crime, and cybercrime in particular, and is related to the Opportunity segment of the Fraud Triangle. According to this theory, cybercrime will take place when three conditions

[11] Donalds, Charlette, and Kweku-Muata Osei-Bryson. "Toward a cybercrime classification ontology: A knowledge-based approach." *Computers in Human Behaviour* 92 (2019): 403-418.

[12] Heartfield, Ryan, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny RJ Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. "A taxonomy of cyber-physical threats and impact in the smart home." *Computers & Security* 78 (2018): 398-428.

[13] Antonescu, Mihail, and R. Birăub. "Financial and non-financial implications of cybercrimes in emerging countries." *Procedia Economics and Finance* 32 (2015): 618-621.

converge, namely: 1) there is a motivated attacker; 2) a target with value; and 3) the absence of a proper preventive mechanism or guardianship[14].

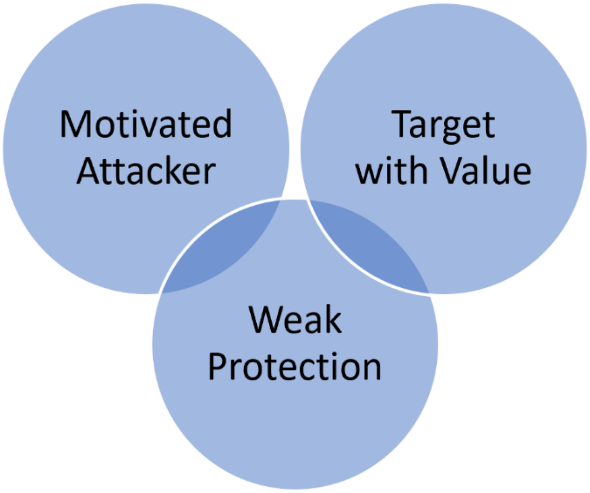


Figure 2: Routine Activity Theory

Previous studies show that one of the obstacles for an effective fight against cybercrime is that it is much less frequently reported by victims compared to traditional crime.[15] Moreover, demographic characteristics of the victims are also argued to determine the reporting of cases of cybercrime. In particular, women are more likely than men to report cybercrime.[16] Identity theft is reported more frequently, whereas hacking is less reported.[17] This results in a lack of a full picture for all types of cybercrime.

Impact of Cybercrime on National Security

When cyber-attacks target commercial entities, the most common motivation is the financial incentive to retrieve trade secrets and sensitive information that can change the

[14] Leukfeldt, Eric Rutger, and Majid Yar. "Applying routine activity theory to cybercrime: A theoretical and empirical analysis." *Deviant Behaviour* 37, no. 3 (2016): 263-280.

[15] Van de Weijer, Steve GA, Rutger Leukfeldt, and Wim Bernasco. "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking." *European Journal of Criminology* 16, no. 4 (2019): 486-508.

[16] Baumer E. and Lauritsen J. Reporting crime to the police, 1973–2005: A multivariate analysis of long-term trends in the National Crime Survey (NCS) and National Crime Victimization Survey (NCVS). *Criminology* 48, no.1 (2010): 131–185

[17] Van de Weijer, Steve GA, Rutger Leukfeldt, and Wim Bernasco. "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking." *European Journal of Criminology* 16, no. 4 (2019): 486-508.

competitive position of the company.[18] However, some types of cybercrime pose an inevitable threat to national security. These include direct hacking of official government websites and servers that can result in leaking sensitive information on the number of military units and objects and their location. A threat to national security can also be posed when cyber-attacks are directed at systemically important private or public companies. In the case of the Arab region and Qatar, this would be oil and gas companies. Disruption in energy security would also lead to threats to national security. Social media activities can also be used to build military opposition to ruling parties and result in another threat to national security.

Forms & Patterns of Cybercrime in Arab Gulf Region

International patterns of cybercrime are mostly determined by the offender's capabilities, including skills and technologies available as well as socio-economic development in the country. The second type of determinants is the opportunity factors that describe potential gains from attacking the target[19]. These determinants can be analysed as a special case of the Fraud Triangle framework by classifying all determinants of crime into opportunity, incentive, and rationalisation factors.[20] Most of the cybercrimes committed in the Arab Gulf region is motivated not only by financial motives, but also ideological and political motives, making the region stand out from the rest of the world.[21] Besides, analysts suggests that the rapid digitisation in the Arab Gulf region as a result of oil-fuelled prosperity has made the region an attractive target of cybercrime.[22] Research on the cybercrime and cybersecurity in the middle east and north African economies[23] revealed some of the instances of cybercrime that have happened in the recent times and the succession of the cybercrime events in Arab Gulf region. The researcher found out that over 796,000 cyberattacks in Saudi Arabia were recorded, comprising 64% of all cyberattacks recorded in the Gulf Cooperation Council (GCC) countries. Also, over 740,000 machines in the GCC countries were actively infected in 2010. Further, the

[18] Basuchoudhary, Atin, and Nicola Searle. "Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets." *Computers & Security* 87 (2019): 1-10.

[19] Kshetri, Nir. "Pattern of global cyber war and crime: A conceptual framework." *Journal of International Management* 11, no. 4 (2005): 541-562.

[20] Lokanan, Mark E. "Challenges to the fraud triangle: Questions on its usefulness." In *Accounting Forum*, vol. 39, no. 3, pp. 201-224. Taylor & Francis, 2015.

[21] Kshetri, Nir. "Cybercrime and Cybersecurity in the Middle East and North African Economies." In *Cybercrime and Cybersecurity in the Global South*, pp. 119-134. Palgrave Macmillan, London, 2013.

[22] Younies, Hassan, and Tareq Na. "Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)." *Journal of Financial Crime* (2020).

[23] Kshetri, Nir. "Cybercrime and cybersecurity in the Middle East and North African economies." In *Cybercrime and Cybersecurity in the Global South*, pp. 119-134. Palgrave Macmillan, London, 2013.

researcher found out that during 2011 and 2012, cyberattacks were conducted on the networks of the Arab Bank on the Gaza Strip and the Central Bank of the United Arab Emirates (UAE), compromising the credit card information of Saudi citizens. Besides, these attacks were recorded among the non-Arab Gulf region were over 2 million computers were attacked in Turkey during 2009 and 2010, leading to more than 2, 871 cybercrime-related arrests in Turkey. Such instances informed the basis of this research by exploring the patterns of cybercrime, and engaging experts in data collection towards policy formulation in pursuit of providing control mechanisms.

Criminal Policies & Legislations

In Qatar, the main legal document regulating the fight against cybercrime is Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law. Prior to the Arab Spring, only the UAE and Saudi Arabia had cybercrime legislation, dating back to 2006 and 2007 respectively. The Arab Spring is also partially responsible for the skew in most Arab cybercrime regulation leaning towards social use of media.[24] Altayar analysed existing cybercrime regulation and legislation in all six GCC countries.[25] This research revealed that Qatar is among the most recent adopters of cybercrime legislation and has the most liberal punishment, with a maximum fine of $137,000 and 10 years in prison, whereas other countries in the GCC region have much stricter regulation, with maximum fines reaching $1.333 million and maximum penalty including even a death sentence in Oman and a life sentence in the UAE and Bahrain. Moreover, all current cybercrime laws in Qatar and other GCC countries are strongly connected to traditional law.[26]

Mechanisms for Improving Professional Capabilities to Combat Cybercrime

Capabilities that can increase the chances of winning the battle against cybercrime include; special police departments that specialise in cybercrime, openness to technological innovations and new methods, improvements in contact management of organisations, and problem-solving.[27] In regard to training, a growing interest is emerging in relation to game-based training of cybercrime specialists.[28] A key strength of this approach is that it allows for realistic simulations of cybercrime and the development of effective strategies in response.

[24] Foody, Mairéad, Muthanna Samara, Aiman El Asam, Hisham Morsi, and Azhar Khattab. "A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators." *International journal of law and psychiatry* 50 (2017): 45-51.

[25] Altayar, Mohammed Saleh. "A comparative study of anti-cybercrime laws in the Gulf Cooperation Council countries." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC),* pp. 148-153. IEEE, 2017.

[26] Redford, M. "U.S. and EU Legislation on Cybercrime," 2011 European Intelligence and Security Informatics Conference, Athens (2011): 34-37. doi: 10.1109/EISIC.2011.38

[27] Staniforth, Andrew. "Police investigation processes: practical tools and techniques for tackling cybercrimes." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*, pp. 31-42. Syngress, 2014.

[28] Altiındağ, Ebru, and Betul Baykan. "Discover the world's research." *Turk J Neurol* 23 (2017): 88-89.

The Role of Institutions in Combating Cybercrime

The first and most well-known international convention aimed at harmonising countries' efforts to combat cybercrime is the Budapest Convention, which was signed in 2001 and became effective in 2004. However, most Arab countries, including Qatar, do not participate in international conventions, which arguably limits the effectiveness of their legislation aimed at combating cybercrime. The United Nations Office on Drugs and Crime identified various institutions and the roles they play in fighting against cybercrimes as follows;[29] first and foremost, national security institutions, such as the national security agency play a significant role of developing cyber-defensive capabilities that are designed to detect and prevent, as well as mitigate the impacts of cybercrime when they occur. Also, these agencies develop cyber-offensive capabilities, such as measures of penetrating the attackers systems and damaging them as well as responding to cyberattacks. Also, national intelligence agencies plays the role of collecting and analysing information about cyberattacks that cannot be obtained publically, leading to combating cybercrime through intelligence gathering. The second institution identified by the United Nations Office on Drugs and Crime is the criminal justice institutions that comprise law enforcement officers, judges and prosecutors who are responsible for mitigation, prevention, detection, prosecution and adjudication of cybercrime.[30] Also, institutions, such as the military department and digital forensics play the role of being first responders in investigation of cybercrime, while legal institutions, such as private and government law firm deal with cases involving cybercrime.[31]

Modern Technologies & Information Security Protection

The development of the world-wide-web and emails facilitated types of cybercrime such as DDoS attacks, phishing, and hacking. The development of social media in the 2000s and 2010s led to a surge in cyberbullying and intellectual property rights violations.[32] However, new block chain technologies allow for taking preventive measures and improving the protection of sensitive information. Moreover, the upcoming development of quantum computing can arguably help eliminate much of cybercrime, due to the introduction of new encryption mechanisms that will require abnormal computation power to hack or brute force.[33]

[29] United Nations Office on Drugs and Crime, "Transnational organized crime threat assessment." TOCTA Report (2010), PP. 217-232. < https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_draft_2603_lores.pdf> Accessed 29 August 2020.

[30] Ibid, 221

[31] Wanyana, Racheal Rose. "Cybercrime in Uganda, an analysis of the Legal Framework." (2019).

[32] Korchenko, Oleksandr, Yevhen Vasiliu, and Sergiy Gnatyuk. "Modern quantum technologies of information security against cyber-terrorist attacks." *Aviation* 14, no. 2 (2010): 58-69.

[33] Ibid, 59

Mechanisms & Strategies to Spread Awareness of Cybercrime & Its Prevention

One of the mechanisms for spreading the awareness of cybercrime is informal and formal education on popular types of crime, such as phishing.[34] However, while education can be effective for preventing cybercrimes that can be recognised by potential victims, it will not be very effective for combating the types of cybercrime that people and organisations can become victims of regardless of whether they recognise it or not. Examples of such crimes include DDoS attacks and hacking. Such crimes could be prevented by implementing technologies for protection of sensitive information. These crimes can be combatted through mechanisms such as cybercrime intelligence gathering[35] aimed at collecting and analysing information to combat penetration of computer systems and subsequent cyberattacks, by intelligence agencies. Moreover, mechanisms, such as development and application of cyber-offensive capabilities can be used by national security agencies who have the capacity to penetrate and attack, as well as damage systems of cyber attackers to prevent cyberattack such as hacking.[36]

3.0 RESEARCH METHODOLOGY

Design of the Study

This research was undertaken from a philosophical stance of pragmatism, which allows resolving the conflict between the interpretivist and positivist stances dictated by the traditional dichotomy.[37] The main argument of the positivist stance is that the phenomenon of cybercrime should be approached scientifically, and its theoretical determinants can be tested objectively in a value-free manner. At the same time, interpretivist suggests that there is no right or wrong policy for fighting cybercrime. This use of pragmatism for investigating cybercrime in Qatar also allows for mixing deductive and inductive approaches, which would help to address all research objectives more effectively. The first two objectives were addressed by a deductive approach and the last two objectives were addressed inductively.

[34] Al-Hamar, Mariam, Ray Dawson, and Jassim Al-Hamar. "The need for education on phishing: a survey comparison of the UK and Qatar." *Campus-Wide Information Systems* 28, no. 5 (2011): 308-319.

[35] Younies, Hassan, and Tareq Na. "Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)." *Journal of Financial Crime* (2020).

[36] Korchenko, Oleksandr, Yevhen Vasiliu, and Sergiy Gnatyuk. "Modern quantum technologies of information security against cyber-terrorist attacks." *Aviation* 14, no. 2 (2010): 58-69.

[37] Aljaroodi, Hussain M., Raymond Chiong, and Marc TP Adam. "Exploring the design of avatars for users from Arabian culture through a hybrid approach of deductive and inductive reasoning." *Computers in Human Behaviour* 106 (2020): 1-8.

Data & Sample

The study used primary data and mixed-method research design. The choice of the mixed-method design was justified by its ability to bring a more comprehensive analysis of the studied phenomenon, namely cybercrime, its determinants, and effective policymaking to prevent or reduce cybercrime in the future. Mixed-method design contribute to greater understanding and more detailed explorations.[38] The main methods by which primary data was collected were structured questionnaires and semi-structured interviews with IT professionals working on cyber security solutions, experts working in Cyber Crime Police Department in Doha, and lawyers who have dealt with cybercrime in Qatar. Out of the 200 targeted participants, filled in questionnaires were returned from 132 participants. The study also targeted up to 10 interviewees but only 4 of the targeted agreed to participate on the interview. These interviewees included a police officer, a lawyer, and two IT experts administered via voice calls, whereas questionnaires were distributed online. The specialist from the police department was interviewed on the strategic role of cybercrime prevention and how it affects national security as well as the role of institutions in combatting cybercrime. The lawyer in turn was interviewed on criminal policies and legislations prevailing in Qatar. The IT experts were asked about technical issues of cybercrime, including the main mechanisms and channels through which this type of crime occurs in Qatar. They were also asked to share their knowledge on how companies, individuals, and public organisations can minimise the chances of becoming victims of cybercrime in Qatar.

Methods of Data Analysis

The results of the survey administered with structured questionnaires were analysed quantitatively, using the statistical software SPSS and respective statistical methods. The data was quantified using the Likert scale. Even though there are different variations of the Likert scale,[39] the purpose of this research was achieved by implementing the most common five-point Likert scale. The first technique of statistical data analysis used was graphical analysis. Frequency distribution graphs allowed for the visual assessment of key patterns in the responses. The next method were the frequency tables, which show the percentage of people adhering to a particular view. This was followed by the factor analysis used to demonstrate how well the answers provided in the survey loaded on actual theoretical factors chosen for the study. The factor analysis method was represented by the principal component analysis (PCA). Finally, it is argued that non-parametric tests should be applied when working with ordinal data. [40] Two groups were surveyed; those with

[38] Taguchi, Naoko. "Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research." *System* 75 (2018): 23-32.

[39] Vonglao, Paothai. "Application of fuzzy logic to improve the Likert scale to measure latent variables." *Kasetsart Journal of Social Sciences* 38, no. 3 (2017): 337-344.

[40] Elliott, Alan C., and Linda S. Hynan. "A SAS® macro implementation of a multiple comparison post hoc test for a Kruskal–Wallis analysis." *Computer methods and programs in biomedicine* 102, no. 1 (2011): 75-80.

technical knowledge and without technical knowledge. Respondents were also distinguished by their experience in the area of cybercrime. Technical recommendations were given more weight if they were based on responses of people with technical background and experience.

Binary logistic regression was used to assess the determinants of cybercrime in Qatar. The dependent variables were constructed from a categorical variable that represented the answers of the surveyed research participants as to which types of cybercrime they considered most prevailing in Qatar. Then, the number of binary variables was constructed, and the number of such variables was equal to the number of categories. These variables took the values of 0 and 1, and the estimated coefficients in the regression were interpreted as probabilities for which a particular type of crime occurs under the influence of the listed independent variables.

The empirical model for the binary logistic regression is represented by the following equation:

$$Cybercrime(website, email, social\ media, online\ banking, mobile, cyber\ terrorism) = \alpha + \beta_1 PoliticalMotive + \beta_2 ReligiousMotive + \beta_3 MonetaryGain + \beta_4 Leisure + \beta_5 Foreign + \varepsilon$$

Where; β represent the vector of regression coefficients for dependent variables, and ε represent any other influence, other than dependent variable (Political motive, religious motive, monetary gain, and leisure) that may influence cybercrime, such as pressure, opportunity to commit crime and rationalisation. Also, an additional control variable is added for a foreign party involved in cybercrime. The regression analysis and factor analysis were estimated in SPSS.

4.0 ANALYSIS, RESULTS & DISCUSSION

4.1Visualisation of Responses

Figure 3 shows that the respondents with short tenure (Cybercrime experience rating 1, 4, 5 & 6), outnumbered senior respondents (Cybercrime experience rating 2 & 3) by a small degree.

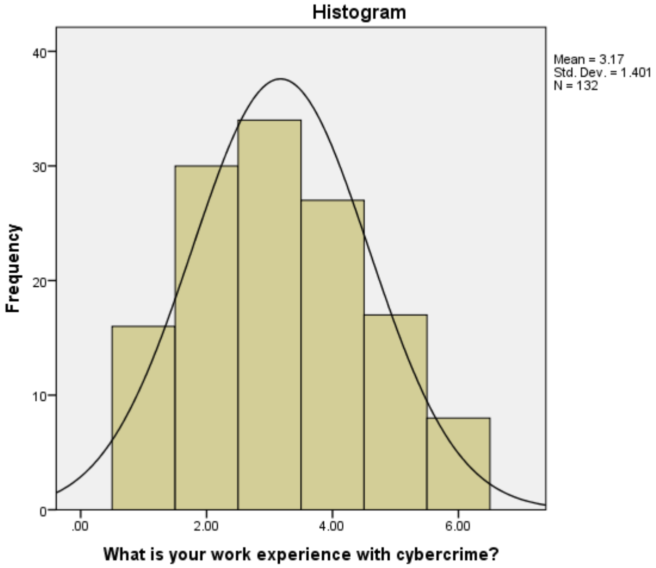


Figure 3: Distribution of Respondents by Work Experience

Figure 4 shows that the survey respondents predominantly believe that government resources are well-protected against cyberattacks. This strong confidence of respondents in the ability of the government to protect its assets from cybercrime is reflected in the asymmetric distribution with the left skewness in the data.

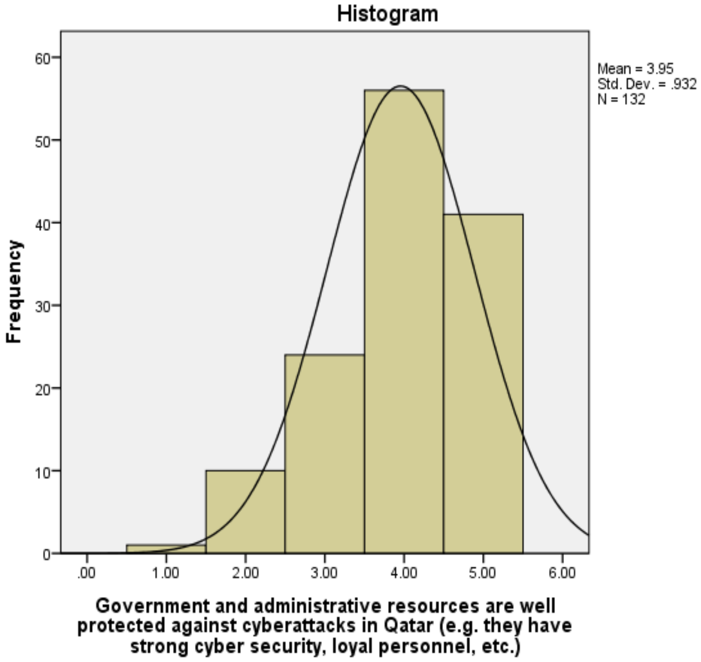


Figure 4: Protection of Government Resources from Cybercrime

Figure 5 shows that the majority of responses showed either disagreement or strong disagreement with the statement that individuals are well aware of cybercrime and well protected. Agreement and strong agreement with this statement was reported only by less than 20% of all respondents, whereas almost 60% of respondents either disagreed or strongly disagreed with this. Most of the respondents asserted that intensifying international cooperation in fighting against cybercrime is a way forward for the country to address this problem more effectively.

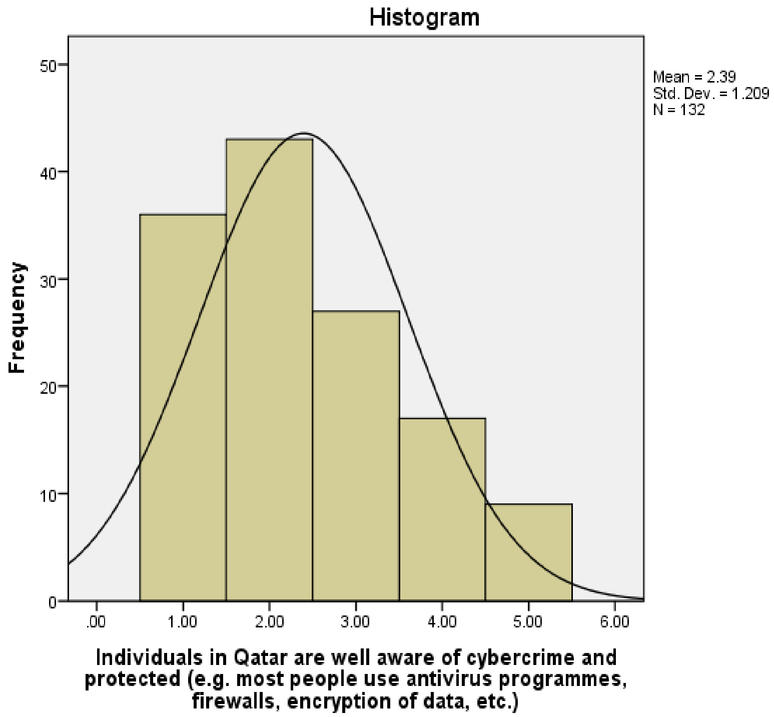


Figure 5: Cybercrime Awareness and Protection of Private Assets

Besides, Predominant number of respondents strongly agreed that international cooperation with other countries should be expanded.

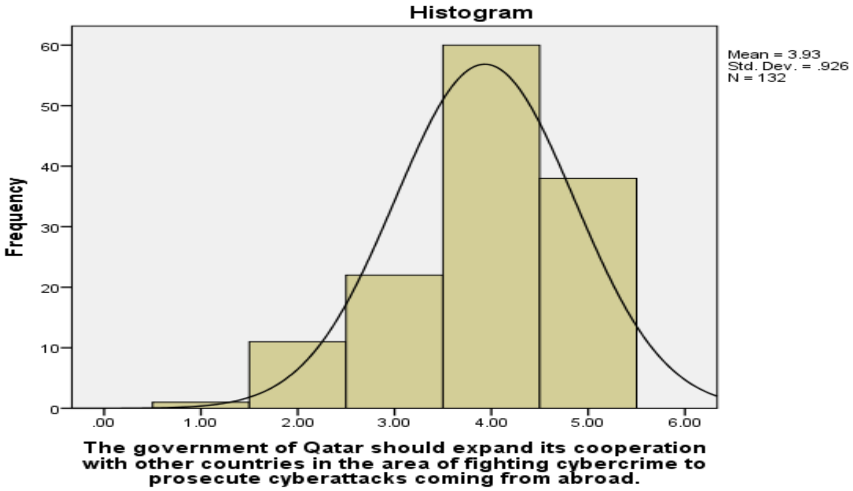


Figure 6: International Cooperation

Current views of the surveyed indicated that most of the cyberattacks in Qatar come from abroad, and, therefore, tighter international cooperation. In fact, the answers to these questions show a moderate positive correlation with the coefficient of 0.248, which supports this view. Figure 7 show that that there is prevalence of the agreement that foreign parties are mostly responsible for cybercrime in the country.

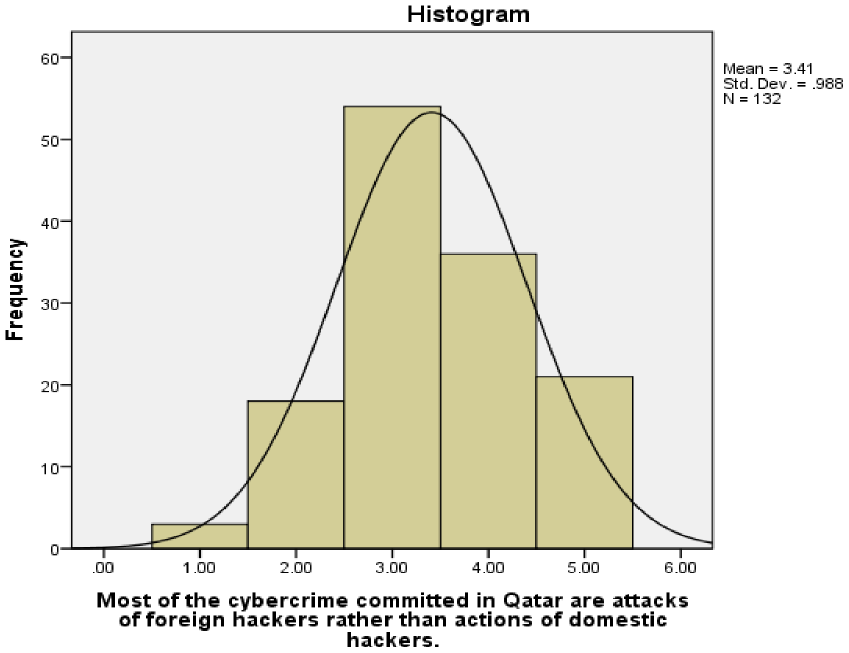


Figure 7: Foreign Involvement in Cybercrimes

Figure 8 shows that the current regulation and punishment is considered insufficient in Qatar, and that regulation and punishment should be more severe.

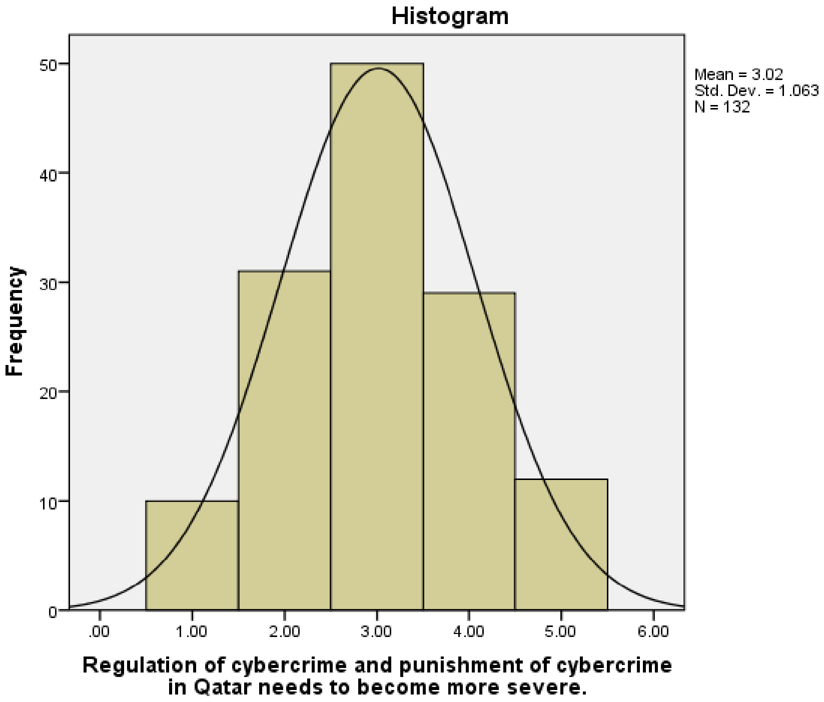


Figure 8: Regulation & Punishment of Cybercrime

4.2 Frequency Tables

The following table shows that over 90% of the people surveyed have a job directly connected with cybersecurity and cybercrime.

Table 1: Job & Cybercrime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	8	6.1	6.1	6.1
	Yes	124	93.9	93.9	100.0
	Total	132	100.0	100.0	

In terms of work experience in this field, the predominant share of respondents, namely 26%, had 3-4 years of experience. Some 6% of the respondents did not have experience or work related to cybercrime.

Table 2: Work Experience with Cybercrime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than a year	16	12.1	12.1	12.1
	1-2 years	30	22.7	22.7	34.8
	3-4 years	34	25.8	25.8	60.6
	5-6 years	27	20.5	20.5	81.1
	More than 6 years	17	12.9	12.9	93.9
	Not applicable	8	6.1	6.1	100.0
	Total	132	100.0	100.0	

In order to facilitate statistical analysis, the responses with the “non-applicable” choice were labelled zero. It is also important to note that almost 79% of the respondents had a technical background.

Table 3: Technical Background of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	28	21.2	21.2	21.2
	Yes	104	78.8	78.8	100.0
	Total	132	100.0	100.0	

The technical background includes knowledge of a programming language, engineering, and knowledge of networks, internet security, and how they work. Around one fifth of the respondents did not have a technical background and specialised in administrative rather than technical issues, albeit working in a field related to cybersecurity. Almost 70% of the surveyed people also had experience of working with cybersecurity or cybercrime outside of Qatar. Thus, most of the respondents also have international experience in this field.

Table 4: International Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	40	30.3	30.3	30.3
	Yes	92	69.7	69.7	100.0
	Total	132	100.0	100.0	

The most frequently cited cybercrime in Qatar is website hacking, with 30% of respondents choosing this option. The least frequently chosen option is cyberterrorism. The second most common type of cybercrime in the country is email attacks, including phishing. Together with website hacking, these two most common cybercrimes in Qatar account for more than fifty percent of all cases.

Table 5: Types of Cybercrime in Qatar

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Website hacking	40	30.3	30.3	30.3
	Email cybercrime	27	20.5	20.5	50.8
	Social media cybercrime	16	12.1	12.1	62.9
	Online banking cybercrime	23	17.4	17.4	80.3
	Mobile cybercrime	15	11.4	11.4	91.7
	Cyber terrorism	11	8.3	8.3	100.0
	Total	132	100.0	100.0	

Criminals are driven by different motives, and the following table illustrates the perception of the surveyed exports as to which primary motives have driven cybercrime in Qatar. The most popular motive according to the results of the survey is the monetary gain from cybercrime. The next most cited motives are defamation and disruption of the targets. Factors such as leisure and terrorism received the lowest weight in the survey.

Table 6: Key Motives of Cybercrime in Qatar

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Monetary gains	47	35.6	35.6	35.6
	Terrorism	9	6.8	6.8	42.4
	Fraud	17	12.9	12.9	55.3
	Defamation	25	18.9	18.9	74.2
	Disruption	23	17.4	17.4	91.7
	Leisure	11	8.3	8.3	100.0
	Total	132	100.0	100.0	

In regards to the assessment of the effectiveness of policies against cybercrime in Qatar, the respondents were divided between those who favoured proactive measures, such as preventive control and spreading awareness of cybercrime, and reactive measures, such as quick recovery measures and devising insurance mechanisms to minimise losses.

Table 7: Policy Effective Against Cybercrime

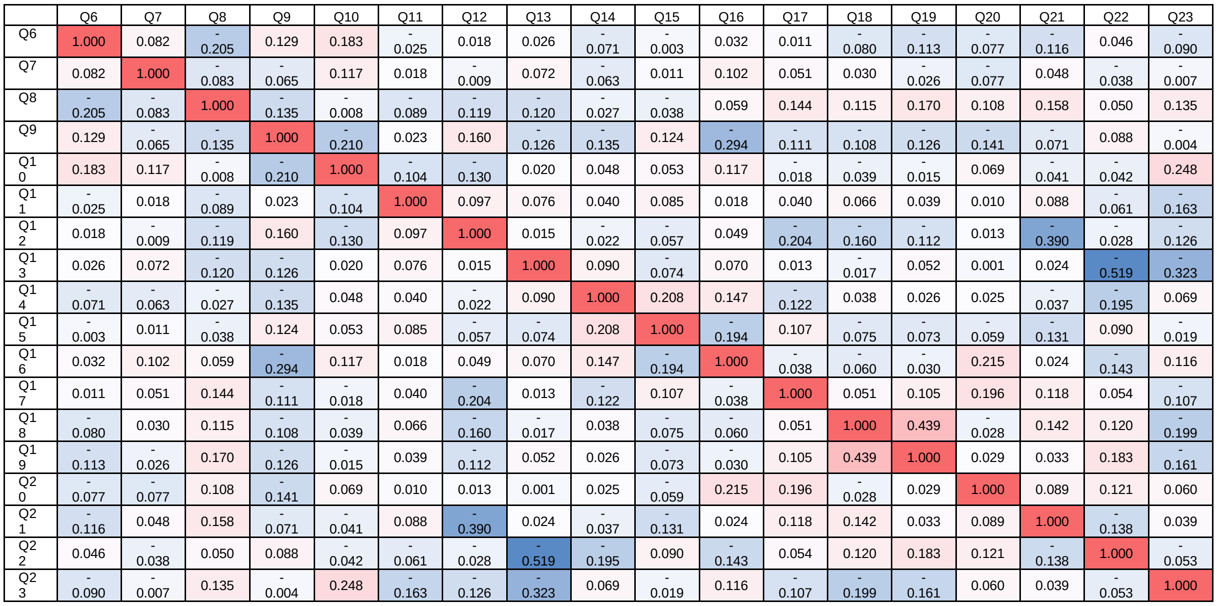
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Preventive control	47	35.6	35.6	35.6
	Quick recovery measures	17	12.9	12.9	48.5
	Awareness	53	40.2	40.2	88.6
	Insurance	15	11.4	11.4	100.0
	Total	132	100.0	100.0	

Proactive measures such as preventive control and awareness are favoured by more than 75% of respondents, with 35% of the surveyed people opting for preventive control and 40% of the surveyed people emphasising the importance of spreading awareness of cybercrime.

4.3 Factor Analysis

The main purpose of the factor analysis was to test how well the responses provided by the surveyed people load on the theoretical construct distinguished in the conceptual framework. These theoretical constructs included Pressure, Opportunity and Rationalisation. The Pressure construct was expected to be correlated with the monetary motive of cybercrime distinguished in the survey. The Opportunity construct was expected to be correlated with the degree of public awareness and protection in both the government and private sector. The Rationalisation construct was expected to be correlated with political and religious motives. The factor analysis was conducted using the PCA method.

Figure 9: Correlation Matrix



	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23
Q6	1.000	0.082	-0.205	0.129	0.183	-0.025	0.018	0.026	-0.071	-0.003	0.032	0.011	-0.080	-0.113	-0.077	-0.116	0.046	-0.090
Q7	0.082	1.000	-0.083	-0.065	0.117	0.018	-0.009	0.072	-0.063	0.011	0.102	0.051	0.030	-0.026	-0.077	0.048	-0.038	-0.007
Q8	-0.205	-0.083	1.000	-0.135	-0.008	-0.089	-0.119	-0.120	-0.027	-0.038	0.059	0.144	0.115	0.170	0.108	0.158	0.050	0.135
Q9	0.129	-0.065	-0.135	1.000	-0.210	0.023	0.160	-0.126	-0.135	0.124	-0.294	-0.111	-0.108	-0.126	-0.141	-0.071	0.088	-0.004
Q10	0.183	0.117	-0.008	-0.210	1.000	-0.104	-0.130	0.020	0.048	0.053	0.117	-0.018	-0.039	-0.015	0.069	-0.041	-0.042	0.248
Q11	-0.025	0.018	-0.089	0.023	-0.104	1.000	0.097	0.076	0.040	0.085	0.018	0.040	0.066	0.039	0.010	0.088	-0.061	-0.163
Q12	0.018	-0.009	-0.119	0.160	-0.130	0.097	1.000	0.015	-0.022	-0.057	0.049	-0.204	-0.160	-0.112	0.013	-0.390	-0.028	-0.126
Q13	0.026	0.072	-0.120	-0.126	0.020	0.076	0.015	1.000	0.090	-0.074	0.070	0.013	-0.017	0.052	0.001	0.024	-0.519	-0.323
Q14	-0.071	-0.063	-0.027	-0.135	0.048	0.040	-0.022	0.090	1.000	0.208	0.147	-0.122	0.038	0.026	0.025	-0.037	-0.195	0.069
Q15	-0.003	0.011	-0.038	0.124	0.053	0.085	-0.057	-0.074	0.208	1.000	-0.194	0.107	-0.075	-0.073	-0.059	-0.131	0.090	-0.019
Q16	0.032	0.102	0.059	-0.294	0.117	0.018	0.049	0.070	0.147	-0.194	1.000	-0.038	-0.060	-0.030	0.215	0.024	-0.143	0.116
Q17	0.011	0.051	0.144	-0.111	-0.018	0.040	-0.204	0.013	-0.122	0.107	-0.038	1.000	0.051	0.105	0.196	0.118	0.054	-0.107
Q18	-0.080	0.030	0.115	-0.108	-0.039	0.066	-0.160	-0.017	0.038	-0.075	-0.060	0.051	1.000	0.439	-0.028	0.142	0.120	-0.199
Q19	-0.113	-0.026	0.170	-0.126	-0.015	0.039	-0.112	0.052	0.026	-0.073	-0.030	0.105	0.439	1.000	0.029	0.033	0.183	-0.161
Q20	-0.077	-0.077	0.108	-0.141	0.069	0.010	0.013	0.001	0.025	-0.059	0.215	0.196	-0.028	0.029	1.000	0.089	0.121	0.060
Q21	-0.116	0.048	0.158	-0.071	-0.041	0.088	-0.390	0.024	-0.037	-0.131	0.024	0.118	0.142	0.033	0.089	1.000	-0.138	0.039
Q22	0.046	-0.038	0.050	0.088	-0.042	-0.061	-0.028	-0.519	-0.195	0.090	-0.143	0.054	0.120	0.183	0.121	-0.138	1.000	-0.053
Q23	-0.090	-0.007	0.135	-0.004	0.248	-0.163	-0.126	-0.323	0.069	-0.019	0.116	-0.107	-0.199	-0.161	0.060	0.039	-0.053	1.000

The results of the correlation test implies that the various motives of cybercrime identified in this study were related to the theoretical constructs (pressure, opportunity and rationalism). The variables are moderately correlated, and therefore the choice of the rotation was made in the favour of oblique methods because the number of variables and the number of individual observations was not too large in this study. The results show that the chosen components in the factor analysis explain more than 30% of the total variance.

Table 8: Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	2.057	11.428	11.428	2.057	11.428	11.428	2.051
2	1.863	10.352	21.780	1.863	10.352	21.780	1.869
3	1.731	9.618	31.399	1.731	9.618	31.399	1.742
4	1.350	7.499	38.898				
5	1.322	7.345	46.243				
6	1.274	7.080	53.323				
7	1.208	6.711	60.034				
8	1.017	5.651	65.685				
9	.936	5.200	70.886				
10	.800	4.442	75.328				
11	.767	4.261	79.589				
12	.742	4.123	83.712				
13	.637	3.538	87.250				
14	.571	3.174	90.424				
15	.525	2.917	93.340				
16	.471	2.617	95.957				
17	.435	2.416	98.372				
18	.293	1.628	100.000				

Table 9: Pattern Matrix

	Component		
	1	2	3
Political Motives	-0.326	0.006	0.011
Religious Motives	-0.024	0.202	-0.012
Monetary Gains Motives	0.514	-0.113	0.228
Leisure Motives	-0.417	-0.456	-0.146
Foreign Involvement	0.002	0.23	0.459
Government Resources Protected	0.011	0.121	-0.402
Private Sector Aware and Protected	-0.519	-0.009	-0.164
Severe Punishment	-0.069	0.701	-0.489
Traditional Crime More Harmful	-0.025	0.348	0.04
Traditional Crime Punishment More Severe	-0.143	-0.213	-0.002
Promotion of Greater Awareness	0.071	0.511	0.289
Reporting of Cybercrime	0.41	-0.065	-0.069
Technological Development	0.582	-0.104	-0.389
Investments in Cybersecurity	0.592	-0.116	-0.344
Increase in Government Budget on Cybersecurity	0.278	0.087	0.244
Increase in Corporate Budgets on Cybersecurity	0.487	0.162	-0.003
Regulation Needs to be More Severe	0.193	-0.753	0.141
International Cooperation	-0.052	-0.051	0.777

The results reveal that the solutions recommended for prevention of cybercrime in Qatar, are strongly correlated with the first component estimated in the course of the factor analysis. The second component is found to load best on the control factors, namely the degree of punishment for cybercrime. The third component is most significantly correlated with the international cooperation and foreign party involvement in cybercrimes committed in Qatar. The motives of cybercrime are not correlated significantly with any specific component, except for the factor of monetary gains and the first component that loads well on the policy variables. The lack of significant loadings observed for the motives of cybercrime can be explained by the fact that different motives can explain different types of cybercrime.

4.4 Binary Logistic Regressions

The significance of the determinants of cybercrime in Qatar was assessed using the method of Binary Logistic Regression analysis. Six binary variables associated with six types of cybercrime have been constructed, and then six binary logistic regressions have been run. The binary variables represent website hacking, email cybercrime, social media cybercrime, online banking cybercrime, mobile cybercrime, and cyber terrorism. The decision on statistical significance of the effects is made on the basis of the p-value (Sig.) and the 10% significance level.

Table 10: Determinants of Cybercrime Related to Online Banking

Variables		B	S.E.	Wald	Df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	.422	.260	2.636	1	.104	1.525
	ReligiousMotives	.340	.230	2.184	1	.139	1.406
	MonetaryGains	.824	.288	8.193	1	.004	2.279
	Fun	-.042	.245	.029	1	.865	.959
	ForeignAttacks	.017	.262	.004	1	.949	1.017
	Constant	-7.087	2.080	11.612	1	.001	.001

The results reveal a statistically significant association between the motive of monetary gains and the probability of cybercrime related to online banking. This relationship is found to be positive and statistically significant at the 1% level. This finding confirms the validity of the Pressure segment of the conceptual framework based on the Fraud Triangle. Monetary motives make people commit cyberattacks on financial organisations or individual accounts.

Table 11: Determinants of Cyber Terrorism

Variables		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	-.011	.301	.001	1	.971	.989
	ReligiousMotives	.309	.312	.979	1	.322	1.362
	MonetaryGains	-.154	.318	.236	1	.627	.857
	Fun	-.234	.341	.472	1	.492	.791
	ForeignAttacks	.667	.369	3.272	1	.070	1.948
	Constant	-4.692	2.477	3.588	1	.058	.009

Cyber terrorism was found to be significantly associated with foreign party involvement. This factor was found to be statistically significant at the 10% level.

Table 12: Determinants of Mobile Cybercrime

Variables		B	S.E.	Wald	Df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	.242	.296	.666	1	.415	1.274
	ReligiousMotives	.319	.274	1.353	1	.245	1.375
	MonetaryGains	-.684	.284	5.816	1	.016	.505
	Fun	-.149	.285	.272	1	.602	.862
	ForeignAttacks	-.148	.322	.213	1	.645	.862
	Constant	-.824	2.100	.154	1	.695	.438

Mobile cybercrime is significantly associated with the monetary gains motive, based on the estimated p-value. At the same time, social media cybercrimes are strongly associated with the political motives.

Table 13: Determinants of Social Media Cybercrime

Variables		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	-.525	.259	4.123	1	.042	.591
	ReligiousMotives	.219	.251	.761	1	.383	1.245
	MonetaryGains	.127	.302	.177	1	.674	1.135
	Fun	.446	.278	2.573	1	.109	1.562
	ForeignAttacks	.364	.288	1.598	1	.206	1.439
	Constant	-3.803	2.065	3.393	1	.065	.022

The political motive has produced a p-value below 0.05, which allows for treating this determinant as statistically significant at the 5% level.

Table 14: Determinants of Email Cybercrime

Variables		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	-.072	.206	.123	1	.725	.930
	ReligiousMotives	-.203	.203	.996	1	.318	.817
	MonetaryGains	.079	.228	.120	1	.729	1.082
	Fun	-.024	.215	.013	1	.910	.976
	ForeignAttacks	-.256	.234	1.191	1	.275	.774
	Constant	.089	1.582	.003	1	.955	1.093

Respondents provided diverse answers in regard to the evaluation of email cyberattacks. The same, however, does not apply to the website hacking.

Table 15: Determinants of Website Hacking

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	PoliticalMotives	-.026	.183	.020	1	.888	.975
	ReligiousMotives	-.394	.185	4.552	1	.033	.674
	MonetaryGains	-.194	.199	.950	1	.330	.823
	Fun	-.017	.190	.008	1	.931	.984
	ForeignAttacks	-.153	.208	.544	1	.461	.858
	Constant	1.594	1.429	1.244	1	.265	4.922

Religious motives were found to have a statistically significant relationship (p value .033) with the occurrence of website hacking activities in Qatar.

Discussion of Interviews

Experts indicated that the most frequently encountered cybercrimes in Qatar include website hacking, infringement of intellectual property rights, and malware. One of the IT experts listed the following types of cybercrimes, namely: ransomware, hacking, spamming, or DoS attacks. The most commonly cited reasons for the surge in cybercrime in the course of the interviews were weak legal protection of intellectual property rights, technological development with a lot of data being transferred online, and easily available access to information and tutorials on hacking. The interviews also shown that the most typical reasons why individuals and private companies are vulnerable to cybercrime are a lack of sufficient investments in developing secure networks in organisations, underestimation of risk or a lack of understanding of the degree to which cybercrime can cause damages, and, finally, the absence of contingency plans. Insurance and quick recovery measures received less weight in the opinions of the surveyed experts.

According to the interviewees, commercial companies should develop stronger networks to help them in protecting assets. Authorities need to update regulations periodically and ensure that they are not missing out on the newer techniques used by criminals. Individuals and households need to be vigilant and protect their private information under all circumstances. This can be done by making use of protective software that ensures complete data security. Companies must make use of the latest software that can detect cyberattacks. The ruling authorities can minimise risks by improving the effectiveness of the laws and ensuring better implementation at a ground level. All companies and individuals must be aware of the laws and regulations, as well as of the risks posed by cybercrime and potential negative consequences that can be entailed. They should also protect their data using the latest security software.

One of the interviewees noted that the US has extremely stringent regulations related to intellectual property rights. Companies should invest in solutions such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). These technologies make sure that the company's data are protected from unsolicited attacks. The survey results revealed a lack of consensus on whether regulations should be made tougher at the government level. However, interviewees argued that ruling authorities must ensure that the regulations are made more stringent and that they include all forms of attacks. Individuals should also be aware of risks when using public Wi-Fi. Households, companies, and individuals are also recommended to use VPN services to protect their privacy when browsing the web. The interviewees also emphasised the importance of using strong passwords, encryption of data, anti-virus software, and not clicking on or opening unrecognised emails, messages, or files.

5.0 CONCLUSION & RECOMMENDATIONS

Conclusion

Results indicated that monetary motive has been the most common determinant of cybercrime in Qatar. Also, among different types of cybercrime, website hacking, email attacks, and online banking attacks are the most common cybercrime activities in Qatar. Fundamentally, monetary gains are the driving predominantly online bank related cyberattacks. Besides, the results have demonstrated that spreading awareness is perceived to be one of the most effective measures. Respondents also preferred preventive control mechanisms, whereas insurance and quick recovery measures received less attention. Interviewees in the qualitative part of the research also insisted that changes in regulation include stricter laws and punishment can help prevent or reduce the cases of cybercrime in the country.

Recommendations of the Research

Several recommendations have been provided to policy makers. While government assets are assumed to be well-protected in Qatar, the legislation in the field of cybercrime is not very strict. It is not even the strictest in the GCC region, based on the results of the interviews and review of previous literature. Furthermore, it is recommended that the country should seek international partnership, not necessarily with GCC countries, but with all countries that have successful experience in fighting cybercrime. Regulators should also converge the legislation in relation to cybercrime with international standards and practices. The main recommendations that can be provided to individuals and companies, so they do not become victims of cybercrime, are as follows. They should learn about new methods of cyberattacks and the ways in which their assets can be vulnerable. Next, there is a need for awareness to the individuals and companies to invest in technological solutions to tackle cybercrime effectively and protect their vital systems, intellectual property, and assets from intrusion and the attacks of criminals.

REFERENCES

Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., & Aldehim, G. (2018). Cyber security crime and punishment: comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and

Saudi Arabia. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *8*(3), 46-59.

Agustina, J. R., & Insa, F. (2011). Challenges before crime in a digital era: Outsmarting cybercrime offenders–Workshop on Cybercrime, Computer Crime Prevention and the Surveillance Society. *Computer Law & Security Review*, *27*(2), 211-212.

Al-Hamar, M., Dawson, R., & Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. *Campus-Wide Information Systems*, *28*(5), 308-319.

Aljaroodi, H. M., Chiong, R., & Adam, M. T. (2020). Exploring the design of avatars for users from Arabian culture through a hybrid approach of deductive and inductive reasoning. *Computers in Human Behaviour*, *106*, 106246.

Altayar, M. S. (2017, March). A comparative study of anti-cybercrime laws in the Gulf Cooperation Council countries. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 148-153). IEEE.

Altiındağ, E., & Baykan, B. (2017). Discover the world's research. *Turk J Neurol*, *23*, 88-89.

Antonescu, M., & Birăub, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance*, *32*, 618-621.

Barn, R., & Barn, B. (2016). An ontological representation of a taxonomy for cybercrime.

Basuchoudhary, A., & Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security*, *87*, 101591.

Baumer, E. P., & Lauritsen, J. L. (2010). Reporting crime to the police, 1973–2005: a multivariate analysis of long-term trends in the National Crime Survey (NCS) and National Crime Victimization Survey (NCVS). *Criminology*, *48*(1), 131-185.

Berger, A., D’Alconzo, A., Gansterer, W. N., & Pescapé, A. (2016). Mining agile DNS traffic using graph analysis for cybercrime detection. *Computer Networks*, *100*, 28-44.

binti Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyber laws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66-76.

Bradbury, D. (2012). When borders collide: legislating against cybercrime. *Computer Fraud & Security*, *2012*(2), 11-15.

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*.

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems*, *41*(3), 669-682.

Corbet, S., & Gurdgiev, C. (2019). What the hack: Systematic risk contagion from cyber events. *International Review of Financial Analysis*, *65*, 101386.

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviours: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security*, *86*, 75-91.

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behaviour*, *92*, 403-418.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behaviour*, *34*, 165-172.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, *2016*(8), 5-8.

Elliott, A. C., & Hynan, L. S. (2011). A SAS® macro implementation of a multiple comparison post hoc test for a Kruskal–Wallis analysis. *Computer methods and programs in biomedicine*, *102*(1), 75-80.

Epps, C. (2017). Best practices to deal with top cybercrime activities. *Computer Fraud & Security*, *2017*(4), 13-15.

Foody, M., Samara, M., El Asam, A., Morsi, H., & Khattab, A. (2017). A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators. *International journal of law and psychiatry*, *50*, 45-51.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398-428.

Ho, L. H., Lin, Y. T., & Huang, C. H. (2012). Influences of Online Lifestyle on Juvenile Cybercrime Behaviours in Taiwan. *Procedia Engineering*, *29*, 2545-2550.

Hooper, C., Martini, B., & Choo, K. K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, *29*(2), 152-163.

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital investigation*, *7*(3-4), 105-113.

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, *28*(2), 201-207.

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, *25*(6), 528-535.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61-67.

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, *58*, 39-46.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541-555.

Korchenko, O., Vasiliu, Y., & Gnatyuk, S. (2010). Modern quantum technologies of information security against cyber-terrorist attacks. *Aviation*, *14*(2), 58-69.Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Springer.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, *11*(4), 541-562.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Springer.

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour*, *37*(3), 263-280.

Lokanan, M. E. (2015, September). Challenges to the fraud triangle: Questions on its usefulness. In *Accounting Forum* (Vol. 39, No. 3, pp. 201-224).

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security* 2013, no. 6 (2013): 9-13.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803-814.

Naheem, M. A. (2020). Legal analysis of Qatar'santi-money laundering and combating terrorist financing legislation and regulation amidst the summer 2017 GCC crisis. *Journal of Money Laundering Control*.

Naheem, M. A. (2017). Legitimacy of the summer 2017 GCC crisis and Qatar's AML framework. *Journal of Money Laundering Control*.

Okutan, A. (2019). A framework for cybercrime investigation. *Procedia Computer Science*, *158*, 287-294.

Redford, M. (2011, September). US and EU Legislation on Cybercrime. In *2011 European Intelligence and Security Informatics Conference* (pp. 34-37). IEEE.

Safavi, S., Shukur, Z., & Razali, R. (2013). Reviews on cybercrime affecting portable devices. *Procedia Technology*, *11*, 650-657.

Schofield, G. (2019). Has your Wi-Fi left you wide open to cybercrime? *Network Security*, *2019*(3), 13-14.

Staniforth, A. (2014). Police investigation processes: practical tools and techniques for tackling cybercrimes. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 31-42). Syngress.

Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). Cases study and analysis of the court judgement of cybercrimes in Taiwan. *International Journal of Law, Crime and Justice*, *43*(4), 412-423.

Tabassum, A., Mustafa, M. S., & Al Maadeed, S. A. (2018, March). The need for a global response against cybercrime: Qatar as a case study. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). IEEE.

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System*, *75*, 23-32.

United Nations Office on Drugs and Crime. (2010). Transnational organized crime threat assessment. TOCTA Report (2010), PP. 217-232. < https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_draft_2603_lores.pdf> Accessed 29 August 2020.

Van de Weijer, S. G., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486-508.

Vonglao, P. (2017). Application of fuzzy logic to improve the Likert scale to measure latent variables. *Kasetsart Journal of Social Sciences*, *38*(3), 337-344.

Wanyana, R. R. (2019). Cybercrime in Uganda, an analysis of the Legal Framework.

Yilma, K. M. (2014). Developments in cybercrime law and practice in Ethiopia. *Computer Law & Security Review*, *30*(6), 720-735.

Younies, H., & Na, T. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*.