Electronic Crimes And The International Community Legislation: Comparative Analytical Study

Mazen Ismaeel Ghareb, Falah Mustafa Sedeeq

Abstract: Cybercrime or cybercrime on computer programs or programs is considered a serious crime at the present time. State legislatures have provided legal protection for the legitimate use of the computer and the information network and the punishment of perpetrators of acts that constitute an attack on the rights of their users Or to prevent misuse of computer crimes. However, Arab countries, especially Iraq, are still far from legislating an e-crime law, despite the proposal by the Iraqi government in early 2011 to undermine the use of information technology and social networking sites through a project called the Cyber Crime Act. Cyber-crimes the off-spring of the cyber-space technology could be just observed; controlled and counteracted through digital enactment. Nations around the world are confronting the threats of digital violations because of a few reasons extending from the poor innovation, inadequacy and nonappearance of enactment to money related requirements, resistance with universal law and authorizing organizations. This examination was attempted to asses and breaks down the current situation with digital violations and enactment in the point of view of creating nations and to distinguish and investigate the difficulties the legislatures of creating nations are looking in the anticipation of the digital wrongdoings .

Index Terms: Cyber-space, Cyber-crimes, Cyber-laws, Cyber-attacks, internet, online documents.

1 INTRODUCTION

The present world's societies are winding up increasingly subject to open systems, for example, the Internet – where business exercises, business exchanges, and taxpayer-supported organizations are figured it out. This has prompted the quick improvement of new digital dangers and various data security issues which are abused by digital offenders. The powerlessness to give confided in secure administrations in contemporary PC organize advancements has a colossal financial effect on worldwide ventures and in addition people. In the present situation the majority of the information is on the web and slanted to advanced risks. There are endless perils and their direct is difficult to ahead of timetable seeing from this time forward hard to restrict in the early times of the cyber attacks. It might have some motivation driving it or might be arranged accidentally. The strikes those are arranged purposefully can be considered as the cybercrime and they have real impacts over the overall population as reasonable irritate, mental issue, hazard to National insurance et cetera. Restriction of advanced infringement is liable to genuine examination of their direct and perception of their belongings over various levels of society. Cybercrime is a kind of wrongdoing that occurs in "the internet", i.e. occurs in the domain of PC and the Internet. Though various people have a confined learning of "cybercrime", this kind of wrongdoing has the veritable potential for genuine impact on our lives and society, in light of the fact that our overall population is transforming into an data society, overflowing with information exchange occurring on the web [1].

- *Mazen Ismaeel Ghareb, Computer Science Department, University of Human Development, Iraq Sulaymaniyah, Iraq mazen.ismaeel@uhd.edu.iq*
- *Falah Mustafa Sedeeq, Assistant Lecturer, College of Law and Political, University of Human Development, Iraq Sulaymaniyah, Iraq falah.mustafa@uhd.edu.iq*

Additionally, the oftentimes happening global cheats force the need to direct the examination of actualities crossing over numerous worldwide fringes. Such examination is frequently subject to various wards and legitimate frameworks. A decent outline of the beforehand said is the Internet, which has made it less demanding to propagate conventional violations. It has gone about as a substitute road for the lawbreakers to lead their exercises, and dispatch assaults with relative namelessness. The expanded multifaceted nature of the correspondences and the systems administration framework is making an examination of the violations troublesome. Hints of illicit computerized exercises are frequently covered in extensive volumes of information, which are difficult to review with the point of identifying offences and gathering proof. These days, the advanced wrongdoing scene capacities like some other system, with devoted managers working as the people on the call. These stances new difficulties for law authorization arrangements and powers the PC social orders to use advanced crime scene investigation to battle the expanding number of cybercrimes. Criminological experts must be completely arranged so as to have the capacity to give court acceptable proof. To make these objectives achievable, scientific methods should keep pace with new advances [2]. Cyber law is a non-specific term which alludes to all the lawful and administrative parts of the web. Distributing a website page is a fantastic path for any business to endlessly build its presentation to a great many people around the world. It is that element of the Internet which is causing much discussion in the legitimate network. Cyber law is an always developing procedure. As the Internet develops, various legitimate issues emerge. A standout amongst the most vital issues concerning the internet today is that of Cyber wrongdoing. At the point when the Internet was created, the establishing fathers of Internet barely had any tendency that the Internet could likewise be abused for criminal exercises [3]. Today, there are numerous irritating things happening on the internet. Digital wrongdoing alludes to every one of the exercises finished with the criminal goal on the internet. These could be either the criminal exercises in the ordinary sense or could be exercises, recently advanced with the development of the new medium. On account of the mysterious idea of the Internet, it is conceivable to connect with into an assortment of criminal exercises with

exemption and individuals with insight, have been terribly abusing this part of the Internet to sustain criminal exercises in the internet. The field of Cyber wrongdoing is simply rising and new types of criminal exercises in the internet are going to the front line with the death of each new day. Since Cyber wrongdoing is a recently concentrated field, developing in Cyber laws, a ton of advancement needs to occur as far as instituting the significant lawful system for controlling and counteracting Cyber wrongdoing [4]. In this research we will investigate the computer crime, cyber crime and electronic crime from international and national law perspective of the countries. The research will review all the computer laws in developed countries and developing countries and evaluated many case studies. Adding more we will evaluate the digital and computer law in Iraq and Kurdistan by comparing with international computer law in the world.

2 LITERATURE REVIEW

2.1 Cyber Crime:

The term Cyberspace was first utilized by [5] which is currently used to depict the whole range of PC organizes and related exercises that occur over PCs and their interconnected systems which are their biggest sign from the web [5]. So it is the virtual place without jurisdictional limits in which individuals cooperate through the system of many thousands if not a huge number of PCs and clients in the meantime, accordingly, this the internet cleared courses for cybercrimes [6]. While, as indicated by [19] digital violations are the offenses which are carried out by people and gatherings against the people, gatherings and associations having criminal thought processes to deliberately harm i.e. physical or mental mischief to the casualty straightforwardly or in a roundabout way, who utilizes media transmission systems like, talk rooms, messages, see sheets and gatherings and cell phones for SMS/MMS. After Iraq war in 2013 Kurdistan Region Government has faced many challenges regarding cyber crime and the government announced many laws to protect it, but still the face challenges of implement these laws [7].adding to that according to [25] in Iraq and KRG there are not a powerful Information Technology to start build a infrastructure for all aspect of Technology such as E-Fininaial system, Cyber Law, E-Commerce, etc. Cybercrime e can be gathered into, to begin with, PC as an objective, assaulting another PC through contaminating infections and spreading malware, and so on second, PC as a weapon, by utilizing the PC to perpetrate conventional wrongdoing i.e. extortion or illicit betting and third, PC as a frill, essentially utilization of a PC to store unlawful or stolen data or information [8]. In any case, there is no concession to the universally settled upon single meaning of digital wrongdoing [9]. However, by and large, it could be alluding to an illicitly web intervened movement that regularly happens in worldwide electronic systems, might be local or universal or transnational – without digital outskirts. In addition, global digital violations are an awesome test to residential and universal law and its compelling usage, as in numerous nations, the present enactment isn't custom fitted to manage cybercrime, hence crooks are progressively leading wrongdoings through web by taking advantages of the poor disciplines or challenges in following the criminal. Along these lines, PC wrongdoing infers any wrongdoing that includes a PC and a system or criminal misuse of the internet. Though, digital wrongdoing is the criminal action, the wellspring of which is a PC or PC arrange utilized for digital assaults and may incorporate misrepresentation, robbery, extortion, imitation and misappropriation, anyway because of virtual mode, it is famously hard to distinguish and rebuff in light of the fact that the specialized intricacy and concealed aggressors sitting a large number of miles away. In spite of the fact that new innovation is helpful, dynamic and developing, and each next spell bring into confront new innovation with cutting edge highlights and security component yet because of the idea of digital wrongdoing, and its capacity to advance with innovation, new dangers are rising with a disturbing level of consistency and the client's capacity to center with winding up all the more difficult, which may likewise debilitate a country's security and monetary wellbeing. The issues rise up out of such wrongdoings have turned out to be prominent, especially those encompassing breaking, copyright encroachment, youngster explicit entertainment, and kid preparing. These are likewise called the issues of protection when programmers/assailants assault the private data to influence purposeful mutilations, to take and capture legally or something else. In spite of the fact that the universal legitimate framework is there which endeavors to consider on-screen characters responsible for criminal acts through International Criminal Court (ICC) [10]. Cybercrime is otherwise called computer crime that refers to any crime that includes a PC and a system. It is an assault on data about people, partnerships, or governments. In spite of the fact that the assaults don't happen on a physical body, they do occur on the individual or corporate virtual body, which is the arrangement of educational characteristics that characterize individuals and establishments on the Internet. The PC can be considered as a device in cybercrime when the individual is the principal focus of digital crime [11]. Likewise, cybercrime additionally incorporates customary violations that been directed with the entrance of the Internet. For instance, telemarketing Internet misrepresentation, data fraud, and charge card account robberies. In basic words, cybercrime can be characterized as any savagery activity that been led by utilizing the PC or different gadgets with the entrance of web. Information technology has a great role of solving many crisis such as cyber war, cyber crime, however the Government must apply all information Technologies roles and regulations [24].

2.2 Type of Cyber crimes behaviors:

Cybercrime extends over a range of exercises. Toward one side, are wrongdoings that include major ruptures of individual or corporate protection, for example, attacks on the respectability of data held in computerized vaults and the utilization of wrongfully got advanced data to coerce a firm or a person. At the opposite end of the range are those wrongdoings that include endeavors to disturb the real workings of the Internet. These reaches from spam, hacking, and foreswearing of administration assaults against particular locales to demonstrations of cyber terrorism—that is, the utilization of the Internet to cause open aggravations and even demise. Hoodlums perpetrating cybercrime utilize the number of techniques, contingent upon their range of abilities and their objective. Here is a portion of the distinctive ways cybercrime can come to fruition:

- Theft of individual information
- Copyright encroachment
- Fraud
- Child explicit entertainment

• Cyberstalking
• Bullying

The expansive scope of cybercrime can be better comprehended by separating them into two classes [12].

Type A:
Generally a solitary occasion from the point of view of the casualty. A case would be the place the casualty accidentally downloads a Trojan steed infection, which introduces a keystroke lumberjack on his or her machine. The keystroke lumberjack enables the programmer to take private information, for example, web managing an account and email passwords. Another type of Type 1 cybercrime is phishing. This is the place the casualty gets an as far as anyone knows genuine email (regularly asserting to be a bank or charge card organization) with a connection that prompts an unfriendly site [13]. Once the connection is clicked, the PC would then be able to be contaminated with a Virus. Hackers frequently do Type 1 cybercrime by exploiting defects in an internet browser to put a Trojan steed infection onto the unprotected casualty's computer. Any cybercrime that identifies with robbery or control of information or administrations through hacking or infections, data fraud, and bank or web based business misrepresentation. Another important issues that the Iraqi national ID contain all information about the Iraqi citizen but there is no of cyber law to protect the data privacy and data protection in Iraq, Therefore, till this moments there is not any system can deal with these huge data they are afraid from cyber crimes [21].

Type B:
They have a tendency to be significantly more genuine and spread things, for example, cyber stalking and badgering, youngster predation, coercion, shakedown, securities exchange control, complex corporate secret activities, and arranging or doing fear based oppressor exercises. It is by and large an on-going arrangement of occasions, including rehashed connections with the objective. For instance, the objective is reached in a visit room by somebody who, after some time, endeavors to set up a relationship. In the end, the criminal endeavors the relationship to perpetrate a wrongdoing. All the more frequently it is encouraged by programs that don't fit under the grouping crime ware [14]. For instance, discussions may happen utilizing IM (texting) customers or documents might be exchanged utilizing FTP.

2.3 Applications USED IN CYBERCRIME
The product instruments utilized as a part of cybercrime are at some point alluded to as crime ware. Crime ware is a product that is:
- utilized as a part of the commission of the criminal demonstration
- not for the most part viewed as an alluring programming or equipment application
- not automatically empowering the crime. Like cybercrime itself, the term crime ware covers an extensive variety of various vindictive or conceivably pernicious programming.

1. Crimeware: Bots
"Bot" term is short for robot – are a standout amongst the most modern sorts of crimeware confronting the Internet today. Bots resemble worms and Trojans, yet acquire their extraordinary name by playing out a wide assortment of mechanized assignments for the benefit of their lord (the cybercriminals) who are frequently securely found some place far over the Internet. Assignments that bots can perform run the range from sending spam to impacting Web locales off the Internet as a component of a planned "foreswearing of-benefit" assault. Bots sneak onto a man's PC from numerous points of view. Bots regularly spread themselves over the Internet via hunting down defenseless, unprotected PCs to taint [15].

2. Crimeware :Trojan
Trojan Horse: A Trojan steed program presents itself as a valuable PC program, while it really makes devastation and harms your computer. Increasingly, Trojans are the main phase of an assault and their basic role is to remain covered up while downloading and introducing a more grounded risk, for example, a bot. Dissimilar to infections and worms, Trojan steeds can't spread without anyone else [16]. They are regularly conveyed to a casualty through an email message where it takes on the appearance of a picture or joke, or by a noxious site, which introduces the Trojan steed on a PC through vulnerabilities in the web browser. Spyware: Spyware is a general term utilized for programs that secretively screen your action on your PC, gathering individual data, for example, usernames, passwords, account numbers, records, and considerably driver's permit or government disability numbers. Some spyware centres around observing a man's Internet conduct; this kind of spyware regularly tracks the spots you visit and things you do on the web, the messages you compose and get, and also your Instant Messaging (IM) discussions [17][18].After social event, this data, the spyware at that point transmits that data to another PC, normally to advertise purposes. There are many methods to improve the network security by using aspect oriented programming will help preventing the criminal activities [20].

3 ANALYZING CYBER CRIME FROM LAW PERSPECTIVE
The United Nations held several conferences to confront these crimes and issued recommendations, including the Seventh and Eighth Congress on the fight against crime and the treatment of offenders, referred to computer crimes and the difficulties related to them and how to combat them, especially the Organization for Economic Cooperation and Development called for intervention to protect information and non-aggression [22]. The Council of the European Union has started an attempt to address the illegal use of computers and information networks by issuing binding recommendations, resulting in the Budapest Convention on Information Crime in 2001 [23]. The Convention dealt with several issues, including: unauthorized access to corruption, information fraud, intellectual property, information fraud, illegal publication, etc.

3.1 Cyber Crime legalization in countries
1. The Australian legislator: dealt with computer crimes by amending the Penal Code of 1995 by banning entry and amending the data and punished by imprisonment for two years [26].
2. The Icelandic Legislator: The Penal Code amended Article 228 in Section I, which provided for the criminalization of any person using any method of entering the data and leaving the judge with discretionary power to rule [27].
3. The Indian and Singapore legislators have added legislation in the name of piracy and prohibited access to

computer materials [28].
4. Belgium legislator: In 2000, he added new texts on computer crimes and applied them one year after it was issued [29].
5. German legislator: Added two sections to the Penal Code, the first dealt with spyware data and the second destruction of the computer [30].
6. The French legislator: punished the crimes of informatics law of information fraud and illegal entry into the information system or the destruction of the data contained therein or the falsification of documents processed and used, and this law was merged with the French Penal Code in Chapter II, and also dealt fraudulent entry in contact With the information system, and punished for fraudulent entry [31].
7. US legislator: dealt with the issue of legislation of independent laws to regulate these crimes, including the law of people's report, the Freedom of Information Act, the law of communications policy, the law of cheating the computer, and others [32].

3.2 The position of Arab legislation

The position of lawmakers in the Arab countries has also differed on the subject of electronic crimes as follows:
1. Bahrain legislator: did not deal with the crimes independent, but applied the traditional texts of the Penal Code and electronic transactions law, despite the existence of an integrated bill, but it was not approved [33].
2. UAE legislator: There is integrated legislation to combat the crimes of information technology issued in 2006 [34]
3. Saudi legislator: dealt with informatics crimes by issuing a system to combat these crimes by the Council of Ministers [35].
4. Sudan legislator: dealt with the issue of the law of information crimes in 2007 [36].
5. The Algerian legislator amended the Penal Code by adding punitive provisions, which criminalized unauthorized entry, forgery, seizure, corruption, fraud, illegal behavior. He set the penalty of imprisonment and a fine [37]
6. The Egyptian's legislator has not passed any special legislation, and only amended some legislation such as the Civil Status Law in articles 72 and 74 concerning the use of electronic data. The Copyright Act No. 29 of 1994 was amended by the inclusion of computer works from programs, databases and data within protected works

3.3 The position of the Iraqi legislator

There is no law on electronic crimes in Iraq, but there is the draft law on communications and informatics. Although all electronic crimes are dealt with in a mixed and random manner, it shows inaccuracies in the selection of names and the definition of elements and elements of cybercrime, but it is a step towards the right path. Iraq currently applies to the Telecommunications Law No. 159 of 1980 and CPA Order No. 65 of 2004 concerning the Iraqi Commission for Communications and Information and the application of the Iraqi Penal Code regarding the crimes set forth in this law, especially fraud, defamation, forgery [38] [40].

3.4 The position of legislator of the Kurdistan region

As for the position of the legislator in the Kurdistan region - Iraq, we find that no law was issued in the Kurdistan region of electronic crimes law, and the Law on the prevention of abuse of telecommunications equipment No. (6) for the year 2008. In Articles 2 and 3, electronic crimes are defined indiscriminately and indiscriminately. These crimes are different and their characteristics change. The legislator has to distinguish them from each other. In other cases, the Iraqi Penal Code applies, including defamation, fraud, etc. Article (2) of the Telecommunications Misuse Law provides that: "Anyone who misuses a cell phone or any wire, wireless, internet or e-mail communication device shall be punished by imprisonment, fine or one of these two penalties by threatening, libel, defame, The publication of fictitious news, which incites terror and leaks of conversations, static images, mobile or unsolicited messages, or taking pictures without a license or authorization, or assigning dishonorable or inciting acts to commit crimes, acts of immorality or immorality, or dissemination of information related to the secrets of private life Or familial family. Article (3) of the law stipulates that: "Anyone who intentionally uses and exploits the cellular telephone or any wire, wireless, internet or e-mail communication equipment to harass others in a manner other than those mentioned in Article 2 Of this law) [41][42][43][44].

4 Conclusion and Recommendations

Although Cybercrime, additionally called as PC wrongdoing, is the utilization of a PC as an instrument to perform illicit errands, for example, carrying out REFERENCES misrepresentation, trafficking in youngster erotic entertainment and protected innovation has developed in significance as the PC has turned out to be vital to trade, amusement, and government. There are sound judgment steps that can forestall or diminish having one's money related data stolen on the web, and in addition to maintain a strategic distance from different tricks and dangers, however cybercrime in these zones holds on to a great extent because of an absence of customer instruction. In this paper the idea of cybercrime and it its different kinds have been considered. Promote we talked about a few instruments to be utilized for cybercrime everywhere throughout the world. At last, it finished up with different strategies to be utilized to distinguish and recuperate from cyber attacks. Two-factor validation utilizes two unique segments in mix to confirm a person. Those segments could be something the client knows, something the client has, or something indistinguishable from the client. To address these crimes in the Kurdistan Region Government in Iraq, we recommend the following:
1. Raise awareness of the judicial cadres on the quality of these crimes and the mechanism to deal with them in the sessions and investigate the evidence and analyze it.
2. The allocation of materials in universities for students of law and electronic science to study this emerging science on the legal scene. Drafting criminal legislation to criminalize electronic crimes to combat them.
3. The conclusion of international agreements to assist in judicial and security cooperation to control criminals and information crimes.
4. Awareness campaigns for individuals in the community on how to protect their privacy when using information systems.

ACKNOWLEDGMENT

We would like to thanks University of Human Development for supporting our research.

REFERENCES

[1] Yar, M., 2013. Cybercrime and society. Sage.
[2] Sunde, I.M., 2017. Cybercrime Law. Digital Forensics, pp.51-116.
[3] Punitha, P., Vidyavathi, S. and Sekharaiah, K.C., 2017. Spatial Cognition Applications towards Swachch Digital India.
[4] Li, X. and Qin, Y., 2018. Research on Criminal Jurisdiction of Computer cybercrime. Procedia computer science, 131, pp.793-799.
[5] Schmitt, M. and Vihul, L., 2017. International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms. Just Security Articles, 30.
[6] Miles, C.A., 2017. Provisional Measures Before International Courts and Tribunals (Vol. 128). Cambridge University Press.
[7] Ghareb, M.I., 2015. Toward Data Protection laws and code of conduct in Kurdistan region government. International Journal Of Engineering And Computer Science, 4(09).
[8] Mullen, J.D. and Reutzel, W., Dynamics Inc, 2017. Credit, security, debit cards and the like with buttons. U.S. Patent 9,727,813.
[9] Combs, C.C., 2017. Terrorism in the twenty-first century. Routledge.
[10] Kittichaisaree, K., 2017. Future prospects of public international law of cyberspace. In Public International Law of Cyberspace (pp. 335-356). Springer, Cham.
[11] Kharat, S., 2017. Cyber Crime–A Threat to Persons, Property, Government and Societies.
[12] Holt, T.J. and Bossler, A.M., 2008. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), pp.1-25.
[13] Zargar, S.T., Joshi, J. and Tipper, D., 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), pp.2046-2069.
[14] Peng, T., Leckie, C. and Ramamohanarao, K., 2004, May. Proactively detecting distributed denial of service attacks using source IP address monitoring. In International conference on research in networking (pp. 771-782). Springer, Berlin, Heidelberg.
[15] Peng, T., Leckie, C. and Ramamohanarao, K., 2004, May. Proactively detecting distributed denial of service attacks using source IP address monitoring. In International conference on research in networking (pp. 771-782). Springer, Berlin, Heidelberg.
[16] Wadhwa, A. and Garg, A., 2015. Studying and Analyzing Virtualization While Transition from Classical to Virtualized Data Center. International Journal of Computer Applications, 117(14).
[17] Reich, P.C. ed., 2011. Cybercrime & Security. West Publications.
[18] Aggarwal, P., Arora, P. and Ghai, R., 2014. Review on cyber crime and security. International Journal of Research in Engineering and Applied Sciences, 2(1), pp.48-51.
[19] Kabir, N., 2018. Cyber Crime a New Form of Violence Against Women: From the Case Study of Bangladesh.
[20] Ghareb, M., Improving Network Security using Aspect Oriented Programming.
[21] Ghareb, M.I., 2015. The Challenges of National e-ID for Kurdistan Region government for Multi-purposes. International Journal Of Engineering And Computer Science, 4(10).
[22] Casey, E., 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.
[23] Lavorgna, A., 2015. Organised crime goes online: Realities and challenges. Journal of Money Laundering Control, 18(2), pp.153-168.
[24] Ghareb, M.I., 2018. Information Technology Roles in Crisis Management: A Case Study in Kurdistan Region Government. International Journal of Computer Engineering and Information Technology, 10(5), pp.71-78.
[25] Jaffar, A.A., Ghareb, M.I. and Sharif, K.H., 2016. The Challenges of Implementing E-Commerce in Kurdistan of Iraq. Journal of University of Human Development/Vol, 2(3).
[26] McSherry, B., 2004. Terrorism offences in the criminal code: Broadening the boundaries of Australian criminal laws. UNSWLJ, 27, p.354.
[27] Olafsdottir, H. and Bragadottir, R., 2006. Crime and criminal policy in Iceland: Criminology on the margins of Europe. European Journal of Criminology, 3(2), pp.221-253.
[28] Gomez, J., 2004. Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia. Pacific Journalism Review, 10(2), p.130.
[29] Nicholson, L.J., Shebar, T.F. and Weinberg, M.R., 2000. Computer crimes. Am. Crim. L. Rev., 37, p.207.
[30] Martin, S.P., 1996. Controlling computer crime in Germany. Information and Communications Technology Law, 5(1), pp.5-28.
[31] Manap, N.A., Rahim, A.A. and Taji, H., 2015. Cyberspace Identity Theft: An Overview. Mediterranean Journal of Social Sciences, 6(4), p.290.
[32] Adams, J.A.M., 1996. Controlling cyberspace: applying the computer fraud and abuse act to the internet. Santa Clara Computer & High Tech. LJ, 12, p.403.
[33] Crystal, J., 2001. Criminal justice in the Middle East. Journal of Criminal Justice, 29(6), pp.469-482.
[34] Rezgui, Y. and Marks, A., 2008. Information security awareness in higher education: An exploratory study. Computers & Security, 27(7-8), pp.241-253.
[35] Al Amro, S., 2017. Cybercrime in Saudi Arabia: fact or fiction?. International Journal of Computer Science Issues (IJCSI), 14(2), p.36.
[36] Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D.K., Goodman, S.E. and Atlanta, G.A., 2008. Cybersecurity in africa: An assessment. Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.
[37] Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D.K., Goodman, S.E. and Atlanta, G.A., 2008. Cybersecurity in africa: An assessment. Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.
[38] Choo, K.K.R., 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), pp.719-731.
[39] Taylor, P., 2012. Hackers: Crime and the digital sublime.

Routledge.
[40] Bantekas, I. and Nash, S., 2003. International criminal law. Routledge-Cavendish.
[41] Ghareb, M.I.,Ahmed, A.M 2016. Factors Affecting the Success of E-Government Implementation in developing Countries: A Case Study of Kurdistan Region of Iraq (KRI) Head of IT Department, 2 Coordinator Teaching Quality Assurance. International Journal of Scientific Development and Research (IJSDR). 8(1), pp. 387-397.
[42] O'Leary, B., McGarry, J. and Salih, K. eds., 2006. The future of Kurdistan in Iraq. University of Pennsylvania Press.
[43] Shareef, S., Pimenidis, E., Arreymbi, J. and Jahankhani, H., 2010. Vision of Electronic Government implementation in Kurdistan region of Iraq.
[44] Kelly, M.J., 2009. The Kurdish Regional Constitutional within the Framework of the Iraqi Federal Constitution: A Struggle for Sovereignty, Oil, Ethnic Identity, and the Prospects for a Reverse Supremacy Clause. Penn St. L. Rev., 114, p.707.