CYBERCRIME IN THE JORDANIAN AND MALAYSIAN LEGAL SYSTEMS: CRIMINAL PROCEDURES AND EVIDENCE

BY

FERAS KHALED ALABDALLAH RJOUB

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Law

Ahmad Ibrahim Kulliyyah of Laws
International Islamic University
Malaysia

NOVEMBER 2012

ABSTRACT

Cybercrimes are an ever growing threat to both states and many persons throughout the globe. Cybercrimes offenders had even intruded governmental websites. Members of communities are no less at risk too from these sorts of crimes perpetrated on them knowingly or unknowingly. Things like *Malwares*, *spywares*, *spamming*, *phishing*, viruses such as *Trojan*, *Worms* etc. have continuously affected computer and internet users financially, personally, and professionally. Computers and internet users' privacy, confidentiality, security etc. are compromised. Their data and communications are compromised without their consent. By so doing, unwittingly or wittingly, those who do them commit offences that do not just fall foul under the Computer Crimes Act, but also under other Acts governing a person's personal data (Personal Data Protection Act), internet usage (Multimedia and Communication Act), personal account (Banking and financial Institution Act) and perhaps many more. This thesis revolves around the various issues faced by the Jordanian legal system in the investigation and prosecution of cybercrimes who is currently addressing them through her the traditional criminal laws i.e. the Penal Code. Developed countries have been very conscious of this matter over the past years. Several agreements have taken place through international treaties, and specific laws were formulated for these types of crimes. This lead to the facilitation of professionally held investigations, as well as prosecutions, in a more legally systematic manner, which in turn resulted in a better degree of control over cybercrimes. England and her former Commonwealth countries such Australia and even Malaysia already have several cybercrime laws. Considering how wide-spread cybercrime has become, serious questions must be raised whether the current Jordanian traditional criminal laws can stand up against the threat by the cybercrimes perpetrators. Does Jordan have the necessary substantive laws on computer crimes to deal with cybercrimes, and the necessary procedural and evidential laws to complement the computer crimes law? Malaysia has adopted a specific set of laws in order to exclusively address the issue of cybercrime including the necessary provisions in her Criminal Procedure Code (Act 593) and the Evidence Act 1950 to complement her cybercrime laws. Malaysia's Computer Crimes Act of 1997 could be an ideal model for Jordan who has yet to have one. A comparative analysis will be carried out between the Malaysian and Jordanian legal systems, with regards to their investigations and prosecutions of cybercrimes, and their procedural and evidential matters such as proof and punishment.

خلاصة البحث

تعتبر الجرائم الإلكترونية من أخطر الجرائم التي تهدد الأمن العام في جميع أنحاء العالم، حيث ان ضحاياها من الناس العاديين، وكذلك من الأجهزة الحكومية على اختلاف أنواعها، ونظراً لخطورة هذه الجرائم وتطورها المستمر عبر السنين الأخيرة فقد لجات الدول المتطورة إلى عقد الكثير من الإتفاقيات الدولية بهدف التعاون فيما بينها لمحاربتها، وكذلك وضعت قوانين خاصة لتسهيل التحقيق والمحاكمات المتخصصة في مثل هذه الجرائم ضمن اطار منظم، إلا انه في المقابل هناك بعض الدول الاخرى التي لم تنضم لمثل هذه الاتفاقيات الدولية، ولم تضع قوانين خاصة للحد من هذه الجرائم الإلكترونية ومكافحتها. إن موضوع هذا البحث يناقش الكثير من المشاكل التي تواجه النظام القانوني الأردني في كيفية التعامل مع الجرائم الإلكترونية، حيث أن المشكلة التي تواجه النظام القانوني الأردني هي غياب القانون الخاص لهذه النوع من الجرائم وقيامه بتطبيق القوانين الجزائية التقليدية، لذلك يحاول البحث الإجابة على تساؤلات عديدة ومن اهمها فيما إذا كانت القوانين التقليدية الحالية في النظام القانوني الأردني كافية للتعامل مع هذا النوع من الجرائم. وللإجابة على هذه التساؤلات فقد تم استخدام المنهج التحليلي المقارن ما بين النظامين القانونين الماليزي والأردني فيما يختص التحقيقات والإجراءات الجنائية والاثبات للجرائم الإلكترونية، حيث تبنت ماليزيا عدة قوانين من أجل التعامل مع الجرائم الإلكترونية بطريقة مباشرة وذلك من خلال قانوني جرائم الحاسوب وقانون الإثبات، وقد خلص البحث إلى انه يوجد فراغ قانوني في النظام القانوني الأردني ينظم بشكل محدد وفعال هذا النوع من الجرائم، وفي نهاية البحث تم تقديم مجموعة من المقترحات التي تتلخص بضرورة تبنى النظام القانوني الأردني قوانين خاصة متعلقة بالجرائم الألكترونية ومنها قانوني جرائم الكمبيوتر وقانون الإثبات الماليزيين.

APPROVAL PAGE

The thesis of Feras Khaled Alabdallah Rjoub has been examined and approved by the following:

_____

Abdul Rani Bin Kamarudin
Supervisor

_____

Co-Supervisor

_____

Internal Examiner

_____

External Examiner

_____

Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigation, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degree at IIUM or other institutions.

Feras Khaled Alabdallah Rjoub

Signature…… Date……..

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

CYBERCRIME IN THE JORDANIAN AND MALAYSIAIAN LEGAL SYSTEMS: CRIMINAL PROCEDURES AND EVIDENCE

Affirmed by Feras Khaled Alabdallah Rjoub

……. ……..

Signature Date

ACKNOWLEDGMENTS

All praise be to Allah, The Lord of the worlds, for easing my way through undertaking this research. May peace and blessings be upon the Prophet Muhammad Bin Abdullah (PBUH), the ideal role-model to the whole of mankind, and through whom the researcher was inspired to carry on in his attempt to achieve the best possible outcome.

Firstly, I'm grateful to my supervisor, Assoc. Prof. Dr. Abul Rani Kamarudin, and I thank him for accepting supervision, for his attentive understanding, valuable thoughts, suggestions, and guidance throughout the period of this research. I also thank Prof. Datuk Dr. Zaleha Binti Kamaraddin, Dr Nik Ahmad Kamal and Associate Prof. Dr. Mohammad Ismail Yunus for their valuable inputs and overall guidance.

Another acknowledgment is due to all the staff of the libraries at the International Islamic University Malaysia, as well as the staff at the postgraduate office of the Ahmad Ibrahim Kulliyyah of laws.

As for Malaysia the country, and the International Islamic University as an educational institution, I couldn't thank them enough; they deserve my prayers to the Almighty Allah for showing the world wonders in becoming a leading State and University on the global scale.

This thesis wouldn't have started without the prayers of my mother, whose wish was the initiating factor of this program, along with the blessing bestowed on me from the piety of my parents. Also, it wouldn't have been possible for me to carry on and achieve the completion of this thesis without the full support and motivation from my beloved wife and children, the ultimate delight of my eyes, Zaid, Mohammad, and Salma.

Last, but certainly not the least, I'd like to thank all those who assisted me by providing information, details, and comments to support and enhance this research. My thanks to those who live with open eyes to protect people's lives, privacy, and financial affairs.

TABLE OF CONTENTS

LIST OF STATUES

The Australia Criminal Code Act 1995 (Act No. 12).

The British Computer Misuse Act 1990.

The Federal Constitution of Malaysia 1957.

The Jordanian Child Code 1968 (Act No. 24).

The Jordanian courts of State Security Code 1959 (Act 17).

The Jordanian Criminal Procedure Code of 1961 (Act 9), as Act (15) for 2006.

The Jordanian Electronic Transactions Law(No. 85) of 2001.

The Jordanian Extradition Act (1927).

The Jordanian High Felonies Court Code 1986 (Act 19).

The Jordanian magistrate courts Act 1952 (No. 15). As (No. 30) for 2008.

The Jordanian Military courts establishment law 2006 (No. 23).

The Jordanian Military Penal Code 2006 (No. 58).

The Jordanian Penal Code 1960 (NO. 16), As Act (12) for 2010.

The Jordanian Police Act 1965 (Act No. 38).

The Malaysia Mutual Assistance in Criminal Matters Act of 2002 (Act 621).

The Malaysian Child Act of 2001 (Act 611).

The Malaysian Communication and Multimedia Act 1998.

The Malaysian Computer Crimes Act of 1997 (Act 563).

The Malaysian Courts of Judicature Act 1952 (Act No. 26).

The Malaysian Criminal Procedure Code (593).

The Malaysian Evidence Act (56).

The Malaysian Extradition Act of 1992 (act 479).

The Malaysian oaths and Affirmation Act 1949 (Act 194).

The Malaysian Police Act (344).

The Malaysian subordinate courts act 1948 (act 92).

The Nizamiyyia Courts Establishment law of 1952 (Act No.26), as act (No. 17) for 2001.

The Singapore Computer Misuse Act 1998.

LIST OF CASES

CHAPTER ONE

INTRODUCTION

1.0 BACKGROUND

The twentieth century has emerged as the century of revolution in communications and information transfer through both the internet and computer, which in turn have led to the merging of the entire world to become like a small village in terms of communication for most people in the world. Consequently, societies around the world are now able to interact with ease in economic, political, social and in other fields.

As much as the societies have benefited from this great shift in technology, the inevitable negative aspects that would come along with it must be addressed too. This swift development of information and communication through internet and computer has led to an increase in crime through electronic methods known as cybercrime in a way which conventional laws and legal rules may not be able to adequately cater, detect or deter them. There are problems such as finding the whereabouts of the offenders committing the cybercrimes, as well as finding admissible evidence to prove the commission of such crimes, hence a mind blogging task for any investigating and prosecuting officers who are new to the nature of these crimes. Also, it is a quite attractive field to make a career of, thus the large number of committed individuals.[1]

The types of cybercrimes committed through modern technology, especially the internet and computers, have become easily fluid, global and open, whether in relation to crimes against individuals or property, resulting in great damages to

[1] J.A. Hitchcock (2002) *Net Crimes & Misdemeanors*, Information today Inc., at 290.

victims' person and property and the public at large. Such crimes include child pornography, internet hacking, internet fraud, credit card fraud, cyber terrorism, illegal interception, data interference, electronic embezzlement, and digital piracy. These crimes are all extremely serious, to an extent that would cause losses of up to billions of dollars yearly, according to FBI statistics.[2] Recorded complaints are relatively low in comparison with the above wide-spread breach of privacy.[3]

The President of USA, Barack Obama said:

> Cyberspace is real and so are the risks that come with it. It's the great irony of our information age - the very technologies that empower us to create and to build also empower those who would disrupt and destroy and this paradox - seen and unseen - is something that we experience every day…we have had to learn a whole new vocabulary just to stay ahead of the cybercriminals who would do us harm - spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives suspended, and their wallets emptied…In this Information Age, one of your greatest strengths…could also be one of your greatest vulnerabilities. This is a matter, as well, of America's economic competitiveness…Its been estimated that [in 2008] alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion. In short, America's economic prosperity in the 21st century will depend on cyber security and this is also a matter of public safety and national security …It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we are not as prepared as we should be, as a government or as a country.[4]

The most common cybercrime committed over internet and computer is unauthorised access to other computer systems. According to the statistics of the Computer Emergency Response Team at Carnegie Mellon University, the number of incidents involving security breaches that have been reported to the team has increased by 458 percent, and the number of cites affected worldwide has increased by

[2] Joseph F. Gustin (2004) *Cyber Terrorism*, The Fairmont Press Inc, at 139.
[3] Ibid.
[4] Ferrera, Reder, Bird, Darrow, Aresty, Klosek & Lichtenstein (2012) *Cyber law - Text and Cases*, 3rd edition, South-Western Cengage Learning, at 401.

702 percent.[5] According to Malaysian police statistic, the number of cases investigated in 2010 was 1050 while in 2011 from January to July 2011 as many as 500 cases with the number of arrest for 2010 at 300 while for 2011 from January to July 2011 was 80. The police informed that the lack of awareness on computer security and mobile phone had caused many citizens to be cheated by cybercriminal syndicates.[6]

The rapid emergence of electronic related crimes, along with the legal requirement of proving them, and coupled by a slow legislative development in their suppression in the Jordanian laws have exacerbated the problems. Thus, it becomes necessary for the researcher to look at them with the aim of suggesting solutions to the above said legal problems/issues for Jordan. Since there are some specialized legislations dealing with cybercrimes in Malaysia, the researcher believes it appropriate to make a comparative analysis between these legislations and the Jordanian general criminal legislative rules in order to deduce specific rules concerning cybercrimes in a way that would benefit the Jordanian legal system. Moreover, Malaysia, once a colony of the UK, is a fast emulator to the laws of the United Kingdom, a leading country in the legislation against cybercrimes. The fact that Malaysia too is an Islamic country makes Malaysia one of the best comparators and sources of reference for Jordan to look up to in legislating her own specific laws against cybercrimes. Cybercrime for the purpose of this research is only focusing on the crimes under the Computer Crimes Act 1997 of Malaysia and is not intended to discuss cybercrimes in other statutes such as the Multimedia and Communication Act

[5] F. Lawrence Street & Mark P Grant (2000) *Law of the Internet*, Lexis Publishing, at 800.
[6] Utusan online, *Ramai tertipu jenayah siber* (many were cheated of cybercrime), http://www.utusan.com.my. 9/12/2011 - viewed on 18/11/2011.

of Malaysia and cyber related crime which may be investigated and prosecuted under the Penal Code of Malaysia.

1.1 STATEMENT OF PROBLEM

The main problem concerning the issue of cybercrime in Jordan stems from the absence in Jordan of a specific code or law regulating cybercrime and the elements thereof. Hence, the Jordanian legislator and the judiciary have been applying the general criminal rules and the criminal procedural rules to cybercrimes, in addition to the application of the general rules of evidence. The traditional Jordanian criminal laws and general rules may not be adequate to deal with cybercrimes which call for special rules to both its substantive (*mens rea & actus reus*) and its adjectival laws (evidence and criminal procedure) for investigating, prosecuting and the punishment to be imposed on cybercrimes offenders. The offenders of cybercrime may call for different ways of punishing them, requiring a distinct penology approach too compared to traditional crime. Both the traditional Jordanian criminal laws and Egyptian criminal law faced many challenges in addressing cybercrimes for lack of the appropriate laws.

Investigating and prosecuting cybercrime is also a complicated problem and is not easy to collect the evidence which often than not is intangible and unseen, and is easily deleted or erased.[7] In the computer crimes field, criminal investigation, apprehension of the cybercriminals, evidence collection, witnesses and prosecution (jurisdiction) are much more difficult and complex than in most areas of criminal prosecution.[8] Combating cybercrimes would require sovereign States to cooperate in

---

[7] Jamīl ʿAbd al-Bāqy al-Ṣaghīr (2001) *Al-Jawānib al-Ijrā'iyyah li Jarā'im Almtaliga bil-Intarnit*, [Procedural aspects of crimes related to the Internet], Dar al-Nahdah al-'Arabiyyah, at 5.

8 F. Lawrence Street & Mark P Grant (2000) *Law of the Internet*, Lexis Publishing, at 799.

extradition of offenders and for mutual assistance in criminal matters to hand over her citizens as witnesses in the prosecuting sovereign State.

In cybercrime, its geographical jurisdiction at times could not be precisely specified due to the fluidity or intangibility of such crimes, as well as the absence of any specific rules concerning the same in the Jordanian legal system. Another issue that adds to the issue at hand is the retroactivity of the criminal rules related to cybercrimes, as well as the specification of the responsible parties. Evidencing cybercrimes is also another important issue that would puzzle the traditional legislators in providing evidence that proves the committing of a certain cybercrime due to their unforeseeable nature i.e. digital and forensic evidence. This is so because a user may gain unauthorized access to a registered computer user and perpetrated crime through it without the registered user knowing it. The presumption in evidence will be that the registered user is the suspect.

The complexity and ignorance of the information network by most people who tend to take for granted the security of their password, the ingenuity of hackers to get access to other registered internet users, as well as the difficulty of discovering the method by which such crimes are being committed only aggravate the problems for the enforcement, investigating, and the prosecuting authorities to convict and to punish cybercrime offenders.[9]

As highlighted above, those ever growing problems have driven the researcher to study how the Jordanian legislators can best addressed her own ever growing problem of cybercrimes. This marked absence of a specialized legislation regulating these type of crimes in the Jordanian legal system makes the Malaysian cybercrime laws crucial into the scope of the proposed research to discover how the Malaysian

[9] Read Colin Taper (1989) *Computer Law,* Longman Group UK Limited, 4th edition, at 367.

legislative system copes with cybercrimes under her specialised substantive law legislations (i.e. the Computer Crimes Act of 1997) as well as her adjectival laws (criminal procedure and evidence) hence the possibility of applying them to the Jordanian legal system. Consequently, Islamic law too shall be examined in this research in order to discover whether these specific regulations are available under Islamic law, at least in its legal theory and how they can be translated into the proposed Jordanian specific laws on cybercrimes.

1.2 OBJECTIVES OF THE RESEARCH

The research shall discuss cybercrimes in the Jordanian and the Malaysian legal systems, their elements, criminal procedures and evidence through the division of the research body into five main chapters, apart from the introductory and concluding chapters.

First, to examine the investigation, prosecution and sentences in the Malaysian criminal justice system for cybercrime offenders.

Second, to examine the investigation, prosecution and sentences in the Jordanian criminal justice system for cybercrime offenders in an analytical and comparative research methodology.

Third, to examine Islamic laws and how they could be translated and incorporated in the Jordanian cybercrime laws to facilitate the investigation, prosecution and punishment of cybercrimes offenders.

Fourth, to propose recommendations for improvement to Jordanian laws in particular to enact her own specific law to deal with cybercrime.

1.3 RESEARCH QUESTIONS

1. How would cybercriminals be investigated, prosecuted and dealt with by the courts in Malaysia and Jordan?
2. Which is the competent court to hear cases and litigations related to cybercrimes? And
3. Are the general rules of evidence on cybercrimes adequate, and what are the effects of the absence of specialised laws that regulate cybercrimes and its evidence?

1.4 SCOPE OF RESEARCH

Cybercrimes for the purpose of this research means cybercrimes under the Computer Crimes Act 1997 of Malaysia, and this research is not intended to discuss cybercrimes in other statutes such as in the Multimedia and Communication Act of Malaysia or cyber related crime under the Penal Code of Malaysia. The cut off date of the applicable laws and regulations related to cybercrimes in the Jordanian and Malaysian legal systems shall be as at 1/6/2010. However, any post development after the date in Malaysia can be mentioned.

The research is not intended to discuss the operational matters or problems such as the competency and lack of manpower on the part of the investigating, prosecuting and judicial officers on cybercrime though those issues may be highlighted wherever relevant in the discussions.

1.5 RESEARCH METHODOLOGY

The research shall adopt the qualitative and doctrinal research methodology using secondary and primary data (the interviews). From the secondary data, primary

sources (statutes) and secondary sources such as case laws, online legal sources, journal articles, books etc) are relevant. Therefore, the researcher will utilise library materials, such as decided cases and statutes, books on cybercrime for the purpose of examining the various legal rules regulating cybercrimes in the Jordanian and Malaysian criminal justice systems.

The relevant statutes that deserve to be looked into are as follows–

MALAYSIA

1. Child Act of 2001 (Act 611);
2. Courts of Judicature Act 1952 (Act No.26);
3. Subordinate Courts Act 1948 (Act 92);
4. Computer Crimes Act of 1997 (Act 563);
5. Criminal Procedure Code (Act 593);
6. Police Act 1967 (Act 344);
7. Communication and Multimedia Act 1998;
8. Extradition Act of 1992 (Act 479);
9. Mutual Assistance in Criminal Matters Act of 2002 (Act 621); and
10. Evidence Act 1950 (Act 56).

JORDAN

1. Criminal Procedure Code of 1961 (Act 9), as Act (15) for 2006;
2. Penal Code 1960 (No. 16), as Act (12) for 2010;
3. The Nizamiyyia Courts Establishment Law of 1952 (Act No.26), as Act (No. 17) for 2001;
4. Police Act 1965(Act No. 38);
5. Military Penal Code 2006 (No. 58);
6. Military Courts Establishment Law 2006(No. 23);

7. Magistrate Courts Act 1952(No. 15) as (No. 30) for 2008;
8. Courts of State Security Code 1959 (Act 17);
9. High Felonies Court Code 1986 (Act 19);
10. Electronic Transactions Law (No. 85) of 2001; and
11. Extradition Act (1927), Child Code 1968 (Act No. 24).

Any international treaties and conventions could be highlighted and the extent to which the Jordanian and Malaysian jurisdictions adhere to such international rules. This would be for the purpose of filling in the gaps to the Jordanian and the Malaysian legislations with regards to the legislative rules regulating cybercrimes, and discovering the links of international cooperation for providing and facilitating evidence that proves such crimes, knowing that cybercrimes are, more often than not, international in nature. Hence, the issue of legal jurisdiction as to the competent jurisdiction in hearing cases of cybercrimes where the crimes are international in nature.

The doctrinal approach will require a comparative analysis of the various laws applicable to cybercrimes in Malaysia and Jordan. The similarities and differences of the two legal systems shall be compared and commented on. This shall be for the purpose of discovering the gaps and weaknesses in the Jordanian legislations, bearing in mind the absence of specialised laws regulating cybercrimes in Jordan, in order to find out the possibility of applying the appropriate Malaysian legislative rules related to cybercrime in Jordan. It will also necessitate a critical approach to be taken in order to discover the shortcomings, if any, in the Malaysian legislations before embarking on such an application or adoption process for Jordan. The researcher also intends to interview a few Jordanian judges for their opinions how computer crimes can be adequately dealt with from both the substantive and adjective laws (evidence &

procedure), and how Islamic law too would deal with them as far as the Islamic legal theory is concerned.

1.6 SIGNIFICANCE OF RESEARCH

The central theme of the research is that Jordan lacks the legal framework or the necessary laws to deal with cybercrimes in as far as investigation, prosecution and punishment of cybercrimes offenders are concerned. Cybercrimes being recent phenomena in most society including Jordan, it is urgent that the Jordanian government addresses it by having specific laws to deal with it. The Malaysian Computer Crimes Act, the relevant provisions provided in the Malaysian Criminal Procedure Code and Evidence Act may provide a good model for Jordan to adopt.

1.7 OUTLINE OF RESEARCH STRUCTURE

Chapter one, which is the present chapter, covers the essential information about the research to give any reader a good insight of the nature and scope of the research.

Chapter two provides the definition of cybercrime in both literal and technical definitions, in addition to the definition of cybercrime under the Malaysian and the Jordanian legal systems. The elements of cybercrime under the Malaysian and the Jordanian legal systems are provided by this chapter. It also serves as the background to the following chapters.

Chapter three which is a continuation of chapter two highlights the legal control that existed in 1997 in Malaysia to regulate the misuse of computer and internet under Computer Crimes Act of 1997. The legal issues related to investigation and prosecution of cybercrime offenders under Malaysian legal system are addressed in this chapter. The legal issues of cybercrime discussed in this chapter are extradition

and mutual assistance in criminal matters which are intertwined with investigation and prosecution (jurisdiction and punishment) of cybercrime offenders.

Chapter four dealt also with investigation and prosecution of cybercrime under the Jordanian legal system which is still applying the traditional criminal rules concerning cybercrime. The legal issues of cybercrime discuss in this chapter are extradition and mutual assistance in criminal matters which are intertwined with investigation and prosecution (jurisdiction and punishment) of cybercrime offenders of which Jordan is not quite equip to deal with cybercrimes. A selective comparison with the Malaysian Computer Crime Act of 1997 will demonstrate the inadequacies or gaps in the Jordanian traditional criminal laws to combat cybercrimes, and how those gaps or inadequacies in Jordanian laws can be minded and mended to effectively combat cybercrimes by having similar legislation.

Chapter five dealt with the evidence of cybercrime under both the Malaysian and Jordanian legal systems. The legal burden and evidential burden of proof, the standard of proof, the modes of evidence, the admissibility and the weight of the evidence to successfully prosecute cybercrime offenders are discussed in this chapter with special reference to Islamic law.

Chapter six which is the final or the concluding chapter, summaries the findings of the research and recommendations for Jordan how she can best addressed the cybercrime problems.