2009

Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence

Alaeldin Mansour Safauq Maghaireh
University of Wollongong

Recommended Citation

Maghaireh, Alaeldin Mansour Safauq, Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence, Doctor of Philosophy thesis, Faculty of Law, University of Wollongong, 2009. http://ro.uow.edu.au/theses/3402

JORDANIAN CYBERCRIME INVESTIGATIONS: A COMPARATIVE ANALYSIS OF SEARCH FOR AND SEIZURE OF DIGITAL EVIDENCE

This thesis is submitted in fulfilment of the requirements for the award of the degree

DOCTOR OF PHILOSOPHY

from the

UNIVERSITY OF WOLLONONG

by

ALAELDIN MANSOUR SAFAUQ MAGHAIREH

FACULTY OF LAW

2009

Certification

I, Alaeldin Mansour Safauq Maghaireh, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Law, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Alaeldin Mansour Safauq Maghaireh

31 March 2009

To
My devoted Mother who sacrificed the most for our joys

Abstract

Over the past half of a century, international society, particularly across the industrially developed world, has experienced an unprecedented technological transformation. The ubiquity of digital technology and its smooth integration with human activities has brought tremendous advantages. Simultaneously, diverse new activities called 'cybercrimes' have emerged in association with this technological revolution. Legal scholars have addressed these crimes and delivered initially controversial arguments regarding the adequacy of the traditional substantive and procedural laws to effectively criminalise and deal with them. Many developed countries, such as Australia and the USA, responded to the problem of cybercrime in a variety of ways. By contrast, in Jordan, there is no comprehensive law addressing cybercrime but a handful of legislative provisions that were originally enacted to protect physical objects.

This study is focused on Jordan and its need for law reform. Australia and the United States were selected for comparative study because they are already well advanced in their experiences of and in their legal responses to cybercrimes, thus providing benchmarks for Jordanian developments. In 2001, Australia enacted a comprehensive law, the *Cybercrime Act* 2001, and established the Australian High-Tech Crime Centre. The USA enacted its *Computer Fraud and Abuse Act* (CFAA) 1984.

Jordan has long understood the importance of Information Technology (IT) as a key element to improve the quality of life of its people. The *Electronic Transaction Act* 2001 and *Telecommunications Law* 1995 demonstrate this. It also established a Computer Crime Unit as a part of the Public Security Directorate to investigate cybercrime and to provide laboratory services in the inspection and analysis of digital evidence. However, Jordan's lack of cybercrime legislation is problematic because cybercrimes are borderless crimes. Jordan's lack can influence the rest of the world by creating, for instance, jurisdictional havens. The novelty of cybercrime challenges the existing Jordanian models of law enforcement investigations. Traditional laws are either too narrow or inappropriate to address all the forms of cybercrimes and deal with search and seizure of digital evidence in adequately.

This thesis examines several major themes associated with cybercrime investigation confronted by Jordanian law enforcement officers executing searches and seizures of computers. It concentrates on the inefficiency and ineffectiveness of traditional Jordanian laws in coping with cybercrime investigations. It critically examines and compares the procedures of search and seizure of computers in Australia and the USA. The thesis aims to contribute to the streamlining and strengthening of search and seizure procedures in Jordanian cybercrime investigations.

Acknowledgment

I wish to express my sincere thanks to the many people who have assisted me with the various aspects of my work. First and foremost, I offer my sincere thanks to my supervisor, Professor Greg Rose, for his valuable guidance and support during the writing of my thesis. I gratefully acknowledge his suggestions and constructive criticism at some crucial points in the course of this thesis. I am also grateful to him for his patience, encouragement, and commitment to this thesis. I am deeply indebted to my co-supervisor, Associate Professor Doug MacKinnon for constant support, encouragement, inspiration and guidance since I started studying English in the University of Wollongong. This thesis would not have progressed to completion without their continual enthusiasm, support, and ideas.

I would like to thank my wife, Dr Lina Saleem, for her love, care and extraordinary support throughout my long journey.

In the early stages of this research I received useful information regarding cybercrime investigation from Australian High Tech Crime investigators, Nigel Phair and Glen Mattocks. Also, I wish to acknowledge the co-operation of the Jordanian Computer Crime Unit for allowing me to obtain limited access to data and to interview one of their investigators, 1st Lieutenant Ayman Bani-Hani. I would like also to record my thanks to Magistrate Judge Montaser Obeidat and lawyers Frias Al-Qudah and Arab Younis for providing me with judicial decisions and information about cybercrime investigation in Jordan.

I would also like to thank my work colleagues at the Centre for Transnational Crime Prevention who are here today for their support and friendship, Tracy Wood, Jessica Lopez, Adam Dolnik, Dan Howard, Peter Ridgway, Mark Loves and Professor Duncan Chappell. I also wish to thank my former colleagues at the CTCP, Hugh Dixon, Gregor Allan, Violeta Trajcevska, and Hoa Phuong.

Last but not least, I would like to thank my beloved family which has supported me endlessly in completing this Ph.D. My mother and my siblings Read, Laith, Khlood, Khaleda, Samar and Sahar, although physically far away from me the whole time, have always been very near to my heart and my mind. Thank you for your love and enduring

patience. Then I thank my mother-in-law, Dr Kawther and my brothers-in-law, Khaldoon, Nabiha, Youns, and Mohammad for their unremitting support and continuous encouragement.

Glossary of Abbreviations and Acronyms

ABA	Australian Banker Association
AFP	Australian Federal Police
APEC	Asian-Pacific Economic Co-operation
ATM	Automatic Teller Machine
ATT	Administrative Appeals Tribunal
BBS	Bulletin Board System
CCC	Computer Chaos Club
CCTV	Closed-Circuit Television
CFAA	Computer Fraud and Abuse Act 1984
CICs	Cybercrime Investigation Centres
CNN	Cable News Network
CoE	Council of Europe
CPPA	Child Pornography Prevention Act
CSI	Computer Security Institute
DDoS	Distributed Denial of Service
DNS	Domain Name System
DOJ	Department of Justice
DoS	Denial of Service
DPP	Director of Public Prosecutions
DSEA	Domestic Security Enhancement Act
DVD	Digital Versatile Disc
EPU	Environmental Police Unit
FACTA	Fair and Accurate Credit Transactions Act
FIDNET	Federal Intrusion Detection Network
FTC	Federal Trade Commission
FRE	Federal Rule of Evidence
GP	General Prosecutor
GPD	General Prosecutorial Department
HTC	High-Tech Crime Centre
HTTP	Hypertext Transfer Protocol

ICMP	Internet Control Message Protocol
IO	Offensive Information Operation
IRC	Internet Relay Chat
ISN	Initial Sequence Number
ITADA	Identity Theft and Assumption Deterrence Act
KB	Kilobytes
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
MLAT	Mutual Legal Assistance Treaty
NII	National Information Infrastructure
IACIS	International Association of Computer Investigative Specialists
IP	Internet Protocol
ISP	Internet Service Provider
ISN	Initial Sequence Number
ITADA	Identity Theft and Assumption Deterrence Act
JCCU	Jordanian Computer Crime Unit
JD	Jordanian Dinar
JPEG	Joint Photographic Experts Group
JPSD	Jordanian Public Security Directorate
MSN	Messenger Service Network
PC	Personal Computer
PDA	Personal Digital Assistance
PSD	Public Security Directorate
PGP	Pretty Good Privacy
PROTECT	Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act
RAM	Random Access Memory
ROM	Read-Only Memory
RTA	Road Traffic Authority
SMTP	Simple Mail Transport Protocol
SNN	Social Security Number
SYN	Synchronize

SWGDE	Scientific Working Group on Digital Evidence
TCP	Transmission Control Protocol
TAP	Technological American Party
TWHS	Three-way Handshake
UDP	User Datagram Protocol
UN	United Nations
URL	Uniform Resource Locator
USB	Universal Serial Bus
WWW	World Wide Web
YIPL	Youth International Party Line

Table of Contents

1 GENERAL INTRODUCTION

Introduction

The invention of the computer is one of the pivotal events in human history. It is compared to the most significant and prominent developments witnessed by human beings in the late eighteenth and early nineteenth centuries.[1] It has culminated in the prevalence of the Personal Computer (PC), which forms the nucleus of the Information Age. In conjunction with such rapid developments, the marriage between computers and communication systems ushered in the birth of cyberspace.[2] Virtual world, Internet, digital community, cyberworld and cyberspace are almost used synonymously.[3]

The prefix 'cyber' is commonly used to describe online activities[4] constantly exchanging information online, and using cyberspace applications, such as chatting, e-mail, World Wide Web (WWW),[5] and so on.[6] Space, on the other hand, was exclusively used for a while in astronomical fields to describe the region beyond earth's atmosphere,[7] such as a solar system, other planets, and stars. The same terminology combined with 'cyber' transmitted to information technology (IT) to describe 'the virtual shared universe of the world's computer networks',[8] such as online conversations, chat rooms, communications, and e-commerce.

It is undoubtedly that new aspects of crimes and criminals have been shaped by cyberspace. The term 'Cybercrime', therefore, is used to describe a wide range of

[1] See generally, Vincent Mosco, *The Digital Sublime* (2004) 18.

[2] The term "Cyberspace" was first coined by William Gibson in his novel *Neuromancer* (1984) to describe a fictional and visionary world experienced by millions of users in every day. See, William Gibson, *Neuromancer* (1984) 67.

[3] See, eg, Narushige Shiode, *An Outlook For Urban Planning in Cyberspace: Toward The Construction of Cyber Cities With The Application of Unique Characteristics of Cyberspace* (1997) UCL Centre for Advanced Spatial Analysis <http://www.casa.ucl.ac.uk/planning/articles2/urban.htm> at 1 May 2006.

[4] Douglas R Groothuis, *The Soul in Cyberspace* (1997) 13.

[5] World Wide Web is one of the common information services available on the Internet. See, ibid.

[6] Tom O'Connor, *Cybercrime: the Internet as Crime Scene* (2005) North Carolina Wesleyan College <http://faculty.ncwc.edu/toconnor/315/315lect12.htm> at 11 April 2006.

[7] See, eg, *Space* <http://www.answers.com/topic/space> at 5 November 2005.

[8] Technologically, cyberspace is defined as 'a bio-electronic environment of knowledge that exists everywhere there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves'. See, Paul Shafer, *Freedom, Community and the Third Wave* (1996) Electronic Frontier Foundation <http://www.eff.org/Misc/Publications/E-journals/CyRev/cyrev4.html#freedom> at 26 August 2005.

virtual illegal activities that takes place in cyberspace, such as hacking, communications systems sabotage and trespass.

This chapter focuses on the fundamental aspects of cybercrimes as a new phenomenon with particular reference to cybercrime definitions, classifications, and criminals of cyberspace. The given definitions of cybercrime will be analysed and divided into two main general definitions, narrow and broad, and a new definition of the cybercrimes will be suggested and analysed. After that, the main common cybercrime classifications will be refined and compiled into two categories to serve the research objectives. Finally, the developing history of hackers as the typical criminal of cyberspace will be analysed and compiled into two main schools, an old and new school, and other criminals involved in cyberspace will be defined and distinguished from different types of cyber criminals.

1.1 Cybercrime Definition

A definition for cybercrime is necessary to delineate the outer limits of the subject of study and to distinguish it from other types of real world crimes and Offensive Information Operation (IO).[9] In addition, a cybercrime definition helps to figure out the most appropriate terminology to be used, such as cybercrime itself, computer-related crime, or other terms. Finally, identifying an accurate term for illegal activities taking place in cyberspace will enable the identification and differentiation of cybercrime sub-categories and investigations responsibility.

Basically, a wide range of differences at the international level usually precludes reaching a unanimous definition of a controversial phenomenon,[10] just as political,

[9] US Department of Defence Directive S-3600.1 defines Information Operations as 'actions taken to affect adversary information and information systems while defending one's own information, and information systems'.Thomas C Wingfield, *Legal Aspects of Offensive Information Operations in Space* Air University <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.doc> at 3 March 2006. Another definition is: 'actions taken to affect adversary information and information systems and defend one's own'. According to Zanini and Edwards, three types of offensive IO can be used by terrorist groups: first, perception management and propaganda; second, a disruptive attack; and, finally, a destructive attack. Cyberterrorism and cyberwar are types of offensive information operations. See, eg, Michele Zanini and Sean J A Edwards,' The Networking of Terror in the Information Age' in John Arquilla et al, (eds), *Networks and Netwars: the Future of Terror, Crime, and Militancy* (2001) 29, 41.

[10] Alaeldin Maghaireh, 'Combating Cyberterrorism: The Response from Australia and New Zealand' in James Veitch (ed), *International Terrorism: New Zealand Perspectives* (2005) 81, 83.

social, economical, and religious concerns all conspire to hamper an accredited definition.[11] For example, the international community has not yet reached an approved definition of terrorism, but more than a hundred scholarly definitions of terrorism have been put forward.[12] In a similar manner, while cybercrime is widely considered as a new phenomenon compared with older, real world crimes, there is no internationally unanimous definition.[13] The principal obstacle to reaching a comprehensive definition of cybercrime is that IT is a rapidly evolving arena, which allows ever more innovative crimes to be committed in cyberspace. Nevertheless, academics researching in the emerging field of cybercrime studies have dedicated their efforts to an exhaustive definition of cybercrime. They interchangeably used terms such as computer crimes, computer-related crimes, electronic crimes, digital crimes, info highway crimes,[14] cyber-related crimes,[15] cyber crimes,[16] high-tech crimes, computer abuse, computer fraud, and Internet crimes, all of which describe illegal activities taking place in cyberspace or ones associated with computer networks. Arguably, this legal jargon can be condensed into no more than two general headings, 'cybercrime' and 'computer crime'. As will be explained later, 'cybercrime' and computer crime terminologies are interchangeably used in this research.

Cybercrime definitions can be divided into two groups. The first group adopts a narrow conception of cybercrime, while the second group presents a wide conception of cybercrime. But first, it is an absolute prerequisite to define a crime.

A 'crime' can be defined generally as 'an act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law'.[17] Two points in this definition are especially worthy of notice as their applicability to cybercrime is different from real

[11] Ibid.

[12] See, eg, Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (2005) Federation of American Scientists < http://www.fas.org/sgp/crs/terror/RL32114.pdf> at 9 July 2005.

[13] Micheal J. O'Brien, *Computer Crime* <http://www.mobrien.com/computer_crime1.htm> at 18 August 2005.

[14] See, eg, Gene Stephens, Computer Crimes Will Increasingly Invade People's Privacy' in Paul A. Winters (ed), *Current Controversies: Computers and Society* (1997).

[15] See, eg, Herman T Tavani, 'The Uniqueness Debate in Computer Ethics: What Exactly is at Issue, and Why Does it Matter' (2004) 4 *Ethics and Information Technology* 37, 39.

[16] See, eg, Peter Stephenson, *Investigating Computer-Related Crimes* (2000) 3.

[17] *Crime definition*, Webster's Ninth New Collegiate Dictionary < http://dict.sztaki.hu/webster/webster> at 22 August 2005.

world crimes. The first is that a person is legally punished for a negative or a positive action committed contrary to the law.[18] The negative element of this point is not applicable to cybercrime because no cybercrime is committed by negative actions. These negative actions are described in chapters 3 and 4. The second point is 'that no matter how immoral, reprehensible, damaging or dangerous an act is, it is not a crime unless it is made such by the authorities of the state'.[19] This point is applicable to cybercrime as some aspects of cybercrime are not criminalised in Jordan. These crimes are also described in chapters 3 and 4.

a) Narrow Conception of Cybercrime

Richard Power identifies computer fraud[20] as 'computer-related crimes involving deliberate misrepresentation or alteration of data in order to get something of value'; he defines computer abuse, on the other hand, as 'wilful or negligent unauthorised activity that affects the availability, confidentiality, or integrity of computer resources'.[21] Forester and Morrison defined computer crime as 'a criminal act that has been committed using a computer as the principal tool'.[22] Parker, in his early writing on computer crimes, defined computer crimes as 'any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain'.[23] As the phenomenon evolved, a new definition was adopted by the same author. That innovative definition, however, focused on the knowledge of computer technologies to commit computer-related crimes as its sole prerequisite.[24] Smith, Grabosky and Urban, renowned cybercrime scholars, distinguish between 'cybercrimes' as a single word and 'cyber crimes' as a descriptive term.[25] They argue that the 'former encompass new criminal offences perpetrated in new ways and the latter is conventional crimes perpetrated using new technologies'.[26]

[18] Katherine S Williams, *Textbook on Criminology* (5th ed, 2004)12.
[19] Ibid.
[20] The terms 'Computer fraud' and 'Computer abuse 'are used here, because the same terms used by Richard Power.
[21] Tavani Q Chirillo, *Information Technology and Citizen's Rights* (2002) 176.
[22] Tom Forester and Perry Morrison, *Computer Ethics* (2nd ed, 1994) 29.
[23] See, Donn Parker, *Crime by Computer* (1976) 12.
[24] K M Jackson, J Hruska, and Donn B Parker, *Computer Security References Book* (1992) 439.
[25] Russell G Smith, Peter Grabosky and Gregor Urbas, *Cyber criminals on trial* (2004) 6.
[26] Ibid.

In a similar vein, the Australian Bankers' Association (ABA) has defined cybercrime as 'any crime effected or progressed using a public or private telecommunications service'.[27] The Department of Justice (DOJ) of USA offers a more comprehensive definition of computer crime than the ABA's. It defines computer crimes as 'any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution.'[28]

It can be seen that these attempts have defined cybercrime by focusing either on a specific type of cybercrime, such as using a computer system to commit a crime, or on the culprit's motivation behind the attack, such as the pursuit of something of value (see Richard, Forester, Morrison, and Parker above). Those definitions are narrow, because of the wide range of cybercrimes motivated by technological challenge, and creativity. Smith, Grabosky and Urban's definition omits the inextricably interlinked cybercrimes. A single offence could be categorised under both terms. For instance, an Internet Protocol (IP) spoofing attack is the creation of IP packets with a forged source IP address (i.e. a new crime). This attack used to gain an initial foothold or root access on the Internet to carry out a further crime such as internet fraud (i.e. a conventional crime perpetrated using new technology). Should such a crime be classified as a cyber crime or a cybercrime? It is a cybercrime in the first act, i.e. creation of IP packets, and a cyber crime for the second act, i.e. using an IP forged to commit a traditional crime. The distinction, however, between cybercrime and cyber crime is important in terms of providing the appropriate benchmark for classifying cybercrimes into two categories. Therefore, the thesis will adopt this distinction to distinguish between two types of crimes, namely cybercrimes and cyber crimes.

In a similar manner, the ABA and DOJ definitions have adopted one technical facet of cybercrime, such as using a communication service to commit a crime or the requirement for specialist knowledge of computer technology (see ABA, DOJ definition above).

[27] *Cybercrime Inquiry* (2004) Australian Bankers' Association Inc < http://www.bankers.asn.au/ArticleDocuments/CybercrimeInquiryFinal.doc> at 3 September 2005.

[28] J Carter and Audrey Perry, 'Computer Crime' (2004) 41 *American Criminal Law Review* 313, 314.

b) Broad Conception of Cybercrime

A second group of scholars and international organisations have adopted a broad conception of cybercrime definition. Steven Branigan, a renowned computer expert, defines cybercrime as occurring when 'the criminal uses technology in the commission of a crime, or a criminal attacks technology and makes it the target of the crime'.[29] The definition identifies the binary nature of cybercrime; the computer is the target or tool of the crime. Similarly, Patrick Hess, the author of *Cyberterrorism and Information War,* defines cybercrime as 'harmful acts committed from or against a computer or network'.[30]

Internationally, the Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders in Vienna in April 2000 defined cybercrime as 'Any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment'.[31]

It seems, however, that both of these groups have to some degree failed to present a fluid conception of cybercrime. The growing concern over cyber attacks against critical infrastructure and the nascent threat of cyberterrorism demand urgent efforts at all levels to reach an agreed definition, which distinguishes between cybercrime and other cyber-illegal activities.

Therefore, the author suggests an exhaustive definition avoiding the shortcomings mentioned earlier. Hence, cybercrimes can be defined as 'any illegal activities simultaneously associated with information technologies and cyberspaces, intentionally perpetrated for tangible or/and intangible benefits and primarily motivated by self-interest'. According to the definition, the theft of computer hardware devices would not qualify as a cybercrime, but a real world crime. Moreover, offences where a computer system is incidentally used in a crime, such as storing illegal drug information, also would not be considered as a cybercrime. In addition, the definition includes cyberterrorism but not cyberwar, because the former is mainly motivated by self-

[29] See, Steven Branigan, *High-Tech Crimes Revealed* (2005) 273.

[30] See, Patrick Hess, *Cyberterrorism and Information War* (2002) 24.

[31] *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* (2000) United Nations <http://www.uncjin.org/Documents/congr10/10e.pdf page4> at 20 August 2005.

interest, such as satisfying a perceived religious duty of cyber Jihad.[32] Meanwhile, the latter is coordinated and committed by states in order to achieve political goals since such action would have an adverse effect on the information technology capabilities of the attacked country. Finally, a crime perpetrated by a stand-alone computer,[33] such as forging a transcript, is a computer-related crime but not a cybercrime, as indicated below.

The line that can be drawn, therefore, to differentiate between cybercrime and computer related crime would depend upon the relationship that exists between a computer and cyberspace. The correlation between cyberspace and computer systems is conceivably parallel to the relationship that exists between a soul and a human body: assuming that the soul is cyberspace and a stand-alone computer is the human body, when the soul leaves the human body, the crime committed on the latter after that would be differently qualified, i.e. corpse abuse. For example, a deliberate act causing death is a homicide, but the same act executed on a deceased person would not be labelled as a murder crime. In the context of search and seizure procedures, however, computer-related crimes and cybercrimes are dealt with equally. Computer forensics procedures are used in both types of crimes.[34]

1.2 Cybercrime Classifications.

Cybercrime classification is significantly derived from the broad definition of cybercrime. However, cybercrime can be divided into different categories. It has been categorised based on the type of attacks or the victim of the crime or the criminal motivations, and the role of the computer in a crime as well.

[32] Terrorist organisations, Muslim clerics and their sympathisers and supporters consider hacking in the name of Islam is justified. See, eg, Alaeldin Mansour Maghaireh, ‘Shariah Law, Cyber-Sectarian Conflict & Cybercrime: How Can Islamic Criminal Law Respond to Cybercrime?’ (2008) 2 *International Journal of Cyber Criminology* <http://www.cybercrimejournal.co.nr>.

[33] A stand-alone computer is a computer not connected to networks, such as the Internet or a local network.

[34] See Section 5.2.2.1 for more information on computer forensics.

The legitimate ground for having a separate category of cybercrime or framing such a category was elucidated by Tavani when he introduced three different perspectives: legal, moral and informative or descriptive perspective.[35] He stressed that:

> From a legal perspective, computer crime might be viewed as a useful category for prosecuting certain kinds of crimes...From a moral perspective the need for a separate moral category is that many of the ethical issues associated with computer crime also border on distinct, but related, issues involving intellectual property, personal privacy, and free speech in cyberspace… From a descriptive perspective…it could help us gain a certain level of clarity and precision in analysing crimes involving the use of computer technology.[36]

Accordingly, from a legal perspective, having a cybercrimes classification is useful for deciding whether a crime involving the presence of IT in its preparation or execution is a cybercrime investigated by a Hi-Tech Crime Unit and prosecuted under *Cybercrime Acts*, or a real world crime. Law enforcement agencies are specialised and assigned the task of investigating particular types of crimes, for example, a Hi-Tech Crime Unit investigating only cybercrime. Indeed, categorising cybercrimes terminates disputes over investigating responsibilities and the prosecution's duties. For example, the manufacture of counterfeit $100 bills (using a computer system) is assigned to the department of forgery, but counterfeiting Internet Protocol (IP) packets is assigned to the department of Hi-Tech Crime Unit.[37] From a descriptive perspective it helps to describe and analyse each cybercrime precisely.

Criminology scholars, therefore, have divided the crime that is associated with IT into different categories. Some of these categories are broad enough to include real world crimes, such as categorising based on the type of the attacks, motivations, and the victim of the crime. Seger, Icove and Vonstroch classify cybercrimes into four categories using the type of the attack and its prevention tactics as a benchmark.[38] The first category they claim as a computer crime is the breaching of physical security, such as Denial of Service (DoS) attack by shutting off the power or by using electromagnetic disturbances. (DoS attacks are described and analysed in Chapter 3.) It can be seen that

[35] See, Herman T Tavani, 'Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace' (2000) *Computers and Society* 3.
[36] Ibid.
[37] See Section 4.4.1 for more information about cybercrimes associated with IP technology.
[38] Karl Seger, David Icove, and William Vonstorch, *Computer Crime a Crime Fighter's Handbook* (1995) 35.

a physical action is necessary to commit the crime in this category and to prevent it as well. The second category is the breaching of personal security, such as by social engineering tricks[39] and committing identity theft.[40] The offender mainly uses a physical form, such as password scavenging, or electronic forms, such as web spoofing. Once the offender obtains confidential information, he can impersonate the victim and withdraw funds from the latter's account.[41] A breach of communication and data security is the third category.[42] This category primarily refers to data attacks or software attacks, such as a virus attack. Finally, breaches of operations security, such as 'IP spoofing',[43] are the fourth category.[44] It can be seen that classifying cybercrimes into four groups based on the type of attack (see Seger, Icove and Vonstroch above) is loose and leaves a broad range of traditional crimes, such as a physical damage of hardware caused by breaching physical security (first category) or breaching personal security (second category), such as password scavenging, to be classified as cybercrimes. On the other classification, Bernadette and Clemens have used the object of cybercrime as a benchmark to divide cybercrime into two categories.[45] The first category is cybercrime resulting in harm to property, such as Denial of Service (DoS), and cyber vandalism.[46] The second category is cybercrime resulting in harm to a person, for example cyberstalking,[47] and cyber pornography.[48] Classification of cybercrime, however, based on the object of the crime creates blurred boundaries among cybercrimes because the vast arrays of cybercrimes intersect and overlap.

[39] Social engineering is a low-tech trick, such as sending enticing e-mails to many Internet users. This trick is always combined with a technical trick such as a web spoofing to lure gullible Internet users to visit a phoney website and divulge their financial data, such as password, account details…etc. For more information. See Section 4.4.

[40] Seger, Icove, and Vonstorch, above n 38.

[41] Ibid.

[42] Ibid.

[43] IP is the abbreviation for Internet Protocol: it is a unique number used by a computer attached to a network to identify each computer connected to a LAN or the Internet. It works like a car plate. The attacker in IP spoofing counterfeits his IP to conceal the attack source and commit further crimes. See Section 4.4 for more information on the IP crimes.

[44] Seger, Icove, and Vonstorch, above n 38.

[45] Bernadette H Schell and Clemens Martin, *Cybercrime: A Reference Handbook* (2004) 30.

[46] Denial of Service attack (DoS) is one of the most recent cyber attacks committed by using hacking programmes, such as SYN Flood Attack. It is temporarily preventing a legitimate network from trafficking, or disrupting a connection between the client (Internet user) and the provider server (Internet provider). For more information. See Chapter 3.

[47] Cyberstalking can be defined as 'the use of information and communications technology (in particular the Internet) in order to harass individuals'. For more information. See Chapter 4.

[48] Cyber pornography is a traditional crime which has migrated into cyberspace and it has now three aspects, adult pornography, child pornography, and virtual child pornography. For more information, see Chapter 4.

A different classification mechanism, in which the vast majority of scholars agree, is that cybercrimes' best classification is based on the role of the computer system in a crime.[49] This classification has three categories.

The first category occurs where the computer may be an instrument used to commit conventional crimes.[50] Information technologies are widely used to commit traditional crimes. This category primarily refers to online and Automatic Teller Machine (ATM) fraud, identity theft, stalking, child pornography, salami technique,[51] and copyright infringements. Although, these offences are traditional crimes facilitated by computer systems, the emergence of cyberspace has created new dimensions which require innovative responses from law enforcement, because physical proximity is no longer intrinsic to commit traditional crime and the criminal capability is now amplified by the advent of cyberspace; the perpetrator may commit the crime anonymously, and without leaving a single trace. Also, because investigation procedures, including searching and seizing, applied to the above crimes are significantly different from the procedures applied to traditional crimes, Hi-Tech Crime Centres (HTCC) are involved in the investigation of such crimes.

The second category occurs where the computer is incidental to the commission of the crime.[52] This category includes all the conventional crimes that are merely facilitated by cyberspace, such as a drug dealer trafficking narcotics on the Internet, or using IT to conceal a crime, such as using encryption technology to hide and encrypt incriminating data. This sort of crime can be committed without utilising cyberspace or IT. The computer system is neither the principal tool in the crime nor the core of the crime, but it helps the crime to occur faster and makes it harder to trace and investigate.[53] Therefore, the suggested definition of cybercrime omits this category of offence.

[49] See, generally, Smith, Grabosky and Urbas, above n 25, 7.

[50] Ibid.

[51] Salami technique is a crime committed by using illegal concealed programmes operating alongside legitimate financial programs to debit a small amount of money from several accounts or from one account. See, eg, Jeremy R Poch, *Cyber-Crime and the Uphill Battle Faced by the Business World* (2005) University of Wisconsin Platteville <http://www.uwplatt.edu/csse/CSSE_411%20Papers%20and%20Presentations/CSSE411Spr2005/PochJ%20-%20%20Final%20Paper.doc> at December 2005.

[52] Smith, Grabosky and Urbas, above n 25.

[53] See, eg, David L Carter, *Computer Crime Categories: How Techno-criminals Operate* (1995) National Security Institute <http://nsi.org/library/compsec/crimecom.html> at 2 September 2005.

However, investigating this type of crime requires the use of similar investigative tools and procedures of cybercrimes.

Finally, the computer as the subject or the target of the crime is the third category of cybercrime.[54] Over the course of only a few decades, the world has become more and more dependent upon computers to function economically and socially. This dependence has spread to the general public with the introduction of the PC and the explosive growth of the Internet. As digital technology has become increasingly integrated into national infrastructures, and as the number of participants has grown, so too has the threat of cybercrime. In this category, the perpetrator attacks computer systems, networks, and cyber-services using cyber-tools. It encompasses TCP/IP crimes, cyber vandalism, cyber trespass and IP spoofing.[55] Crimes fall under this category - the subject of chapters 3 and 4 - are new crimes[56] perpetrated by a new generation of criminals. They are mainly motivated by human curiosity and the challenge of the computer system. The next section will explore the history and the new path taken by cybercriminals.

1.3 Cybercriminals

It is widely known that alongside cyberspace advantages, the dark side has been the advent of a novel pattern of crimes, perpetrators and motivations. While the real world criminal's character and motivations were deeply investigated by psychologists, the criminals of cyberspace as a new phenomenon of delinquency have been relatively ignored.[57]

Little research has been done regarding cybercriminal psychology.[58] Some patterns of cybercriminal psychologies are different from other real criminals.[59] Nevertheless, there

[54] Smith, Grabosky and Urbas, above n 25.

[55] These crimes are described in Chapters 3 and 4 respectively.

[56] Susan W Brenner, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 *Virginia Journal of Law and Technology* 13.

[57] See, eg, Gordon R Meyer, 'Hackers, Phreakers, and Pirates: The Semantics of the Computer Underground' in Grover Maurice Godwin (ed), *Criminal Psychology and Forensic Technology: a Collaborative Approach to Effective Profiling* (2001) 207, 208.

[58] Psychology is a scientific study of human behaviour, mental processes, and how they are affected and/or affect an individual's or a group's physical state, mental state, and external environment. *E Social Science Dictionary* <http://www.elissetche.org/dico/P.htm> at 3 July 2006.

[59] Some of the real world offenders, i.e. paedophiles, who have embraced cyberspace, have the same psychology as offline predators. For example, Operation Ore has revealed a wide range of male offenders ranging in age from 16 to 70 with a diverse range of occupations, including school teachers, police

is an implicit consensus among academics and computer experts on the basic traits that a typical cybercriminal owns. These attributes enable the cybercriminal to be categorised under the traditional theories or schools of psychology, for example the cognitive school or behavioural school.[60] Cognitive theories focus on an individual's mentality and internal feeling, such as anger, frustration, desire and despair.[61] In contrast, the behavioural theories address individual mentality in the social context, such as the impact of socio-economic status, race, and ethnicity on individuals. Cybercriminals can be classified under one or other of these schools, because they vary from an inept hacker to a professional criminal[62] and from middle class and desperate families to the bourgeoisie.[63]

Nowadays, cybercriminals are widely known as hackers[64] and their activities are called hacking,[65] which generally mean 'the process of attempting to gain unauthorised access into computer and communication systems'.[66] 'Hackers' and their activities, however, are a controversial issue amongst academics, law enforcers, computer experts, and

officers, university lecturers, students, postmen, scout leaders, and managers from commercial industry. Some of these offenders are non-computer literate. The operation was the first to shed light and provide an insight into the extent, breadth and diversity of cyber-paedophiles, their behaviours and offending types. See, Christiane Sanderson, *The Seduction of Children: Empowering Parents and Teachers to Protect Children from Child Sexual Abuse* (2004) 149. See also, Allyson MacVean, 'Understanding Sexual Predators on the Internet: Towards a Greater Knowledge' in Allyson MacVean and Peter Spindler (eds), *Policing Paedophiles on the Internet* (1st ed, 2003) 2, 4.

[60] Williams, above n 18, 174.

[61] Ibid 170.

[62] See, eg, Tai-hoon Kim, and Seung-youn Lee,' Design Procedures of IT Systems Security Countermeasures' in Osvaldo Gervasi, et al (eds), *Computational Science and Its Applications ICCSA* (2005) 468, 470.

[63] See, eg, Ed Norris, ' Protecting against Hacker Attacks' in Sanjiv Purba (ed), *Architectures for E-Business Systems: Building the Foundation for Tomorrow's Success* (2001) 699, 700.

[64] In his book, *Information Warfare*, Winn Schwartau says that the term hacker is derived from the word 'hackney' which means drudgery. See, Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (1st ed, 1994) 192. The *New Hacker's Dictionary* defines a hacker as 'A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary'. The *Oxford English Dictionary* defines a hacker as 'A person with an enthusiasm for programming or using computers as an end in itself'. See, Greg Lehey, *The term "hacker"* (2002) LEMIS <http://www.lemis.com/hacker.html> at 20 August 2005.

[65] The term 'hack' in information technology means an original move in programming or software usage, which enabled unforeseen computer operations or ones that were thought impossible. See generally, Olga Skorodumova, 'Hackers as Information Space Phenomenon' (2004) 35 (4) *Social Sciences* 105. Jude Milhon defined hacking 'the clever circumvention of imposed limits whether imposed by your government, your own skills or the laws of physics'. See Jude Milhon, *Hackers Lose a Patron Saint* (2003) WIRED <http://www.wired.com/news/technology/0,1282,59711,00.html> at 20 September 2005. For more information about other meanings of hacking, see generally, Forester and Morrison, above n 22, 77.

[66] Parker (ed), above n 24, 543.

hackers themselves. The argument has led to a distinction between different types of cybercriminals.

1.3.1 Hackers

Peter Lilly has stressed in his book *Hacked, Attacked and Abused* that, based on several studies which focused on hacker psychology, through interviews conducted with hackers, that the hacker profile, in general, is:[67]

- A white teenager;
- Having poor social skills;
- Speaking too loudly and/or quickly and/or in an unremitting monotone;
- Unresponsive to humour;
- Easily distracted but able to focus intently on technical problems; and
- Having an exceptional ability to mentally retain long strings of numbers.

According to Winn Schwartau the following personal qualities can be added.[68] They are:

- From dysfunctional families;
- Misfits and misunderstood; and
- They cannot get a date.

Ironically, it seems that the notion of mental disturbance among hackers has played a key role in the prosecution and sentencing of a number of young hackers.[69] Several convicted hackers have benefited from the psychological notion of mental disturbance and Internet addiction disorder.[70] For example, the British hacker, Paul Bedworth, a 19-year-old student accused of unauthorised access to several computer systems, was acquitted on the grounds that he was addicted to computing.[71]

[67] Peter Lilley, *Hacked, Attacked, and Abused: Digital Crime Exposed* (2002) 42.

[68] Schwartau, above n 64, 196.

[69] See, eg, Maura Conway, 'Cyberterrorism: Academic Perspectives' (Paper presented at the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, 28-29 June 2004) 45.

[70] See especially, Carla G Surratt, *Netaholics: The Creation of a Pathology* (1999) 58-59.

[71] Steve Gold, 'UK - Court Acquits Teenage Hacker', *Newsbytes News Network* (London), 17 March 1993.

The public and the media, however, have engaged in the debate pertaining to the controversial legitimacy of hackers' activities.[72] Some part of the debate has deviated to declare the myth of the hacker's and superhacker's existence,[73] and another to depict a white picture for hacking subculture.[74] This debate, however, has merely promoted vagueness about the real malignant of the hacking subculture, and the relationship between hackers and cybercriminals as well.

Initially, the public and the computing community praised the hacking world, believing that hacking would explore a computer system's vulnerabilities,[75] and lead to improving security measures. In contrast, law enforcers have strongly condemned hacking activities and consider hackers as criminals.[76] The debate has been significantly influenced by both the historical development of hacking, which spans nearly forty years, and the media.

The hacking phenomenon can be divided historically into two different schools, an old and a new school of hackers. The ideologies and behaviours of the hackers in each are different from the other school.

The old school of hacker was informally formed in 1950s by small and well-known groups of students and professors affiliated to technological institutions in the USA who acted for non-profit purposes.[77] In the early days of the hackers, the computing and programming industry were not completely integrated into public services nor considered a phenomenon worthy of mention in the mass media.

Nevertheless, commentators on the hacking phenomenon have described the first stage of hacking as a 'golden era of hacking'[78] or these hackers as 'computer virtuosos'.[79]

[72] See eg, Douglas Thomas, *Hacker Culture* (2002) 94. See also, Ryan Russell et al, *Hack Proofing Your E-Commerce Site: the Only Way to Stop a Hacker is to Think like One* (2001) 69.

[73] According to Pipkin the superhacker is a hacker who does not brag, does not post information on the internet; rather he watches and absorbs the information about new different ways of hacking and then attacks without leaving a trace. See, Donald L Pipkin, *Halting the Hacker: a Practical Guide to Computer Security* (2nd ed, 2002) 15.

[74] Thomas, above n 72.

[75] Vulnerabilities are weaknesses in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorised access to information systems. See, *Vulnerability* (2006) <http://www.answers.com/topic/vulnerability> at 3 April 2006.

[76] See, eg, Forester and Morrison, above n 22, 84.

[77] S Arrieta, *Hacker Categorized* (2000) MSC Institute of Technology <http://msc.edu.ph/wired/netspeak-15a.html> at 2 September 2005. See also, Andrew Ross, 'Hacking Away at the Counter-Culture' in David Bell, and Barbara M Kennedy (eds), *The Cybercultures Reader* (2000) 254, 256.

[78] See, eg, Steven Levy, *Hackers: Heroes of the Computer Revolution* (1st ed, 1984).

Hackers engaged in decoding intricate programmes and analysing computer puzzles. They spent long lonely hours in front of the little screen to learn more about a computer system and then to develop it by using their own ideas and techniques.[80] They were fascinated by the computer system and unintentionally observed an implicit ethical code.[81] During this era an ethical code was explicitly published and expressed in Steven Lavy's 1984 book, *Hackers: Heroes of the Computer Revolution*. In essence, the hacker golden era ethic reads as follows:[82]

1) All information should be free;
2) Access to all computer systems should be free;
3) Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position;
4) You can create art and beauty on a computer; and
5) Computer can change your life for the better.

The hackers' code of ethics demonstrated an independent set of principles as well as a first brick in the construction of the hackers' subculture.[83] However, hackers' ethics are not recognised by law enforcement agencies, because it seems like a virtual code written to justify illegal hacking activities. Nevertheless, most importantly, the old school of hackers did not show any sign of a malicious intention to destroy or interrupt computer systems. They were driven by the intellectual challenge and curiosity. Moreover, none of its members was ever prosecuted or accused of any criminal offences.[84] On the contrary, most of them have crafted a vast array of software programmes sparking the proliferation of information technologies and Silicon Valley start-up companies.[85]

[79] Sara Baase, *A Gift of Fire: Social, Legal, and Ethical Issues for Computer and the Internet* (2nd ed, 2003) 282.
[80] Ibid.
[81] Levy, above n 78, 26.
[82] Ibid 27.
[83] See, eg, Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (1995) 31. See also, Douglas Thomas, 'New Ways to Break the Law; Cybercrime and the Politics of Hacking' in Yvonne Jewkes, and Gayle Letherby (eds), *Criminology: A Reader* (2002) 388.
[84] In parallel, there were a few cases where a computer was used to commit offences. For example, in 1969, a young man, who was working as an expert accountant in a company, was sentenced to 10 years in prison for computer embezzlement. See Parker, above n 23, 71-79.
[85] For example, the former 'phone phreaker' Steve Wozniak became rich by co-founding Apple, one of the biggest computer companies. Also, the infamous hacker Kevin Poulsen, who went to prison, is now editorial director of a leading security information group called SecurityFocus.com. See, Thomas, above n 72, xi.

The new school of hackers, on the other hand, can be divided into two phases; each a new kind of hacker. The first stage of the new school of hackers, spanning from the 1970s to the mid-1990s, was triggered by the widespread use of the PC in developed countries and later on by the creation of cyberspace.[86] The transition of hacking from innovative exploration of computer systems to unauthorised intrusions and other sorts of illegal activities motivated by self-interest[87] was a fundamental shift in the hackers' subculture.[88] The ethical code gradually deteriorated, but in many cases where hackers were applauded by the mass media and described as 'White Hat' hackers or 'Heroes of Digital Culture'.[89] For example, a hacker who trespassed onto computer systems belonging to wealthy individuals and large corporations and then transferred money to poor individuals and small organisations was depicted as a 'Digital Robin Hood'.[90] As more new people joined the hacking community,[91] the term 'Cracker' was coined by the old school of hackers to distinguish between themselves and criminal hackers.[92] Scholars and computer experts have described the latter as the dark side of the hackers.[93] It is worth mentioning that there is a growing recognition of the crackers' own subculture. The majority of hackers do not show a malicious intention to destroy or interrupt a service, but crackers are driven by malevolent incentives. Crackers believe

[86] See, Young Susan and Dave Aitel, *The hacker's handbook: The Strategy behind Breaking into and Defending Networks* (2004).

[87] The first hacking activity motivated by self-interest was reported in the early 1970s, when an American student hacked in the Pacific Telephone Corporation's central computer. See Ulrich Sieber, *the International Handbook on Computer Crime* (1986) 9.

[88] Skorodumova, above n 65.

[89] Paul Taylor, 'Hacktivism: in Search of Lost Ethics' in David S Wall (ed), *Crime and the Internet* (2001) 59.

[90] Herman T Tavani, *Ethics and technology: ethical issues in an age of information and communication technology* (2004) 176.

[91] The first positive impression of hacking activities was delivered to the public by the release of the movie 'War Games' in 1983. See, Marc D Goodman, 'Why the Police Don't Care about Computer Crime' (1997) 10 *Harvard journal of law and technology* 465,469.

[92] 'White Hat' hacker is a term used by hackers and the computing community to describe a hacker who is interested in computer security and illegally exploring system vulnerabilities and who would impart information and cooperate with the owner before divulging it to the public. In contrast to a 'White Hat', 'Black Hat' hackers do not sensitively handle security holes. Cracker, on the other hand, is a controversial term used by computer experts and hackers to describe a hacker with a malicious intent. See, Young and Aitel, above n 86. See also, Majid Yar, 'Computer hacking: Just another case of juvenile delinquency?' (2005) 44 (4) *Howard Journal* 387. See also, Tavani, above n 90.

[93] Lilley, above n 67, 42.

that cracking activities should not be illegal or immoral;[94] while hackers keep a delicate line between immoral and ethical hacking.[95]

During this era, the political motivations of hacking also began to take a new shape. For instance, an American group established the 'Youth International Party Line'[96] (YIPL), which is the first American hackers' organisation to adopt a political agenda for cyberspace.[97] Nonetheless, this phase of hacking witnessed waves of legislation and criminal procedures against the phenomenon.[98] For example, in 1986 the USA enacted the *Computer Fraud and Abuse Act* (CFAA). Moreover, several notorious hackers were arrested and brought to trial. In 1987, for instance, eighteen hackers from New York were arrested on charges of illegally reprogramming memory chips in their mobile phones in order to make free calls[99] and, in 1990, 'Operation Sun Devil' was launched in fourteen USA cities to crack down on illegal computer hacking activities.[100] This stage in hacking culminated with the maturation of a complete virtual world: websites,[101] organisations,[102] magazines,[103] hacking tools, books,[104] conferences,[105] the Bulletin Board System (BBS), all supporting various agendas and motivations.

The second phase of the new school is the New Millennium hackers' school, or the hackers of the 21st Century. The participation of developing countries in this cyberspace world has enriched the hacking subculture. Vast arrays of hackers from the third world have joined the hacking community. They have created innovative hacking techniques,

[94] Bruce J Baird, Lindsay L Baird Jr and Ronald P Ranauro, 'The Moral Cracker?' (1987) 6 (6) *Computer & Security* 471.

[95] Kanaley Reid, 'Computer Hackers Wrestle with Often Ambiguous Morals of Cyberspace', *Knight Ridder/Tribune News Service* 23 August 1995.

[96] In 1973 the YIPL changed its name to the 'Technological American Party' (TAP). It published newsletter and information about 'phone freak' or 'freaking' - a type of computer-related crime that is perpetrated by a hacker to exploit telephone systems for the purpose of making free long-distance calls- after TAP terminated, the hackers' magazine 2600 was launched. See Taylor, above n 89, 62.

[97] Taylor, above n 89, 62-65.

[98] Kovacich Gerald L, 'Hackers: Freedom Fighters of the 21st Century' (1999) 18 (7) *Computers & Security* 573, 573.

[99] Forester and Morrison, above n 22, 35.

[100] Shredder, *Operation Sundevil* (1993) Hack Canada <http://www.hackcanada.com/blackcrawl/general/sundevil.txt> at 30 August 2005.

[101] For example, http://www.hackerscatalog.com.

[102] For example, Foundstone's Hacking School.

[103] For example, the quarterly 2600 Hackers Organisation Magazine.

[104] For example, *The Hackers Bible*, and *Hacking for the Beginning: Methods and Secrets* by Maxim Levin.

[105] For example, the Annual World Hacker Congress in Germany sponsored by Computer Chaos Club (CCC), and annual DefCon hacker gathering.

for instance the 'love bug' or 'I LOVE YOU' virus[106] was launched from the Philippines.[107] However, the new generation of cyber attacks have significantly turned the world's view against hacking activities. For example, the recent waves of cyber attacks against eBay, Yahoo, CNN, Amazon and other prominent websites were ample to revise media and public attitudes to hacking activities.[108]

Simultaneously, a new front of hackers' advocates was born to defend the hackers' subculture against a distorted image drawn by the mass media. For example, Goldstein, the founder and editor of the *Hacker Quarterly 2600* magazine, in an attempt to defend hackers writes:

> So far, the corporate media has done a very bad job… blaming hackers and in the next sentence admitting they have no idea who's behind it… claiming that hackers are behind it indicates some sort of knowledge of the motives and people involved. This could be the work of someone who lost their life savings to electronic commerce. Or maybe it's the work of communists. It could even be corporate America itself! After all, who would be better served by a further denigration of the hacker image with more restrictions on individual liberties?[109]

To distinguish among different types of the hackers, several academic scholars and organisations categorise hackers according to their own characteristics and motivations. For example, Peter Lilley and the Information Security School of Moscow have divided hackers into four categories. The former has named them as neo-hackers, crackers, freakers and script kiddies,[110] and the latter has classified hackers as jokers, frackers, professional crackers, and vandals.[111] Other scholars such as Donn Parker classify hackers into three different categories: benign, unsavoury and malicious hackers.[112] Also, Steven Philippsohn distinguishes between two types of hackers: external and

[106] See Section 3.2.2.1 for more information on viruses and methods of attack.

[107] See generally, Roderic Broadhurst, and Peter Grabosky, 'Computer-Related Crime in Asia: Emergent Issues' in Roderic Broadhurst and Peter N Grabosky (eds) *Cyber-Crime: The Challenge in Asia* (2005)1, 9.

[108] In 2000, an inept young hacker known as a MafiaBoy, for example, launched DoS attacks against prominent websites including CNN, Yahoo and Ebay, using Malware available online. See generally, Schell and Martin, above n 45, 59.

[109] Reid Skibell, 'The Myth of the Computer Hacker' (2002) 5 (3) *Information, Communication & Society* 336, 351.

[110] Lilley, above n 67, 41-42.

[111] Skorodumova, above n 65.

[112] Donn B Parker, *Donn Parker's Categories of Hackers* (1996) VirginiaTech <http://courses.cs.vt.edu/~cs3604/lib/Hacking/Parker.html#1> at 30 August 2005.

internal hackers.[113] The hackers' motivations are considered the principal point of distinction between hackers and crackers, as well as hacking capabilities.

1.3.2 Internal Cybercriminals

Computer crime surveys clearly demonstrate that a significant number of cybercrimes are perpetrated by internal culprits.[114] The surveys have come to support the conventional wisdom that the 'threat from inside the organisation is far greater than the threat from outside the organisation'.[115] The internal perpetrators range from high-ranking employees such as executive security managers, to disgruntled retired employees. Ulrich Sieber, a renowned computer crime expert, has mentioned in his book, *The International Handbook on Computer Crime,* that 'the majority of acts of sabotage recorded in Western countries up to 1986 have been committed by angry employees seeking revenge, protesting against rationalisation of their company, or just wishing to retire early'.[116]

The relationship between the internal cybercriminals and other hackers, however, is weak and uncertain. In most cases, they do not share the same ethical values as the hackers, although they do share with hackers the advanced knowledge to carry out the offence.[117] For the majority of computer crimes that are committed by internal perpetrators, for example, the Local Area Network (LAN) is used. Moreover, they enjoy a high level of understanding of the complexities surrounding the victimised systems, including company security procedures.[118] In 2000, Vitek Boden, for example, became the archetypal disgruntled former employee who attacked public infrastructure.[119] Boden hacked into a municipal council's sewage control computer system and altered

[113] Steven Philippsohn, 'Trends in Cybercrime: An Overview of Current Financial Crimes on the Internet' (2001) 20 (1) *Computers & Security* 53.

[114] A computer crime study carried out by Keith Hearnden shows that 80% of computer crimes are committed by insiders: 25% of them were managers or supervisors, 24% computer staff and 31% were clerks and cashiers. See, Forester and Morrison, above n 22, 42.

[115] Joseph D Serio and Alexander Gorkin, 'Changing Lenses: Striving for Sharper Focus on the Nature of the 'Russian Mafia' and its Impact on the Computer Realm' (2003) 17 (2) *international review of law computers* 191.

[116] Sieber, above n 87, 17.

[117] Skibell, above n 109.

[118] Ibid.

[119] *The cyberspace invaders* (2003) The Age Company <http://www.theage.com.au/articles/2003/06/21/1056119529509.html?oneclick=true> at 13 October 2005.

pump station operations.[120] Consequently, up to one million litres of raw sewage flowed into public parks and creeks on Queensland's Sunshine Coast.[121]

One can conclude that not all internal cybercriminal are hackers. On the contrary, a wide range of crimes are committed by insiders such as disgruntled employees or contractors who do not share hackers ethics and are not involved in other hacking activities.

1.3.3 Malware Writers

Malware is 'any programme or file that is harmful to a computer user'.[122] It is a programme that causes a variety of damage to an infected computer system, such as deleting or altering sensitive files.[123] Malware includes computer viruses, Trojan horses, worms, and other miscellaneous programmes.[124] Although writing Malware requires a high level of knowledge of computer programming language, executing a Malware attack sometimes needs no more than a little knowledge of the basic principles of computer system usage.

Just as criminal law distinguishes between different types of murder, comparable distinctions should be applied to Malware writers, because they have different motivations and seek to achieve differing objectives.[125] They create the weapon of the crime and, therefore, it is not necessary to be used by the creator but it offers script kiddies[126] and other cybercriminals[127] the widest range of abilities to cause cyber-chaos. For example, the most significant portion of cybercrimes that inflict massive damage on information technology systems is caused by Malware attacks.[128] They also cause enormous pecuniary losses more than any other cyber attacks and are usually committed

[120] Rosemary Desmond, 'Qld: Angry Hacker Jailed Over Sewage Dumping', *AAP General News* 31 October 2001.

[121] Ibid.

[122] Debra Lee, *Malware* (2004) Search Security <http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci762187,00.html> at 18 October 2005.

[123] Ed Skoudis and Lenny Zeltser, *Malware: Fighting Malicious Code* (2004) 3.

[124] See Section 3.2.2.1 for more information on Malware.

[125] Steven Furnell, *Cybercrime: Vandalizing the Information Society* (2002) 144.

[126] Script Kiddies are baby hackers who merely download a ready made programme from the Internet and proceed to try and use it until they get lucky, see Lilley, above n 67, 42-42.

[127] Young and Aitel, above n 86.

[128] Roger A Grimes, *Malicious Mobile Code: Virus Protection for Windows* (2001). In 2003, the National Hi-Tech Crime Unit (NHTCU) survey in London found that 77% of respondents said they were the victim of a virus attack. See, 'Cybercrime Costs Huge Losses for British Business says survey.' *Xinhua News Agency* 24 February 2004.

without leaving any trace. For example, mi2g Intelligence, the London-based security consultancy, estimates that the total damages worldwide from Malware infection lies between $166 and $202 billion dollars in global economic damages.[129] Therefore, the Malware creators should be classified under cybercriminal categories, if their motivation was to create a programme causing cyber-chaos.

1.3.4 Cyber Organised Crime

Recently, organised crime syndicates have benefited from the globalisation process, including privatisations, free trade zones, off shore banking centres, and Internet facilities.[130] The attitude of organised crime towards the virtual world is utterly different from other kinds of cybercriminals. The accessibility and continuity of online services are important to quickly and surreptitiously achieve their agendas. Consequently, cyberspace and computer systems are used in the organised crime environment to facilitate traditional crimes rather than to disrupt cyberspace itself.[131] For example, a professional Russian pensioner, a former computer programmer, teamed up with four hackers to steal details of Western credit cards. They had managed to steal $10,000 online before they were caught.[132]

The anonymity and proximity privileges that cyberspace offers entice an organised crime syndicate to partially migrate their operations to cyberspace. Thus, there is a great likelihood that hackers or disgruntled employees might be recruited or coerced by organised crime to carry out a part of their activities online.[133]

1.3.5 Cyber Terrorists

Cyber terrorism is the convergence of terrorism and cyberspace,[134] which is slightly different from cybercrime. Although there is no consensus on the definition of

[129] *2004: Year of the Global Malware Epidemic- Top Ten Lessons* (2004) Gale Group. <http://www.highbeam.com/library/doc3.asp?DOCID=1G1:125077476&num=1&ctrlInfo=Round18%3AProd%3ASR%3AResult&ao=&FreePremium=BOTH> at 18 October 2005.

[130] 'Laundering Money: Obscuring the Link between the Criminal and the Crime', *UN Chronicle* 6/22/1998 1998.

[131] See, eg, Phil Williams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses* Computer Crime Research Centre <http://www.crime-research.org/library/Cybercrime.htm> at 25 April 2006.

[132] See, eg, 'Russia Arrests Grandfather of Cybercrime', *BBC News* 26 May 2001.

[133] Joseph D Serio and Alexander Gorkin, above n 115, 197.

[134] Denning Dorothy, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services* (2000) Georgetown University <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> at 26 April 2006.

cyberterrorism, definitions given are largely derived from the definition of real world terrorism.[135] The latter by nature is difficult to define,[136] because of several factors including the cliché 'One man's terrorist is another man's freedom fighter',[137] and also because the relationship between terrorism and crime remains unresolved,[138] even though that the relationship between them is evident.[139] However, Dorothy Denning, a professor of computer science at Georgetown University, defined cyber-terrorism as 'unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives'.[140] The perpetrators of cyberterrorism, and the magnitude of disruption or destruction inflicted by such attacks, and the motivation, are important factors used to distinguish between a hacker attack -cybercrime- and a technologically skilful terrorist attack.

Since the 2001 multi-terrorists attacks that took place in New York and Washington, and then spread around the world, the picture of terrorist organisations malignantly embracing cyberspace has been widely absorbed. It has generated countless horrific scenarios of cyberattacks against American National Informational Infrastructure (NII),[141] nuclear plants, power grid, dams etc. Dan Verton's book, *Black Ice: the Invisible Threat of Cyber-Terror*, for example, depicts an extraordinary hypothetical cyberterrorism scenario.[142] The scenario hypothesises a massive information system disruption leading to devastating physical destruction inflicted by cyber terrorism.[143]

[135] Maghaireh, above n 10.

[136] Serge Krasavin, *What is Cyber-terrorism?* (2000) Global Information Assurance Certification <http://www.giac.org/certified_professionals/practicals/gsec/1774.php> at 26 April 2006.

[137] This cliché has been distorted and misused to legitimise terrorist attacks. Senator Jackson was 'quoted in Benyamin Netanyahu's book *Terrorism: How the West Can Win* as saying,
'The idea that one person's "terrorist" is another's "freedom fighter" cannot be sanctioned. Freedom fighters or revolutionaries don't blow up buses containing non-combatants; terrorist murderers do. Freedom fighters don't set out to capture and slaughter schoolchildren; terrorist murderers do . . . It is a disgrace that democracies would allow the treasured word "freedom" to be associated with acts of terrorists'. Boaz Ganor, *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?* International Institute for Counter-Terrorism <http://www.ict.org.il/Articles/define.htm> at 27 April 2006. See also, Krasavin, above n 136.

[138] See, eg, Ganor, Ibid.

[139] See, eg, Gavin Cameron, 'The Likelihood of Nuclear Terrorism' (1998) 18 *Journal of Conflict Studies.*

[140] Dorothy, above n 134.

[141] National Information Infrastructure (NII) can be defined as 'that system of advanced computer systems, databases and telecommunication networks…that make electronic information widely available and accessible'. Kevin A O'Brien, 'Information Age Terrorism and Warfare' in David Martin Jones (ed), *Globalisation and the New Terror* (2004) 12, 129.

[142] Dan Verton, *Black Ice: the Invisible Threat of Cyber-Terrorism* (2003) xxi.

[143] Ibid 1-16.

These scenarios were based mainly on reports indicating that American critical infrastructure were susceptible to cyberattacks.[144]

In 2002, 'Digital Pearl Harbor', a simulated massive cyberattack on America's critical infrastructure sponsored by the Naval War College,[145] followed by 'Operation Livewire', a more recent simulation of a cyberterror attack,[146] came to refute the surreal theoretical speculations about looming devastation cyberterrorism. The simulations found that the cyber security preparedness of American NII is substantially immune. Furthermore, a report issued by the Centre for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, concluded that a concentrated devastating cyberattack is, at least in the near future, significantly beyond the capabilities of Al-Qeada and other terrorist organisations.[147]

Up to the time of writing, there is no incident of cyberterrorism recorded nor a cyberattack characterised as a cyberterrorism. The disruption of non-essential services typically is not seen as cyberterrorism.[148] Dorothy Denning stresses that 'while past cyber attacks have caused billions of dollars in damage, they cannot be characterised as terrorism. Rather, past events are better described as cybercrimes. True cyber-terrorism is something far more devastating in terms of its scope and impact on a society'.[149]

Indeed, cyberspace is a vital tool for terrorist organisations to communicate and deliver their propaganda, and therefore, it is unlikely that they will target cyberspace. Nevertheless, the most likely scenario for cyberterrorism to happen is in tandem with physical attacks. For example, in October 2000, the cyber war began between Arab and Israeli hackers shortly after the Lebanese Shi'ite Hezbollah movement abducted three Israeli soldiers.[150] Cyberterrorism takes three different forms of attack. The first form of

[144] For example, in 1991 Winn Schwartau told a congressional committee 'Government and commercial computer systems are so poorly protected today that they can essentially be considered defenceless-an electronic Pearl Harbor waiting to happen…' See, Schwartau, above n 64, 13. Bill Nelson et al, 'Cyberterror: Prospects and Implications' (Defense Intelligence Agency, 1999) 2.

[145] See, eg, Abraham R Wagner, 'Terrorism and the Internet: Use and Abuse' in Mark Last and Abraham Kandel (eds), *Fighting Terror in Cyberspace* (2005) 1, 25.

[146] See, eg, Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (2006) 168.

[147] Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?' (2005) 28 (2) *Studies in Conflict & Terrorism* 129.144.

[148] Mohammad Iqbal, 'Defining Cybeterrorism' (2004) 22 *The John Marshall Journal of Computer & Information Law* 397, 408.

[149] Denning Dorothy, 'Cyberwarriors' (2001) 23 (2) *Harvard International Review* 70.

[150] Ibid.

cyberterrorism is perception management and propaganda.[151] This form, which unfortunately has been excluded from the above definition, completely relies on cyberspace accessibility; the cyber multimedia in this form play a key role in recruiting and funding terrorism. Therefore, an innovative definition of cyberterrorism is needed to include this form of cyberterrorism. It aims to influence public opinion, communicate, recruit new terrorists and generate funding. The *Times* newspaper, for example, reported that Omar Bakri Mohammad,[152] a Lebanese fundamentalist, is continuing to reach and preach his followers in Britain through websites and Internet chat rooms.[153] In addition, it is widely recognised that Al-Qaeda utilised cyberspace, before and in the aftermath of the 9/11 attack.[154] Recently, on 6 of October 2005, it was reported that Al-Qaeda was operating a website containing guidance and full instructions about preparing and making traditional bombs as well as a nuclear bomb.[155]

The second form of cyberterrorism is disruptive attacks.[156] One of the most known pictures of disruptive attacks is the Distributed Denial of Service (DDoS) attack.[157] Although this sort of attack is neither lethal nor sophisticated, the financial damage incurred might be immense.[158]

The third pattern of cyberterrorism is 'destructive attacks'.[159] This type is a combination of digital and physical destruction perpetrated online, but the ultimate objective is to cause critical physical damage,[160] such as shutting down the aviation system.

It is noticeable that terrorism inexorably inhabits cyberspace and, while the first form of cyberterrorism is booming and becoming more sophisticated, the second and third forms

[151] Zanini and Edwards, above n 9, 41.

[152] In 18 November 2002 Omar Bakri said, 'In a matter of time, you will see attacks on the stock market. That is what al-Qaeda is skilful with. I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies'. See, Verton, above n 142, 84.

[153] Sean O'Neill and Yaakovlapppin, 'Extremist Islamist has Returned - via Internet', *The Times* 21 October 2005.

[154] A O'Brien, 'Information Age, Terrorism and Warfare' (2003) 14 (1) *Small Wars and Insurgencies* 183, 199.

[155] Uzi Mahnaimi and Tom Walker, 'Al-Qaeda Woos Recruits with Nuclear Bomb Website', *The Sunday Times* 6 November 2005.

[156] Zanini and Edwards, above n 9, 44.

[157] Lech J Janczewski and Andrew M Colarik, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* (2005) 46.

[158] See Section 3.2 for more information about DDoS attacks.

[159] Zanini and Edwards, above n 9, 45.

[160] Ibid.

of cyberterrorism are plausible, and worthy of being on the agenda of governments and international organisations.

1.4 Conclusion

The burgeoning of information technology and cyberspace has created a new independent field of legal studies. While the lion's share of these studies have addressed the emerging cyberspace legal issues, such as electronic commerce, intellectual property, and privacy, the dark side of information technologies and cyberspace are addressed by criminologists, who deem cybercrime to be an independent field of criminology and criminal justice.

Several scholars, computing experts, and organisations, however, who speak, write and publish extensively on cybercrime, have introduced definitions covering the principal points of the phenomenon. These definitions are either broad or narrow, always leaving the door open for new definitions. The definition suggested by this author, therefore, was necessary to address the shortcomings found in the prior definitions as well as to distinguish between cybercrime and other related offences.

Cybercrime classifications, on the other hand, outline the ambit of cybercrimes in further detail. This will particularly help law enforcement investigating cybercrimes as Tavani mentioned in his statement about cybercrime classification perspectives. The new phenomenon of online illegal activities has delivered a new pattern of crimes perpetrated by a class of neo-criminals. Several nascent studies have been carried out by both criminologists and psychologists to understand the hackers' world. The majority of these studies have come up with a general hackers' psychology map. While the hackers have dominated cyberspace and been depicted as sole cybercriminals, statistics and recorded incidents of cybercrime indicate that they are a wide spectrum of different kinds of cybercriminals ranging from the inept young hacker and the highly gifted hacker to the disgruntled employee.

Cyberspace creates a unique environment for criminals and terrorists to be able to interact, work together and learn from each other. The risk of recruiting hackers to work with organised crimes or terrorist organisations is growing remarkably fast. This unique environment i.e. cyberspace requires the initiation of a comprehensive anti-hacking strategy policies, regulations, and traditional laws must be evaluated and adjusted as required, to facilitate law enforcement efforts to combat cybercrime.

2 OBJECTIVE AND METHODS OF THE STUDY

2.1 Introduction

Following the general background review of the global picture on cybercrimes, this chapter considers some methodological and other relevant issues concerning the research. It states the research problem, the research questions, the research scope and methodology. The chapter proceeds with a discussion of the significance and benefits of the study and provides a brief overview of chapters.

2.2 Statement of the Problem

Many modern states have sought and succeeded in fostering an information society by providing their service online. In the developed world today, critical infrastructure and vital utilities such as hospitals, communications, trading, universities, the banking systems and governmental operations completely rely on information technology.[161] The Jordanian government and lawmakers both recognise the ubiquity of information technology and its usefulness. In 1999, a High-Tech crimes force was established as a part of the Public Security Directorate. The more recently established Department of Computer Crime Prevention is equipped with advanced technologies designed to crack down on computer offences, and has a number of computer forensics experts and computer technicians. Unfortunately, this development has not yet been accompanied by a parallel development in legal and regulatory reforms. The process of obtaining digital evidence that is used to establish conclusive evidence of cyber wrongdoing is a crucial stage in cybercrime investigations and successful prosecutions. Therefore, the absence of comprehensive legislation that specifically addresses cybercrime, and the lack of guidelines and instructions pertaining to cybercrime investigation priorities, challenges, and inappropriate search and seizure procedures make it difficult for law enforcement officers to respond to cybercrime adequately. An appropriate approach to

[161] See, eg, Michael A Vatis, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks*: *A National Needs Assessment* (2002) Institute for Security Technology Studies at Dartmouth College< http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf > at 19 September 2004.

cybercrime investigation should protect law enforcement efforts as well as individual confidentiality, evidence integrity, and privacy.

The existing laws and procedures are generally insufficient to criminalise all forms of cybercrimes and recognise digital evidence. Search and seizure procedures are also inadequate to cope with cybercrime's challenges and the seizure of intangible items. For this reason, lawmakers must admit the need for change in the law in this area and enforcement officers and general prosecutors must understand how search and seizure procedures can be efficiently applied to cybercrime and how digital evidence that is used to establish conclusive evidence of wrongdoing can be obtained.

Although the main subject of this thesis is to address the procedures of search for and seize of digital evidence extracted from cybercrime scenes to establish admissible and probative evidence of cyber wrongdoing, this study will also address procedures concerning digital evidence extracted from other non-cybercrime scenes to prosecute offenders committing traditional crimes.

2.3 Research Questions

This dissertation argues that the general principles of search and seizure in criminal investigation have failed to be applied efficiently to investigating cybercrime. This is because the existing laws do not fit smoothly within cyberspace and the scope of computer systems is beyond the traditional approaches of criminal investigation. The classical laws are accordingly unable to fully protect and fulfil the interests both of law enforcement agencies and the cyber-suspects, nor third parties' privacy rights. Therefore, the main research questions of this study are:

Are the existing legal provisions in place to search and seize physical evidence efficient to search computers in cybercrime investigation?

How can the investigative authority maintain and improve a legitimate regime that can be employed to investigate and gather the required data and Internet contents with respect to a third party's rights of privacy and confidentiality of personal data as well as extracting admissible digital evidence?

The answers to these questions are primarily provided in Chapters 5, 6, 7, 8 and 9. Chapters 3 and 4 provide a very insightful perspective on the capacity of existing laws to deal with cybercrime. The final chapter provides a summary and recommendations for improving laws, policies, and search and seizure procedures in the realm of cybercrimes investigations.

However, in order to answer these main questions, the following sub-questions need to be addressed:

(1) To what extent are existing laws equipped to handle cybercrimes?

A comprehensive response to cybercrime offences is a prerequisite to success in searching and seizing computers and obtaining digital evidence.

(2) How should law enforcement and prosecutors approach a cybercrime investigation?

The availability of investigative guidelines coupled with an experienced investigator are pivotal in executing a successful investigation. The question will be answered through exploring law enforcement's understanding of cybercrimes as well as the ramifications of imposing classical tactics of investigation in cybercrime investigation. Therefore, the first sub-question is Do cybercrimes constitute a high priority within law enforcement? What parameters should be used to decide whether it is appropriate to investigate cybercrime? Do the current procedures for handling cybercrime crime scene provide an optimal approach to enhancing cybercrime investigation? How can law enforcement personnel and, particularly, public prosecutors exercise their power to compel a cyber-suspect or third party to divulge encrypted data in cybercrime investigation?

(3) How do the existing laws stand in respect to the admissibility of various kinds of computer data as evidence? How and to what extent are judges likely to recognise various kinds of digital evidence?

(4) How do traditional search and seizure procedures that are applicable to physical objects apply to the intangible objects?

The courts' decisions are intrinsic to understanding the particularity of cyberspace and computer systems in the absence of decisive legislation. Over recent years court decisions which articulate cyberspace have inspired investigative authorities to draw an admissible approach for conducting a successful investigation. However, answering this question requires addressing issues of the applicability of traditional principles of search and seizure to cyberspace. This leads to the following further sub-questions:

Does the computer data enjoy a high level of legal protection? Is the conventional threshold for issuing a search warrant applicable to cybercrime searches? Is the subject of the search warrants addressed by existing law applicable to intangible objects? How does the concept of particularity apply in the context of cyber searches? How must a cyber search warrant be executed? Who should execute the cyber search warrant? When can the prosecutor seize a whole computer? Does an off-site search warrant present an exception to the search warrant? What are the parameters used to permit off-site searches?

(5) How can a Jordanian prosecutor carry out search and seizure procedures without a warrant? What are the exceptions that allow Jordanian enforcement officers and prosecutors to conduct searches without warrants? How can these exceptions apply to the cybercrime searches?

(6) How can Jordanian enforcement officers and prosecutors obtain digital evidence located in a foreign jurisdiction, and vice versa? What are the trans-jurisdictional concerns that are precluding international co-operation in cybercrime investigations? What are the appropriate mechanisms to obtain digital evidence situated in a foreign jurisdiction? How and to what extent is the existing Jordanian legal system capable of providing mutual legal assistance in cybercrime investigation? How does a Jordanian investigative authority respond to a search request by a foreign country for digital evidence located on its national soil?

The answers to these sub-questions will, cumulatively, provide an answer to the central research questions of the thesis.

2.4 *Scope of the Study and Methodology*

Cybercrime investigation and techniques are multi-faceted, encompassing issues such as surveillance, undercover operations, interview and interrogation techniques, arrest, detention, crime scene investigation, fingerprinting, and so on. This thesis, however, examines only some of the main challenges associated with the process of search and seizure of computers in cybercrime investigation to establish and maintain a national response capability to investigate this type of criminal activity. The first two substantive chapters, 3 and 4, compare and contrast various aspects of cybercrime criminalisation in the selected countries. Cybercrimes are mostly classified under four categories as referred to in Chapter 1. First, the computer can be the object of the attack, as when a computer as a piece of hardware equipment is physically damaged.[162] Second, a computer system can be incidental to the commission of other crimes; hence this role is described as 'computer-supported crime', for example, using encryption or steganography technologies to conceal information from law enforcement.[163] Third, the computer can be used as a tool for conducting or facilitating a crime,[164] for example, cyber forgery, cyber pornography, cyber identity theft, and cyberstalking. Fourth, a computer can be the subject of a crime, when the contents of the computer or a network itself are targeted by intangible attacks for example, TCP/IP crimes and cybersabotage. The first category of crime, however, is excluded from this study, because search and seizure procedures that can be applied to such crimes are precisely akin to traditional crime scene procedures. In addition, the majority of legal scholars exclude this category of crime from cybercrime classifications.[165]Although the second category is not considered as typical of cybercrime, it will be addressed although the emphasis will primarily be on the "target" and "tool" crimes.

The subsequent two chapters, 5 and 6, are concerned with issues influencing the performance of cybercrime investigation. Cybercrime investigative models and digital evidence are a new phenomenon in Jordan, although they have been widely used in Australia and the USA for many years with some degree of success in investigating and prosecuting cybercrimes. Law enforcement officers face a difficult task in investigating

[162] Neil Barrett, *Digital Crime: Policing the Cybernation* (1997) 34.
[163] Ibid.
[164] Ibid 166.
[165] See Section 1.3 for more information on cybercrime classifications.

cybercrime as the approach to a cybercrime scene is different from a traditional crime scene, mainly with respect to strategies used to collect evidence that is used to establish conclusive evidence of cyber wrongdoing. Therefore, in examining a Jordanian investigative model for cybercrime, this thesis addresses also those models developed by Australian and US law enforcement agencies (Australia and the USA have long-standing experience of handling several substantive and procedural cybercrime laws including judicial expositions) and distinguished scholars. Jordanian law enforcement officers and general prosecutors have the benefit of learning from the experience of developed countries and scholars in this regard. In addressing the investigative models, the thesis endeavours to determine the characteristics of an optimal investigative model for cybercrime. An optimal formula for investigating cybercrime, however, may not be a robust formula, unless investigative challenges, such as privacy concerns and encryption are addressed. This study is not concerned, however, with technical challenges; the study only focuses on the legal aspects of how investigators handle privacy and encryption problems during the investigation process.

The last three chapters of this thesis, which are dedicated to studying search and seizure procedures including cross-border searches, attempt to establish the arguments that the traditional procedures of search and seizure are not fully applicable and a different approach may be necessary for cyber searches. The European Cybercrimes Convention is considered as the sole international accord for addressing online offences and cybercrime's international co-operation procedures. Thus, the final chapter addresses the Convention in the terms of international mutual legal assistance in cybercrime.

To achieve the objectives of the research, it is important first to study the Jordanian practice of cybercrimes investigation, and then compare and contrast Jordan's approach to criminal procedures with developed countries' approaches, especially Australia and the USA. By studying the criminal procedures of developed nations, both positive and negative experience, reasons will be found to create, change or maintain the current Jordanian approach to cybercrimes investigation. Therefore, a combination of methods and approaches will be used in this research.

The main problem of the research will be approached through splitting it into three stages. The first stage examines and analyses Jordan's approach to criminal investigation and procedures of search and seizure applied to cybercrime investigation.

This stage of the study aims at building a firm theoretical background with a critical view of Jordanian criminal investigation procedures as applied to cybercrimes investigation. It is expected that this will show to what extent existing investigation procedures are ill-equipped to serve the justice.

In the second stage, a Jordanian national model of investigation will be compared with developed countries' models of searching and seizing digital evidence. Data analysis will be used to elucidate the unique nature of digital evidence and particularities of cybercrime investigation to finalise their pattern of investigation.

Finally, synthesising the results found and the particular features of cybercrime investigations will shed light on the optimal approach to search for and seize digital evidence in cybercrime investigation. Consequently, these findings will guide the researcher to make recommendations for improving both law enforcement practices and public prosecutors, which consequently leads to individual privacy protection and digital evidence admissibility.

2.5 Significance and Benefits of the Study

This research project stems from the particularity of cyberspace and cybercrime. Cybercrime is a subject about which many people, including legal society, know very little. This sort of crime, which initially was known as a story in science fiction has dramatically turned to a malignant technological epidemic threatening global prosperity.[166]

In developed countries, however, a partially comprehensive framework of prevention policy is being developed to stem the rise of cybercrime. For example, the co-operation and coordination between the private sectors and the public sector are improving. Public awareness and ethical online education issues are on the agenda. A group of digital legislation instruments has been enacted to crack down on online offences and protect data privacy. Although numerous publications (including books, surveys and articles) have deeply detailed and widely articulated the cybercrime phenomenon, the issues of cybercrime investigation not well understood and, in particular, searching and seizing

[166] R E Bell, 'The Prosecution of Computer Crime' (2002) 9 *Journal of Financial Crime.*

computer systems remains rare. It is believed that the investigation process is an important cornerstone of a comprehensive crime prevention policy. Gathering and presenting robust evidence is not only necessary for guaranteeing a fair trial, but also for protecting law enforcement against civil liability.

Therefore, examining cybercrimes' investigation and analysing principles of search and seizing tangible evidence and their compatibility with computer systems and the Internet will enrich the literature of this area and provide national guidelines to both Jordanian law enforcement agencies and public prosecutors. The study will shed light on the issues of confidentiality and individual privacy in the course of the investigation of cybercrimes. The main objective, however, is to streamline and strengthen procedures concerning cybercrime investigation and to eliminate or lessen impediments that hinder the collection of digital evidence to establish conclusive evidence of cyber wrongdoing.

Internationally, cybercrimes are transnational crimes; hence, the research is a comparative study. Examining criminal investigation procedures of cybercrimes and launching fixed guidelines will enhance international cybercrimes investigation consistency and cooperation.

2.6 Synopsis of the Thesis

This thesis is structured into ten chapters. Chapter 3 entitled 'Criminalisation of cybercrime' introduces a fundamental overview of the most popular types of cybercrimes and the legal response to them. Because the criminalisation of cybercrime is an indispensable prerequisite for law enforcement personnel to respond effectively and build, at both national and international levels, a strategy against cybercrime, it is necessary for law enforcement agencies, particularly Cybercrime Units, to identify and understand the various types of cybercrime. Therefore, the chapter first describes a brief account of the recent modes used to perpetrate cybercrime and then assesses the legal responses to them in order to assess the adequacy and insufficiency of the current laws of Jordan, Australia, and the US.

In Chapter 4, in which cyberspace is the object of the crime, the illegal uses of cyberspace as a tool to engage in crimes against public trust, morality, property and individuals are defined. The chapter describes four types of cybercrimes: cyber forgery, pornography, identity theft, and cyberstalking. In each cybercrime, a brief account of the recent modes of attacks used to perpetrate crime is explained and the legal response is analysed and assessed in order to assess the adequacy or insufficiency of the current laws.

Chapter 5 critically examines factors necessary for a successful investigation and identifies challenges. It hypothesises that the approach model to cybercrimes investigation which was adopted by the Jordanian Computer Crime Unit (JCCU) is deficient in some components. Therefore, formulated protocols and models of investigation, which are formulated mainly by the Australian High Tech Crime Centre (AHTCC) and the US Department of Justice (DOJ) and forensic experts are analysed and compared with the Jordanian investigative approach. These models were chosen because they are known for their robustness and include important and intricate procedures.

Chapter 6 chapter examines the volatility, integrity, and admissibility of the evidence extracted from computers and the Internet in cybercrime investigation. It demonstrates the characteristic features and inherent risks associated with digital evidence from both technical and legal perspectives. The nature and characteristics of digital evidence are examined for their effects on evidence admissibility. The chapter then evaluates digital evidence in terms of its legal admissibility and discusses the role of judges in evaluating digital evidence. Therefore, this chapter is divided into three sections. The first examines the different types of data and its volatility. The second section examines digital evidence integrity. The third section addresses digital evidence admissibility, the legal responses and judicial role in accepting evidence.

Chapter 7 provides a critique the conventional rules of search and seizure in the context of the digital search and assesses their impact on conducting effective search and seizure. It addresses the fundamental principles and rules of search and seizure set forth under the Jordanian *Criminal Procedure Law* 1961 as applied to searches of evidence stored in digital formats. It deals with the traditional legal concepts of search and seizure as established in the Jordanian *Criminal Procedure Law* 1961 compared with

Australian and US patterns and explores the fundamental differences between conventional and digital search and the extent to which the present search and seizure rules are compatible with the digital environment.

Chapter 8 deals with the traditional legal concepts of warrantless searches and seizures as established in the Jordanian *Criminal Procedure Law* 1961. It addresses different aspects of search warrant exceptions as applied to searches of digital evidence in cybercrime investigation. It examines and assesses each exception and its applicability and compatibility with searches and seizures of digital evidence.

Chapter 9 examines the jurisdictional hurdles that may hinder cross-border searches and seizures and the ways in which law enforcement officers approach cross-border searches. It discusses legal mechanisms used to obtain evidence located in a foreign jurisdiction and Jordan's response.

Finally, Chapter 10 concludes with a number of recommendations formulated on the basis of the findings and summery of chapters.

3 CYBERSPACE AS THE TARGET OF THE CRIME

Introduction

The objective of this chapter is to give a fundamental overview of the most popular types of cybercrimes and the legal response to them. It is necessary for law enforcement agencies, particularly Cybercrime Units, to identify and understand the various types of cybercrime and the differences between them as well as the legal response to them, because criminalisation of cybercrimes is an indispensable prerequisite for law enforcement personnel to respond and build effectively, at both national and international levels, a strategy against cybercrime. Consequently, a clear legal response to cybercrime offences is a prerequisite to success in searching and seizing computers and obtaining digital evidence.

Criminalisation of cybercrimes requires, first, definition of those actions involving computerised technology which may cause harm in any way and, second, the criminalisation of those actions. In this chapter, both the strengths and weaknesses of these laws, the Jordanian *Criminal Law* 1960, *Telecommunications Law* 1995 as well as the *Electronic Transactions Law* 2001 will be examined in addressing different aspects of cybercrimes.

The methodology for assessing these laws involves two approaches: first, critical analysis of the content of particular provisions; and, second, a comparative analysis undertaken by contrasting these provisions with similar articles from cybercrime laws in Australia and the USA. These two countries were selected because they are already well advanced in their experiences of, and their legal responses to cybercrimes, thus providing benchmarks for Jordan's response.

Over the past half of a century, international society, particularly across the industrially developed world, has experienced an unprecedented technological transformation. Simultaneously, diverse new activities called cybercrimes have emerged in association with this technological revolution. Legal scholars addressed these activities and delivered initially controversial arguments regarding the adequacy of the existing substantive criminal law to criminalise them effectively.[167] However, it has since become mainstream opinion that the existing criminal law was ill equipped to deal with and to criminalise cybercrimes effectively.[168]

Initially, in the late 1980s, while Western parliaments were obviously well acquainted with a cybercrime threat, the developing world, including Jordan, was unaware of the problem. Indeed, it took years and great efforts in many countries to persuade legislators to enact special cybercrime legislation. Currently, a few developing countries have either enacted cybercrime laws or have amended existing criminal laws. For example, after experiencing problems in applying its existing criminal law to cybercrimes, the Philippines drafted its *Cybercrime Prevention Act* 2001.[169] That Act came into being following the prosecution failure of the notorious 'Onel de Guzman' who had released the 'Love Bug' computer virus in 2000.[170] To keep abreast of developments, China amended its criminal law in 2000 by modifying articles 285, 286, and 287 of the *Criminal Law* of the People's Republic of China.[171]

However, cybercrimes are borderless crimes. The lack of cybercrime legislation in one country can influence directly or indirectly the rest of the world by creating, for instance, jurisdictional havens.[172] The 'Love Bug' virus was an example. Therefore, the legal situation in country B could affect country A or several countries.

[167] See, eg, Eric J Sinrod and William P Reilly, 'Cyber-Crime: A Practical Approach to the Application of Federal Computer Crime Laws' (2000) 16 *Santa Clara Computer and High Technology Law Journal* 177,180. See also, Douglas H Hancock, 'To What Extent Should Computer Related Crimes Be The Subject Of Specific Legislative Attention' (2001) 12 *Albany Law Journal of Science & Technology* 97, 105.

[168] See, eg, Sieber, above n 87, 38. See also, Hancock, Ibid. Sofya Peysakhovich, 'Virtual Child Pornography: Why American and British Laws are at Odds With Each Other' (2004) 14 *Albany Law Journal of Science & Technology* 799, 805.

[169] See, eg, Lawrence Casiraya, *Philippines Cybercrime Bill to Cover Cell Phones* (2005) Computer Crime Research Center <http://www.crime-research.org/news/05.01.2005/878/> at 21 November 2006.

[170] 'Love Bug' was the world's fastest and most malicious code after it was written in the Philippines, appeared in Hong Kong and rapidly spread worldwide. See, eg, Lev Grossman, 'Attack of the Love Bug', *Time Europe*, May 15, 2000 < http://www.time.com/time/europe/magazine/2000/0515/cover.html>at 20 November 2005.

[171] See, eg, *People's Republic of China* (2005) A Global Survey of Cybercrime Legislation <http://www.cybercrimelaw.net/countries/china.html> at 22 November 2005.

[172] See, eg, Susan W Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' (2001) 8 (2) *E Law- Murdoch University Electronic Journal of Law* < http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html> at January 2005.

To examine the strength and weakness of the capabilities of the existing Jordanian laws to address cybercrimes, this chapter will first define the various forms of cybercrimes. These specific forms of cybercrimes are the most popular, being recorded all over the world including Australia and the USA, so it might be useful for lawyers, law enforcement personnel, and prosecutors to be acquainted with them. Then the relevant laws of Jordan, Australia, and the USA will each be scrutinised.

Each of these countries has taken an independent legal response. In Jordan, no comprehensive law addresses cybercrimes, only a handful of legislative provisions that were originally enacted to protect physical objects. These laws are either too narrow or are inappropriate to address adequately all the forms of cybercrimes.[173] In Australia, by contrast, the parliament has enacted a comprehensive law, the *Cybercrime Act* 2001. In a similar manner, the USA has addressed cybercrimes through its *Computer Fraud and Abuse Act* (CFAA) 1984.

Since information is a precious commodity, the integrity,[174] availability[175] and confidentiality[176] of information in cyberspace is continually being compromised. The crime is invisible and the victims as well as losses are almost intangible. Indeed, crimes falling under this label are described as 'new wine in new bottles'.[177] Nowadays, the most common patterns of cybercrimes under this category are what might be called 'TCP/IP crimes', cybertrespass, and cybersabotage.

[173] It is important to bear in mind that a general proposition of substantive law is that criminal laws are to be construed narrowly. This means that the fundamental ground of criminology is that 'no matter how immoral, reprehensible, damaging or dangerous an act is, it is not a crime unless it is made such by the authorities of the state'. Hancock, above n 167. See also, Williams, above n 18.

[174] An 'Integrity' breach occurs where information has been modified or changed inappropriately. In some instances, this occurs as a form of malicious damage, but a breach can also occur as a way to commit a traditional crime, such as fraud. For example, a website providing banking services might be exploited by copying its information and redesigning it to make it looks like the genuine website. See, eg, D Cotroneo et al, 'An Architecture for Security-Oriented Perfective Maintenance of Legacy Software' (2003) 45 *Information and Software Technology* 619, 622. See also, *RASC: Confidentiality, Integrity and Availability (CIA)* (2004) Purdue University <http://www.itap.purdue.edu/security/files/documents/RASCCIAv13.pdf> at 1 May 2006.

[175] 'Availability' refers to the accessibility of specific information, such as websites or databases, to an authorised person. See, eg, *RASC: Confidentiality, Integrity and Availability (CIA)* (2004) Purdue University <http://www.itap.purdue.edu/security/files/documents/RASCCIAv13.pdf> at 1 May 2006.

[176] 'Confidentiality' refers to the privacy of information assets. See, eg, *RASC: Confidentiality, Integrity and Availability (CIA)* (2004) Purdue University <http://www.itap.purdue.edu/security/files/documents/RASCCIAv13.pdf> at 1 May 2006.

[177] See, eg, Brenner, above n 56,13. Actually, this phrase comes from the Bible and is actually 'new wine in new wine skins' because they did not have wine bottles then in Israel/Palestine.

This chapter describes a number of cybercrimes: TCP/IP crimes, cybertrespass and cybersabotage. In each cybercrime, a brief account of the recent modes used to perpetrate crime is explained and the legal response to such crimes will be analysed comparatively so as to identify the common features and differences between the three countries in order to assess the adequacy and insufficiency of the current laws. In these types of crimes the main problem is caused by the fact that the existing laws were formulated in the past century, and before the arrival of the Internet revolution in Jordan in 1998, primarily to protect physical, tangible, and visible objects against traditional criminal acts.[178]

3.1 TCP/IP Crimes

The term TCP is an abbreviation for Transmission Control Protocol and IP stands for Internet Protocol.[179] They refer to one of the core elements of the set of Internet communication protocols[180] or one of the most important elements of the Internet's core code.[181] In other words, they are the backbone of Internet communication[182] and an integral part of the four layers of Internet architecture.[183]

[178] See, eg, Sieber, above n 87, 37. See also, Hancock, above n 167, 97.

[179] TCP is a military designed communication protocol to support multi-network applications and to be a highly reliable, securable logical communication protocol between interconnected computers. It is defined as 'a protocol used for transmitting data between computers and as the basis for standard protocols on the Internet'. *TCP/IP,* msn <http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?refid=1861718624> at 22 November 2005. See also, *Transmission Control Protocol* Catalyst Development: Software Applications, Components and Libraries <http://www.catalyst.com/products/socketwrench/tutorial/tcpdoc02.html> at 22 November 2005.

[180] 'Communications protocols are sets of rules or standards designed to enable computers to connect with each other and exchange data'. See, *Definitions of Communications Protocol on the Web* <http://www.google.com.au/search?hl=en&lr=&oi=defmore&defl=en&q=define:communications+protocol> at 23 November 2005.

[181] Wikipedia, above n 179.

[182] See, eg, Grandmaster Plague, *Myths About TCP Spoofing* (2002) <http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=6394&mode=thread&order=0&thold=0> at 21 November 2005.

[183] Mctaggart divides the Internet into four layers: The first layer is the content, such as web pages; the second is the application layer, such as software programs; the third layer is the operational layer, such as Internet Service Providers; and fourth is the physical layer, such as hardware devices. According to this classification, TCP/IP crimes are crimes against the second and third layers to prevent first layer from reaching its ultimate distination (Internet users). See generally, Craig Mctaggart, 'A Layered Approach to Internet Legal Analysis.' (2003) 48 (4) *McGill Law Journal* 571.

Basically, cyberspace access needs a computer provided with a modem[184] connected to a communications network such as by a phone cable or high-speed line.[185] However, to transmit information from one computer to another, a computer user, also called a 'client', has to start a process known as the 'Three-way Handshake' (TWHS).[186] This connection process starts by establishing a TCP connection to a system (or server), that provides cyber services, such as website, e-mail, and so forth.[187]

The client and the server exchange a set sequence of messages. The first part of the process is started by sending the first message (SYN message)[188] by the client asking for information from the server. Once the server acknowledges the SYN message, it sends back a SYN-ACK message,[189] which includes an Initial Sequence Number (ISN),[190] to the client as the second part of the TWHS connection process. Finally, the client finishes the process by responding to the server's message with an ACK message. By completing the three parts of the TWHS connection process, the information can be smoothly transmitted between the client and the server. Fig (3.1) illustrates this TWHS connection process.

[184] A Modem short for (Modulator-Demodulator) is a device that allows a computer or terminal to transmit data over a standard telephone line or high-speed cable. See, Farlex, *Modem* The Free Dictionary <http://computing-dictionary.thefreedictionary.com/Computer+modem> at 24 November 2005.

[185] A High-Speed line is a technology for transferring digital data in high frequency signal ranges from one place to another in a moment of time. An example of a High-Speed line is a DSL (Digital Subscriber Line). See generally, *Fast Guide to DSL* <http://whatis.techtarget.com/definition/0,,sid9_gci213915,00.html#adsl> at 3 May 2006.

[186] See, eg, Jeremy Andrews, *Understanding TCP Reset Attacks* (2005) Kernel Trap <http://kerneltrap.org/node/3072> at 23 November 2005. See also, 'Teardrops and Land Bugs Denial of Service Attacks Exploit TCP/IP Vulnerabilities' (1998) *Software Magazine.*

[187] See, eg, Computer Emergency Response Team, *CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks* (2000) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1996-21.html> at 24 November 2005.

[188] 'SYN' stands for 'Synchronise Sequence Number'. It is used to initiate a TCP connection. See generally, Robbie Tarte, *Understanding Computers: an Overview for the Non-Geek* 155.

[189] 'ACK' is an abbreviation for Acknowledgment. Ibid.

[190] As there is no guarantee that the data will follow the same route and therefore arrive in the order they were sent, theTCP protocol uses sequence numbers to ensure that the application layer receives data in the same order that it was sent. See generally, B Harris and R Hunt, 'TCP/IP Security Threats and Attack Methods' (1999) 22 *Computer Communication* 885, 888.

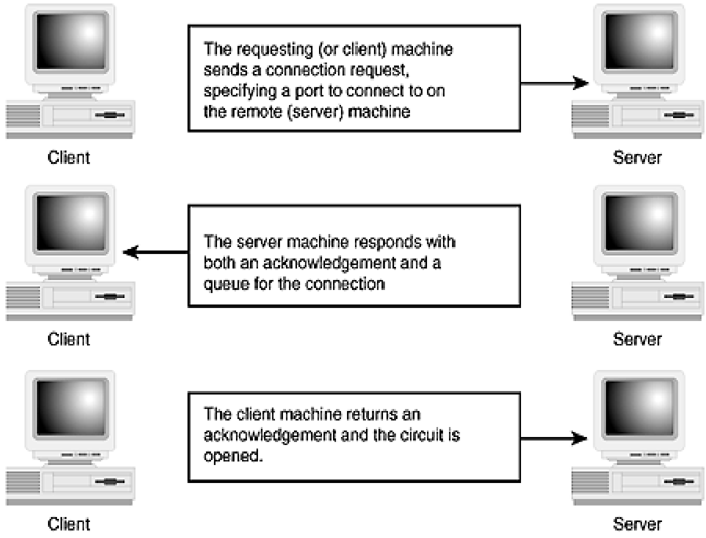

The requesting (or client) machine sends a connection request, specifying a port to connect to on the remote (server) machine
Client
Server
The server machine responds with both an acknowledgement and a queue for the connection
Client
Server
The client machine returns an acknowledgement and the circuit is opened.
Client
Server

Figure 3.1 TCP Three-Way Handshake[191]

The transmitted information is broken into datagrams.[192] Each datagram is directed to its destination and is packaged in a bundle of instructions called a packet.[193] The TCP assigns a sequence number to every byte transmitted online.[194] As TCP is a connection-oriented protocol,[195] it guarantees delivery of data and also that each packet will be received without errors.[196]

[191] See, Anonymous, *Maximum Security* (2001) 108.

[192] A datagram is an independent, self-contained message sent over the network whose arrival time and content are not guaranteed. See generally, *Lesson: All About Datagrams* <http://java.sun.com/docs/books/tutorial/networking/datagrams/index.html> at 26 November 2005. See also, Jeremy Andrews, *Understanding TCP Reset Attacks* (2005) Kernel Trap <http://kerneltrap.org/node/3072> at 23 November 2005.

[193] A packet is the fundamental unit of information carriage in all modern computer networks. These networks breaks, for example an e-mail message into parts of a certain size in bytes. These are the packets. See generally, *What Is A Packet?* <http://computer.howstuffworks.com/question525.htm> at 26 November 2005.

[194] According to the Wikipedia, byte is a unit of measurement of information memory consisting of 8 binary digits or bite. The bite is a binary digit either 1 or 0. See generally, *Byte* <http://en.wikipedia.org/wiki/Byte> at 26 September 2007. See also, Joe Casad, *Teach Yourself TCP/IP in 24 Hours* (3rd ed, 2004) 92.

[195] A connection-oriented protocol is often called a 'reliable' network service, because it guarantees that data will arrive in the proper sequence or in the same order. See, Free On-Line Dictionary of Computing, <http://foldoc.org/foldoc.cgi?query=connection+oriented> at 25 November 2005.

[196] See, eg, Casad, above n 194, 85.

The IP,[197] on the other hand, funnels the packets across the Internet to the right client,[198] because each computer connected to the Internet has a unique IP number or address that tells the location of the host.[199]

A number of serious inherent vulnerabilities in the TCP/IP system are repeatedly exploited and misused. Although advanced security shields are regularly set up and new versions of TCP/IP are being used, they have been continuously exposed to a number of illegal activities, such as Denial of Service attack (DoS) and Distributed Denial of Service attack (DDoS).

3.1.1 Denial of Service Attack (DoS)

The DoS attack is a typical pattern of cybercrime, caused by hacking programmes freely distributed from hackers' websites.[200] The immediate victim is the Internet website that provides cyber-services, such as e-mails, websites, and communications, but the intended victim is the client who stands behind the compromised system.[201]

The DoS attack either temporarily prevents legitimate information traffic from transmitting, or disrupts connections between two systems. For example, it prevents users from accessing a website or a specific online service.[202] Also, the infected system might be exposed to serious intangible damage.[203]

[197] The IP address is a 32-bit number represented by four-part decimal parts. It is akin to a zip code, and the other part of the address is akin to the street address. See, Casad, above n 194, 52. See also, Mark Joseph Edwards, *Understanding TCP/IP* (1997) Windows IT Library <http://www.windowsitlibrary.com/Content/121/01/2.html> at 26 November 2005. See also, Linda Volonino and Stephen R Robinson, *Principles and Practice of Information Security* (2004) 117.

[198] Rolf Oppliger, *Internet and Intranet Security* (1998) 34.

[199] Volonino & Robinson, above n 197.

[200] For example, "مجموعة الهاكر المسلم" Muslim Group Hackers is an Arabic hackers group website which provides Muslim Hackers with free hacking tools. See, <http://groups.google.com.sa/group/mslamhaker?hl=ar>at 11 November 2008.

[201] See, eg, Computer Emergency Response Team, *CERT Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks* (2000) Computer Emergency Response Team <http://www.cert.org/advisories/CA-2000-21.html> at 24 November 2005.

[202] See, eg, *Denial of Service Attacks* (2001) Computer Emergency Team <http://www.cert.org/tech_tips/denial_of_service.html> at 24 November 2005.

[203] See, eg, Diane E Levine and Gary C Kessler, 'Denial of Service Attacks' in Seymour Bosworth and M E Kabay (eds), *Computer Security Handbook* (4th ed, 2002) 67.

Varieties of tactics and technologies, however, may be used to launch a DoS attack. In order to figure them out and assess the capability of the Jordanian laws to address a DoS attack, a basic understanding of its mechanism is important.

a) SYN Flood Attack

Basically, a SYN attack occurs by not completing the three parts of the TWHS connection process, mentioned earlier, thereby creating a half-open connection state.[204]

The attacker fires off many SYN messages using spoofed IP addresses.[205] When the server sends back SYN-ACK message (part two) to the client who has already sent a spate of SYN messages (part one) with spoofed IP addresses, the latter withholds the final ACK message (part three).[206] Consequently, the TCP capacity to handle an overwhelming number of half-open connections overflows the buffer space[207] and denies any further incoming legitimate SYN messages. This then causes a denial of service state.[208]

b) Ping of Death

A Ping is a programme that tests whether a host is reachable and operating properly by sending an Internet Control Message Protocol (ICMP).[209] In a nutshell, the attacker in this type of attack sends a spate of large ping requests to the victim system.[210] The victimised system cannot quickly handle the oversized ping requests.[211] As a result, the

[204] See, eg, Vasilios A Siris and Fotini Papagalou, 'Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks' (2005) *Computer Communication* 1. See also, Haining Wang, Danlu Zhang and Kang G Shin, *Detecting SYN Flooding Attacks* College of William and Mary <http://www.cs.wm.edu/~hnw/paper/attack.pdf> at 24 December 2005.

[205] IP Spoofing means to cheat others by using false IP addresses instead of one's own. See Section 4.2.3 for more information on IP attacks. See also, Yi Gao, *Efficient Trapdoor-Based Client Puzzle System Against DoS Attacks* (Master of Computer Science, University of Wollongong, 2005) 12.

[206] See, eg, Jan L Harrington, *Network Security: A Practical Approach* (2005) 160.

[207] In computer science, buffer space means an intangible area used to store data temporarily. See *Buffer* <http://www.webopedia.com/TERM/b/buffer.html> at 9 May 2006.

[208] See, eg, Harris and Hunt, above n 190.

[209] The ICMP is one of the core protocols of the Internet protocol suite. It is used by an operating system to send an error message indicating, for instance, that a requested service is not available. See *Ping* Wikipedia <http://en.wikipedia.org/wiki/Ping> at 20 December 2005.

[210] Harrington, above n 206,164. See also, Sean Dugan, 'Enterprise Computing: Cybersabotage' (1995) *InfoWorld* . Debra Littlejohn Shinder, and Ed Tittel, *Scene of the Cybercrime: Computer Forensics Handbook* (2002) 320.

[211] Paul J Criscuolo, *Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht* (2000) Computer Incident Advisory Capability - Department of Energy <http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf> at 1 December 2005.

targeted host or applications become very slow due to the congestion and in this way denies service.[212]

c) SMTP Flood Attack

The Simple Mail Transport Protocol (SMTP) flood attack is similar to the SYN and ping attack methods. The SMTP, which is used for sending and receiving e-mail messages across the Internet,[213] is often misused to launch a DoS attack.[214] The computer system or the network inherently has a limited capability to handle a volume of data sent at one time. Hence, the attacker sends a spate of oversized messages or many e-mails to jam the SMTP mail server. As a result, the flooding temporarily prevents users from getting legitimate access to the system.[215]

d) UDP and ICMP Flood Attack

The User Datagram Protocol (UDP) flood attack and the Internet Control Message Protocol (ICMP) flood attack methods work in very much the same manner as the SYN flood attack.[216]

The UDP is an integral part of the Internet protocol suite.[217] It is a protocol used to send short messages, known as 'datagrams', from one computer to another.[218] The UDP flood attack occurs when the attacker sends a spate of UDP packets to specified or random ports[219] on the victim system.[220] This generates a flood of traffic between the two systems (the attacker and the server) and then the victimised server cannot quickly

[212] *More Nuke Information and Patches* <http://www.irchelp.org/irchelp/nuke/info.html#icmpflood> at 1 December 2005. See also, Shinder & Tittel, above n 210.

[213] *SMTP* whatis.com <http://searchexchange.techtarget.com/sDefinition/0,, sid43_gci214219,00.html> at 19 December 2005.

[214] See, Shinder & Ed Tittel, above n 210.

[215] Harris and Hunt, above n 190.

[216] Sinrod and Reilly, above n 167. See also, Levine and Kessler, above n 203, 84.

[217] See, eg, Madalina Baltatu et al, 'Security Issues in Control, Management and Routing Protocols' (2000) 34 (6) *Computer Networks 34* 881, 882.

[218] See, eg, 'UDP Port Denial-of-Service Attack' (1996) (2) *Network Security* 2. See also, Wikipedia, *User Datagram Protocol* <http://en.wikipedia.org/wiki/User_Datagram_Protocol> at 24 December 2005.

[219] TCP and UDP Ports are special numbers, which are recognised by Internet and other network protocols, enabling the computer to interact with others, such as port 20 is FTP data port and port 25 is SMTP used for sending e-mails. See generally, *TCP and UDP Ports* The Free Encyclopaedia <http://en.wikipedia.org/wiki/Computer_port> at 11 May 2006.

[220] *What is UDP Flood Attack?* <http://www.csie.ncu.edu.tw/~cs102085/DDoS/bruteforce/udpflood/description.htm> at 20 December 2005. See also, Shinder & Ed Tittel, above n 210, 321.

handle a large number of packets, which leads to a DoS attack or seriously slows down the system.[221]

The ICMP is a protocol used between operating systems to report error messages indicating, for instance, that a router[222] is unreachable or overloaded or there is a problem with a particular path.[223] The ICMP attack is accomplished by sending such a large number of ping requests to the target system that it cannot handle them.[224] This attack usually affects both the attacker and the victim systems unless the attacker has used a forged IP addresses.[225] Thus, the attacker will not experience congestion or a system crash but the victimised system will clog up.[226]

3.1.2 Distributed Denial of Service Attacks (DDoS)

Some of the DoS attack techniques have been crippled by installing security patches and anti-DoS attack programmes.[227] However, a new generation of TCP/IP attacks, called DDoS is being used to multiply the effectiveness of a DoS attack.[228] For example, in February 2000, a 'script kiddie' successfully executed DDoS attacks against prominent commercial websites and media, such as eBay, Yahoo, Amazon, and CNN websites.[229]

[221] See, above n 218.

[222] A router is a device or software in a computer that determines the next network point to which a packet should be forwarded toward its destination. See, *Router* whatis.com <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html> at 20 December 2005.

[223] Pete Loshin, *TCP/IP Clearly Explained* (2nd ed, 1997) 128. See also, Baltatu, above n 217, 883.

[224] Advanced Networking Management Lab, *Distributed Denial of Service Attacks (DDoS) Resources* (2001) Indiana University <http://www.anml.iu.edu/ddos/types.html> at 20 December 2005.

[225] Criscuolo, above n 211, 13.

[226] Ibid.

[227] See, eg, Roger A Grimes, *Honeypots for Windows* (2005) 194.

[228] According to the World Wide Web (WWW) Security FAQ statement on Distributed Denial of Service (DDoS) attacks: 'A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly'. See, eg, Christos Douligeris and Aikaterini Mitrokotsa, 'DDoS Attacks and Defence Mechanisms: Classification and State-of-the-Art' (2004) 44 (5) *Computer Networks* 643-645. See also, Alefiya Hussain, John Heidemann and Christos Papadopoulos, 'Distinguishing between Single and Multi-Source Attacks Using Signal Processing' (2004) 46 (4) *Computer Networks* 479, 480.

[229] See, eg, Hinde Stephen, 'Smurfing, Swamping, Spamming, Spoofing, Squatting, Slandering, Surfing, Scamming and Other Mischiefs of the World Wide Web' (2000) 19 (4) *Computers & Security* 312, 312.

The DDoS attack techniques mainly work in the same manner as DoS attacks.[230] But the attacker, also known as the 'Master' in DDoS, plants a malicious computer code in as many computers as possible, making them his 'zombies'.[231] When the attack is triggered, the zombies controlled by the 'Master' will execute the attack command and flood the victim system with forged codes.[232] The victimised system cannot quickly handle a large number of packets, which may lead the system to suffer congestion and denial of legitimate access.[233]

As described above, DoS and DDoS attacks are launched either to prevent a user from establishing a connection or to choke legitimate data traffic. The DDoS attack involves unauthorised access to an unwitting client system to plant a malicious computer code which orders the system to work as a zombie, in addition to the DoS attack against a particular system. These attacks do not cause permanent damage to a user's data or loss of service, but they temporarily compromise the availability of the Internet. They thwart online service operators and Internet Service Providers (ISPs) from providing secure online services. Finally, these attacks bring not only transient service interruptions but also cause significant financial losses and degradation of cyberspace security credibility.

Survey of Legal Responses

a) Jordan

Basically, criminalisation of DoS and DDoS attacks in Jordan is closely akin to the Australian and the American approaches. There is no decisive and unequivocal text criminalising DoS and DDoS attacks. The only legal ground available to successfully prosecute DoS and DDoS attacks is the Jordanian *Telecommunications Law* 1995. Section 11 Article (72) of the Act, imposes criminal liability on 'Any person who

[230] DDoS tools are Trinoo, Tribe Flood Network (TFN), Tribe Floodnet 2K (TFN2K) and Stacheldraht. See generally, Levine and Kessler, above n 203.

[231] 'Zombie' is a computer or server that has been hacked to help a hacker perform a DoS attack or DDoS attack. See, *Computer Security Definitions* <http://www.computerhope.com/jargon/z/zombie.htm> at 12 December 2005. See also, Douligeris and Mitrokotsa, above n 228, 547. See also, Hussain, Heidemann and Papadopoulos, above n 228, 482.

[232] *UK DDoS Attacks Rise as Zombie Plague Spreads; TeleCity and Prolexic Defend Customers against Cyber-terrorists.* (2005) M2 Presswire <http://www.highbeam.com/library/doc3.asp?DOCID=1G1:131169139&num=6&ctrlInfo=Round18%3AProd%3ASR%3AResult&ao=&FreePremium=BOTH> at 23 December 2005.

[233] Ibid.

intentionally sabotages telecommunications installations or deliberately causes damage thereto…the penalty shall be doubled if his act causes break down of the telecommunications traffic'. Article (79) of the same law also criminalises 'Any person who uses a Public or Private Telecommunications network in an illegal way… or hinders the delivery of services from another telecommunications network, or endangers the national good…'

The DoS and the DDoS attackers, who intentionally launch an attack, would be liable under Article 72 because, while they do not inflict permanent damage or sabotage of the telecommunications installations, they cause temporary loss of communications service and the breaking down of communications traffic. Also, DoS and DDoS attacks constitute an act of illegal use of telecommunications networks mentioned in Article (79). The attacker is initially liable to up to two years in prison and/or a fine of up to JD 5000.[234] However, the punishment is doubled if the offence caused a communications breakdown. For cases of negligent damage, the punishment is reduced to no more than three months and/or fine up to JD 100.

b) Australia

The Australian *Cybercrime Act* 2001 is a specialised anti-hacking statute. It criminalises many forms of illegal cyberspace activities, such as hacking, destroying, sabotaging, and interrupting online services. Although the Act does not explicitly proscribe DoS or DDoS attacks, it generally prohibits unauthorised prevention of electronic communication traffic to or from a computer system. Section 477.3 (1) (a) of the Australian *Cybercrime Act* applies to whoever 'causes any unauthorised impairment of electronic communication to or from a computer…[where]…(i) the electronic communication is sent to or from the computer by means of a telecommunications service'.

The DoS and DDoS attackers who wilfully launch an attack would be liable under this section, because impairment of electronic communication to or from a computer includes preventing computers from establishing a connection and communications trafficking.[235] But communication prevention, which is mentioned in the Act, is

[234] JD is an abbreviation for Jordanian currency (Jordanian Diner). 5,000.00 JD equals about A$10,700.00 (Australian Dollars).

[235] *Cybercrime Act 2001* (Cth) div 476(1).

undefined and a mere interception of any electronic communication is not considered a crime.[236] Nevertheless, DoS and DDoS attacks, without a doubt, temporarily force the server to shut down and preclude the service from reaching its targeted computers. Hence, DoS and DDoS attacks are crimes according to the above section. Moreover, the DDoS attack, which involves insertion of a malicious 'zombie' into the client systems, also constitutes cybertrespass under Section 478.1 (1) (a), which stipulates that 'A person is guilty of an offence if …the person causes any unauthorized access to, or modification of, restricted data'.[237]

The penalties imposed on DoS and DDoS attackers fluctuate. They depend, first, on the scale of the destruction inflicted and, second, on the criminal intention. The defendant is initially liable to up to ten years in prison; but, if the attacker's intention was to commit a serious offence, for instance, to disrupt critical infrastructure, the attacker would be liable to imprisonment for life or a period of no less than five years.[238]

c) USA

In a similar vein, the *Computer Fraud and Abuse Act* 1984 (CFAA) in USA, which is the backbone of the federal anti-hacking laws, has no provision explicitly addressing DoS or DDoS attacks. [239] However, the Act imposes criminal liability on 'whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorisation, to a protected computer'.[240] The provision is used to prosecute those who launch DDoS attacks.[241] It specifically addresses the crimes of hacking which affect the integrity or availability of data by intentionally transmitting a malicious code or planting it in a

[236] *Cybercrime Act 2001* (Cth) div 476(1). Stipulates: 'Impairment of electronic communication to or from a computer includes:(a) the prevention of any such communication; or (b) the impairment of any such communication on an electronic link or network used by the computer; but does not include a mere interception of any such communication.'

[237] *Cybercrime Act 2001* (Cth) div 478 (1), (1) (a). Division 478.1 (3) defined restricted data as (a) data held in a computer; and (b) to which access is restricted by an access control system associated with a function of the computer.

[238] *Cybercrime Act 2001* (Cth) div 477(1), (9).

[239] Sinrod and Reilly, above n 167, 201. See also, Jeff Nemerofsky, 'The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?' (2000) 6 (23) *Richmond Journal of Law & Technology*.

[240] *Computer Fraud and Abuse Act* 18 USC §§1030 s (a) (5) (a) (1984).

[241] See, U.S. v Guzner, Plea Agreement for Defendant Dmitriy Guzner (2008) < http://secretdox.wordpress.com/2008/10/18/usa-v-guzner-plea-agreement-for-defendant-dmitriy-guzner/> at 27 September 2009.

protected computer. Any computer connected to the Internet is a protected computer.[242] Both the DoS and DDoS attacks cause the transmission of a code indirectly (by zombie) or directly to the victim system and affect the availability of online services.

The punishment prescribed for first the conviction is up to ten years in prison and/or a fine of up to $250,000; while a repeat offence is punishable by up to twenty years in prison and/or a fine of up to $250,000.[243] For cases of reckless damage, however, the punishment is reduced to five years and/or a $250,000 fine and the crime is treated as a misdemeanour if the damage was caused merely by negligence.[244]

d) Comparative Legal Analysis

Apparently, legislators in these three countries avoided making any specific references to DoS and DDoS attacks, but rather aimed at setting out a broad framework addressing communications interruption and impairment. They distinguish between serious crimes that can possibly endanger the national security and minor crimes. However, unlike the Jordanian approach, the Australian and the US statutes impose harsh penalties in the case of serious offences.

The Jordanian statute is so broad as to include both physical attacks, such as bomb attacks, and virtual attacks, such as DoS attacks, because communications installations and telecommunications traffic, mentioned in the law, refer to both physical and virtual devices, such as modems, and TCP/IP protocols. This breadth does not differentiate between hackers, virus writers, script kiddies, and terrorists attacking communications systems. This is problematic for a number of reasons. First, it treats alike those with differing motivations and objectives. Script kiddies breaking down a website, for example, could be punished as severely as the writers or the distributors of the various modes of attacks. Second, it ignores the differences between the physical and virtual worlds in terms of the destruction and casualties that they cause; therefore, a tougher punishment should be correlated with the severity of the crime. Jordanian *Telecommunications Law* 1995 does not offer such a correlation.

[242] Protected computer, according to the section (e) (2)(B) ‘is a computer used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States’. *Computer Fraud and Abuse Act* 18 USC §§1030 s (e) (2) (B) (1984).

[243] *Computer Fraud and Abuse Act*, 18 USC§§ 1030 s (c) (4) (c) (1984).

[244] *Computer Fraud and Abuse Act,* 18 USC §§ 1030 s (c) (4) (c) (1984).

3.2 Cybersabotage

It is widely recognised that physical damage to computer systems and peripherals, such as printers, screens, hard disks, and so on, could jeopardise a business operation and cause pecuniary losses. Ulrich Sieber has mentioned several methods that can be used to inflict tangible damage,[245] such as the use of explosive materials, pouring a liquid into electronic equipment or setting fire to a building where computers are operating.[246] For example, computer centres were attacked by terrorist groups, such as the Red Brigade in Italy and Committee for Liquidation and Subversion of Computers (CLODO) in France.[247] Nevertheless, physical damage to computer systems is excluded from the classifications of cybercrimes because traditional criminal and procedural codes already effectively apply to physical damage. The legal problems arise when intangible properties, such as data and programmes, are the victims.

Intangible damage to computer systems, such as information, data, and software programmes is more ferocious, the damage more extensive, and the consequence more dangerous than that of physical damage to computer hardware. It is more ferocious because it comes unexpectedly and is difficult to predict as well as to recover from. It is more extensive because it spreads instantaneously over the whole virtual world like a malignant cancer and the consequences are potentially devastating, both operationally and economically.

This subsection, therefore, starts by examining various techniques and methods used to inflict logical damage and gain access to computers, Viruses, Worms and Trojan horses, and then comparatively analyses the relevant Jordanian, Australian, and the US laws.

3.2.1 Methods of Attack

a) Viruses

The term ‘Virus’ used to be exclusive to medical circles to describe a ‘foreign agent injecting itself into a living body, spreading and causing health problems’.[248] The same terminology has since been transferred to cyberspace to describe malicious programmes

[245] Sieber, above n 87, 15.

[246] Ibid 16.

[247] See, eg, Martin Wasik, *Crime and the Computer* (1991) 135.

[248] Joseph Migga Kizza, *Computer Network Security* (2005) 393.

that have the same functions as a biological virus, such as random breeding, being uncontrollable, and causing internal damage.

A computer virus can be defined as a 'set of computer instructions that propagates copies or versions of itself into computer programmes or data when it is executed within contaminated programmes'.[249] Thus, it has the capacity to duplicate itself inside a computer's memory[250] and to maliciously amend and control computer programmes, or to reprogram computer systems, and to execute functions, such as erasing or deleting hard drive contents.[251]

The proliferation of computer networks as well as the inter-operationalism of computer systems, such as Microsoft Windows, has dramatically increased cyberspace vulnerability to malicious programme attacks.[252] For example, the number of widespread viruses jumped to nearly 140,000 in 2003 and surveys show that between 400 and 500 new viruses are discovered monthly.[253] Nevertheless, virus attacks are decreasing in number relative to other types of malware attacks, such as worms and Trojans, because of the criminalisation of virus attacks, and because virus attacks do not necessarily lead to financial gain and sensitive information collection.[254]

b) Worms

In the same manner as viruses, worms are malicious programmes that duplicate themselves in computer systems by exploiting the software system's vulnerabilities. They surreptitiously sneak from one computer to another through connected computers networks.[255] Recent worm attacks, 'Zotob' and 'Mytob'[256] for example, have exploited

[249] See, Michael Erbschole, *Trojans, Worms, and Spyware* (2005)19. See also, Parker (ed), above n 24, 459, 473. Another definition is 'software programs deliberately designed to interfere with computer operation, record, corrupt, or delete data, or spread themselves to other computers and throughout the Internet, often slowing things down and causing other problems in the process'. *What Is a Computer Virus?* (2005) Microsoft <http://www.microsoft.com/athome/security/viruses/intro_viruses_what.mspx> at 18 January 2006.

[250] Ibid.

[251] See, eg, Catherine Holahan and Staff Writer, '*Computer Viruses at Epidemic Proportion*', 3 July 2004, <http://www.highbeam.com/library/doc3.asp?DOCID=1P1:91913140&num=5&ctrlInfo=Round18%3AProd%3ASR%3AResult&ao=1&FreePremium=BOTH> at 8 December 2005.

[252] See, eg, Kizza, above n 247, 394.

[253] Ibid. See also, Holahan, above n 247.

[254] See, eg, *Breeding Brand New Viruses* (2006) Computer Crime Research Centre <http://www.crime-research.org/news/17.01.2006/1764/> at 23 January 2006.

[255] See generally, Erbschole, above n 249, 23.

[256] On 14 of August 2005 two teenagers from Turkey and Morocco launched a couple of malicious codes called Zotob and Mytob against several international media websites including CNN, ABC, and the New

flaws in Microsoft's Windows Plug and Play[257] functionality.[258] The worm attack is considered the fiercest kind of malicious code and can inflict massive damage worldwide. The 'I LOVE YOU' and 'Code-Red' worms, for instance, inflicted billions of dollars worth of damage worldwide.[259]

c) Trojan Horses

The term *Trojan horse* is derived from the historical story of the city of Troy, which was defended by an impregnable wall. The legend of Troy tells that Greek warriors besieged the city for ten years[260] and eventually got in by using a giant wooden horse in which a few Greek soldiers had hidden to open the gate of the city of Troy.[261] In a similar way, the mechanism of computer horses mimics the horse of Troy.

In contrast to Viruses and Worms, Trojan horses are spyware[262] that operate surreptitiously inside the victim's system.[263] They are dynamic, offering criminals the capability to access, change, steal and corrupt computer systems.[264] The mere unauthorised access of computer data can easily compromise network security and harm data confidentiality and integrity and perform other forms of illegal activities and/or exploitation of illegal entry. Different methods are used for inserting the horse into a

York Times. See, Joe O'Halloran, 'FBI arrests young Turk and Moroccan for Zotob' (2005) (5) *Network Security* 1.

[257] Plug-and-Play is a computer technology developed by Microsoft that give the user the ability to plug a new device such as a modem, Universal Serial Bus (USB), network cards, etc into computer system without needing to set up a new configuration. Hence, once a device is plugged into a system it will recognise it directly. For more information, see David S Lawyer, *Plug-and-Play-HOWTO* (2005) The Linux Documentation Project <http://www.tldp.org/HOWTO/Plug-and-Play-HOWTO.html> at 20 January 2006.

[258] See, eg, O'Halloran, above n 256.

[259] See, eg, Paul A Henry, *A Brief Look at the Evolution of Killer Worms* (2003) CyberGuard Corporation <http://www.csoonline.com/whitepapers/050504_cyberguard/EvolutionoftheKillerWorms.pdf> at 22 January 2006.

[260] See, eg, *The Trojan War: The Judgement of Paris* (1998) The World of Royalty <http://www.royalty.nu/legends/Troy.html> at 20 January 2006.

[261] See, eg, Volonino & Robinson, above n 197, 40. See also, Kizza, above n 248, 398.

[262] 'Spyware' aka 'stealware' or 'adware' is a malicious code used to gather online information about a person or organisation using Internet services without their knowledge or permission; also it is a surveillance program that can be directly or remotely installed to track all the user online activities. See generally, Erbschole, above n 249, 25-26. See also, Stalking Resource Center, *Who's Watching You--Spyware and Stalkers* (2005) Stalking Resource Center <http://www.ncvc.org/src/main.aspx?dbID=DB_WhosWatchingYou--SpywareandStalkers128> at 15 January 2006.

[263] See, eg, Parker Donn B, 'Computer Crime' in K M Jackson and J Hruska (eds), *Computer Security: Reference Book* (1992) 457.

[264] See, Erbschole, above n 249, 22.

system. Social engineering methods, for example are frequently used to sneak Trojan Horses into computer systems.[265]

3.2.2 Legal Analysis of cybersabotage

It can be seen that malicious codes are insidious programmes designed for a wide range of criminal offences. For example, unleashing a Trojan horse is an indispensable step to further illicit access. Therefore, unleashing a malicious computer programme on a communications network without causing damage is considered 'unauthorised access', also known as 'cybertrespass'. Performing a similar action in which intangible properties of a communication system, such as information storage, are destroyed is considered 'cybersabotage'. Thus, Viruses, Worms and Trojan Horses, either cause intangible damage to computer systems or unauthorised access to people's computers.

In this subsection, two types of cybercrimes will be analysed, namely cybertrespass and cybersabotage. Criminalisation of cybertrespass and cybersabotage will be analysed in order to evaluate the effectiveness of existing laws of Jordan, Australia and the USA to address these types of cybercrimes. Because cybertrespass and cybersabotage can be committed by the use of the same malicious codes, including Viruses, Worms and Trojan horses, and in order to delineate each offence and its legal response, it is important to distinguish between two forms of criminal intention. The first intention is related to cybertrespass, and the second one will be discussed under cybersabotage.

1. Cybertrespass

Cybertrespass tools are designed either to give the attacker the ability to display, amend, delete, corrupt, or access and control programmes and data which are saved in the internal hard disk or remotely in the ISP's computer memory. Therefore, in this type of crime, i.e. cybertrespass, the criminal intention is either to access without permission, to exceed permission, or to alter parts of, or the entire system, or to commit further crimes, such as identity theft. Thus, the trespasser's intention is the real subject of inquiry, because Trojan horses and other forms of harmful programmes can be exploited to carry out different tasks. Therefore, to better understand the legal response, it is important to

[265] See, eg, Cert, *Advisory CA-1999-02 Trojan Horses* (1999) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1999-02.html> at 19 January 2006.

distinguish between the two following forms of criminal intention for trespassing computer systems.

The first intention is wilfully and knowingly accessing without permission any computer system, i.e. inserting a Trojan or any other forms of harmful programmes. In other words, there is no ulterior purpose to commit further crimes. For example, inserting a Trojan horse into a computer system and accessing it without consent.

The second intention goes further than that, i.e. inserting a Trojan horse and tampering with operating system or data. For example, deleting a programme in a bank's computer memory may be intended to create a space in which to conceal a programme debiting small fractions of the total amount of customers' accounts.

a) Jordan

In the case of the first intention, Section 11 Article (79) of the Jordanian *Telecommunications Law* 1995 imposes criminal liability on 'Any person…who uses a telecommunications network in an illegal way or connects his network with another Telecommunications network without having the right to do so, or hinders the delivery of services from other Telecommunication networks'. While this article does not specify the meaning and scope of the illegal use and does not explicitly criminalise cybertrespass, it can be applied to trespass, because, for example, a Trojan horse illegally connects the attacker's system with the victim's whereby the former can execute multiple activities simultaneously, such as compromising data availability, confidentiality and integrity. Therefore, the mere trespass to networks, contrary to the rights of the owner, is an offence under the above provision. However, this provision does not apply if the user legitimately accessed a network, exceeds the permission, or goes beyond a pre-determined period of time. The criminalisation provision should be more precise and describe clearly the offence. And the above article does not address a use that goes beyond legitimate access.

b) Australia

In Australia, in contrast, the deliberate unauthorised access into computer systems and networks is considered a crime. Division 478.1 (a), (b) and (c) of the Australian *Cybercrime Act* 2001 applies to whoever '(a)…causes any unauthorised access…

(b)…intends to cause the access… [or] (c)…knows that the access…is unauthorised'.[266] Thus, a person is guilty of cybertrespass once he wilfully and knowingly accesses a computer system illegally. However, the Act requires that the access should be to a system protected by an access control system, such as a password or any software or hardware device installed to protect it.[267]

c) USA

In a different way, Section 1030 (a) (2) of the CFAA proscribes acting in excess of authorisation so as to intentionally access a computer without authorisation, or obtain information from a financial institution, any department or agency, or any protected computer involved in interstate or foreign communication.

2. Cybersabotage

Cybersabotage usually occurs when a malicious code is used to access a system and then deletes, corrupts, or damages data. A Trojan horse, for example, gives the launcher full access to hard drives and operating systems,[268] providing capability to delete and to compromise information,[269] or to launch attacks from the victim's system against other systems.[270]

In the second form of criminal intention is to wilfully and knowingly access without permission computer systems and networks to amend, delete and damage data. The attacker's intention goes further than accessing computer systems without permission to commit a further crime of sabotage.

a) Jordan

Criminalisation of cybersabotage according to the Jordanian *Criminal Law* 1960 poses a problem, because of the intangible nature of programmes and data. In Jordan, nothing in any legal provision protects intangible objects except materials protected under the *Copyright Law.* Article (443) of the Jordanian *Criminal Law* 1960, for example, only

[266] *Cybercrime Act 2001* (Cth) div 478(1), (a) (b) (c).

[267] *Cybercrime Act 2001* (Cth) div 478(3).

[268] See, eg, *Trojans: Myths and Facts* (2002) EMSI Software <http://www.emsisoft.com/en/kb/articles/tec021007/> at 27 January 2006.

[269] See, eg, Barrie Mccombs, 'Phoney Phishing and Pharming' (2005) 10 (3) *Canadian Journal of Rural Medicine* 186.

[270] See, eg, Joseph Lo, *Trojan Horse Attacks* (2004) <http://www.irchelp.org/irchelp/security/trojan.html> at 29 January 2006.

protects tangible properties against physical damage. Damaging or altering a digital property, therefore, is not punishable, unless the culpable action extended to physical destruction, such as smashing hardware. Therefore, deleting or modifying data and programmes without damaging the physical medium, as a Trojan horse does, does not fall under the above provision.

However, specific aspects of cybersabotage can be prosecuted under Article (76) of the Jordanian *Communications Law* 1995. It proscribes a particular breed of cybersabotage offences, particularly illegally interrupting, corrupting, or damaging messages being transmitted through communications network. It provides that 'Any person who intercepts, obstructs, alters or strikes off the contents of a message carried through the telecommunications networks or encourages others to do so, shall be punished by imprisonment for a period not less than one month and not exceeding six months, or by a fine not more than JD. 200, or by both penalties.'[271]

Unfortunately, the meaning of 'contents of message' excludes any further data not considered a part of a message. As a result, a deliberate action of sabotage which goes beyond destruction of a mere message, such as alteration of programmes or static data stored in a computer memory, does not fall under the above provision.

b) Australia

The Australian *Cybercrime Act* 2001 makes cybersabotage a felony. Section 477.2 (1) (a) applies to whomever '…causes any unauthorised modification of data held in a computer'.[272] This section defines the intentional modification as any act of alteration or removal data or an addition of data to the data held in a computer without authorisation. The culprit would be liable under this subsection once the malicious code caused damage.

c) USA

The CFAA, in contrast, explicitly prohibits unleashing a malicious code. The fifth subsection, 1030 (a) (5), applies to whomever 'knowingly causes the transmission of a

[271] *Telecommunications Law 1995,* 11(76).

[272] *Cybercrime Act 2001* (Cth) div 477.2 (1).

program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.'[273]

d) Comparative Legal Analysis

From the above analysis and comparison, one can conclude that the current laws relating to cybertrespass and cybersabotage in Jordan are not satisfactory. They are insufficient and cannot adequately deal with all aspects of cyber offences. It seems that the current Jordanian laws have very little to do with the current situation.

The cybertrespass provision, Article (79), is not comprehensive and is intended only to provide limited protection against physical access. It does not capture all aspects of cybertrespass. Exceeding authorised access, for example, is not criminalised. Furthermore, the provision does not criminalise any attempt at unauthorised access to a telecommunications network.

Cybersabotage provisions lack protective and comprehensive safeguards against corruption or other damage to digital objects. On one hand, the Jordanian *Criminal Law* 1960 has failed to protect intangible property against logical attacks. It protects only physical property, such as hardware against any physical attacks. This is because the current law was written so long ago; in a time before digital property was introduced in Jordan. On the other hand, the new communication law partially addresses the issue of cybersabotage. Article (76) only criminalises actions specifically intended to inflict damage on the contents of a message. This narrow protection leaves many cyber contents, such as websites, programmes and data, unprotected against other aspects of cybersabotage.

With the pervasiveness of the Internet, and cyber offences, it becomes ever more imperative to enact a comprehensive and developed cybercrime law. In this part, it has been useful to learn and borrow from the experience of countries with advanced legislation in this field. However, while there is no intention that Jordanian legislators will follow all the details of the Australian or US cybercrime laws, it is important that attention be given to the Australian and US counterparts and to how they are being

[273] *Computer Fraud and Abuse Act,* 18 USC §§1030 s (c) (4) (c) (1984).

implemented. Some provisions in both the *Cybercrime Act* 2001 and CFAA relating to cybertrespass and cybersabotage can be adopted.

From the Australian *Cybercrime Act* 2001, Division 478.1 might be adopted. This division states that a person would only commit a cybertrespass offence if he bypassed an access control system, such as a password or any software or hardware device, such as CCTV[274] installed to protect it. This provision has no parallel in the Jordanian *Telecommunications Law* 1995. The importance of this provision lies in the fact that it distinguishes between two computer systems, protected and unprotected systems. This distinction leads to the identification of how the unauthorised access occurred as well as lessens the burden on investigators responding to cybertrespass. It identifies any attempt at unauthorised access, so it can be detected and investigated; because access control systems can capture unauthorised access attempts. In addition, adopting such a provision would mean accessing an unprotected system is not a crime of trespassing. From the CFAA, might be adopted the second section, 1030 (a) (2), which criminalises exceeding authorisation.

Unlike the Jordanian one, Australian's model for the criminalisation of cybersabotage, Section 477.2 (1) (a), is flexible enough to include any type of sabotage action against data held in stand-alone computers or networks. Any unauthorised modification of data including alteration, deletion, or addition of data constitutes cybersabotage. This flexibility is necessary because of the vast number of sabotage actions against cyberspace as well as the subjects of sabotage, such as websites, programmes, information, and data. The narrowness of Article (76) of the Jordanian *Telecommunications Law* 1995, which exclusively protects the contents of messages carried through telecommunications networks, can be solved by adopting a more flexible provision. However, the adopted provision should only criminalise offences against protected computers and networks. Thus, the desired flexibility can be adopted from the Australian *Cybercrime Act* 2001 and the protection boundary from the CFAA section 1030 (a) (5).

[274] The term CCTV is an abbreviation for Closed-Circuit Television and is often used for security surveillance.

3.4 Conclusion

Information and communications technology has the potential to offer unprecedented opportunities for criminals to commit illegal acts, because of the unique environment in which users interact with each other as well as with virtual objects. Thus, different forms of illegal activities have emerged posing real dangers in cyberspace. The most popular of these activities are denial of services (DoS and DDoS) attacks.[275] The seriousness of these crimes ranges from minor interruptions of insignificant web sites or computer systems to preventing access by millions of users surfing popular Internet web sites such as Google.com.

Cybersabotage, on the other hand, is more devastating to the victim than denial of service attacks and is harder to recover from. The evidence extracted from this sort of crime also takes different forms, such as code programs, metadata and log files.

These illegal activities are in continuous evolution and represent a challenge for lawmakers to devise new laws and amend others to deal with new forms of crimes as well as with new faces on old crimes.

While the Australian and US lawmakers continue to develop the legal response necessary to prosecute cybercrimes - Australian legislators have enacted the *Cybercrime Act 2001* and the US Congress has introduced the *Computer Fraud and Abuse Act* 1984, which has been revised several times to keep abreast with cyberspace illegal activities developments, Jordanian legislators responded to cybercrimes by enacting a few articles in the *Telecommunications Law* 1995, which was amended by Law No. 8 for year 2002.

The current Jordanian laws in the context of other issues indirectly address the new forms of cybercrimes, such as TCP/IP attacks and cybertrespass. The *Telecommunications Law* 1995 was enacted before the advent of the Internet in Jordan mainly to protect the physical components of communications infrastructure as well as messages transmitted via telecommunications networks. However, while this law can be applied to TCP/IP attacks yet neither the above legislation nor the Jordanian *Criminal Law* 1960 apply to offences that are not directly connected to the telecommunications networks, such as static data saved on PCs, or offences that do not interrupt

[275] See, eg, Stephenson, above n 16, 26.

communications traffic, or access to communications networks which goes beyond legitimate access. By contrast, the *Cybercrime Act* 2001 and the CFAA effectively criminalise all forms of TCP/IP attacks as well as cybertrespass.

No provision in existing Jordanian laws addresses cybersabotage offences, except one provision in the *Telecommunications Law* 1995 which criminalises offences targeting messages transmitted via telecommunications networks. The Jordanian *Criminal Law* 1960, which is the major criminal law, is incompetent to protect digital property, because the definition of property which is eligible for legal protection under the Jordanian *Criminal Law* 1960, is a physical moveable or immovable object, such as gold, cars, houses, or lands. By comparison, the *Cybercrime Act* 2001 and the CFAA sufficiently and directly address all forms of cybersabotage.

4 CYBERSPACE AS THE MEANS OF THE CRIME

Introduction

In this chapter, in which cyberspace is the object of the crime, the illegal uses of cyberspace as a tool to engage in crimes against public trust, morality, property and individuals will be defined. This chapter describes four types of cybercrimes, cyber forgery, cyber pornography, cyber identity theft, and cyberstalking. In each cybercrime, a brief account of the recent modes of attack used to perpetrate crime is explained and the legal response to such crimes will be analysed in order to assess the adequacy and sufficiency of the current laws.

In similar manner to the pervious chapter, the objective of this chapter is to provide a basic understanding of the most popular types of cybercrimes, i.e. in which cyberspace is the object of the crime, and the legal response to them. It is necessary for law enforcement agencies, particularly Cybercrime Units, lawyers, and prosecutors, to be acquainted with forms of crimes, to understand them various types of cybercrime and the differences between them, as well as the legal responses to them. This is because criminalisation of cybercrimes is an indispensable prerequisite for law enforcement personnel to respond and build effectively, at both national and international levels, a strategy against cybercrimes. Consequently, a clear legal response to cybercrimes offences is a prerequisite to success in searching and seizing computers and obtaining digital evidence.

Cyberspace misuse takes many forms and shapes. Nowadays, the vast majority of traditional crimes, such as forgery, pornography, stalking, and so forth can be facilitated by computers. However, in contrast to the crimes committed against computer systems, the majority of these types of crimes fall within the scope of traditional criminal law provisions enacted to combat traditional offences of forgery, pornography, and so on. Some of these statutes could be applied successfully to particular computer-related crimes while other crimes, particularly stalking, are not dealt with at all in the traditional provisions in a way that can address the challenges caused by information technology.

Because a wide range of traditional crimes can be facilitated by computers, cyberspace as the object of the crime can be classified into four categories, depending upon the victim, for example, crimes against public trust, crimes against morality, crimes against property, and crimes against persons.[276] Under these classifications a wide rage of crimes can be studied, though this chapter is of necessity an illustrative study, not an exhaustive treatment of the interaction of computer technology and traditional criminal activity. It will be divided into four subsections, dealing respectively with four major crimes, cyber forgery, cyber pornography, cyber identity theft, and cyberstalking.

4.1 Cyber Forgery

While there is no generally accepted definition of forgery worldwide, some scholars attempt to define very broadly documents which may be the subject of forgery to include electronically stored information. Johan Smith, for example, has defined the term 'document' as 'any written group of letters, figures or any other symbols written on a paper or any material and used for conveying information'.[277] According to this definition, disks, tapes, sound tracks, or other devices on or in which information is recorded or stored are considered to be documents.

In the context of cyberspace, Yearwood and Hayers define cyber forgery as 'any misrepresentations produced via computer, whether generated to a hard copy such as in making counterfeit money or submitted electronically using fraudulently obtained credit or credentials'.[278] Another definition is 'the input, alteration, erasure or suppression of computer data or computer programmes, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence'.[279] According to these definitions, cyber forgery takes two forms. First, it is the use of computer systems to forge computer copies of physical records, such as birth certificates.[280] Second, it is the use of computer systems

[276] See, generally, Brenner, above n 172.

[277] Johan Smith, *Criminal Law* (9th ed, 1999) 655.

[278] Douglas L Yearwood, and Richard Hayes, *Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys* (2003) North Carolina Department of Crime Control & Public Safety <http://www.ncgccd.org/PDFs/Pubs/NCCJAC/cybercrime.pdf> 7 May 2006.

[279] See, George Papapavlou, 'Legal Aspects of New Information Technologies' (Working Paper No DG XIII-E1, National Institute of Standards and Technology, 1992) K-3.

[280] علاء الدين منصور مغايرة, *The Modern Aspect of Information Crimes: Comparative Study* (Alaeldin Mansour Maghaireh trans, 2000) [trans of: الاوجه الحديثة للجرائم المعلوماتية " دراسة مقارنة].

to forge electronic or software dependent records, such as e-mails, and bank account statements.[281]

a) Jordan

Traditional forgery is a felony addressed in the Jordanian *Criminal Law* 1960 (Chapter 2, Section 5/Articles 260, 261, and 263) under the title 'Crimes against public trust'. It is a crime against public confidence in formal documents. The Jordanian *Criminal Law* 1960 defines forgery as 'an intentional modification of truth and data in an authentic document or instrument having legal efficacy and resulting in physical, incorporeal, or social harm'.[282] From the definition, three legal elements should be considered in the establishment of a forgery offence.[283] The first element is the counterfeiting or falsifying of a formal document or an instrument; the second element is that harm must be caused by the first element; and the third element is the criminal intention to use the false document to gain profit or status.[284] Accordingly, forgery occurs when one makes or alters a document having legal force and effect and causing harm thereby. Thus, the definition of a document is important to determine whether Jordan's forgery law applies to its cyber content. In other words, if the computer generated documents have legal force and effect, the Jordanian *Criminal Law* 1960 would apply.

However, while none of the forms of cyber forgery are explicitly addressed in the Jordanian *Criminal Law* 1960, the Jordanian *Electronic Transaction Law 2001* criminalises traditional crimes committed by computers. The first form of forgery, i.e. forging computer copies of physical documents, does not raise the problem of the applicability of Jordanian *Criminal Law* 1960 to cyber forgery, because digital copies of physical records are considered formal documents. Scholars agree to apply traditional forgery provisions to computer printouts as long as they comply with forgery provisions.[285] Furthermore, Article 38 of the *Electronic Transactions Law* 2001 provides that any traditional crime perpetrated using a computer is deemed a crime. This provision criminalises the first form of cyber forgery. Accordingly, forging a certificate

[281] See, Brenner, above n 172.

[282] *Criminal Law 1960* (2) (5) (260).

[283] ابراهيم حامد طنطاوي, *The Criminal responsibility of forgery crimes on formal documents scholarly and Judicial* (Alaeldin Mansour Maghaireh trans, 1995) 17 [trans of: " المسؤلية الجنائية عن جرائم التزوير في المحرارات فقهاء وقضاء].

[284] Ibid.

[285] Ibid

of marriage using a computer is a crime under Jordanian *Criminal Law* 1961. Criminalisation of the second form of cyber forgery i.e. the use of computer systems to forge electronic or software dependent records, collides with two obstacles:

Firstly, the Jordanian *Criminal Law* 1960 does not protect intangible assets. It is clear from article (443) of the *Criminal Law* 1960 that protection is only available for tangible properties. Therefore, intangible records stand beyond that protection.

Secondly, *Criminal Law* 1960 does not recognise a digital document as a formal document. Unfortunately, Jordanian law does not define the term 'document'. In addition, Jordanian scholars in defining 'document' have excluded disks, tapes and other devices from the documents which have legal efficacy.[286] They argue that, despite these instruments conveying thoughts and ideas, they contain invisible letters and symbols and, consequently, are not documents.[287] They assume that the forged modification of 'truth in document' which is mentioned in the legislation, takes place either by adding or amending documents written using durable rather than digital materials.[288] Kamel Al-Seed, a prominent Jordanian legal scholar, has opined that, 'The United Kingdom forgery law of 1981 has failed to prosecute computer forgery, despite the fact that it does not distinguish between a written document and a cassette or tape or any other device, hence, undoubtedly, the Jordanian forgery law is insufficient to do so'.[289]

b) Australia

The Australian law by contrast, has closed the loopholes that made it possible for a forger to evade prosecution for cyber forgery. According to the Australian *Cybercrime Act* 2001, both using computers to forge documents and using computers to forge electronic records is criminalised. Division 477.1 of the *Cybercrime Act* 2001 imposes criminal liability on any person who intentionally amends data held in a computer.[290]

[286] محمود نجيب حسني, " *Criminal Code explanation – crimes division* (Alaeldin Mansour Maghaireh trans, 1992) 247 [trans of: شرح قانون العقوبات-القسم الخاص]. See also, ابراهيم حامد طنطاوي, above n 282.
[287] حسني Ibid.
[288] سامي الشوا, *Informatics Fraud as a New Phenomenon* (Alaeldin Mansour Maghaireh trans, 1993) 157 [trans of: الغش المعلوماتي كظاهرة اجرامية مستحدثة].
[289] كامل السعيد, *Computer and Information Technology Crimes* (Alaeldin Mansour Maghaireh trans, 1993). [trans of: جرائم الكمبيوتر والجرائم الاخري في مجال التكنولوجيا].
[290] *Cybercrime Act 2001* (Cth) div 477.1 (1).

Data according to Division 476.1 includes information in any form; or any programme.[291]

c) USA

In the same manner of the Jordanian, the USA legislatures have not explicitly criminalised cyber forgery. The US *Criminal Code* lacks any provision specifically addressing using computers to forge documents or using computers to forge electronic records. Some States, however, criminalise cyber forgery. For example, New York legislation has amended the definition of written instrument to include computer data or a computer programme.[292] In Virginia, the Criminal Code expands the definition of forgery to include 'creation, alteration or deletion of computer data while it is contained within a computer or computer network'.[293]

d) Comparative Legal Analysis

The Jordanian definition of forgery is controversial and narrow, particularly in the context of cyberspace and computer systems. It excludes new methods of forgery, such as using a computer to forge documents or digital records. Scholars, therefore, exclude digital records from the definition of document. The *Criminal Law* 1960, however, does not limit methods of forgery and therefore using computers to forge a document is considered a forgery. Article 38 of the *Electronic Transactions Law* 2001 criminalises the use of computers to commit traditional crimes. And cyber forgery is a traditional crime committed in an electronic environment. The above laws, however, are not applicable to using computers to forge electronic records, because the nature of the document mentioned in the *Criminal Law* 1960 differs significantly from digital records. Australian law makers closed the gap when they implicitly criminalised both forms of the cyber forgery.

Jordanian lawmakers should device adequate laws to close the loopholes that facilitate using computers to forge digital records. The Australian approach provides a model for Jordanian lawmakers to adopt and follow, because the *Cybercrime Act* 2001 addresses the two aspects of cyber forgery.

[291] *Cybercrime Act 2001* (Cth) div 476.

[292] See, Hugh Scott, *Computer and Intellectual Property Crime: Federal and State Law* (2001) 1063.

[293] See, Hugh Scott, *Computer and Intellectual Property Crime: Federal and State Law Cumulative Supplement* (2006) 75-10.

4.2 Cyber Pornography

The word 'pornography' literally means 'the writing of harlots'.[294] In this section, two closely related issues of cyber pornography are discussed. The first is the use of computers and, in particular, the Internet, to disseminate pornographic materials, i.e. cyber pornography. The second is the use of computer technology to produce 'virtual child' pornography.

4.2.1 Cyber Pornography

Cyber pornography is the use of cyberspace to disseminate pornographic materials.[295] Government prohibition on the publication of offensive materials has been significantly compromised by the pervasiveness of the Internet.[296] With the emergence of the Internet and other communications technologies, the Jordanian government and many neighbouring countries have installed Internet filtering devices that block anti-regime websites. For example, www.arabtimes.com., an Arabic news website antagonistic towards Arabic regimes is blocked across the Arab world, including Jordan. Pornographic materials, however, which do not pose an immediate danger to governments, are ignored. It seems that the government is willing to rely on traditional legal protections to combat cyber pornography and other offensive materials rather than to set up technological protections.

In Australia and the USA, adult pornography is not a crime, thus this section only addresses Jordan's response to cyber pornography and the second part will address pornography offences in both Australia and the USA.

Jordan

Jordan's legal response towards pornography starts from a different premise than western countries. While the latter shows a serious concern for the production, display or possession only of child pornography, because of its harmful ramifications for both

[294] Stephen T Holmes and Ronald M Holmes, *Sex Crimes: Patterns and Behavior* (3rd ed, 2007) 340.

[295] See, eg, Susan M Easton, '*The Problem of Pornography: Regulation and the Right to Free Speech*' (1994) 141.

[296] See, eg, Bela Bonita Chatterjee, 'Last of the Rainmacs: Thinking about Pornography in Cyberspace' in David Wall (ed), *Crime and the Internet: Cybercrime and Cyberfears* (2001) 74.

children and adults who watch such materials,[297] the Jordanian legal system, on the other hand, backed by cultural and religious doctrines, generally prohibits all forms of pornography. Two provisions from the *Criminal Law* 1960 and a one provision from the *Electronic Transactions Law* 2001 prohibit different aspects pornography.

Article 319 of the *Criminal Law* 1960 explicitly outlaws the intentional publishing, selling, distributing, displaying or possessing of any offensive materials that corrupt community morals.[298] The prohibition includes both the physical materials, such as hard copy, and intangible images, such as Jpegs, as long as the act is committed for the purpose of selling, distributing, or publicly displaying offensive materials in any manner.[299] Thus, displaying pornographic images at a dwelling or possessing it for one's own personal use on a hard disk are not prohibited. Article 320 of the *Criminal Law* 1960 criminalises any abusive conduct or obscene gesture displayed in a public place or that can be seen by many people. The legislators use general terms in both articles 319 and 320, such as 'any offensive materials' and 'any abusive conduct' to protect the community from abusive and obscene materials.

In the realm of cyberspace, although the *Criminal Law* 1960 law was enacted before the advent of computer systems and the Internet, it can arguably be applied to cyber pornography. This would contradict, however, the core principle of every code of criminal law, which states that criminal laws are to be construed narrowly.[300] Applying this principle would prevent any attempt to broaden the scope of the above articles to include cyber pornography. It is a necessary condition for cyber pornography criminalisation to insert a more specific phrase, such as 'computerised materials' into Articles 319 and 320.[301] However, to close the loopholes and inadequacies of the above articles, Jordanian legislators passed the *Electronic Transactions Law* 2001. Most of its articles focus on electronic transactions, but one article is a 'catch all'. Article 38 of the *Electronic Transactions Law* 2001 imposes criminal liability on 'any person who

[297] See, eg, Peter Grabosky and Russel G Smith, *Crime in the Digital Age: Countering Telecommunications and Cyberspace Illegalities* (1998) 120. See also, Smith, Grabosky and Urbas, above n 25, 34.

[298] *Criminal Law 1960* (319).

[299] علاء الدين منصور مغايرة, above n 280.

[300] Hancock, above n167.

[301] For example, many countries, such as Israel have adopted new terms. Israeli legislators have used the term 'computerised materials' as a phrase to describe digital images and computer programme materials. See, eg, Miguel Deutch, 'Computer Legislation: Israel's New Codified Approach' (1996) 14 *The John Marshall Journal of Computer & Information Law* 461, 465.

commits an act that constitutes a crime pursuant to legislation in force by using electronic means shall be subject to the penalty of imprisonment for a period no less than three months and no more than one year, or a fine of no less than 3,000 JD and no more than 10,000 JD, or to both penalties jointly'.[302] This article, when combined with articles 319 and 320, may be used to criminalise cyber pornography.

4.2.2 Cyber Child Pornography

Child pornography has received a great deal of attention in recent years from sociologists, criminologists, media, and legislatures, as reflected by enacting child pornography prevention laws. However, it appears that there is no definitive parameter of what constitutes a child among countries, because of differences in their cultural, social and religious values.[303] For example, in the USA, the age of consent for girls is eighteen,[304] while it is sixteen in Australia,[305] and fifteen in Jordan. As a result of significant differences in definition and criminalisation, what actually constitutes child pornography varies considerably between countries.[306]

Cyber child pornography takes two forms, namely, against real human beings, usually called 'child pornography', and against 'virtual children'[307] or 'animated puppets'. Child pornography is defined as 'the visual or audio depiction of a child for the sexual gratification of the user and involves production, distribution, or use of such material'.[308] While this definition is broad enough to include a wide range of illegal activities ranging from producing to viewing real images of child pornography, it does not include virtual child pornography production, distribution, or possession.

[302] *Electronic Transaction Law 2001* (38).

[303] See, eg, Philip Jenkins, *Beyond Tolerance: Child Pornography on the Internet* (2001) 25-26. See also, Max Taylor and Ethel Quayle, *Child Pornography: An Internet Crime* (2003) 3.

[304] Ibid.

[305] Gordon Moyes, *Is there a Paedophile in Cabinet* (2003) Gordon Moyes Website <http://www.gordonmoyes.com/2003/06/03/is-there-a-paedophile-in-cabinet> at 26 June 2008.

[306] Majid Yar, *Cybercrime and Society: Crime and Punishment in the Information Age* (2006) 116.

[307] Cynthia S Osborne and Thomas N Wise, 'Paraphilias' in Richard Balon, and Taylor Segraves (eds), *Handbook of Sexual Dysfunction* (2005) 293, 306.

[308] Jayne Hosse, Stephen Clift and Simon Carter, 'Combating Tourist Sexual Exploitation of Children' in Stephen Clift, and Simon Carter (eds), *Tourism and Sex: Culture, Commerce and Coercion* (2000) 74, 76. See also, Thomas Milhorn, *Cybercrime: How to Avoid Becoming a Victim* (2007) 52.

Virtual child pornography consists of computerised images including animated movies of young children without using actual children[309] engaged in sex acts or other erotic activities with adult persons or between children themselves.[310] The computerised images are indistinguishable from real children.[311] This technological innovation came about to avoid child pornography statutes, putting the latter at risk of irrelevancy. Criminalisation of virtual child pornography requires the updating of child pornography statutes to keep them abreast of information technology developments and to sustain children protection against new predators,[312] because virtual child pornography poses a high risk to both adults and children.[313] Adults who watch child pornography are more prone than others to be child molesters and pedophiles;[314] also, the virtual pictures can easily lure children and help the predators to break the ice with children.[315] In other words, it encourages the children to build a sexual relationship with adult persons.

a) Jordan

Children have been given additional protection under the *Criminal Law* 1960. Chapter two, section 6, addresses crimes against the family, including crimes against children, such as rape, kidnapping, exposing children to indecent matter, seduction, sexual molestation, and all forms of sexual abuse against minors. The prohibition on cyber pornography can be applied to virtual child pornography, because the laws do not distinguish between adult and juvenile or between real and virtual images. This would contradict the core principle of criminal law, however, which states that criminal laws are to be construed narrowly.[316] Applying this principle would prevent any attempt to broaden the scope of the above articles to include virtual child pornography.

[309] James E Bristol, 'Free Expression in Motion Pictures: Children Sexuality and a Satisfied Society' (2007) 25 *Cardozo Arts & Entertainment* 333-345.

[310] See, eg, Schell and Martin, above n 45, 40.

[311] *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act* 18 USC §§ 501-4 (A) (2003).

[312] See, eg, Carter and Perry, above n 28, 320.

[313] See generally, David J Kolko and Elissa J Brown,' Child Sexual Abuse' in Robert T Ammerman and Michel Hersen (ed), *Case Studies in Family Violence* (2nd ed, 2000) 177, 178.

[314] See, eg, Seth L Goldstein, *The Sexual Exploitation of Children: A Practical Guide to Assessment, Investigation, and Intervention* (2nd ed, 1998) 35. See also, *Information about Legal and Illegal Pornography: Child Porn Offending The* Internet Safety Group <http://www.netsafe.org.nz/legal/child_porn2.aspx> at 6 October 2007.

[315] Ibid.

[316] Hancock, above n 167.

b) Australia

Since the advent of Internet services a decade ago, Australian legislation pertaining to traditional child pornography possession has been amended to include virtual materials. For example, the Australian *Broadcasting Service Amendment Act* 1999, the *Online Service Amendment Act* 1999 and, more recently, the *Commonwealth Criminal Code* amendments in 2004 are all intended to close the gaps and loopholes that were caused by the advent of the new technology.

The Australian *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) 2004* therefore, defines child pornography as 'material that depicts or describes, in a manner that would in all the circumstances cause offence to reasonable persons, a person under (or apparently under) the age of 16 years: (a) engaged in sexual activity, or (b) in a sexual context, or (c) as the victim of torture, cruelty or physical abuse (whether or not in a sexual context)'.[317] To include the broadest range of computerised materials, including virtual products, the same Act defines material as 'any form, or combination of forms, capable of constituting a communication'.[318] Division 474 of the same Act criminalises the act of production, dissemination or possession of child pornography.[319]

Nowadays, mere possession of child pornography in a computer memory is considered a felony in all of the Australian territories and states. Nevertheless, in some state jurisdictions,[320] proof of knowledge or intentional possession is required as a prerequisite to convict a person of possession of child pornography.[321]

c) USA

In the USA, child pornography is undoubtedly prohibited, but a legal conflict arose between the federal government and the Free Speech Coalition and American Civil

[317] *Crimes Act 1995* (Cth) div 473. 1 amended by *(Telecommunications Offences and Other Measures) Act 2004* (Cth).
[318] *Crimes Act 1995* (Cth) div 473. 1 amended by *(Telecommunications Offences and Other Measures) Act 2004* (Cth).
[319] *Crimes Act 1995* (Cth) div 474. 20 amended by *(Telecommunications Offences and Other Measures) Act 2004* (Cth).
[320] These states are QLD, VIC, and ACT.
[321] Penfold Carolyn, 'Child Pornography Laws: the Luck of the Locale' (2005) 30 (3) *Alternative Law Journal* 123.

Liberties Union over the banning of virtual child pornography.[322] The conflict culminated in the elimination of a portion of the *Child Pornography Prevention Act* of 1996 (CPPA) that had expanded the definition of child pornography to include computerised images.[323] In 2003, the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act* (the PROTECT Act) was introduced in order to correct the language of the CPPA and avoid any inconsistency with the First Amendment's objectives.[324] The PROTECT Act imposes criminal liability on 'any person who intentionally distributes, offers, sends, or provides to a minor any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, where such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct'.[325] It specifically addresses computer generated images or pictures, in other words, virtual child pornography. In the event of conviction, the offender would be liable to imprisonment for a term not exceeding twenty years or a period of no less than five years.[326]

[322] The legal battle over child pornography criminalisation in the USA started with the passing of the *Protection of Children against Exploitation Act* in 1977. The statute made illegal the use of children under the age of sixteen in the production of sexually explicit material to be distributed in interstate commerce. *The Child Protection and Obscenity Enforcement Act* of 1988, however, was the first American legislation to ban transporting, distributing, or receiving child pornography using Internet or computer technology. See generally, Ryan P Kennedy, 'Ashcroft v. Free Speech Coalition: Can We Roast the Pig Without Burning Down the House in Regulating "Virtual" Child Pornography?' (2004) 37 *Akron Law Review* 379, 384.

[323] The CPPA was originally enacted to expand the definition of child pornography to include 'virtual' child pornography. See generally, Sue Ann Mota, *The U.S. Supreme Court Addresses the Child Pornography Prevention Act and Child Online Protection Act in Ashcroft v. Free Speech Coalition and Ashcroft v. American Civil Liberties Union* (2002) Indiana University <http://www.law.indiana.edu/fclj/pubs/v55/no1/mota.pdf> at 18 February 2006. See also, Peysakhovich, above n 168, 810. The *Child Pornography Prevention Act* of 1996 defined child pornography as 'Any visual depiction, such as a photograph, film, videotape or computer image, which is produced by any means, including electronically by computer, of sexually explicit conduct will be classified as child pornography if: (a) its production involved the use of a minor engaging in sexually explicit conduct; (b) it depicts, or appears to depict, a minor engaging in …[such] conduct; (c) it has been created, adapted or modified to appear that an identifiable minor is engaging in …[such] conduct; or (d) it is promoted or advertised as depicting a minor engaging in …[such] conduct.'

[324] See, eg, Peysakhovich, above n 168. See also, Title V—Obscenity and Pornography Subtitle A—Child Obscenity and Pornography Prevention
Sec. 502. Improvements to prohibition on virtual child pornography. *Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act,* 18 USC §§ 502 -513 (2003).

[325] *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act,* 18 U.S.C §§ 18 USC 2252A (a) (6) (2003).

[326] *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act,* 18 U.S.C §§ 18 U.S.C. § 2252A (b) (1) (2003).

d) *Comparative Legal Analysis*

Western governments which regulate cyberspace content usually experience significant challenges. Finding the balance between protecting individual privacy, allowing freedom of expression, and protecting children from sex offenders is especially difficult, as was obvious in the USA experience. Jordan's situation is completely unlike that of Australia or of the USA in terms of banning offensive Internet content. Jordan did not face any serious challenge from any party to its prohibition of all forms of the dissemination of pornography. In contrast to Australian and US laws, in Jordan there is a loophole that needs to be addressed if the *Criminal Law* 1960 pornography provisions are to remain effective. Jordanian laws do not distinguish between virtual child pornography and other forms of pornography, or between child pornography and adult pornography. This loophole ignores the fact that child pornography threatens the physical and psychological well-being of the children; the punishment must be proportionate to the crime. Finally, Jordan and some Australian state jurisdictions require proof of knowledge and intention to punish the crime. This is laudable because hacking techniques, which are widely used, facilitate remote accessing and planting of such materials in a person's computer and without the latter's knowledge.

4.3 Cyber Identity Theft

Cyber identity theft has been described as the 'crime of the new millennium',[327] and the 'greatest threat to business after terrorism'.[328] It is 'one of the fastest growing financial crimes in the USA'.[329] Cyber identity theft can be defined as unauthorised access and use of someone's personal information, such as name, address, and credit card details, or social insurance number, in an illegal way.[330] Its negative impact on victims can include profound harm that extends beyond financial losses.[331] For example, an identity

[327] Sean B Hoar, 'Identity Theft: The Crime of the New Millennium' (2001) 80 *Oregon Law Review* 1423.

[328] See, eg, Bruce Arnold, 'Identity Theft' (2005) 38 *Security Solutions* 55.

[329] See, Hoar, above n 327. See also, Holly K Towle, 'Identity Theft: Myths, Methods, and New Law' (2004) 30 *Rutgers Computer & Tech* 237.

[330] Ibid. Vacca has defined identity theft as 'the appropriation of an individual's personal information in order to impersonate that person in a legal sense'. John R Vacca, *Computer Forensics: Computer Crime Scene Investigation* (2nd ed, 2005) 137.

[331] Ibid.

theft scenario was depicted by the movie 'The Net',[332] where the victim who was completely stripped of her identity by another woman, suffered not only monetary losses, but also non-monetary harm including emotional distress.[333]

The illegal use of identity information has increased exponentially in recent years.[334] In fiscal year 2005 alone, the USA Federal Trade Commission (FTC) received approximately 686,000 complaints of fraud (63%) and identity theft (37%).[335] While Internet auction fraud[336] was the most common form of fraud crime, credit card fraud was the most common form of reported identity theft complaint.[337]

While in both Australia and the USA statistics show that through cyber identity theft and fraud, annual large-scale monetary losses are being caused, Jordan's situation is significantly different. The use of the Internet for credit cards transactions is still in its infancy.[338] Jordan's official cybercrime statistics indicates that only 29 cybercrimes were reported in 2001 and that none of them was a cyber identity theft or a fraud crime,[339] because the value of personal information transmitted via the Internet, such as national identification number, has little value to identity thieves. However, there are no genuinely reliable statistics on cybercrimes in Jordan that can be used to determine how common identity theft and Internet fraud really are, due to the lack of law enforcement

[332] See, eg, Barbara Hemphill, 'Who Are You?(Preventing Identity Theft)' (2003) *The National Public Accountant* .

[333] Ibid. See also, Emily Finch, 'What a Tangled Web we Weave: Identity Theft and the Internet' in Yvonne Jewkes (ed), *Dot.cons: Crime, Deviance and Identity on the Internet* (2002) 86, 97.

[334] See, eg, Richard M Stana, 'Identity Theft: Prevalence and Cost Appear to be Growing' in Claudia L. Hayward (ed), *Identity Theft* (2004) 17, 20.

[335] Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data* (2005) http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf > at 12 February 2006.

[336] The various types of Internet auction fraud include non-delivery goods, misrepresentation, triangulation, black-market goods, multiple bidding and shill bidding. For more information, see: *Internet Scam Guide* New York City Government <http://www.nyc.gov/html/dca/downloads/pdf/internet.pdf> at 28 February 2006.

[337] Internet Auction was the leading complaint category with 12% of the overall complaints, followed by Foreign Money Offers (8%), Shop-at-Home/Catalog Sales (8%), Prizes/Sweepstakes and Lotteries (7%), Internet Services and Computer Complaints (5%), Business Opportunities and Work-at-Home Plans (2%). Credit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%). See generally, Federal Trade Commission, 'Consumer Fraud and Identity Theft Complaint Data' (2005) http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf > at 12 February 2006.

[338] See, eg, *King of Cards* (2005) Jordan Business <http://www.zawya.com/printstory.cfm?storyid=ZAWYA20051107090132&SecIndustries/pagE-Banking&l=000000051113> at 26 February 2006.

[339] مديرية الامن العام الاردني , *Annual Report, Department of Laboratories and Criminal Evidence* (Alaeldin Mansour Maghaireh trans, 2002) [trans of: التقرير السنوي, ادارة المختبرات والادلة الجرمية].

agency expertise and to weak public and private sector support for studies pertaining to cybercrimes.

Identity thieves exploit a variety of ploys to acquire personal information and commit their crimes.

4.3.1 Cyber Identity Theft Tactics

Cyber identity theft can be accomplished by using low-tech methods, such as scavenging (dumpster diving) a password and other electronic access code from actual physical garbage or by highly sophisticated methods, such as hacking into web sites and computers storing consumer information, including credit card details.[340] Spoofing is one of the most common cyber identity theft tactics. Web spoofing, Domain Name System (DNS), TCP, and IP spoofing, are popular tactics used to steal identity and commit fraud.[341]

A basic understanding the mechanism of those attacks is essential in order to ascertain the applicability of criminal provisions to this kind of cybercrime.

a) Web Spoofing

In the virtual world, the 'term *spoofing* applies to actions that make an electronic transaction appear to originate from somewhere that it does not'.[342] This sort of chicanery is increasingly common in cyberspace, because there are a number of serious security flaws inherent in the TCP/IP protocol suite.[343]

Web spoofing is a technique used for convincing an Internet user that a particular website is legitimate, where in reality it is not.[344] It is usually accomplished through both technical and social engineering tricks which attract gullible users to visit and engage with a phoney website.[345] The tactic starts with buying a domain name[346] that is

[340] Hoar, above n 325, 1426. See also, Federal Trade Commission, *Take Charge: Fighting Back Against Identity Theft* <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#How> at 23 February 2006. See also, Towle, above n 329, 241.

[341] Steven M Bellovin, *Security Problems in the TCP/IP Protocol Suite* (1989) <http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html> at 4 January 2006.

[342] Harrington, above n 206, 134.

[343] Bellovin, above n 341.

[344] See, eg, Bill Hancock, 'Site Spoofing Becomes More Popular' (2000) 19 (7) *Computer & Security* 581. See also, Kris A Jamsa, and Lars Klander, *Hacker Proof: the Ultimate Guide to Network Security* (2nd ed, 2002) 292.

[345] Ibid.

similar but slightly different to that of a popular company, such as by putting in a single extra letter or a lower case character instead of a capital letter.[347] Consequently, Internet users browsing the web may unwittingly visit a fraudulent website and enter personal data.[348] Because technical tricks alone are not sufficient to lure Internet users, spoofers might employ social engineering tactics, such as sending Phishing e-mails[349] to many users at one time. Phishing e-mails (figure 4.1) 'lead consumers to a counterfeit website (figure 4.2) designed to trick recipients into divulging financial data, such as credit card numbers, account usernames, passwords and social security numbers'.[350] Figures 4.1 and 4.2 respectively demonstrate the phishing and web spoofing technical and social engineering techniques.[351]

[346] The domain name can be purchased either from local or international providers and is designed in a manner copying the original content of the spoofed website. See, eg, Chula G King and W Timothy O'Keefe, 'Online Identity Theft and Business' (2004) 74 (4) *The CPA Journal* 50.

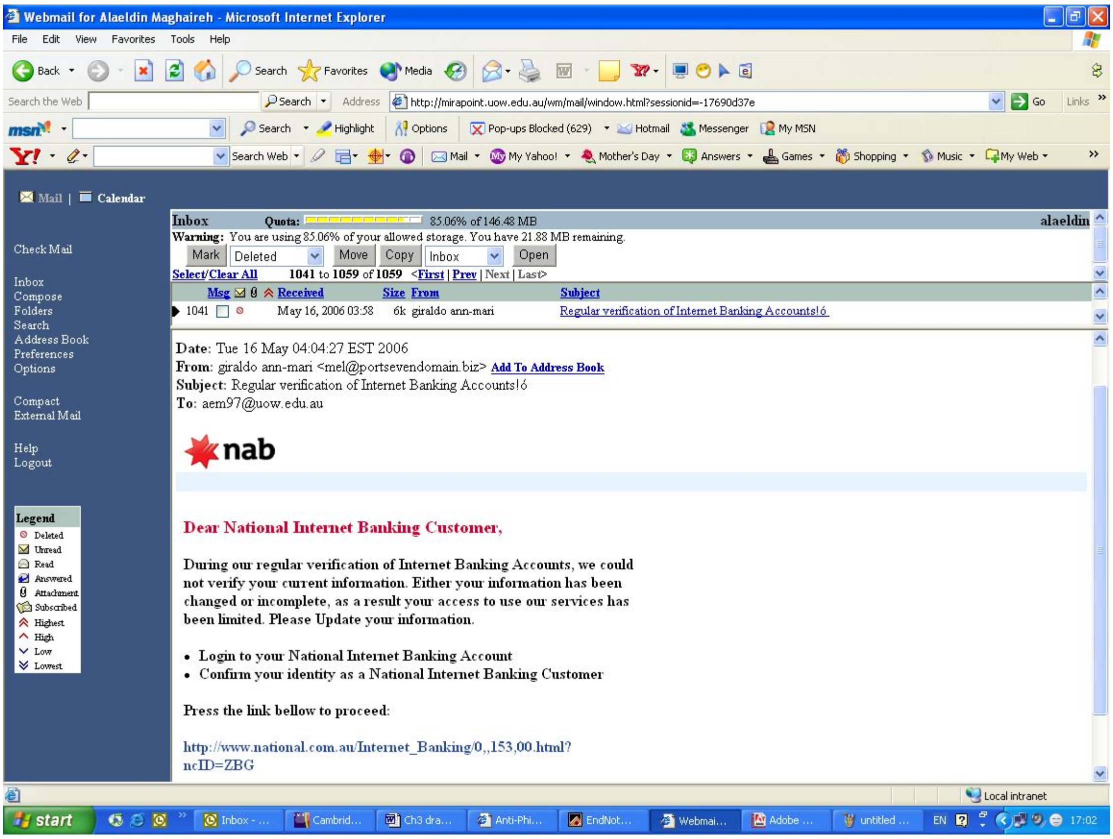
[347] Ibid.

[348] Ibid.

[349] Phishing indeed, has become more prevalent and sophisticated. It is 'a social engineering attack in that it does not exploit technical flaws, but fools people into revealing information'. Phishing usually catches its victims through social engineering tactics, such as sending an e-mail (spoofed e-mail) with a spoofed website attachment. The spoofed e-mail looks like a genuine one sent from a legitimate source, and states that a recipient's account may have been compromised or will be shut down if the recipient does not confirm or update access information and personal details by clicking on a spoofed website The immediate victim is an individual, such as the bank's patrons who are online banking customers, though the bank may experience not only monetary losses but also reputation damage. Thus, banks and other financial institutions are the eventual victims. See, eg, Harry A Valetk, 'Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies' (2004) 2 *Stanford Technology Law Review.* See also, Jennifer Lynch, 'Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks' (2005) 20 *Berkeley Technology Law Journal* 259, 267.

[350] *What is Phishing and Pharming?* Anti-Phishing Working Group <http://www.antiphishing.org/index.html> at 17 May 2006.

[351] Below is a typical phishing e-mail disguised as coming from the National Australia Bank (NAB).
Dear National Australia Bank customer,
'We at National Australia Bank would like to remind you that your National Australia Bank Account has not been updated to the latest Online Access Agreement for National Australia Bank Online Services.
In order for us, at National Australia Bank to guarantee your online security, you need to update your account information. We urge you to partner with us to prevent consumer fraud, by going through the 2 steps National Australia Bank Account Confirmation process. This operation involves logging in and confirming your identity over a secure connection at:
http://www.national.com.au/?ncID=ZBG
After completing this process, you will be informed that your account has been updated and you will be redirected to the actual Online Access Agreement, for you to review.
Thank you for choosing National Australia Bank as your Financial Institution.
© National Australia Bank Limited. Use of the information contained on this page is governed by Australian law and is subject to the disclaimers, which can be read on the disclaimer page. View the National Privacy Policy.'


Webmail for Alaeldin Maghaireh - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Search the Web Search Address http://mirapoint.uow.edu.au/wm/mail/window.html?sessionid=-17690d37e Go Links
Search Highlight Options Pop-ups Blocked (629) Hotmail Messenger My MSN
Search Web Mail My Yahoo! Mother's Day Answers Games Shopping Music My Web
Mail | Calendar
Check Mail
Inbox
Compose
Folders
Search
Address Book
Preferences
Options
Compact
External Mail
Help
Logout
Legend
Deleted
Unread
Read
Answered
Attachment
Subscribed
Highest
High
Low
Lowest
Mark Deleted Move Copy Inbox Open
Select/Clear All
Add To Address Book
Local intranet
start Inbox - ... Cambrid... Ch3 dra... Anti-Phi... EndNot... Webmai... Adobe ... untitled ... EN 17:02

Inbox **Quota:** 85.06% of 146.48 MB **alaeldin**

Warning: You are using 85.06% of your allowed storage. You have 21.88 MB remaining.

1041 to 1059 of 1059 <First | Prev | Next | Last>

Msg	Received	Size	From	Subject
1041	May 16, 2006 03:58	6k	giraldo ann-mari	Regular verification of Internet Banking Accounts!ó

Date: Tue 16 May 04:04:27 EST 2006
From: giraldo ann-mari <mel@portsevendomain.biz>
Subject: Regular verification of Internet Banking Accounts!ó
To: aem97@uow.edu.au

nab

Dear National Internet Banking Customer,

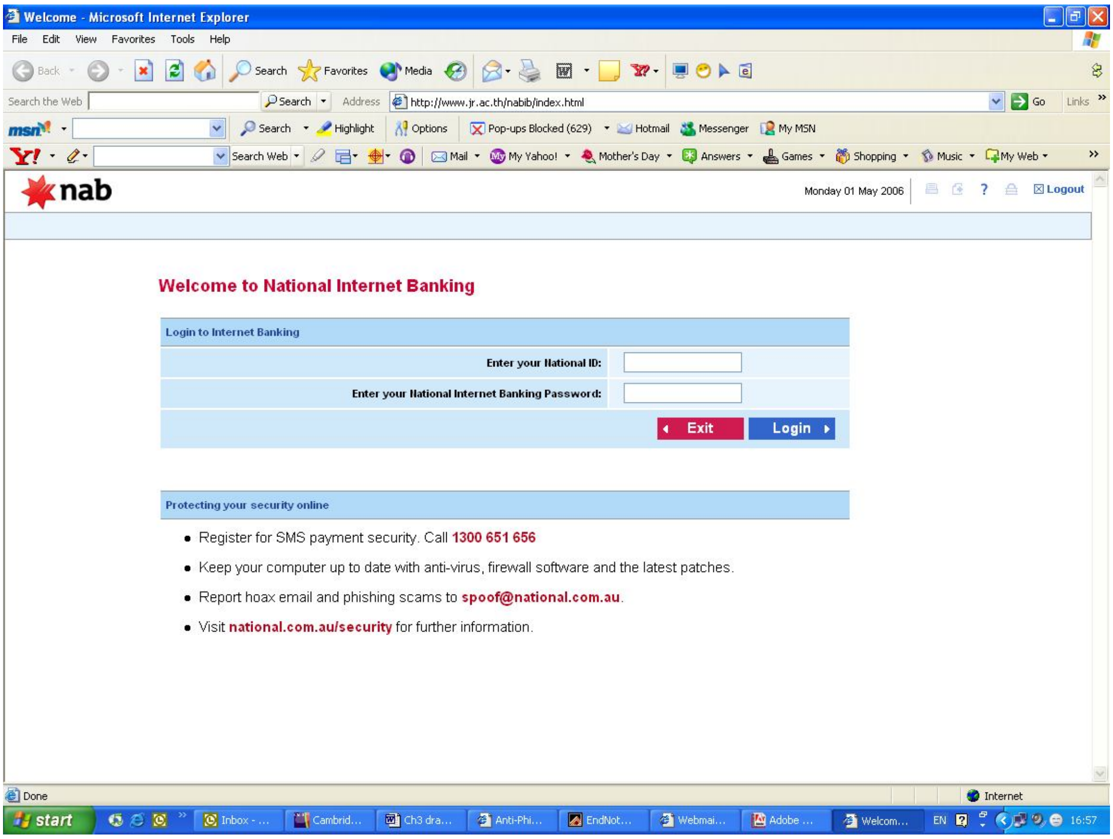
During our regular verification of Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please Update your information.

- **Login to your National Internet Banking Account**
- **Confirm your identity as a National Internet Banking Customer**

Press the link bellow to proceed:

http://www.national.com.au/Internet_Banking/0,,153,00.html?ncID=ZBG

Figure 4.1 An example of a Phishing E-mail


Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Search the Web Search Address
Go Links
Search Highlight Options Pop-ups Blocked (629) Hotmail Messenger My MSN
Search Web Mail My Yahoo! Mother's Day Answers Games Shopping Music My Web
Done
Internet
start Inbox - ... Cambrid... Ch3 dra... Anti-Phi... EndNot... Webmai... Adobe ... Welcom... EN 16:57

Address: http://www.jr.ac.th/nabib/index.html

nab

Monday 01 May 2006

Logout

Welcome to National Internet Banking

Login to Internet Banking

Enter your National ID:

Enter your National Internet Banking Password:

Exit Login

Protecting your security online

- Register for SMS payment security. Call 1300 651 656
- Keep your computer up to date with anti-virus, firewall software and the latest patches.
- Report hoax email and phishing scams to spoof@national.com.au.
- Visit national.com.au/security for further information.

Figure 4.2 An example of a Spoofed Website

b) DNS Spoofing

Using a different technique known as DNS Spoofing, the attacker positions himself between the victim machine and the rest of the WWW.[352] This is accomplished by the use of URL-rewriting.[353] The URL-rewriting technique mechanism has been delineated in five steps as follows:[354]

[352] See, eg, Sean Dugan, 'Enterprise Computing : Cybersabotage' (1995) *InfoWorld* . See also, Mattias Eriksson, *An Example of a Man-in-the-Middle Attack Against Server Authenticated SSL-Sessions* UMEA University <http://www.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf> at 6 January 2006. See also, Jamsa and Klander, above n 344, 293.

[353] The acronym URL stands for 'Universal Resource Locator'. It is a unique address assigned to every location on the Web, such as 'http://' as in http://www.uow.edu.au. See, Veljko Milutinovic, *Infrastructure for Electronic Business on the Internet: Lessons Learned* (2001) 25.

[354] Edward W Felten et al, *Web Spoofing: An Internet Con Game* (paper presented at the 20th National Information Systems Security Conference, Baltimore, Maryland October 1997) 4.

1) The victim's browser requests the page from the attacker's server.[355] For example, the attacker server is http://www:attacker.org and the victim wants to visit www: commbank.com.au. The URL-rewriting application will take him to the http://www: attacker.org/http://commbank.com.au.
2) The attacker's server requests the page from the real server;[356]
3) The real server provides the page to the attacker's server;[357]
4) The attacker's server rewrites the page;[358]
5) The attacker's server provides the rewritten version to the victim.[359]

From a technological perspective, a slight difference between Web and DNS spoofing can be noticed. The former does not require unauthorised access to be accomplished, while DNS spoofing involves unauthorised access to the victim's system. Hence, DNS spoofing may be punishable under the provisions of unauthorised access.[360]

c) TCP Spoofing

TCP sequence number prediction attacks, known as 'the man in the middle attack'[361] or 'TCP Spoofing', are commonly implemented by taking advantage of the inherently weak trust relationship present in the TWHS connection process.[362] The attacker interferes and hides between the client and the server in the second part of the TWHS[363] process by predicting or guessing the server's correct sequence number and then spoofs that TCP segment,[364] which will be accepted by the client who assumes that the segment originated from a legitimate server source.[365] Once the spoofed TCP segment is accepted, the attacker can surreptitiously read, insert and modify messages cycling between the two parties (the client and the server). In such a position the identity thief

[355] M Warren and W Hutchinson, 'Deception: A Tool and Curse for Security Management' in Michel Dupuy, and Pierre Paradinas (ed), *Trusted Information: The New Decade Challenge* (2001) 327, 333.
[356] Ibid.
[357] Ibid.
[358] Ibid.
[359] Ibid.
[360] See Section 3.2.2 for more information on cybertrespass.
[361] See, eg, Eriksson, above n 352, 7. See also, Harrington, above n 206, 134.
[362] See, eg, B Dave, *Simple TCP Spoofing Attack* (1997) Tech Forums <http://www.tech-forums.net/computer/topic/1807.html> at 6 January 2006.
[363] See Section 3.2.1 for more information on TWHS connection process.
[364] A TCP segment is a portion of data, mainly 536 bytes, transferred between devices. See, Douglas Comer, *Q & A on TCP Segment Size* (2003) Purdue University <http://www.netbook.cs.purdue.edu/othrpags/qanda110.htm> at 16 May 2006.
[365] See, eg, Harris and Hunt, above n 190, 888. See also, Terrance a Roebuck, *Network Security: DoS vs DDoS Attacks* (2005) Computer Crime Research Center <http://www.crime-research.org/articles/network-security-dos-ddos-attacks/4> at 6 January 2006.

can not only steal passwords, but also compromise confidentiality, integrity or availability of information.[366]

d) IP Spoofing

IP spoofing involves the creation of IP packets with a forged (spoofed) source IP address.[367] IP spoofing is primarily used to anonymously gain initial access to the Internet.[368] Once the IP is spoofed, the attacker can initiate several types of crimes associated with IP including unauthorised access and impersonating a legitimate e-mail to make it look like it originated and was sent from a legitimate source.[369]

4.3.2 Survey Legal Responses

a) Jordan

The *Criminal Law* 1960 addresses two pictures of identity theft, namely, use a false identification and impersonating law enforcement officers.[370]

First, Articles 212 and 213 of the *Criminal Law* 1960 criminalise any person using a false identification during proceedings before a magistrate, prosecutors or other law enforcement officer. This picture of identity theft, therefore, aims at protecting justice and maintaining the integrity of the investigation process. Second, Article 266 criminalises the act of impersonating an officer or employee of the government.[371]

None of these pictures of identity theft address cyber identity theft, because they focus only on physical identity theft and protect a particular type of person's identity, such public employees.

[366] Ian Green, *DNS Spoofing by the Man in the Middle* (2005) SysAdmin, Audit, Network, Security Institute <http://www.sans.org/rr/whitepapers/dns/1567.php> at 9 January 2006.

[367] For example: if the real IP is 138.13.233.182 and has been spoofed to 199.199.199.199 then the IP address would show up as 199.199.199.199 in the remote machine's logs, keeping the real IP address unknown. See, Grandmaster Plague, *Myths About TCP Spoofing* (2002) <http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=6394&mode=thread&order=0&thold=0> at 3 January 2006. See also, Harrington, above n 206, 134. See also, *Internet Protocol Spoofing* Wikipedia <http://en.wikipedia.org/wiki/IP_spoofing> at 7 January 2006. See also, *IP Spoofing Attacks and Hijacked Terminal Connections* (1995) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1995-01.html> at 8 January 2006.

[368] Dan Thomsen, 'IP spoofing and session hijacking' (1995) (3) *Network Security* 6, 7. See also, *IP Spoofing Attacks and Hijacked Terminal Connections* (1995) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1995-01.html> at 8 January 2006.

[369] Harrington, above n 206, 142.

[370] *Criminal Law 1960* (212), (213).

[371] *Criminal Law 1960* (266).

b) Australia

In Australia, the response to cyber identity theft is relatively mature, with many provisions addressing different aspects of identity theft offences. Legislation at both federal and state levels is adequate for combating the various forms of cyber identity theft.

At the federal level, the *Cybercrime Act* 2001 and the *Criminal Code Amendment (Theft, Fraud, Bribery & Related Offences) Act* 2000 omit any direct reference to cyber identity theft, but provide enough protection against identity thieves. The *Cybercrime Act* 2001 concerns cyber identity theft only indirectly.[372] Section 477.1 (d) criminalises unauthorised access to computer systems with intent to commit or facilitate an offence, such as identity theft. Accordingly, DNS, TCP and IP spoofing forms can be prosecuted under this division, because unauthorised access to the computer system is essential for the spoofers to steal identity and financial data. However, web spoofing cannot be prosecuted under the same provision, because it does not require access to the victim's system. Therefore, sub-sections 478.3 and 478.4 establish the legal basis for prosecuting those who possess, control, produce, supply, or obtain data with intent to commit a computer offence. As a result, obtaining data through web spoofing to commit cyber identity theft is also criminalised under the same Act.

In the same manner as the *Cybercrime Act* 2001, the *Criminal Code Amendment Act* 2000 criminalises obtaining property and financial advantage by deception (Chapter 7 Division 134.1 and 2). Deception is defined as 'an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes… (b) conduct by a person that causes a computer…to make a response that the person is not authorised to cause it to do'.[373]

At the Australian state levels, identity theft and fraud offences are prosecuted under common law and statute law. However, South Australia is the only state that has enacted specific legislation regarding identity theft. This law makes it an offence to intentionally use another persons' identification to commit, or help to commit, a serious

[372] *Cybercrime Act 2001* (Cth) div 477.1
[373] *Criminal Code Act 1995* (Cth), amended by *Criminal Code Amendment* (*Theft, Fraud, Bribery & Related Offence Act) 2000* (Cth) div 133 (1).

crime.[374] Furthermore, the new legislation aims at assisting identity theft victims to restore their reputation after the damage inflicted upon it by the offenders.[375] Section 54 for example, gives the victims of identity theft the right to apply for a certificate. The certificate is to give details of the offence and the name of the victim and any other matters considered by the court to be relevant to restore his reputation.[376]

c) USA

In the USA, cyber identity theft and fraud schemes can be prosecuted under several laws. The *Identity Theft and Assumption Deterrence Act* 1998 (ITADA) has made identity theft a federal crime. The statute makes it an offence for a person 'knowingly, transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law'.[377] A 'means of identification' is broadly defined to include a wide range of personal identifying information.[378] It 'includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any name, Social Security Number (SSN), date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, or employer or taxpayer identification number'.[379]

The ITADA was criticised for failing to provide preventive measures.[380] It is a reactive law rather than a proactive one. It addresses identity theft only after a crime has occurred.[381] The act was amended in 2004 to broaden its scope and expanded the range of conduct that may be considered identity theft to include any misuse of identification that may cause harm to an individual or entity.[382]

[374] *Criminal Law Consolidation Act 1935* (SA), amended by *Criminal Law Consolidation Act 2004* (SA).
[375] *Criminal Law Consolidation Act 1935* (SA), amended by *Criminal Law Consolidation Act 2004* (SA
[376] *Criminal Law Sentencing Act 1988* (SA) amended by *Criminal Law Sentencing Amendment Act 2004* (SA) Pt 5A s 54.
[377] *Identity Theft and Assumption Deterrence Act*, 18 USCS § 1028 (a) (1998).
[378] *Identity Theft and Assumption Deterrence Act*, 18 USCS § 1028 (a) (1998).
[379] Valetk, above n 335.
[380] See, eg Katherine Slosarik, 'Identity Theft: An Overview of the Problem' (2002) 14 (4) *The Justice Professional* 329, 331.
[381] Ibid.
[382] *Identity Theft Penalty Enhancement Act*, 18 USCS §§ 1028A (2004).

The legislator adopted preventive legal measures against identity theft in the *Fair and Accurate Credit Transactions Act* 2003 (FACTA). It provides that customers holding credit cards, such as Visa and MasterCard, have the right to request a free consumer report every 12 months from major credit reporting agencies.[383] This mechanism encourages customers to conduct self-monitoring. Furthermore, customers can place an alert on their credit files that puts potential creditors on notice that they must proceed with caution when granting credit.[384]

d) Comparative Legal Analysis

Cyber identity theft presents a unique environment of theft that requires an effective and efficient law. Pertaining provisions of the *Criminal Law* 1960 only address particular pictures of the identity theft, such as use of a false identification card during a criminal investigation or judicial proceeding, or impersonating a public employee. Thus, no form cyber identity theft can be prosecuted under the *Criminal Law* 1960 unless a physical appearance or I.D. card has been used to deceive specific individuals. By contrast, the *Cybercrime Act* 2001 criminalises all the forms of cyber identity theft. On the other hand, because cyber identity theft causes substantial harm to the victim's reputation or credit record, South Australian identity theft provisions provide the victims of identity theft with a certificate for cleaning up their credit records and maintaining and restoring their reputation.

However, neither the *Criminal Law* 1960 nor the *Cybercrime Act* 2001 is equivalent to the ITADA and FACTA because, while the latter provides not only reactive, but also proactive responses, by granting the customers the right to obtain annually a free copy of their credit report, the ITADA directly and specifically criminalises identity theft. Thus, there are no obstacles to prevent the Jordanian legislator from enacting a cyber identity theft law that provides sufficient protection against spoofers and cyber identity thieves as well as restoring identity theft damage.

[383] *The Fair and Accurate Credit Transaction Act*, 18 USCS §§ 1028 (3) (d) (2) (a) (2003).

[384] See, eg, Federal Trade Commission, *Provisions of New Fair and Accurate Credit Transactions Act Will Help Reduce Identity Theft and Help Victims Recover* (2004) Federal Trade Commission <http://www.ftc.gov/opa/2004/06/factaidt.shtm> at 23 April 2007. See also, Lynch, above n 349, 279.

4.4 Cyberstalking

There are various definitions of cyberstalking. Bocij simply defines cyberstalking as 'the use of information and communications technology (in particular the Internet) in order to harass individuals'.[385] This definition clearly emphasises the conventional character of a stalking crime, i.e. as harassment, and that the internet is not the only means of harassing the victims. Computers, fax machines, cell phones and other devices, for example, are used to commit stalking crimes, but the Internet now provides the most convenient platform for stalkers.

Cyberstalking takes many forms and the victims are people of all ages and genders. However, whilst stalking is a long-established behaviour,[386] mainly committed by a male against a female, anecdotal statistics indicate that cyberstalking is a significant and growing problem targeting a specific person and motivated by hate, revenge, racism, and so on.[387] The report of an American organisation, called *Working to Halt Online Abuse*, for example, shows that, between 1 January and 31 December 2005, it handled 443 cases of cyberstalking.[388] Sixty seven per cent of the cases involved female victims; [389] 43.5% of the cases involved harassment by a male; 21.5% of the harassers were female.[390] This seems inconsistent with the stereotype that stalking is solely a crime perpetuated by men against women involving violence that appears serious and would result in death or grievous bodily harm.[391] Although not all types of cyberstalking involve sexual harassment or even malicious behaviour, such as a simple 'love obsession',[392] cyberstalking gradually scales up from a remote threat to actual physical

[385] Paul Bocij, Mark Griffith and Leroy Mcfarlane, 'Cyberstalking: A New Challenge for Criminal Law' (2002) 122 *The Criminal Lawyer* 3.

[386] Yogesh Barua and Denzle P Dayal, *Cyber Crimes: Notorious Aspect of the Humans and the Net Spam Attacks, Cyber Stalking and Abuse* (2001) 179.

[387] See, eg, Janice Joseph,' Cyberstalking: An International Perspective' in Yvonne Jewkes (ed), *Dot.cons Crime, Deviance and Identity on the Interent* (2003) 105, 106. See also, Bocij, above n 385. See also, Paul Bocij, *Victims of Cyberstalking: An Exploratory Study of Harassment Perpetrated Via the Internet* (2003) <http://www.firstmonday.dk/issues/issue8_10/bocij/index.html> at 5 March 2006.

[388] See, Working to Halt Online Abuse, *Online Harassment/ Cyberstalking Statistics* (2006) <http://www.haltabuse.org/resources/stats/index.shtml> at 6 March 2006.

[389] Ibid.

[390] See, Working to Halt Online Abuse, *Online Harassment Statistics Gender of Victims* (2006) <http://www.haltabuse.org/resources/stats/genderv.shtml> at 6 March 2006.

[391] See, eg, Barua and Dayal, above n 386, 159.

[392] According to the psychological and behavioural profile of stalker, there are two types of stalker: Love obsession stalkers represent 20-25% of all stalking cases and simple obsession stalkers represents 70-80% of all stalking cases. See, *Stalking* Nova Network of Victim Assistance <

harm or injury.[393] For example, in the four cases of cyberstalking studied by Bocij, the victim in each was first digitally stalked and soon afterwards physically harmed by their cyber-stalker.[394]

4.4.1 Survey Legal Responses

a) Jordan

In Jordan, neither actual physical nor cyberstalking behaviour has been observed. This is primarily because tribal and religious traditions govern the response to sexual behaviour within the Jordanian community. Moreover, the paucity of personal information transmitted via the Internet, and the relatively rare use of computers to save personal information, particularly by females, prevents cyberstalking incidents. However, cyberstalking and online harassment are escalating rapidly because of increased internet use. Actual physical stalking is not a named crime in the *Criminal Law* 1960 but related types of crimes are. For example, Articles 305 and 320 criminalise physical sexual harassment against a female or a juvenile male, and sexual harassment conducted in a public place, respectively. Article 38 of the *Electronic Transactions Law* 2001 criminalises conventional crimes, such as sexual harassment committed by using electronic means. The Internet can be considered as a public place because many users can simultaneously share different activates. Thus, cyberstalking involving sexual harassment against a female or a juvenile male can be criminalised under article 320 of the *Criminal Law* 1960 combined with article 38 of *Electronic Transactions Law* 2001. However, this would contradict the core principle of criminal law, which states that criminal laws are to be construed narrowly.

b) Australia

The laws concerning cyberstalking and harassment in Australia vary between federal and state levels, as well as among the states. At the federal level, there is no overreaching statute that is specifically concerned with cyberstalking. The Federal *Criminal Code* 1995, updated through the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill* 2004 provides that individuals

http://www.novabucks.org/info/stalking.htm > at April 2 2006. See, eg, Stephen Andert and Donald K. Burleson, *Web Stalkers: Protect Yourself from Internet Criminals & Psychopaths* (2005) 93.

[393] See, eg, Joseph, above n 389, 109. See also, Diana Lamplugh and Paul Infield, 'Harmonising Anti-Stalking Laws' (2003) 34 *George Washington International Law Review* 853, 853-859.

[394] See, eg, Bocij, above n 385.

using telecommunications services in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive, would be liable under Section 474.17 of this Act.

At the state level, the first anti-stalking law was enacted by the State of Queensland in 1999 (*Criminal Code (Stalking) Amendment Act*) and a few other states have enacted cyberstalking offences. Victoria, Queensland, and South Australia are the only states to include the use of the Internet in their legislation. Section 19AA of the South Australian *Criminal law Consolidated Act 1935* for example, specifies an offence when '… any person communicates with the other person…by way of mail, telephone (including associated technology), facsimile transmission or the Internet or some other form of electronic communication in a manner that could reasonably be expected to arouse apprehension or fear in the other person…'[395]

c) USA

In the USA, specific legal tools have been designed to combat cyberstalking. At the federal level, it is a crime, punishable by up to 20 years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure and harass the person of another.[396]

At the state level, the Illinois state *Criminal Code*, for instance, makes harassment of another person through the use of electronic communication a felony, punishable by up to ten years in prison and a fine of up to $100.000.[397] However, while, the Illinois anti-cyberstalking law applies to communications of threat of immediate or future bodily harm, and also to comments, requests, and suggestions or proposals which are obscene, the federal code applies only to communication of actual threats. Therefore, the federal law is inadequate to enable law enforcement agencies to take pre-emptive measures to address the looming danger of cyberstalking.

In 2006, President Gorge W Bush signed the *'Violence against Women and Department of Justice Reauthorization'*. This law amended section 223h of the *Communications Act 1934*. Section 113 provides that whoever '…utilizes any device or software that can be

[395] *Criminal Law Consolidation Act 1935* (SA), amended by *Criminal Law Consolidation Act* 2004 (SA)
[396] *Criminal and Crime Procedure Act,* §§18.U.S.C 875 (c) (1996).
[397] *The Criminal Code of 1961, amended by Cyberstalking Act* §§ 720 ILCS 5/12-7.5 (2001). For more information about states level, see Joseph, above n 387, 111.

used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet…without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person ... who receives the communications ... shall be fined under title 18 or imprisoned not more than two years, or both'.[398] The new law makes it a federal crime to annoy, abuse, threaten, or harass another person over the Internet. This legislation, however, is overly broad because it does not define the term 'annoy' and refers instead to the subjective effect of the offender conduct on the victim.[399] For example, for merely sending blank messages to someone's e-mail box, the sender can be prosecuted under the *'Violence Against Women and Department of Justice Reauthorization'*.[400] This is because the law does not look at the effect of the annoying abuse, threat, and harassment on the victims.

d) Comparative Legal Analysis

The Jordanian law concerned with sexual harassment and related issues addresses only a subset of potential cyberstalking activities. This is because the law focuses on the physical aspects of sexual harassment and avoids addressing the offence of stalking. Thus, cyberstalking which escalates into physical harm can be prosecuted under the current Jordanian laws. For example, in cyber-love obsession stalking, there will be no punishment unless in conjunction with physical violence. Inflicting physical harm is necessary for the criminal prosecution of a cyber stalker. Australian Federal and State laws, South Australia in particular, have introduced models that effectively criminalise cyberstalking by addressing the use of the Internet in a way that would be expected to cause fear or apprehension on the victim. The new US legislation provides protection against cyberstalking that is too broad, as the term 'annoy' is subjective, because there are various opinions about what constitutes annoyance.

4.5 Conclusion

Information and communications technology has offered criminals unprecedented opportunities to commit traditional crimes via computer systems. The commission of

[398] *Communications Act 1934* amended by *Violence against Women and Department of Justice Reauthorization Act* §§ 18.U.S.C 223 s (s) (2005).

[399] See, David L Hudson Jr, '*New Cyberstalking Law Challenged Over "Annoy" Language'* (2006) First Amendment Center < http://www.firstamendmentcenter.org/news.aspx?id=16535> at 7 May 2006.

[400] Ibid.

the old crimes supported by new tools leaves cyber fingerprints that provide law enforcement with a wide range of digital evidence that can be used to establish conclusive evidence of wrongdoing. Digital images, video clips, information content, internet forums and so on can provide digital evidence sought obtained from cybercrime scenes for the purpose of establishing criminal liability.

Forgery, pornography, identity theft and stalking are traditional crimes but need to be re-addressed in the context of cyberspace. These crimes are increasingly occurring in cyberspace, particularly cyber pornography and identity theft crimes. Their impact on Internet users, children, and internet development is profound.

The existing legislation does not recognise the data stored in a PC as a property having legal efficacy, nor is the term ‘document’ which is mentioned in the law meant include a digital object. As a result, the *Criminal Law* 1960 is incompetent to address cyber forgery unless digital data is given a legal efficacy or the use of computers to forge digital records or documents directly criminalised.

In the context of cyberspace, pornography and identity theft take different forms and different routes from those of the classical patterns. Cyber pornography, for instance takes different forms, such as adult pornography, child pornography, and virtual child pornography. While the first form is not a crime in Australia or in the USA, the other forms are classified as serious crimes in both countries. Australia’s pornography legislation, at both federal and state levels, parallels American legal safeguards against child pornography. In both jurisdictions, offenders are subjected to harsh punishment. However, on the contrary, most of the Australian States adopted fanatical laws that made a crime the mere possession of child pornography stored on one’s personal computer. By contrast, the current Jordanian laws prosecute any of the pornography forms without differentiating between them. However, to avoid any problems due to the lack of specific terms, such as computerised images, amendment is necessary to keep the law current with evolving technology and crimes tools.

In a similar manner, cyberspace has changed tremendously the pattern of identity theft offences. New methods of identity theft involving highly sophisticated techniques were effectively addressed and appropriate measures were taken to prevent cyber identity theft. The South Australian *Criminal Law consolidation Act 1935*, amended by

Criminal Consolidation Act 2004 for example, was crafted to provide appropriate protection from identity theft, while Jordanian laws, by contrast, are incompetent to criminalise cyber identity theft. This is because the *Criminal Law* 1960 criminalises specific conceptions of classical identity theft. Those conceptions are completely different from the ones used by spoofers and cyber-offenders.

Cyberstalking differs from the variety of forms of physical sexual harassment. The *Criminal Law* 1960 failed to address cyberstalking, where the latter does not escalate into physical harm, and addresses only physical harm. Nevertheless, there is no a barrier to preventing Jordanian legislators from taking deterrent legal measures to protect cyber users by enacting cybercrime legislation including cyberstalking.

5 CYBERCRIME INVESTIGATION APPROACHES AND CHALLENGES

Introduction

Streamlining and strengthening procedures in cybercrime investigation and eliminating or reducing impediments to law enforcement efforts are important prerequisites to successful investigation. An effective response to cybercrime requires a two-pronged solution: criminalisation itself and the approach to investigation. The criminalisation response, which was addressed in the previous chapter, shows that traditional substantive laws, which were formulated to deal with real-world crimes, were insufficient to address all forms of cybercrimes. It was suggested that a comprehensive substantive law is needed. Promulgating a comprehensive law, however, is only half of the solution. The other half is the existence of an effective and efficient investigative approach to cybercrime. This approach requires, first, identifying the optimum investigation models and, second, responding to the legal challenges that hinder law enforcement's ability to investigate cybercrimes.

The objective of this chapter is to streamline the investigation process and harmonise policies and procedures designed for investigating cybercrimes. Also, it examines the factors necessary for successful investigation and identifying and eliminating legal challenges. It hypothesises that the approach model to cybercrime investigation adopted by the Jordanian Computer Crime Unit (JCCU) is deficient in some components. Therefore, formulated protocols and models of investigation, which were formulated mainly by the Australian High Tech Crime Centre (AHTCC) and the US Department of Justice (DOJ) and by forensic experts, will be analysed and compared with the Jordanian investigative approach. These approaches were chosen because they are known for their robustness and their ability to handle different sorts of cybercrimes. Furthermore, they include important and intricate procedures.

The Jordanian government recognises the importance of Information Technology (IT) as a key element to improve administration as well as security. Policies and procedures that specifically aim at strengthening economic performance and internal security were adopted, the Electronic Government Initiative, for example. The Jordanian Public

Security Directorate (PSD), a public organisation in charge of internal security, and the General Prosecutorial Department (GPD) both play a vital role in thoroughly evaluating, applying and monitoring criminal policies, directives and criminal procedures. The PSD is assigned to investigate criminal cases, gather information, including searching for and seizing evidence, and then to hand over the case to the GPD. The GPD, which is a part of judicial system, is one of the main divisions of judicial authority conducting further investigation, analysing and labelling the crimes, and finally standing before the court to seek conviction for offences.

Since the establishment of the PSD in 1958, it has experienced remarkable advances, intended to overcome investigative challenges and keep abreast of IT developments.[401] This has translated into growth of quality and quantity of police departments, and in the appointment of specialised criminal investigation officers and detectives dealing with particular crimes.[402] In recent years, for example, the PSD has established numbers of new departments, such as the Environmental Police Unit (EPU), as well as the JCCU.[403] The latter, which is a part of the forensic laboratories division, investigates cybercrimes and provides laboratory services in the inspection and analysis of digital evidence. For this purpose, the JCCU has formulated a sketchy guideline for the procedure to be followed in dealing with cybercrimes scene and digital evidence.[404] Nowadays, however, law enforcement agencies during their day-to-day duties are very likely to encounter crimes where computers are the target, the storage medium, or the tools of crimes.[405] The novelty of cybercrime challenges traditional models of law enforcement investigation. Therefore, the absence of diligent investigation guidelines in Jordan,

[401] See generally, مديرية الامن العام الاردني *Public Security Directorate: Overview and Achievements* (Alaeldin Mansour Maghaireh trans) [trans of: الامن العام في سطور تاريخ وانجاز]. <http://www.psd.gov.jo/arabic/index.php?option=com_content&task=view&id=571&Itemid=384> at 7 December 2006.

[402] Ibid.

[403] See, مديرية الامن العام الاردني *Environmental Police Department* (Alaeldin Mansour Maghaireh trans) [trans of:إدارة الشرطة البيئية]. http://www.psd.gov.jo/arabic/index.php?option=com_content&task=view&id=62&Itemid=139> 7 December 2006.

[404] The guideline was obtained by the author from the JCCU.

[405] Cybercrime is booming, and expected to keep growing substantially in the years to come. An upublished annual report issued by the Jordanian Public Security Department (JPSD) in 2002 shows a dramatic increase in cybercrimes reported and investigated by law enforcement over the period 1999-2001. For example, during the first year of its existence, in 1999, the Jordanian Computer Crime Unit (JCCU) investigated 7 crimes. Comparatively, in 2001 the number has jumped four times. See, كمال, احمد*The Practical Principles of Computer Crime Investigation* (Alaeldin Maghaireh trans, 2002 Unpublished [trans of: الاصول الفنية للتحقيق في جرائم الحاسوب].

coupled with legal impediments that inhibit the investigation process, poses significant problems for law enforcement in investigation of cybercrimes.

This chapter is divided into two parts. The first is concerned with the investigation approaches and the second identifies investigation challenges. The first part is further divided into two sections. The first will address the importance of cybercrime investigation, and investigation priorities. It examines the need for a mechanism that quantifies and assesses which cybercrimes are to be considered significant and, thus, worth investigating. The second section will address the investigation approaches of Jordan, Australia, and the USA and comparatively analyse the component structure of each model with the Jordanian guideline, noting any strengths or weakness that would affect an investigation. Investigation approaches formulated by scholars Seamus O Ciardhuain and Eoghan Casey will also be examined and compared with the Jordanian approach. Part two examines the legal and technical problems that arise in cybercrime investigation, focusing on privacy and encryption. Then the legal response to such impediments will be surveyed and assessed in order to arrive at an optimal response.

5.1 Cybercrime Investigation Approaches

Fostering and strengthening cybercrime investigation is a two-pronged process. The first is to implement administrative procedures within the investigation unit to ensure effective control over cybercrime cases. The second is to formulate forensic models or guidelines to perform successful investigation.

5.1.1 Priority Investigations

An investigative priority for certain categories of cybercrimes is important because the capability of Cybercrime Units to perform a variety of cybercrime investigations is limited compared to the investigation of traditional crimes.[406] This is for two reasons. The first is because the volume and diversity of cybercrimes have increased significantly in recent years. For example, statistics published by the CSI/FBI Computer

[406] Smith, Grabosky, and Urbas, above 25, 32.

Crime Survey in 2005,[407] and the Australian Computer Crime & Security Survey in 2006,[408] foresee a continuing increase in the number of complaints and crimes. The second reason is because trivial traditional crimes, such as misdemeanours and traffic violations, need much less time and fewer resources to be investigated. Meanwhile, trivial cybercrimes require more investigative resources, such as first responders, technical teams, forensic experts and equipment commensurate with serious cybercrimes.

There are several factors used to determine whether a crime is a trivial or a high profile crime. Traditionally, law enforcement agencies and the mass media held the key to determining which crime is a high profile case. Twenty years ago, heinous and violent crimes always had priority over cybercrimes.[409] Meanwhile, the latter was not a priority for law enforcement or to the mass media worldwide for a number of reasons, among them that internal police culture places a lower value on catching non-violent offenders,[410] and that investigative priority is primarily set according to the scale and significance of the complaints and their physical damage. For example, Ken Hunt, a former Australian Federal Police (AFP) detective superintendent, said: ‘Most of my colleagues, most of the other people at my level, thought computer crime was a wank. And that I should be out there investigating “real crime”.’[411] This situation, however,

[407] Lawrence a Gordon et al, 'CSI/FBI Computer Crime and Security Survey' (2005). Some of the highlights of the “2005 Computer Crime and Security Survey” are:

- Frequency of attacks. Nearly nine out of 10 organisations experienced computer security incidents in any one year; 20% of them indicated they had experienced 20 or more attacks.
- Types of attacks. Viruses (83.7%) and Spyware (79.5%) headed the list. More than one in five organisations said they experienced port scans and network or data sabotage.
- Financial impact. Over 64% of the respondents incurred a loss. Viruses and Worms cost the most, accounting for $12 million of the $32 million in total losses.
- Sources of the attacks. They came from 36 different countries. The U.S. (26.1%) and China (23.9%) were the source of over half of the intrusion attempts, though masking technologies make it difficult to get an accurate reading.
- Defences. Most said they installed new security updates and software following incidents, but advanced security techniques such as biometrics (4%) and smart cards (7%) were used infrequently.
- Reporting. Just 9% said they reported incidents to law enforcement, believing the infractions were not illegal or that there was little law enforcement could or would do. Of those reporting, however, 91% were satisfied with law enforcement's response. And 81% said they'd report future incidents to the FBI or other law enforcement agencies.

[408] *Computer Crime & Security Survey* (2006) The Australian High Tech Crime Centre (AHTCC) <http://www.auscert.org.au/images/ACCSS2006.pdf> at 3 January 2007.

[409] See, eg, Goodman, above n 91, 477. See also, Simon Bronitt and Miriam Gani, ‘Cyber-Crime in the 21st Century: Windows on Australian Law’ in Roderic Broadhurst and Peter Grabosky (ed), *Cyber-Crime: The Challenge in Asia* (2005) 141-162.

[410] Goodman, above n 91, 479.

[411] Shane McKenzie, *Partnership Policing of Electronic Crime: An Evaluation of Public and Private Police Investigative Relationship* (PhD Thesis, Melbourne University, 2006) 28.

has been changed entirely by the rapid and continuing expansion of cybercrimes, because of the prevalence of cybercrime offences and the establishment of Cybercrime Units which have significantly contributed to the positive change in both knowledge and attitudes to the seriousness and priorities of cybercrimes.

Basically, traditional violent crimes are ranked in seriousness as either felonies or misdemeanours, depending upon the severity of the crime and the maximum punishment that can be imposed. Law enforcement agencies place serious crimes on the front line. For example, in the USA, the 'Quality over Quantity' programme was ordered by Clarence Kelley, the director of FBI in 1975, to establish parameters for prioritising traditional crimes.[412] Serious and important crimes were put on the front line, and less serious crimes were placed on the back burner.[413] By contrast, different types of cybercrimes are not ranked as felonies or misdemeanours, and therefore, Cybercrime Units must apply internal guidelines, measures, or policies to ensure that serious cybercrimes are investigated immediately.

a) Jordanian Computer Crime Unit (JCCU)

The JCCU has not established parameters that specify which cybercrimes are worthy to be investigated.[414] Conversely, the Unit investigated all the reported incidents.[415] This is because the number of the cases investigated so far is very small and the Unit has not received complaints about all the criminal activities committed within cyberspace.

b) Australian High-Tech Crime Centre (AHTCC)

By contrast, the AHTCC established a guideline that quantifies and assesses which cybercrime is to be investigated first. The AHTCC assigns an investigative priority based on four different criteria: level of affect, sophistication of the attack, nature of target, and target significance.[416] The first criterion, i.e. level of effect, assesses the severity of the attack and damage inflicted on the victim which is either human or

[412] See generally, James Q Wilson, *The Investigators: Managing FBI and Narcotics Agents* (1978).
[413] Ibid.
[414] Interview with Ayman Bani Hani, 1st Lieutenant (Jordanian Computer Crime Unit, Criminal Forensics Department, June 2005).
[415] Ibid.
[416] See, Australian High Tech Crimes Centre, *Computer Intrusion and Denial-of-Service*, AHTCC <http://www.ahtcc.gov.au/tech_crimes_types/computer_intrusion.htm> at 15 March 2008.

computer systems or networks.[417] For example, online auction fraud, spamming and spreading viruses are excluded from the AHTCC priority of investigation,[418] because they do not inflict serious harm. Meanwhile, child cyber-pornography offences have received extreme attention, such as 'Operation Auxin' led by the Australian Federal Police (AFP) and 'Operation Cathedral' led by the National Crime Squad, a British police organisation, and which was the world's largest policing operation against cyber paedophiles.[419] Sophistication of the attack, criterion number two, scales security breaches and discovers who is behind the attack.[420] For example, attacks launched by organised crime or terrorist organisations receive a higher priority than hacking attacks. The third and fourth criteria assess the importance and the value of the victim.[421] How big is the target? How big was the impact? For example, attacks targeting an unprotected network receive a low priority.

c) USA

In the USA, Cybercrime Units also rank cybercrime investigations. They exclude several sorts of cybercrimes from their investigation priorities and focus more on particular types of cybercrimes. For instance, some investigators placed online gambling and cyber prostitution near the very bottom of their list of investigations;[422] meanwhile, intellectual property and child pornography offences have received a high priority.[423] In addition, federal cybercrime units have set three criteria that need to be met before launching an investigation. The first criterion is the magnitude of the pecuniary losses caused by a cybercrime.[424] The threshold set is $5000 or more worth of damages or losses caused. Accordingly, cybercrime units decline to conduct a criminal investigation if the threshold value is not reached; however, if the same crime were committed against several victims, the agency accumulates them to reach an amount above the

[417] Ibid.

[418] See, Australian High Tech Crime, *Online Fraud*, AHTCC <http://www.ahtcc.gov.au/tech_crimes_types/fraud.htm> at 15 March 2008.

[419] See, eg, Peter Spindler, 'Combating Child Abuse on the Internet: A Law Enforcement Strategy' in Allyson Macvean and Peter Spindles (eds), *Policing Paedophiles on the Internet* (2003) 34.

[420] See, Australian High Tech Crimes Centre, above n 414.

[421] Ibid.

[422] See, eg, Darin Walker, 'Faceless-Oriented Policing: Traditional Policing Theories Are Not Adequate in a Cyber World' (2006) 79 (32) *The Police Journal* 169.

[423] See, eg, Smith, Grabosky, and Urbas, above n 25, 34.

[424] See generally, Stephenson, above n 16.

investigative threshold.[425] For instance, if one hundred victims each lost $100; the centre will treat them as a $10,000 case, taking them over the threshold. However, in September, 2008 the Congress revised the CFAA in order to give federal prosecutors the ability to use the statute in a wider variety of cases. The amended revision of the statute removed the $5000 requirement from § 1030 (a) (5). The second criterion is that the crime has been committed within the limits of the jurisdiction of the agency. Finally, cybercrime units sketch out a preliminary investigation to determine whether the crime is solvable by studying the scene of the crime,[426] and prosecutable by applicable USA law,[427] otherwise terminating the investigation process.[428]

d) Comparative Analysis

The five criteria set by the AHTCC are reliable in yielding accurate information about priority of crime investigation. Investigators come to know and expect a level of effect in a wide range of cybercrime. It is well known, for example, that DoS attacks against popular websites such as eBay have more negative effects than unpopular websites.

The application of the US criteria is problematic, because there is no mechanism that can be applied to ensure that the complaints are genuine and the financial losses attributed to the crimes are accurate. Furthermore, sketching out a preliminary investigation is time-consuming and expensive, because it involves technical and legal issues, such as evidence collection, and analysis.

Ranking specific crimes with a high or low priority enhances law enforcement investigation management, by freeing resources such as staffing and equipment, to investigate high-profile crimes.[429] Furthermore, it provides more consistency and clarity in the investigation process across the national and international level. On the national level, it helps the Cybercrime Units to make the links among investigation responsibilities, and to assign the job to the right department. On the international level,

[425] See eg, Daniel Larkin, *FBI Works To Protect Global Citizens From Online Crime* (2006) Internet Crime Complaint Centre (IC3), Federal Bureau of Investigation < http://dhaka.usembassy.gov/uploads/images/-feh04ECK4GeURwNBFPPqA/pre2apr02_06.pdf >at 14 December 2006.

[426] Stephenson, above n 16.

[427] See, eg, Smith, Grabosky and Urbas, above n 25, 36-48.

[428] This key was mentioned as the second phase in Casey's model of cybercrime investigation, 'Assessment of worth'. The model is described in the next section. See generally, Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2nd ed, 2004) 104.

[429] See, eg, James Q Wilson, *The Investigators: Managing FBI and Narcotics Agents* (1978) 129.

the general picture worldwide is that cybercrime investigation priorities vary widely. While, for example, the USA and Australia show extreme interest in pursuing, capturing, and prosecuting paedophiles,[430] JCCU shows no interest even in co-operation in investigating such cases. This highlights the importance of liaising among the Cybercrime Units and Interpol in order to define a mission statement identifying objectives, goals, resources, and investigation priorities among the Cybercrime Units worldwide. Therefore, while the 'Quality over Quantity' programme was applied to traditional crimes, such as murder and other violent crimes, it optimises cybercrime investigations too.

5.1.2 The Particulars of Cybercrime Investigation Approaches

This section addresses the legal aspects of computer forensic approaches that have been formulated by law enforcement agencies and by computing experts. It examines the emergence of computer forensics fields and selected models of cybercrime investigation. Then it assesses what an optimal model for handling digital evidence should look like. But first it is helpful to give a brief description of computer forensics.

5.1.2.1 Computer Forensics

The origins of computer forensic science can be traced back to the mid-1980s, when a few computer hobbyists devised software programmes to solve some particular pragmatic problems associated with individual cases.[431] Within the next few years, and in response to the escalation of cybercrimes,[432] investigation of computer crimes took shape as an independent discipline called 'computer forensics'.

Computer forensics has witnessed dramatic developments in recent years. It is now a separate and firmly established area of specialisation within law enforcement agencies. For example, law enforcement agencies in Australia and the USA established specialised teams for handling digital evidence, such as crime scene technicians,

[430] Cathy Cobely, *Sex Offenders: Law, Policy and Practice* (2nd ed, 2005) 17.
[431] Alan E Brill, Mark Pollitt and Carrier M Whitcomb, 'The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications' (2006) *Journal of Digital Practice* 3, 2.
[432] See, eg, Venansius Baryamureeba and Florence Tushabe, *The Enhanced Digital Investigation Process Model* (2004) Institute of Computer Science, Makerere University <http://www.forensicfocus.com/enhanced-digital-investigation-model> at 22 September 2006. See also, ibid Brill, Pollitt and Whitcomb, 8.

collection teams, examiners processing the acquired evidence, and digital investigators analysing all available evidence to build the case in question.[433]

While there is no consensus on a definition of the term ‘computer forensics’, many experts consider computer forensics as one aspect of a broader concept called ‘data discovery’. They restrict ‘computer forensics’ to data recovery. Data recovery according to Kay refers to ‘any process in which data from a particular computer or network is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case’.[434] This definition is similar to Ieong’s. He defines computer forensics as ‘the process to determine and relate extracted information and digital evidence to establish factual information for judicial review’.[435] Erin Kenneally defines computer forensics by stating that:

> Since forensic science is the application of a scientific discipline to the law, the essence of all forensic disciplines concerns the principles applied to the detection, collection, preservation, and analysis of evidence to ensure its admissibility in legal proceedings. Computer forensics refers to the tools and techniques to recover, preserve, and examine data stored or transmitted in binary form.[436]

However, some computing experts, such as Kruse and Heiser, refrain from defining computer forensics. They agree with many other experts that the basic aspect of computer forensics[437] ‘involves the preservation, identification, extraction, documentation and interpretation of computer data’.[438] Other experts argue that computer forensics should include three fundamental elements. These elements, according to Matthew and Christopher Stippich, are:[439]

1) Proper acquisition and preservation of computer evidence,

[433] Eoghan, above n 428, 27.
[434] Russel Kay, 'Computer Forensics', *Computerworld* April 17 2006, 49. See also, Robert M Slade, *Software Forensic: Collecting Evidence from the Scene of a Digital Crime* (2004) 3.
[435] Ricci Ieong, ‘FORZ Digital Forensics Investigation Framework That Incorporate Legal Issues’ (2006) 3 *International Journal of Digital Investigation* 29, 30.
[436] Erin Kenneally, 'Computer Forensic ' (2002) 27 (4) *The Magazine of Usenix & Sage*, <http://www.usenix.org/publications/login/2002-08/pdfs/kenneally.pdf> at 5 October 2006.
[437] See, eg, Warren G Kruse and Jay G Heiser, *Computer Forensic: Incident Response Essentials* (2002).
[438] Ibid 3.
[439] Matthew J Stippich and Christopher J Stippich, 'A Holistic Perspective on the Science of Computer Forensic' (2005) 1 (1) *Journal of Information Privacy & Security* 27.

2) Documentation, examination, analysis, and authentication of collected data for court presentation; and

3) Recovery of all available data, including deleted files, unallocated file space, slack space[440] and other forms of digital trace evidence.

Despite the fact that the three components of the computer forensic process mentioned above are not presented in chronological order, because the recovery process must come first, then analysis and court presentation at the end, they remain the backbone for structuring the cybercrime investigation process. As is discussed below, they are essential to what might be called a 'Cybercrime Scene Investigation Approach'.

5.1.2.2 Cybercrimes Scene Investigation Approaches

The newborn science of cybercrime investigation has evolved[441] and investigation models have been formed by governmental agencies,[442] such as the USA Department of Justice (DOJ) and by non-profit organisations, such as the International Organisation on Computer Evidence (IOCE),[443] the Scientific Working Group on Digital Evidence (SWGDE),[444] and the International Association of Computer Investigative Specialists (IACIS).[445] These organisations, and many others, have developed different types of legal models and techniques for computer forensics. Furthermore, prominent computing figures like Eoghan Casey, Seamus O Ciardhuain, Brian Carrier, Kruse and Heiser have significantly contributed to the process. These models vary in their structure; however, they must comply with specific criteria outlined by Carrier and Spafford as follows:[446]

1) The model must be based on existing theory for physical crime investigations.

[440] Slack space or file slack is the area of a disk that is empty, because the data on the disk was deleted. This space may still contain data and it can be retrieved. Some websites freely offer a programme called Disk Investigators. This programme can retrieve deleted data. See generally, Nikki Swartz, 'Canada to Increase Internet Surveillance' (2005) 39 (6) *Information Management Journal* 22.

[441] See, eg, George Mohay et al, *Computer and Intrusion Forensics* (2003) 14.

[442] See, eg, Keith H Whitworth, Carol Y Thompson and Ronald G Burns, 'Assessing Law Enforcement Preparedness to Address Internet Fraud' (2004) 32 (5) *Journal of Criminal Justice* 477.

[443] See, eg, Baryamureeba, above n 432.

[444] See, *Best Practice For Computer Forensics* (2006) Scientific Working Group on Digital Evidence <http://www.ncfs.org/swgde/documents/swgde2006/Best_Practices for Computer Forensics%July06.pdf> at 22 November 2006.

[445] Brill, Pollitt and Whitcomb, above n 431, 20.

[446] Brian Carrier, and Eugene H Spafford, 'Getting Physical with the Digital Investigation Process' (2003) 2 (2) *International Journal of Digital Evidence.*

2) The model must be practical and follow the same steps that an actual investigation would take.

3) The model must be general with respect to technology and not be constrained to current products and procedures.

4) The model must be specific enough that general technology requirements for each phase can be developed.

5) The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

The existing models must comply with all of these criteria, because they address both of the legal and technological perspectives of cybercrime investigation. The first and the second criteria, for example, address the legal aspects of computer forensics, i.e. the chain of custody that should be established for evidence. The third and fourth criteria, on the other hand, focus on the technological aspects of computer forensics. The last criterion ensures that the model can be easily applied to private and public investigations. However, while the legal criteria - chain of custody - of cybercrime investigation models apply to various cybercrimes, such as TCP/IP crimes, cyberstalking, and others,[447] the technological features of each model vary considerably from crime to crime. For example, forensics programmes might be designated to investigate specific types of cybercrimes, such as intrusion software forensic programmes which are different from cyberstalking forensic programmes. In other words, each model agrees on its essential legal elements but differs in some technological details.

According to Kruse and Heiser, forensics investigation models consist of three basic steps: acquiring, authenticating, and analysing the evidence.[448] Stephenson has also divided them into three phases. The first is called 'launch activities' which involves protecting the cybercrime scene from contamination, hypothesising how the attack took place, and collecting evidence.[449] The second phase analyses the incident and consists of three different steps: reconstructing the crime scene, conducting trace back

[447] It does not matter whether the crime is being investigated is a crime where the computer is the target, the storage medium, or the tools of the crime. See, eg, Kay, above n 434. See also, Stephenson, above n 16.

[448] Kruse and Heiser, above n 437, 5-14.

[449] Stephenson, above n 16.

investigation, and performing detailed analysis.[450] The final phase of investigation is evidence analysis and report preparation.[451] These steps are intended to provide incontestable proof that the digital evidence was not contaminated and that it remained intact during the computer forensic process.[452] Therefore, the major goal of these models is to yield admissible digital evidence.

In this section, the investigation models applied by the JCCU, AHTCC, and the USA DOJ will be identified as well as the models formulated by two prominent forensic scientists, O Ciardhuain and Casey.

a) Jordanian Cybercrime Investigation Model.

The JCCU's model is entitled 'Computer & Cyber Crimes Digital Evidence'.[453] It consists of two phases. The first one describes the physical procedures that should be adopted at the crime scene. This phase consists of the following steps: securing the crime scene to prevent loss, contamination and destruction of evidence, and preservation of the state of the physical scene.[454] The second phase consists of nine generalised instructions for the first responders who are affiliated with the JCCU.[455] It describes procedures that should be taken in the crime scene as follows:[456]

1) Documentation; which involves recording the complete details of the crime scene, such as whether the computer is plugged in or not.

2) Identification; which involves systematically numbering each computer and peripheral device found at the crime scene. If the investigators find a computer and its peripheral equipment is in more than one room, each computer and the attached peripheral equipment should be given a unique number, such as computer A, scanner A1, printer A2, etc

3) Identification and documentation of storage devices, such as CDs and DVDs found in the crime scene.

4) Photographing the crime scene.

[450] Ibid.
[451] Ibid.
[452] See eg, John Mallery, 'Cyberforensics: The Ultimate Investigative Tool: The Right Way and The Wrong Way to Run a Computer Investigation' (2005) *Security Technology and Design.*
[453] الادلة الرقمية في مسرح الجريمة ,مديرية الامن العام, ادارة المختبرات و الادلة الجرمية , قسم جرائم الحاسوب *Computer & Cyber Crime Digital Evidence*, (Alaeldin Mansour Maghaireh, trans unpublished) [trans of: الادلة الرقمية في مسرح الجريمة].
[454] Ibid.
[455] Ibid.
[456] Ibid.

5) Preservation of digitalised materials.

6) Preservation of printouts and hard copy documents found at the crime scene.

7) Preservation of hardware materials.

8) Recovery process by printing pending documents, i.e. documents wait in the print queue.

9) Transportation of the collected evidence.

b) Australian Cybercrime Investigation Model

The AHTCC has adopted '*HB 171: Guidelines for the Management of IT Evidence'* model for the preservation and collection of digital evidence.[457] The guideline is part of the Commonwealth Government E-Security National Agenda.[458] It consists of six phases:[459]

1) Designing for evidence; which involves identifying the evidence, author, time and data of evidence creation and alteration, establishing the authenticity of evidence, and reliability of computer programmes.

2) Producing records; that ensure that the system producing evidence is reliable. For example, organisations should be able to demonstrate that a computer programme which produced evidence was operating correctly. [460]

3) Collection; involves search and locate all relevant information and documentation of digital evidence.[461]

4) Analysing; looks at the examination products for its significance and probative value to the case.[462]

5) Reporting and presentation that involves writing a final report showing that all previous steps done according to the best practice or law.[463]

6) Determining evidentiary weight or the final assessment is performed by a natural arbitrator.[464]

[457] E-mail from Nigel Phair to Alaeldin Maghaireh, 7 October 2007.
[458] Ajoy Ghosh et al, *Guidelines for the Management of IT Evidence* (2003) 8.
[459] Ibid 8.
[460] Ibid 20.
[461] Ibid 21.
[462] Ibid 24.
[463] Ibid 25.
[464] Ibid 26.

c) The USA Department of Justice Model

The US Department of Justice model is called 'Electronic Crime Scene Investigation: A Guide for First Responders'.[465] It consists of four different stages, starting with evidence collection, followed by examination of the collected data, then analysis, and finally reporting.[466]

1) Evidence collection involves search, recognition, collection and documentation of digital evidence.

2) Examination process is referred to as separating the wheat from the chaff via making the evidence visible and explains its origin and significance.

3) Analysis looks at the examination products for its significance and probative value to the case.

4) A written report outlining the examination process and pertinent data recovered from the overall investigation is the final stage.

d) Overview of the Models

There are remarkable similarities between the Australian and the US DOJ's models, while the JCCU's model is mildly different. The AHTCC and DOJ models meet the criteria outlined by Carrier and Spafford (see page 113) as well as the fundamental elements of computer forensics, proper acquisition, preservation, documentation, examination, analysis, authentication, and recovery of data. The JCCU's model, by contrast, does not include all the fundamental elements. While it addresses the proper acquisition and preservation of computer evidence, as well as documentation, it does not address recovery of all available data, including deleted files.

The JCCU's guideline provides basic instructions for the first responders on how to deal with the cybercrime scene and then more detail for investigators. The responders collect evidence and send it to the JCCU's lab for analysis by forensics staff. The examination process, analysis, and reporting are not mentioned anywhere in the guideline, but step nine orders the first responders to dispatch the collected evidence to the JCCU for

[465] U.S Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2001) National Criminal Justice Reference Service < http://www.ncjrs.gov/pdffiles1/nij/219941.pdf > at 11 October 2006.

[466] Ibid.

examination, analysis, and finalising a report.[467] Meanwhile, the Australian and the DOJ's models are more technical and require more advanced computer forensic skills. They require the highly skilled forensics investigators to collect evidence and send it to the lab for further investigation. However, the DOJ's model has been criticised for the following reasons: [468]

1) It does not give much attention to the examination and analysis process.
2) Its scope is limited by not including the earlier and later stages of investigation, such as Awareness, persuasion and testimony.

To avoid the above criticism, forensic computing experts, such as O Ciardhuain and Casey each developed what is claimed to be an optimal model for cybercrime investigation.

e) Models Developed by Computing Experts

O Ciardhuain Model

Seamus O Ciardhuain developed a model called 'An Extended Model of Cybercrime Investigations' which takes into account not only the processing of digital evidence - the middle part of the process of investigation - but also the earlier and later stages of investigation, such as awareness, testimony, and dissemination of information. The model has the following key steps:[469]

1) Awareness: that involves setting up a system recognises the need for investigation. This awareness created by events external to the organisation.

2) Authorisation: which involves either having informal authorisation, such as simple verbal approval from company management, or formal authorisation, such as s search warrant.

[467] Ibid.

[468] Brian Carrier and Eugene H Spafford, 'Getting Physical with the Digital Investigation Process' (2003) 2 (2) *International Journal of Digital Evidence*, 3. See also, Baryamureeba, above n 432. See, Seamus O Ciardhuain, 'An Extended Model of Cybercrime Investigation ' (2004) 3 (1) *International Journal of Digital Evidence* .

[469] Ciardhuain, ibid.

3) Planning: which involves several information flows to the investigating team from outside the organisation, such as policies, regulations, and legislation or from inside it such as internal policies which must be followed by the investigators.

4) Notification: which means informing the subject of investigation or other concerned party that the investigation is taking place.

5) Search and identification of evidence: which involves locating, or tracing the evidence.

6) Collection.

7) Transport: which involves physical transport of the collected evidence.

8) Storage of the collected evidence.

9) Examination of the evidence collected.

10) Hypothesis: which involves the reconstruction of the incident to establish a clear picture of what occurred.

11) Presentation of the hypothesis.

12) Proof/Defence: involves preparing a contrary hypothesis and supporting evidence.

13) Dissemination: that entails disseminating information from the investigation to the public.

Eoghan Casey Model

Eoghan Casey, on the other hand, developed a professional digital forensic process consists of ten components:[470]

1) Accusation or incident alert: which involves setting up an alarm system, such as intrusion detection system, multiple security sensors, network mentoring system reporting the incident to law enforcement.

2) Assessment of worth: which involves conducting initial investigation in order to measure the seriousness of the incident.

3) Crime scene protocols: which involves applying physical crime scene to cybercrime scene. For example, all the physical things, and activities attached to digital evidence must be retained, and documented.

[470] Casey, above n 428, 103.

4) Identification and seizure: which involves the separation and distinction between what should be seized and what should not.

5) Preservation process: which ensure that the original items are untouched and an exact copy of the original materials is scrutinised.

6) Recovery process: which involves retrieving deleted, hidden, and encrypted data.

7) Harvesting: means performing a thorough investigation into collected evidence.

8) Analysis harvested information.

9) Reporting: involves writing a final report showing that all previous steps done according to the best practice.

10) Persuasion and testimony: involves preparing for court hearing.

Overview of the Experts' Models

Both of the models incorporate innovative investigation components. Notification and dissemination are, for the first time, incorporated in O Ciardhuain's model, and harvesting in Casey's model. However, none of them can be considered as an optimal model. O Ciardhuain's model, for example, makes notification and dissemination parts of the process of the investigation. This completely contradicts law enforcement policy in relation to confidentiality of information that is collected during the investigation. Casey's model, on the other hand, places the assessment of worth in the second phase despite the fact that initial assessment requires an investigator to undertake various components of the investigation, such as the recovery process, and analysis. Indeed, some phases of the models, particularly awareness and accusation, are beyond the Cybercrime Units' authority range, because they are not a part of the investigation process.

f) Comparative Analysis of Models

Although computer forensics experts and investigators generally agree on the main principles of cybercrime investigation, there is no single, widely-accepted model for conducting and managing investigations.[471] Nevertheless, the AHTCC and the DOJ's

[471] Brill, Pollitt & Whitcomb, above n 431, 4. See also, Mark Reith, Clint Carr and Gregg Gunsch, 'An Examination of Digital Forensic Models' (2002) 1 (3) *International Journal of Digital Evidence* . See also, Brain D Carrier and Euguen H Spafford, 'Categories of Digital Investigation Analysis Techniques

models in most respects are similar and have common features. They are applied in a very similar fashion to collect, authenticate, and analyse digital evidence.[472] Indeed, it is difficult to assess whether one approach or the other is better suited for cybercrime investigation, because both of them include the main features of investigative protocols.[473] The JCCU's model, on the other hand, is a road map which puts the onus of collecting digital evidence on investigators who are trained to handle physical evidence; meanwhile, computer forensic experts examine and analyse data and report findings and recommendations.[474] The findings and recommendations may subsequently be used by someone else (such as the first responders) to develop an opinion about the incident. Thus, the JCCU's approach is a guideline for use by the first responders to deal with and collect hardware devices. An advantage and drawback are highlighted with this approach. The advantage is to provide immediate protection against evidence contamination. According to this model, first responders are able to act swiftly and independently to secure evidence. Meanwhile, the drawback to this is that the first responders in most incidents lack adequate skills and training to deal with the particular requirements of cybercrime scenes, the first element of computer forensics.

In his article 'The Digital Investigative Unit: Staffing, Training, and Issues' Malinowski lists a number of challenges confronting law enforcement that need to be addressed in order to train skilled investigators, who are capable of managing cybercrime scenes. For example, investigators investigating cyberstalking need to be familiar with Internet terminology, applications, netiquette, emoticon, and acronyms.[475] Jordanian law enforcement officers (first responders) lack the opportunity to participate in special training programmes designed to enhance and maintain law enforcement agencies' skills for investigating cybercrime. Such training programmes are expensive, costing at least $10,000 for each participant.[476] Nevertheless, although JCCU forensics investigators know a great deal about software and hardware issues, for example, the

Based on the Computer History Model' (2006) 3 *Digital Investigation* 121. See also, Keith H Whitworth, Carol Y Thompson and Ronald G Burns, above n 440, 477.

[472] Brill, Pollitt & Whitcomb, above n 431, 5.

[473] See Section 5.2.2.1 for more information on the main principles of computer forensics.

[474] The ideal investigative team has expertise in information security, digital forensics penetration testing, reverse engineering, programming, and behavioural profiling. See generally, Eoghan Casey, 'Investigating Sophisticated Security Breaches' (2006) 49 (2) *Communications of the ACM* 48, 50.

[475] See, eg, Chris Malinowski, 'The Digital Investigative Unit: Staffing, Training, and Issues' in Johnson Thomas Alfred (ed), *Forensic Computer Crime Investigatio*n (2006) 21, 30.

[476] See, Charles Rusnell, 'Cybercops' (2001) 49 (6) *Law & Order* 52.

normal function of the operating system in question, the internals of the operating system, the various file systems and technological aspects of cybercrime investigation, they lack legal knowledge to deal with a real crime scene. Thus, the development of human resources is critical to the success of efforts to improve Jordanian cybercrime investigation.

In addition, to the two phases included in the JCCU's model, the guideline should be developed to clarify more aspects of cybercrime investigation. Examination process, analysis and reporting should be incorporated in the model.

5.2 Cybercrime Investigation Challenges

In the previous sub-section it was demonstrated that an accurate investigation priorities and robust investigative model grant investigators more latitude in managing investigation resources and reducing caseloads as well as strengthening the investigation process. However, officers investigating cybercrime often confront tremendous impediments associated with issues concerning privacy and encryption.

This section addresses and analyses legal and technical issues, which investigators may encounter during investigation process.

5.2.1 Privacy

With the rapid growth of information technology over the past decade, privacy, confidentiality, and cyberspace have gained considerable importance,[477] because they are essential to the functioning of democratic societies, governmental performance, and robust economics.[478] For example, privacy and cyberspace promote creativeness,

[477] In his inquiry into the law enforcement implications of new technology before the Parliamentary Joint Committee on the National Crime Authority, Crompton states that 'Privacy is clearly perceived by Australians as a fundamental human right, and a right we are eager to preserve in a rapidly changing global environment.' See, Malcolm Crompton, *Inquiry Into the Law Enforcement Implications of New Technology* (2001) Parliament of Australia <http://www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/1999-02/itlaw/submissions/sub27.doc> at 22 November 2006.

[478] See, Richard W Downing, *Drafting Procedural Laws: Empowering Law Enforcement with the Legal Tools Needed to Investigate and Deter Cybercrime* (2002) <http://www.cybersecuritycooperation.org/moredocuments/Drafting%20Cybercrime%20Laws/Procedural%20LawsText.pdf> at 22 November 2006.

innovation, and competitiveness,[479] as well as a necessary pre-condition for the development of individual autonomy, and a prosperous community.[480]

However, privacy is slowly dissolving with the emergence of technology and security concerns. Four decades ago, Professor Greenawalt, a member of the civil rights committee of the New York City Bar Association and its subcommittee on wiretapping and eavesdropping, raised three questions about the legitimacy of using tapping and bugging devices by law enforcement agencies.[481] Thirty-five years later, Crompton raised similar questions about when and how such devices are to be used while respecting the values of the community, including its privacy[482] values.[483] Nowadays, it assumed that the use of tapping and bugging devices is a common practice in broader types of investigation.

The marriage between cyberspace and privacy creates a problematic situation and poses a serious threat to individual privacy as well as to law enforcement for many reasons.[484] That happens because cyberspace is not only used as a classic repository medium or communication tool, but also as a medium for transactions, data mining, and data aggregation.[485] Information on credit history, sexual or political orientation, goods purchased, sites visited,[486] and bills paid online, are collected from various sources, and aggregated by different organisations, in both private and public sectors. The aggregated data provides indispensable sources of information for law enforcement agencies and is

[479] See generally, Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public* (1998) Online Ethic Center <http://www.onlineethics.org/com/nissenbaum/privacy.html> at 18 November 2006.

[480] See eg, Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (2005) 41.

[481] See eg, Kent Greenawalt, 'Wiretapping and Bugging: Striking a Balance Between Privacy and Law Enforcement' (1966-1967) 50 *Judicature* . There are several general reasons behind the trend for many countries to enact laws protecting privacy. Some of these reasons are: 1) Electronic commerce advancement; 2) Consistent application with Pan-European laws; 3) Consumer pressure; and 4) Technological advancement. See generally, Gary Bahadur, William Chan and Chris Weber, *Privacy Defended: Protecting Yourself Online* (2002).

[482] Privacy was defined by the Supreme Court Justice Louis Brandeis as 'an individual's right to be left alone'. See, Bahadur, Chan, and Weber, ibid.

[483] See eg, Crompton, above n 477.

[484] Doyle and Bagaric, above n 480, 169.

[485] Nissenbaum, above n 479.

[486] Information about users' online activities can be collected by one or more of the three methods of online data collection, cookies, web bugs, and HTTP technology. On the web, a cookie is a small text file that is planted on a user's computer from a web site being viewed without the former's knowledge. Its mission is to recognise, record, and remember the user's browsing habits and personal information, such as user name and password. See generally, Harold Joseph, 'The Threats on the Web' (1997) 1997 (6) *Computer Fraud & Security* 7. See also, Mariyana Vasileva, *Delete Cookies* (2004) <http://www.developer.com/directories/item.php/211041> at 22 November 2006.

vital for investigating cybercrimes. For example, from online credit card transactions and sites visited, law enforcement is able to collect information to track cyber offenders. Thus, cyberspace becomes a vital environment for law enforcement agencies to combat cybercrimes. Nevertheless, law enforcement agencies which probe into cyberspace must conform to the privacy principles as set out in the privacy laws.

Investigating cybercrimes, however, requires more than just probing into static databases that have finite information. Mining dynamic data, web mining,[487] and exercising ongoing timely cyber-surveillance to collect evidence of cyber wrongdoing, such as monitoring chat rooms, are important in the virtual environment to sustain ongoing investigation or to benefit a case.[488] They are important as well to lead law enforcement investigators to recognise and discover patterns of criminal activity. For example, multiple sources of data, including mined data, help law enforcement to sketch a chart or a map showing a paedophile's orientation, or to establish a relationship between a suspect and a physical location.[489] Therefore, law enforcement agencies are continuously urging the implementation of aggressive approaches, maintaining their capability to collect, survey, and monitor cyber traffic as well as to be able to compel ISPs to disclose subscribers' information without requiring a warrant or any other legal document.[490] Nevertheless, law enforcement demands are likely to be hindered by privacy laws. The capability of privacy laws to impede cybercrimes investigation varies from country to country.

a) Jordan

In Jordan, and up till now, there is no particular law concerning privacy. However, there are different provisions concerning privacy, even though none of them can be used

[487] Web mining can be defined as 'discovering, analysing and processing the information from the World Wide Web'. Also, it has been described as 'the art and science of teasing meaningful information and patterns out of large quantities of data turning 'dusty' data that organisations have already collected into valuable information, operationally and strategically'. See, L E Akman, B Akkan and N Baykal, *Optimization of an Online Course with Web Usage Mining* (Paper presented at the Conference on Artificial Intelligence and Applications, Innsbruck, Austria, February 2004). See also, John Galloway and Simeon J Simoff, *Network Data Mining : Methods and Techniques for Discovering Deep Linkage Between Attributes* (Paper presented at the3rd Asia-Pacific Conference on Conceptual Modelling , Hobart, Australia, 2006) 21.

[488] See generally, Jesus Mena, *Investigative Data Mining For Security and Criminal Detection* (2003) 1.

[489] Ibid 5.

[490] For example, the Canadian government has proposed a controversial legal project called 'lawful access'. According to the proposal, ISPs are to install and upgrade new interception tools for tracking and monitoring Internet users. See, Nikki Swartz, 'Canada to Increase Internet Surveillance' (2005) 39 (6) *Information Management Journal* 22.

specifically to protect individual privacy in full.[491] Private premises are generally protected by Article Ten of the *Jordanian Constitution*. This protection is derived from Shariah principles, the foundation of the Jordanian legal system.[492] The Holy Qur'an primary source of the Shariah law for example, addresses the right of an individual not to be bothered in his home.[493] It prohibits entering the property of another without the owner's consent. Consequently, Article Ten of the *Jordanian Constitution* came to mimic the Quranic verse as well as to fulfil the Universal Declaration of Human Rights, which sets a common standard for individual privacy rights.[494] It stipulates that 'Dwelling houses shall be inviolable and shall not be entered except in the circumstances and in the manner prescribed by law.'[495] Furthermore, in 2003, the Jordanian legislature passed unprecedented legislation that bars companies from public disclosure of private information, including a person's name, national security number, age, nationality, residency, current and previous work places, social status, education, address and wife's name.[496] This legislation also prohibits the private sector or organisations from releasing information concerning an individual's financial situation

[491] In the absence of equivalent legislation governing privacy and a parallel to 'reasonable expectation of privacy' as understood in developed countries, the Jordanian government has been accused by the Human Rights Organization (HRO) of violating human rights including privacy, freedom of assembly and speech. According to the HRO's report released in 2007, 'government restricted the right to be free of arbitrary interference… security officers monitored telephone conversations and Internet communication, read private correspondence, and engaged in surveillance of persons considered to pose a threat to the government or national security'. In a similar manner, in 2007, the Human Rights Watch (HRW) in its dubious report titled '*Shutting out the Critics*' urged the countries providing Jordan with financial assistance to halt their commitments, alleging that the Jordanian government violates the rights to peaceful assembly and freedom of association. Although the credibility and the accuracy of these reports have been subject to compelling criticism from the government, they highlight the importance of enacting and maintaining privacy legislation. See, Human Rights Watch, *Shutting out the Critics* (2007) Human Rights Watch <http://hrw.org/reports/2007/jordan1207/jordan1207web.pdf> at 20 February 2008. See also, 'Human Rights Liberties Protected', *The Jordan Times* (Amman), Monday, February 18th, 2008.

[492] The Jordanian legal system is derived from Shariah law and the French legal system. The personal concerns including marriage, divorce, inheritance, civil disputes, and child custody are governed by Shariah law. Criminal offences, investigation procedures, court trials and punishments are founded on the French legal system.

[493] 'O believers! Do not enter houses other than your own until you have sought permission and said greetings of peace to the occupants; this is better for you, so that you may be mindful'. Holy Qur'an, 24: 27.

[494] Jordan is a signatory to the International Covenant on Civil and Political Rights. Article 12 of the Universal Declaration of Human Rights stipulates 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. See, *The United Nation Convention on Civil and Political Rights* art 12.

[495] *Jordanian Constitution Act 1952*, art 10.

[496] *Jordanian Credit Information Law 2003* para 5/1.

and medical information.[497] Nevertheless, the Act exempts law enforcement agencies and government entities from that prohibition.

Communication privacy in Jordan is established and maintained by the constitution in a limited way.[498] Article 18 states that 'postal, telegraphic and telephonic communications are protected and shall not be subject to censorship or suspension except in circumstances prescribed by law'.[499] This article provides a preliminary sketch of privacy protection for dwellings, and specific types of electronic communications. There is no legislation or regulation that specifically addresses the rules of cyberspace surveillance, searches and seizures. Jordan's *Telecommunications Law of* 1995 and *Electronic Transaction Law* 2001 include no provisions or mechanism to guide law enforcement officers on when they may install and run surveillance systems or tracking devices for investigation purposes. The *Jordanian Criminal Procedure Law* 1961, however, only prohibits searches and seizures of physical items without a warrant.

b) Australia

To date, although Australian does not have a Bill of Rights, various aspects of privacy right are contained in a variety of Federal and State legislative provisions.[500] Since 2004, this privacy legislation has witnessed major modifications. Prior to 15 December 2004, there were laws in place that protected privacy and restricted law enforcement access to personal information and communication systems, including personal computers.[501] The *Telecommunications (Interceptions) Act 1979* and *Privacy Act 1988,* until recently, protected individual privacy against illegal communications interception, alteration, and disclosure of personal information. The former prohibits the interception of communications[502] carried on telecommunication systems and a warrant must be issued for law enforcement to intercept communication systems.[503] After December 2004, 'the balance has been shifting away from privacy protection to allowing greater

[497] *Jordanian Credit Information Law 2003* para 5/2 and 7.

[498] See, Maghaireh, above n 280.

[499] *Jordanian Constitution Act 1952*, art 18.

[500] See, eg, Doyle and Bagaric, above n 480, 63. See also, Russell G Smith, 'Crime Control in the Digital Age: An Exploration of Human Rights Implications' (2007) 1 *International Journal of Cyber Criminology* 167.

[501] Ibid.

[502] According to the *Telecommunications (Interception) (State Provisions) Act 1988,* 'communications includes conversation and a message, and any part of a conversation or message, whether- (a) in the form of (i) speech, music or other sounds; or (ii) data; or (iii) text; or (iv) visual images, whether or not animated; or (v) signals; or (b) in any other form or in any combination of forms.'

[503] Doyle and Bagaric, above n 480, 146.

access and surveillance by law enforcement agencies'.[504] This 'shifting' can be observed in the forms of new and amended legislation.[505] The *Surveillance Devices Act 2004* and amended *Telecommunications (Interception and Access) Act 1979* now provide law enforcement agencies with significant investigative powers.

The *Surveillance Devices Act* 2004 grants law enforcement officers the authority to install and run key logging devices, surveillance[506] or tracking devices[507] on suspects' systems on the grounds that:[508]

1) One or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
2) An investigation into those offences is being, will be, or is likely to be, conducted; and
3) The use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

In June 2006, the *Telecommunications (Interception) Act 1979* was amended and renamed as the *Telecommunications (Interception & Access) Act 1979*.[509] The Act allows law enforcement officers to apply for two types of interception warrants.[510] The first type of interception warrant is a telecommunications service warrant. Under this type of warrant, law enforcement officers can apply to an eligible judge or nominated AAT member[511] for a warrant in respect of a particular telecommunications service being used either by the suspect or another person to communicate with the suspect at a

[504] *Telecommunications Privacy Laws (2006)* Electronic Frontiers Australia <http://www.efa.org.au/Issues/Privacy/privacy-telec.html> at 3 January 2007.
[505] Ibid.
[506] Data surveillance device means 'any device or programme capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device'. *Surveillance Device Act 2004* (Cth) pt 1(6).
[507] Tracking device means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object. *Surveillance Device Act 2004* (Cth) pt 1(6).
[508] *Surveillance Device Act 2004* (Cth) div 2 (14) (1).
[509] See, Electronic Frontiers Australia, above n 504.
[510] *The Telecommunications Act 1979* (Cth) as amended by *The Telecommunications (Interception & Access) Act 1979* p 2-5 div 3 & 4.
[511] Nominated AAT member means a member of the Administrative Appeals Tribunal, deputy president, full-time or part-time senior member, or member of the Administrative Appeals Tribunal nominated by the Minister of the Crown of the State. *The Telecommunications Act 1979* (Cth) amended by *The Telecommunications (Interception & Access) Act 1979* p 1-2 s 6DA.

given time.[512] The second type of interception warrant is called a 'named person' warrant.[513] This type of warrant is more comprehensive than the telecommunications service warrant. It authorises law enforcement officers to intercept all the communications services being used by the suspect, such as e-mail, chatting, MSN Messenger service…and so on.

c) USA

In the USA, the relationship between privacy groups and law enforcement agencies is a pressing topic. Lack of trust, coupled with ineffective anti-terrorism strategies and flaws embodied in Carnivore,[514] forced privacy groups to challenge law enforcement efforts on fighting cybercrimes.[515] For example, the FBI launched an initiative called the 'Federal Intrusion Detection Network' (FIDNET), designed to fight cybercrime by monitoring government computers for security breaches,[516] and the controversial 'Carnivore' Internet surveillance system collided with the principles of privacy advocate groups.[517] The latter argued that such initiatives, which aim to curb illegal activities on cyberspace, would weaken privacy and had amorphous limits,[518] despite the legitimate need to tap and monitor Internet traffic.[519] The core problem is that no parameters are set to guide the scope of surveillance systems, such as Carnivore. This is despite the fact that there are laws, including constitutional and legislative articles, protecting privacy rights.

[512] *The Telecommunications Act 1979* (Cth) amended by *The Telecommunications (Interception & Access) Act* (Cth) *1979*. p 2-5 div 4 s 46 (1) (d) (i) (ii).
[513] *The Telecommunications Act* 1979 (Cth) as amended by *The Telecommunications (Interception & Access) Act* (Cth) *1979*. p 2-5 div 4 s 46A.
[514] Carnivore is a computer programme. Because computer programmes inherently have vulnerabilities, the possibility of mistakes during its operation is unavoidable. Associate General Counsel for National Security Affairs Bowman has recounted how Carnivore didn't work correctly and consequently collected unauthorised data. See generally, *FBI's Carnivore System Disrupted Anti-Terror Probe* (2002) Electronic Privacy Information Centre <http://www.epic.org/privacy/carnivore/5_02_release.html> at 24 November 2006.
[515] See, eg, Geoffrey A North, 'Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance' (2002) 28 *Rutgers Computer & Technology Law Journal* 155-159.
[516] See, eg, David L Speer, 'Redefining Borders: The Challenges of Cybercrime' (2000) 34 (3) *Crime, Law and Social Change* 259. See also, Miroslav Nincic, 'Information Warfare & Democratic Accountability' in Emily O Goldman (ed), *National Security in the Information Age* (2004) 140, 155.
[517] See, eg, Kevin M Keenan, *Invasion of Privacy: a Reference Handbook* (2005) 71.
[518] Electronic Privacy Information Centre, above n 514.
[519] See eg, North, above 515.

Constitutionally, the well-known concept of 'reasonable expectation of privacy', which was derived from the Constitutional Fourth Amendment,[520] primarily serves as a defensive instrument against warrantless search and seizure of private property and also against illegal Internet surveillance.[521] The Fourth Amendment protection for physical objects, was extended to include intangible assets, such as conversation and Internet activities, by the United State Supreme Court's prominent decision in *Katz v. United States*.[522] Katz 'was convicted of transmitting wagering information by telephone in violation of a federal statute'.[523] The information 'was overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth where Katz had made his calls'.[524] The Court found by seven votes to two that[525] 'The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'[526] Nevertheless, the concept of a 'reasonable expectation of privacy', which was first formulated by Justice Harlan who deliberated in the case,[527] has become a test of privacy. This test requires an actual subjective expectation of privacy that society is willing to recognise as acceptable,[528] as well as a balance between the people's right to privacy and the government's interest in

[520] The Fourth Amendment is meant to regulate 'seizures' of persons as well as searches for things. It stipulates 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized'.

[521] See, generally, John N Ferdico, *Criminal Procedure for the Criminal Justice Professional* (9th ed, 2005) 483.

[522] *Katz v. United States*, 389 U.S. 347 (1967).

[523] For many years before the Supreme Court decision in the Katz case, the Court interpreted the Fourth Amendment very literally and it was not applied to a virtual environment, such as cyberspace, or to an oral conversation. This interpretation was obvious in the case of *Olmsted v. United States* where the courts rejected the extension of the Fourth Amendment beyond its literal meaning, commenting that 'the courts may not adopt such a policy by attributing an enlarged and unusual meaning to the Fourth Amendment'. See generally, Joginder S Dhillon and Robert I Smith, 'Defensive Information Operation and Domestic Law: Limitations on Government Investigative Techniques' (2001) 50 *The Air Force Law Review* 135, 149.

[524] *Katz v. United States*, above n 522.

[525] The judges who concurred to stretch the meaning of the Fourth Amendment are Warren, Black, Douglas, Harlan, Brennan, Stewart, White, Fortas and Marshall.

[526] Ibid.

[527] See, eg, Christopher Slobogin and Joseph E Schumacher, 'Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look At "Understanding Recognized and Permitted By Society".' (1993) 42 *Duke Law Journal* 727-728.

[528] See generally, Steven Penny, 'Reasonable Expectation of Privacy and Novel Search Technologies: An Economic Approach' (2007) 97 *The Journal of Criminal Law & Criminology* 477, 481. See also, Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (1997) 20.

crime prevention.[529] The same concept has also been applied to protect individual privacy on the Internet and in all aspects of the virtual world. Consequently, as a general principle, individuals enjoy a reasonable expectation of privacy in governmental treatment of their computerised personal information and data concerning different aspects of their cyberspace applications, such as e-mails, as long as they show caution and a concern not to divulge this information to others.[530] This test is applied by the US courts in each case when law enforcement officers search and seize evidence without a warrant. If there is a reasonable expectation of privacy, the evidence obtained without a search warrant will be inadmissible.

This principle, however, creates a state of confusion in which law enforcement is disorientated about how to apply the aforementioned concept in a dynamic environment.[531] Hunsucker listed the difficulties associated with applying this concept to a dynamic environment. He concluded that law enforcement officers are not aware of parameters for a reasonable expectation of privacy.[532]

Legislatively, the PATRIOT Act, which was enacted to protect and support law enforcement agencies efforts in fighting terrorism and other illegal activities, provides law enforcement with broad powers to perform surveillance and retrieve information.[533] It allows ISPs to voluntarily disclose users' information and other content in case of emergency.[534] It increases and enhances the ability and the power of law enforcement to track suspects with 'roving wiretaps' which may be placed on communications devices, such as the Internet.[535] Also, it provides law enforcement the ability to secretly install software on individual computers or deliver surveillance software by Trojan horse.[536]

[529] See, eg, Doug Cochran et al, *Rules of Evidence: a Practical Approach* (2007) 187.

[530] See, eg, Bruce Middleton, *Cyber Crime Investigator's Field Guide* (2005) 171. See also, Jean Veta et al, ' Cybersecurity: Risk and Liability in the New Information Environment' in Mark E. Plotkin, Bert Wells, and Kurt A Wimmer (ed), *E-Commerce Law & Business* (2003) 16-1, 16-82.

[531] Keith Hunsucker, *Right to Be, Right to See: Practical Fourth Amendment Application for Law Enforcement Officers* (2003) The Police Chief <http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=95&issue_id=092003> at 18 December 2006.

[532] See, eg, ibid.

[533] See, eg, Otis H Stephens and Richard A Glenn, *Unreasonable Searches and Seizures: Rights and Liberties under the Law* (2006) 193.

[534] Ibid.

[535] See Lynn M Kuzma, 'Security Versus Liberty: 9/11 and the American Public' in William J Crotty (ed), *The Politics of Terror: The U.S. Response to 9/11* (2004) 160, 162.

[536] *PATRIOT Act*, 18 USC §201-16 (2001).

d) *Comparative Legal Analysis*

Though communications privacy is encompassed in the Jordan Constitution, protection of the right of individual privacy in cyberspace is not enshrined in the constitution. Article 18 of the *Jordanian Constitution* cannot be extended to cyberspace, because cyberspace is something different from telegraphic and telephonic communication; different aspects are accentuated in each. On one hand, 'Telegraphic' is defined as 'of or relating to or transmitted by telegraph'[537] and 'telegraph' is defined as 'A machine for communicating intelligence from a distance by various signals or movements previously agreed on; which signals represent letters, words or ideas which can be transmitted from one station to another, as far as the signals can be seen.'[538] 'Telephonic', on the other hand, is defined as 'of, pertaining to, or happening by means of a telephone system'[539] and 'telephone' is defined as 'an apparatus, system, or process for transmission of sound or speech to a distant point, especially by an electrical device'.[540] Thus, telegraphic and telephonic communications are characterised as the transmission of writings, signs, signals, pictures, and sounds over distance. Meanwhile, cyberspace is not only used for transmission of writings and voices, but used for a much broader array of communications and transactions. Furthermore, the 'reasonable expectation of privacy' concept has no parallel in Jordanian legal thought. Jordanian law enforcement officers, therefore, can monitor cyberspace and install and run key logging devices without being liable for breaching privacy laws or concern for privacy advocacy groups.

By contrast, in Australia and the USA, the importance of enacting laws protecting privacy on one hand, and of implementing monitoring and surveillance systems in cyberspace on the other hand, always poses a considerable dilemma not only for law enforcement, but also for civil liberties groups. In the words of legal scholars Grabosky, Smith and Dempsey:

> Personal privacy has become and is destined to remain one of the most strongly contested areas of public policy in democratic societies. It seems likely that government access to personal information will remain strictly circumscribed, at least in theory. While governments will

[537] See, *The New Webster's Encyclopedic Dictionary of the English Language* (1997) 681.
[538] Ibid.
[539] Ibid.
[540] Ibid.

> continue at least to play lip service to the importance of privacy, they will maintain that a degree of access to personal information is essential for law enforcement…[541]

It is highly likely that the schism between law enforcement and privacy advocates about the parameters of the cyberspace surveillance system will continue to grow as the Carnivore Internet Surveillance System is misapplied,[542] and government anti-terrorism tactics are perceived as ineffective or unacceptable methods to prevent terrorism.[543] In Australia, for example, the recent two cases involving respectively the terrorist suspects Mr. Haque [544] and Dr. Haneef have highlighted the credibility of the law enforcement counter-terrorism policy.[545] Nevertheless, the investigative power as provided in the Australian *Surveillance Devices Act* 2004, division two, is not narrowly confined. Under this provision, law enforcement officers are less likely to worry about close scrutiny and obtaining permission to install surveillance devices like tracking cookies on the suspect's PC. This is because the phrases 'offences are likely to be committed' and 'investigation is likely to be conducted' are phrased to grant a law enforcement officer the potential latitude and power to install and run key logging devices. Accordingly, a mere suspicion is sufficient to justify installing and running surveillance devices.

5.2.2 Encryption

Encryption[546] is an integral part of information technology and pertains to information security, authentication and access control.[547] In 1991, Phil Zimmermann, a prominent

[541] Peter N Grabosky, Russell G Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (2001) 176.

[542] See, eg, Drew Clark, *Privacy Experts Urge Vigilance Against Surveillance* (2003) The Computer Freedom & Privacy <http://www.cfp2003.org/cfp2003/njtd1.html> at 3 December 2006. Also see, *FBI's Carnivore System Disrupted Anti-Terror Probe* (2002) Electronic Privacy Information Center <http://www.epic.org/privacy/carnivore/5_02_release.html> at 24 November 2006.

[543] See, eg, *Experts Call White House Anti-Terrorism Efforts Ineffective* (2003) The Computer Freedom & Privacy <http://www.cfp2003.org/cfp2003/njtd1.html. > at 2 December 2006.

[544]Mr Izhar ul-Haque was accused of attending a terrorist training camp in Pakistan. The Justice Adams dismissed the case, because the law enforcement officers mishandled the case. The judge, Adams, accused the Australian Security Intelligence Organization of false imprisonment and kidnapping. See, Tim Johnston, *Australian Judge Dismisses Terrorism Case*, (2007) The New York Times http://www.nytimes.com/2007/11/13/world/asia/13australia.html> at 25 March 2008.

[545] In 2007, Dr. Mohammad Haneef was accused of giving 'reckless support' to the terror attempts in London and Glasgow by providing his cousin in Britain with his mobile phone SIM card. See, Mohib Ahmad, *Dr. Mohammad Haneef to Be Released* (2007) Indian Muslim Blog < http://indianmuslims.in/dr-mohammad-haneef-to-be-released/> at 25 March 2008.

[546] The first military usage of encryption has been traced back to 50 BC to the Roman emperor Julius Caesar. In modern times, intelligence agencies, such as the NSA in USA, GCHQ in England, and the KGB in the former Soviet Union, have spent billions of dollars designing and decoding algorithms technology for military purposes. See generally, Brain Holley, Henry Schimke and Erin Ebeler, *Caesar*

programmer, was the first to release a sophisticated form of encryption programme called Pretty Good Privacy (PGP) online.[548] To understand encryption as a cybercrime investigation impediment, however, it is important first to explain the basic concepts of encryption technology.

Encryption is the science of converting readable data into an unintelligible form, or turning plain text into cipher text, that cannot be read or understood by unauthorised persons,[549] to protect the confidentiality, privacy and to prove integrity.[550] It has become pervasive in the private sector and between individual users,[551] because encryption programmes are freely available online and are easy to download and install from several websites for personal use.[552] For example, encryption is commonly used in commercial electronic transactions, such as ATM transactions, net banking, and Internet multi-services.[553] Strong encryption technology is a two-edged sword combining potential benefits with potential harms.[554] On one hand, it can be legitimately used to protect the fundamental human rights of both privacy and freedom of speech and to provide integrity, authentication, and confidentiality to electronic transactions.[555] On the other hand, it can be used by criminals to conceal incriminating data or/and to send encrypted messages and photographs without being intercepted or accessed by law enforcement. In the latter case, the primary goal of law enforcement therefore, is to ensure that encryption technology not being used to encrypt illegal content or hamper investigators' ability to conduct effective investigations. Nevertheless, law enforcement officers investigating cybercrime often encounter an encrypted crime scene which

Shift Cipher and General Shift Cipher University of Nebraska-Lincoln <http://cse.unl.edu/~bholley/Cypher%20Tutorial.html> at 17 October 2006.

[547] *Cryptography* Wikipedia <http://en.wikipedia.org/wiki/Cryptography> at 17 October 2006.

[548] See, eg, Smith, Grabosky, and Urbas, above n 25, 39.

[549] Samuel S Wagstaff, *Cryptanalysis of Number Theoretic Ciphers* (2003) 3.

[550] Kruse and Heiser, above n 437, 83.

[551] Wayne Madsen, *Cryptography and Liberty: an International Survey of Encryption Policy* (1998) Global Internet Liberty Gampaign <http://www.gilc.org/crypto/crypto-survey.html> at 19 October 2006.

[552] For example, Cryptainer EL is 128 bit high encryption software program available online for free download. The 128 bit key size is impregnable against brute attack that would take all the computers in the world working together more than the age of the universe to decrypt. See, *Cypherix Strong Encryption* <http://www.cypherix.co.uk/cryptainerle/faqs.htm> at 11 October 2006.

[553] Simon A Price, 'Understanding Contemporary Cryptography and its Wider Impact upon the General Law' (1999) 13 (2) *International Review of Law Computers* 95.

[554] See, eg, Keith H Whitworth and Carol Y Thomspon Ronald G. Burns, 'Assessing Law Enforcement Preparedness to Address Internet Fraud' (2004) 32 (5) *Journal of Criminal Justice* 477, 194.

[555] See, eg, Simon A Price, 'Understanding Contemporary Cryptography and its Wider Impact upon the General Law' (1999) 13 (2) *International Review of Law Computers.* 95.

hinders the investigation process and criminal prosecution.[556] Therefore, law enforcement officers should be provided with the necessary power to deal with encrypted crime scenes.

a) Jordan

Encryption programmes - their production, trade and use - are not regulated by the law in Jordan. Encryption consequences in crime investigation have not yet come to the attention of the Jordanian authorities. Thus, law enforcement has no power to apply for an order to enforce a suspect or a third party to reveal his private encryption keys. However, article 39 of the *Criminal Procedure Law* 1960 authorises law enforcement officers and prosecutors to hire experts. For example, in cybercrime investigation a general prosecutor can hire computer forensic experts to decrypt the encrypted data and to provide technical assistance.

b) Australia

In Australia the picture is different. Law enforcement engaged in a criminal investigation involving encryption has recently been given the power to compel a defendant or third party to divulge encryption keys.[557] Under section 3LA of the *Crimes Act* 1914, investigators can apply for an order requiring the computer owner or a user to reveal encryption keys or any other information enabling the investigators to access information held on the computer. Failure to comply with the order is punishable with up to six months' imprisonment.[558]

c) USA

In the USA, controversial debates have been entertained concerning the right of public authorities, such as law enforcement, to possess or access devices or codes that decrypt encryption algorithms. The Clinton administration, for example, proposed legislation to enable law enforcement agencies to effectively decode algorithms by building 'backdoors' into encryption products,[559] or to force users to provide a copy of

[556] See generally, Smith, Grabosky, and Urbas, above n 25, 26.

[557] See, eg, Bronitt and Gani, above 409, 161.

[558] *Crimes Act 1914* (Cth).

[559] Amitai Etzioni, 'Implications of Select New Technologies for Individual Rights and Public Safety' (2002) 15 *Harvard Journal of Law & Technology* 258.

encryption keys to a third party or public authorities.[560] However, none of those attempts were successful because, inter alia, they were expensive and technologically difficult to implement and, more importantly, they lacked international co-operation and consistency.[561] For example, if the proposed statute had been adopted, criminals could avoid using or buying American encryption products with a built in 'backdoor' key to read encrypted applications and turn, instead, to other impregnable foreign products, such as provided by Russian technology.[562] Instead, a guideline has been presented for presidential approval setting out three initiatives that the government should undertake: first, to establish the right of law enforcement to get swift access to the encrypted information stored in a third party; second, to provide law enforcement with the latest advanced technologies and tools to decrypt illegal data; and, finally, build a relationship of trust between the encryption industry and law enforcement.[563] These initiatives, if adopted, would strengthen law enforcement's capacity to deal with encryption.

Amazingly, Title 18 of the USA Code and the *PATRIOT Act*, which shifted the balance towards law enforcement, each provide no power for law enforcement to obtain encryption keys because to do so could be inconsistent with the Fifth Amendment, which protects individuals against compulsory self-incrimination.[564] Nevertheless, section 404 of the *Domestic Security Enhancement Act* 2003 (DSEA) imposes penalties on those who knowingly and wilfully use encryption during the commission of, or the attempt to commit, a federal felony.[565]

d) Comparative Legal Analysis

The Jordanian legislature did not take legal action to backup officers investigating cybercrime when they encounter an encrypted crime scene. The only tool available to

[560] The former FBI Director Louis Freeh argued that without access to encryption keys, the agency's ability to fight terrorism and cybercrime would be crippled. He describes the issues in his report (presented before a congressional panel) this way: 'we're in favour of strong encryption, robust encryption. The country needs it, industry needs it. We just want to make sure we have a trap door and key under some judges' authority where we can get there if somebody is planning a crime'. See generally, Arnold, above n 328, 676. See also, Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age* (2003) 160. See also, Amitai Etzioni, above n 559.

[561] James A Lewis, *Security and Surveillance* (2002) The Internet Society's 12th Annual INET Conference <http://www.inet2002.org/CD-ROM/lu65rw2n/papers/g10-b.pdf> at 3 November 2006.

[562] See, eg, Godwin, above 560, 161.

[563] *Crypto Politics,* Electronic Frontiers Australia http://www/efa.org.au/Issues/Crypto2.html#usa at 6 November 2006, 199.

[564] Grabosky, above n 25, 67.

[565]*Domestic Security Enhancement Act,* USC §§ 404 (2003).

investigators encountering an encryption problem is to obtain forensic computing experts in the field of encryption. The Australian *Crimes Act* 1914 amendment is advantageous, because it provides law enforcement with a strong mechanism to deal with encrypted data. It even extends law enforcement power to third parties, such as the users who share the computer with a suspect. In many cases, however, the amendment has negligible influence over the suspect, because the sentence upon conviction for a felony which the suspect would face, if he chose to abide by the order and divulge the key, is tougher than the six months maximum sentence if he did not comply with the order and thereby avoided conviction for the felony.

Although the USA administration is one of the world's strongest proponents of tight controls on encryption products exports,[566] it can be clearly seen that its attempts to acquire powers to combat criminal uses of encryption have failed. US initiatives and the Australian amendment have no parallel in Jordan. Hiring forensic experts to do the job is the only tool, but it is expensive and time consuming because, in some cases, it takes a long time to decrypt the data. Law enforcement must be provided with the appropriate power in Jordan to force third parties to divulge the encryption keys, as in Australia. The first and the second proposed initiative in the USA, to draft guidelines, are critical for law enforcement to conduct effective investigation, but the third initiative is inapplicable, because Jordan has no encryption industry. Jordanian lawmakers should simply impose additional penalties on those who knowingly and wilfully use encryption during the commission of, or the attempt to commit and conceal, a crime.

5.3 Conclusion

Cybercrime investigation is an evolving science that covers complex technological issues that have legal implications. Computer forensics initially emerged as a new forensic science and developed gradually into a legal process. This legal process has taken shape in the form of various investigation models developed by governmental and non-governmental organisations and among computing experts. These models have been formulated in accordance with classical investigation procedures, particularly

[566] The US government restricts cryptography exports on the grounds that information technology might be used by terrorists and criminals to conceal incriminating data. See eg, Matt Friedman, *Canada Frees Up Crypto* (1998) <http://www.wired.com/news/politics/0,1283,15362,00.html> at 1 October 2006.

relating to evidence admissibility doctrines. Four of these models were selected and examined and compared with the Jordanian model. Optimality was not evident in any of these models as there was no benchmark available to measure the models' robustness. However, weaknesses and strengths were identified in each, and the lack of comprehensiveness and the omission of significant steps were identified in the Jordanian model.

Building a robust model for cybercrime investigations is necessary in order to present admissible and reliable evidence and, moreover, technological development is intrinsic to the investigation process. Prevailing computer forensic software, investigation models, and the ever-growing motivation among law enforcement agencies to work together cooperatively to fight cybercrime will provide grounds for more consistency in handling cybercrime investigations. Therefore, it is conceivable that a comprehensive or an optimal model will be identified and subsequently adopted by law enforcement agencies worldwide.

Privacy restrictions and encryption technology are obstacles to effective investigation. Law enforcement and privacy advocacy groups are continue to be involved in a bitter quarrel over approaches to cyber-surveillance. Law enforcement agencies are needed for a stronger approach to cyber-surveillance and access to encrypted data. Law enforcement investigating cybercrimes in both Australia and the USA have benefited from ani-terrorism legislation. Investigation capabilities prior to 2001 were not appropriate to suit cyberspace's unique environment. Australian law enforcement has been provided with new search warrants and surveillance powers, and the legal mechanism to deal with anyone hiding or refusing to reveal encryption keys, whereas the USA *PATRIOT Act* and DSEA expanded law enforcement powers to surveillance and retrieve information. In Jordan, on the other hand, the Constitution specifically recognises a limited right to privacy, because though it does not address cyberspace. Therefore, law enforcement conducts electronic surveillance or e-mail opening but this power is hindered by the lack of knowledge and an available legal instrument regarding encryption, such as the legal power to force a holder or a third party to divulge decryption keys.

6 DIGITAL EVIDENCE ADMISSIBILITY

Introduction

Evidence takes two major forms: the first is the traditional form, such as testimony of witnesses, oath, physical evidence, and so on. The second form is non-traditional evidence, commonly known as digital evidence. Each of them varies in its integrity and admissibility. While the first form of evidence has been scrutinised and analysed thoroughly, digital evidence is not widely understood, because it is new and has little precedent, particularly in Jordan.

Digital evidence plays a critical role in the prosecution of cybercrime cases as well as in other sorts of classical crimes, such as drugs trafficking and terrorism.[567] It either supports or refutes allegations in a wide range of crimes, from high-profile murder cases to obscure investigations into cybercrime. For example, one serial killer who called himself "BTK" has been sentenced to ten consecutive life terms in prison for killing ten people following the electronic recovery of deleted files on a floppy disk by the criminal on a church's computer.[568] This role has evolved with the growth of information technology. 'Digital evidence is becoming a feature of most criminal cases,' says cybercrime scholar Susan Brenner.[569] For example, digital evidence is becoming prevalent among many types of cybercrime including child pornography cases. In their report, *'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutor',* the USA's Department of Justice (DOJ) reported 'that it is rare to find a child pornography case that involves anything other than digital images (and

[567] Digital evidence is being used to support or refute a wide range of cases and civil wrongs. For example, Garry Mathiason, a lawyer, who defends major corporations in employment cases, said 'almost every case they handle has a "smoking e-mail" component'. Volonino and Robinson, above n 197, 137. See also, Eoghan Casey,' Reconstruction Digital Evidence' in W Jerry Chisum and Brent E Turvey (eds), *Crime Reconstruction* (2006) 419, 420.

[568] See, Sam Coates, *Rader Gets 175 Years for BTK Slayings* (2005) The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/18/AR2005081800201.html> at 3 April 2007.

[569] Susan Brenner is a renowned cybercrime scholar. She is a member of the American Bar Association's International Cybercrime Project and has published articles dealing with cybercrime, and established website providing extensive information about cybercrimes. See, Susan Brenner Quotes, <http://thinkexist.com/quotes/susan_brenner/> at 12 April 2008.

occasionally printouts of the digital evidence)'.[570] Therefore, reliable digital evidence will contribute strongly to the success of cybercrime prosecutions as well as many types of traditional crimes.

In the developed world, such as Australia and the USA, for instance, the numbers of trials that have involved digital evidence have increased enormously, because of the rapid escalation of cybercrimes.[571] Australian and US lawmakers responded positively by addressing technological developments that affect the existing laws, and adopted provisions that recognise digital evidence. Their Jordanian counterparts have not yet responded effectively to the digital revolution. Indeed, digital evidence is still alien to the Jordanian legal system. Lawmakers have not yet shown a willingness to comprehensively address the admissibility of some types of digital evidence. Existing rules of criminal procedure and evidence were drafted to regulate the admissibility of physical evidence. The most important issues concerning digital evidence that Jordanian law enforcement and prosecutors are likely to encounter is the integrity and therefore the admissibility of evidence extracted from computers and the Internet. The integrity and the admissibility of digital evidence play a critical role in cybercrime investigation, because in many cybercrime investigations, digital evidence is the only evidence presented to the court. Thus, Jordanian lawmakers will have to move quickly to make sure that digital evidence receives the same attention as physical evidence.

The objective of this chapter is to examine the volatility, the integrity, and the admissibility of the evidence extracted from computers and the Internet in cybercrime investigation. It demonstrates the particular characteristic features and inherent risks associated with digital evidence from both technical and legal perspectives. The nature and characteristics of digital evidence will be examined for their effects on evidence admissibility. The chapter then evaluates digital evidence in terms of its legal admissibility and discusses the role of the judges in evaluating digital evidence. Therefore, this chapter is divided into three sections. The first examines the different types of data and their volatility. The second section examines digital evidence integrity.

[570] *Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation* (2003) The National Center for Forensic Science <http://www.ncfs.org/DE_courtroomdraft.pdf> at 10 June 2007.
[571] Volonino and Robinson, above n 197, 29.

The third section addresses digital evidence admissibility. The legal responses and judicial role in accepting evidence will also be analysed.

6.1 The Volatile Nature of Digital Evidence

The commission of cybercrime leaves digital imprints or cybertrails.[572] Unlike physical evidence, these cybertrails are invisible or virtually visible, volatile and reside in two different memory storage systems: permanent storage units, such as hard disks, CDs, and network servers or/and temporary storage units, such as Random Access Memory (RAM) and Read-Only Memory (ROM).[573] Cybertrails take three different forms: active files, archival data, and latent data or deleted files.[574]

First form, active files: these are dynamic and visible forms of information that need no particular skills or forensic tools to display them and are usually not passworded or otherwise protected from view.[575] This type of data can be detected by the naked eye[576] and includes temporary Internet directories, cookies, and history files.[577] They are retrieved without using any forensic tools, but by searching and browsing data and then opening the required files.[578] However, forensic tools such as SafeBack[579] are used to copy and analyse them. These files are very volatile and need more care and diligence in their handling to achieve the highest possible standard of integrity and admissibility. They are extremely susceptible to contamination, because they often reside in the temporary storage memory that requires a consistent power supply. This memory holds the data as long as the computer is on; therefore, it is more volatile than its storage counterpart, i.e. hard disk drives, due to the transient nature of the data.[580] Scholars of digital forensics describe the methods that are used to recover and extract evidence from

[572]See, eg, Casey, above n 428, 115.

[573] See, eg, Peter Grabosky, *Electronic Crime* (2007) 73.

[574] Adam I Cohen and Lender David J, *Electronic Discovery: Law and Practice* (2004) 40.

[575] See, eg, ibid 1-41.

[576] See, eg, Michele C S Lange and Kristin M Nimsger, *Electronic and Discovery: What Every Lawyer Should Know* (2004) 92.

[577] See, eg, Ball Craig, *Computer Forensic For Lawyers Who Can't Set the Clock on Their VCR* (2005) <http://www.craigball.com/cf_vcr.pdf> at 4 June 2007, 11.

[578] Cohen, and David J, above n 574.

[579] SafeBack is used to create mirror-image backup files of hard disks. See, *Computer Forensic Software Tools Downloads*, Forensic Computing Ltd < http://www.forensic-computing.ltd.uk/tools.htm#forensic_windows> at 1 March 2009.

[580] See generally, Brain D Carrier and Joe Grand, *A Hardware-Based Memory Acquisition Procedure for Digital Investigation* (2004) Digital Investigation/Forensic and Evidence Research <http://www.digital-evidence.org/papers/tribble-preprint.pdf> at 2 June 2007.

the temporary system memory as non-traditional digital forensic techniques, as compared with techniques used to collect digital evidence that resides in hard drives and other digital media, such as CDs and USB.[581] Active data often provides highly valuable digital evidence, either while a crime is actually being committed,[582] or soon after its commission,[583] concerning matters such as loaded libraries, logged-in users, and open files.[584] Investigating this type of data requires implementing enabling forensic tools to provide better means of data collection and analysis. FATKit, for example, is an innovative forensic tool designed to handle volatile system memories and transient data.[585]

The second form, archival data, consists of backed up and data residing in permanent storage units, such as CDs, floppy disks, network servers or on the Internet.[586] In a similar manner as the active data, archival data are visible and need no particular forensic tools to copy the required files.[587] Archival files, however, are less volatile than active data, because they reside in permanent storage units and can be printed out in hard copy form.

The third form, latent data, comprises files which have been deleted files but can still be retrieved using forensic tools.[588] Contrary to popular belief, deleted files and files emptied from recycle bins have not completely vanished, but are automatically and temporarily stored in a particular part of the electronic storage devices known as slack space**.**[589] However, they stay there until new data or files are written and saved over the deleted files. In many cases, nevertheless, the old and overwritten files can be completely or partially recovered if the new files do not take up all the space occupied

[581] Petroni Jr Nick L et al, 'FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory' (2006) 3 (4) *Digital Investigation* 197.
[582] This scenario involves the tracing, monitoring and collecting evidence from the victim's system and then may require the officer to move to the suspect's premises or the place where the system is located to conduct a search. See generally, Russell G Smith, 'Investigating Cybercrimes: Barriers and Solutions' (Paper presented at the Association of Certified Fraud Examiners, Sydney, 11 September 2003). See also, Wang Shiuh-Jeng and Kao Da-Yu, 'Internet Forensics on the Basis of Evidence Gathering With Peep Attacks' (2006) 29 (4) *Computer Standards & Interfaces* 423, 424.
[583] Some sort of investigation should be conducted swiftly before the opportunities of collecting evidence are lost, such as DoS attack.
[584] See, Petroni, above n 581.
[585] Ibid 200.
[586] See, Lange and Nimsger, above 576, 99.
[587] Cohen, and David J, above n 574.
[588] See, eg, Mohay et al, above n 441, 55.
[589] See specially, Jonathan Henry, 'Computer Based Media' in Peter White (ed), *Crime Scene to Court: The Essentials of Forensic Science* (2nd ed, 2004) 172, 199. See also, Eoghan Casey, above n 428, 205.

by the deleted files.[590] This is because the capacity of a cluster[591] is up to 16 kilobytes (16 KB), and therefore, when a file of 32 kilobytes is stored on a hard drive, it will take up two entire clusters. Later, if this file is deleted and another file that is only 20 kilobytes in size is saved over the old file (32 KB), this will leave 12 KB from the old deleted file recoverable using forensic data recovery software, such as Encase.[592] Figure 6.1 illustrates the slack space and cluster.

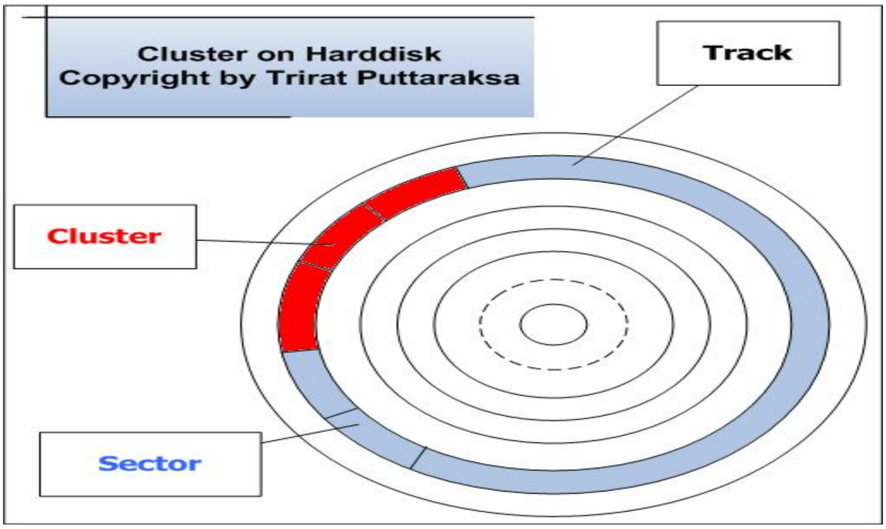


Figure 6.1

<u>Source</u>: *Thailand's Computer Forensics and Incident Response* <http://trirat-puttaraksa.blogspot.com/> at 17 June 2007.

The three forms of data differ markedly with respect to their location on electronic storage devices, and their volatility. The forensic process should be carefully handled to avoid damage or alteration, because the information is fragile and can be easily lost. Therefore, law enforcement officers must not perform any type of forensic process on

[590] Henry, ibid.

[591] The electronic storage device, such as a hard disk is a physical unit that contains a number of invisible storage tracks. Each track is divided into several sectors. The sector corresponds 512 bytes of storage capacity. Several sectors make one cluster. See Figure 6.1.

[592] Henry, above n 589, 193. According to Budge, an independent forensic computer analyst, Encase is a forensic tool 'provides a powerful search engine to enable location of information anywhere on the physical or logical media'. It enables an analyst to:

- Verify the exact copy of the collected evidence.
- Recover deleted folders, which are still readable.
- Review visible files including images.
- Recover deleted images.
- Review and recover deleted Internet history.

See, *A Firm of Solicitors v. District Court at Auckland* [2004] 3 NZLR 748.

the original data, but a mirror copy[593] must be used to make a record of the original data. The unique nature and location of the digital evidence raises difficult questions about the integrity of evidence. The investigators' responsibilities are not only to uncover the incriminating evidence, but they must do it in an efficient and effective manner to maintain evidence integrity and admissibility in court.[594]

6.2 Integrity of Digital Evidence

Evidence integrity is vital to the success of any criminal investigation and successful persecution. But in cybercrime investigation, digital evidence integrity is of the utmost concern due to the volatile nature of digital evidence.[595] Because the latter is fragile, it can be easily tampered with, accidentally modified, or contaminated. If any of these actions occurred, evidence would be inadmissible. Therefore, computer forensic investigators, first responders, and prosecutors are responsible for ensuring that digital evidence is handled in an appropriate manner to minimise the potential risk of evidence contamination. The possibility of digital evidence being lost or altered is extremely high as Brenner and Frederiksen opined 'the simple act of starting a Microsoft Windows system will destroy more than 4,000,000 characters of evidence, and the spoliation will be far greater if the system is used to run any programs'.[596] Therefore, digital evidence is more prone to be suppressed due to the potential risk of contamination. Robert Moore described two scenarios in which a defendant can challenge digital evidence integrity.[597] In the first scenario, a defendant might argue that the file access time stamp was changed during the forensic process, because every time the computer was turned on

[593] A 'mirror image' or bit-by-bit image is the copy of a hard drive, i.e. a complete replication of the physical drive. From an imaged copy of a hard drive it is possible to reconstruct the entire contents and organisation of the source drive from which it was taken. Cohen and David J, above n 574, 1-89.

[594]See, eg, Wegman Jerry, *Computer Forensics: Admissibility of Evidence in Criminal Cases* (2004) University of Idaho <http://www.cbe.uidaho.edu/wegman/computer%20Forensics%20AA%202004.htm> at 29 May 2007.

[595] See specially, Smith, Grabosky and Urbas, above n 25, 81.

[596] Susan Brenner and Barbara Frederiksen 'Computer Searches and Seizures: Some Unresolved Issues ' (2001 / 2002) *Michigan Telecommunication and Technology Law Review* 28.

[597] Robert Emest Moore, *Search and Seizure of Digital Evidence: An Examination of Constitutional and Procedural Issues* (PhD Thesis, the University of Southern Mississippi, 2003) 70. See also, Peter Grabosky, *Electronic Crime* (2007) 74. Brown Christopher, *Computer evidence: collection & preservation* (1st ed, 2006) 16. Peter and Brown Christopher depicted three scenarios in which a defendant can challenge digital evidence integrity. First, the defendant denies that he is the person who was involved in the commission of the crime (it wasn't me; it was somebody else). Second is where the defendant might challenge the integrity of the evidence. Third, the defendant might claim that the computer program which produced the evidence is unreliable.

and the files were viewed, the files' access time stamps were changed accordingly.[598] The second scenario is more a common one. The defendant might challenge the integrity of the files, claiming that the investigators changed or altered the content of the evidence or that the digital evidence was tampered with.[599]

The first scenario does not focus on the content of the evidence; but on the handling process. It emphasises the importance of not using the original version of the evidence in the forensic process, particularly collection and recovery. For this reason, the forensic investigators must always assure that the original version of the evidence is kept intact and make a mirror image copy of it.[600] The mirror image copy can assist the investigators by showing that the original version of the evidence is untouched and is an exact copy of the original hard drive, and the only material subjected to the forensic examination.

The second scenario encompasses situations in which the defendant argues that digital document contents are altered intentionally or inadvertently or that the duplication of those materials, i.e. the mirror copy, is conducted improperly or incompletely. In either case, however, digital technology provides a critical means for forensic investigators to identify and authenticate digital evidence. Metadata and hash value[601] provide pivotal evidence regarding the evidence integrity. Forensic investigators use them to authenticate and verify its integrity, because they provide precise information that is essential for determining the authenticity of the evidence. [602]

[598] Ibid.

[599] Ibid.

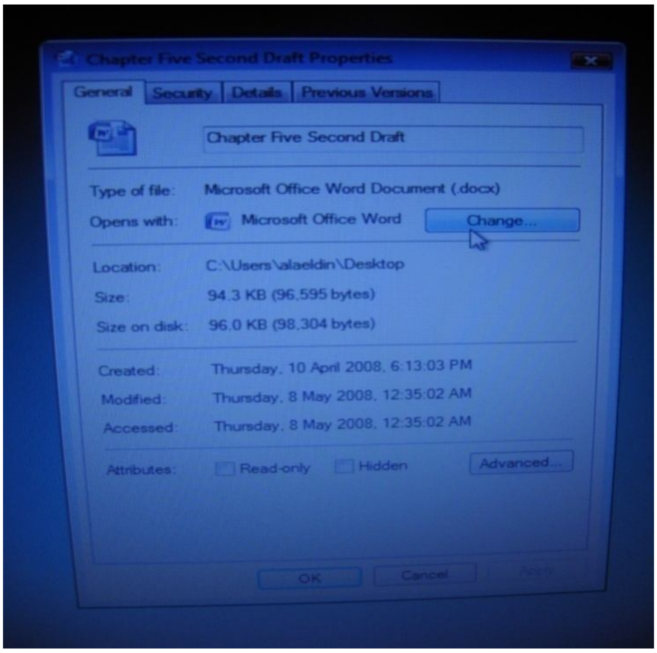
[600] See, eg, Patzakis John, *Maintaining the Digital Chain of Custody,* Infosecurity Europe <http://www.infosec.co.uk/files/quidance_software_04_12_03.pdf> at 2 June 2007. See also, Philip Craiger, *Computer Forensic Procedures and Methods,* National Center for Forensic Science < http://ncfs.org/craiger.forensics.methods.procedures.final.pdf> at 5 May 2008.

[601] Hash value is generated by using an algorithm called a hash algorithm, or hash function. In fact, there are quite a few hash functions, but the most commonly used are MD5, and Secure Hash Algorithm (SHA-1). See, Rashi Gupta, *Windows 2000 Security* (2000) 203. See also, Thompson Eric, 'MD5 Collisions and the Impact on Computer Forensic' (2005) 2 (1) *Digital Investigation* 36, 101-106. See also, Satoh Akashi and Inoue Tadanobu, 'ASIC-Hardware-Focused Comparison For Hash Functions MD5, RIPEMD-160, and SHS' (2007) 40 *The VLSI Journal* 3. Bruce Schneier, *Opinion: Cryptanalysis of MD5 and SHA: Time for a New Standard* (2004)<http://www.landfield.com/isn/mail-archive/2004/Aug/0071.html> at 19 April 2008.

[602] See, eg, Cid Carlos, 'Recent Development in Cryptographic Hash Functions: Security Implications and Future Directions' (2006) 11 (2) *Information Security Technical Report* 100, 105.

Metadata

Metadata is information stored automatically in documents that are prepared with office software programmes, such as Word processors, Spreadsheet, and PowerPoint applications. Metadata information is virtually visible without the use of forensic tools.[603] Figure 6.2 shows an example of metadata information.



Chapter Five Second Draft

Type of file: Microsoft Office Word Document (.docx)

Opens with: Microsoft Office Word

Location: C:\Users\alaeldin\Desktop

Size: 94.3 KB (96,595 bytes)

Size on disk: 96.0 KB (98,304 bytes)

Created: Thursday, 10 April 2008, 6:13:03 PM

Modified: Thursday, 8 May 2008, 12:35:02 AM

Accessed: Thursday, 8 May 2008, 12:35:02 AM

Attributes: □ Read-only □ Hidden

Figure 6.2

Metadata provides vital information about the history of the files since their creation to date, because it describes how, when, and by whom the files was collected, created, accessed, or modified and how it is formatted,[604] and thus all the information needed to identify and certify the scope, authenticity, and integrity of active or archival data.[605] Some examples of metadata are: a file's name, location, format or type, file size, and file dates (for example, creation date, date of last data modification, date of last data access, and date of last metadata modification).[606] This information can be useful to demonstrate whether the digital evidence was contaminated or tampered with after leaving the suspect's possession.

[603] Michael Vahey, *Understanding Metadata CAN Professional Counsel* < http://www.pearlinsurance.com/risk-lawyer/metadata.pdf> at 16 April 2008.

[604] Ibid.

[605] Charles Regan et al, (eds) 'Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age' (Paper presented at The Sedona Conference, September 2007) 29.

[606] Vahey, above n 603.

Hash Value

Hash value (commonly known as hash algorithm or one way function) on the other hand, works like a fingerprint image to authenticate the mirror copy and to determine whether the evidence contained in the copy has been the subject of any improper alteration.[607] Hash value is a short string of random-looking letters and numbers generated by using an algorithm called a hash function, i.e. a mathematical formula used to encrypt and decrypt information, inserted into original electronic documents when they are created to provide them with distinctive characteristics that will prove their authentication.[608] Hence, each digital file has invisible and unique letters and numbers (i.e. 37af194dda37b28f294e982aaa36db37) which function like human fingerprints, so it is impossible to create two different files that have the same hash value.[609] These unique characteristics are embedded and hidden within the original documents, so when law enforcement officers create a mirror copy, the hash value is also copied.

Hash value plays a critical role in computer forensics in providing a means for forensic investigators to prove that the mirror copy in case of authenticity and integrity challenges is an identical to the original copy.[610] For example, if the hash value of the mirror copy matches the hash value of the original copy the mirror copy is authenticated. Thompson pointed out that 'Changing one bit in the evidence will still cause a cascade effect that dramatically changes the… hash result...'[611] This means that a slight discrepancy between the original and mirror copy or two different messages having the same hash value will make the evidence inadmissible because one of the two messages is inauthentic.[612]

Eoghan Casey advised that forensic investigators must take extreme care when creating the mirror copy and must calculate the hash value code of the original disk to

[607] See generally, Joe Kovara and Ray Kaplan, 'Implementing Kerberos in Distributed Systems' in Harold F Tipton and Micki Krause (eds), *Information Security Management Handbook* (6th ed, 2007) 1197, 1251.

[608] See, Gupta, above n 601, 203. See also, Xiaoyun Wang and Hongbo Yu 'How to Break MD5 and Other Hash Functions' (Paper presented at the 24thAnnual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005) 19.

[609] See, eg, Eoghan Casey, above n 428, 219. See also, Steve Anson, and Steve Bunting, *Mastering Windows Network Forensics and Investigation* (2007) 78.

[610] See, eg, Eric, above n 601, 37.

[611] Ibid 39.

[612] See generally, Garretson Cara, *Vulnerable Security Algorithms Raise Concerns* (2005) NetworkWorld <http://www.networkworld.com/news/2005/110105-nist-crypto.html> at 7 May 2007.

demonstrate that the mirror copy and the original version are identical.[613] If a defendant claims that the mirror image created by the forensic investigators has been tampered with and some files have been changed, the forensic investigators can use the hash value to prove that the original data and the mirror copy are identical and no changes happened, because they have the same hash value. For example, the MD5 hash function[614] works as follows:[615]

First, if the original version of the recovered file says: 'I have got different types of legal drugs' the hash value of this document would be:[616]

Original copy: 37af194dda37b28f294e982aaa36db37

Second, once the forensic investigator creates a mirror image copy, the latter and each copy will contain the exact MD5 hash function.

Original copy: 37af194dda37b28f294e982aaa36db37

Mirror copy: 37af194dda37b28f294e982aaa36db37

Third, if the investigator accidentally or deliberately changes the above message by replacing the word 'illegal' with 'legal', the hash value will change accordingly.

Original copy: 37af194dda37b28f294e982aaa36db37

Altered Mirror Copy: 041ad5e8c945959728a57414f520782c

Recently, the usage of the MD5 hash function in different applications, such as in speed cameras, has been brought into question and subjected to court scrutiny, potentially opening the door for challenging the credibility of the MD5 hash value as an authentic

[613] Eoghan Casey, above n 428, 226.

[614] MD5 is a hash function designed in 1994 by cryptographer Ron Rivest as an improvement on MD4. MD4 and MD5 are part of a series of algorithms used to secure digital signature applications, password protection and information authentication. In 1993, the National Security Agency published a hash function very similar to MD5, called the Secure Hash Algorithm (SHA). Then, in 1995, citing a newly discovered weakness that it refused to elaborate on, the NSA made a change to SHA. The new algorithm was called SHA-1. Today, the most popular hash function is SHA-1, with MD5 still being used in older applications. See generally, Gupta, above n 601, 203. See also, Eric, above n 599, 101-106. Akashi and Tadanobu, above n 599.

[615] See specially, Moore, above n 597.

[616] The author used the File Format Info website to compute the hash value. See, *Hash Function,* <http://www.fileformat.info/tool/hash.htm> at 21 April 2008.

source for evidence integrity.[617] In Australia, for example, in *Roads and Traffic Authority v. McNaughton*, the defendant's lawyer filed a motion to suppress digital evidence produced by a speed camera on the ground that the MD5 algorithm used to authenticate the evidence was weak.[618] The Hornsby Court dismissed the charge because the Road Traffic Authority (RTA) failed to find an expert willing to testify that the photos had not been tempered with.[619] By contrast, in *Bursleon v. United States,* the court determined that the evidence was authentic because, among other things, the programme or the system which processed the documents (the evidence) was known to be trustworthy and reliable within the computer industry.[620]

After the Hornsby Local Court decision, Tony Morris, Security Software Engineer, commented:

> … it is quite clear from some of the comments of both the defence and prosecution that neither really understands what a hash algorithm is…speed camera photographs are typically associated with MD5 hash in a flawed attempt to verify integrity of the photograph. That is to say, in transit from the camera to your letter box, integrity of the document can be (but isn't) guaranteed, since any modifications of the document would mean that a different MD5 hash is generated upon verification.[621]

Morris's comment highlights two critical points. The first is that prosecutors lack the skill, experience, and understanding necessary to effectively support hash value role in authenticating evidence. Unfortunately, this lack of expertise will open the doors for more failed prosecutions. Law enforcement, therefore, should be provided with the necessary tools and experts to defend hash value and prosecutors and Judges provided with a precise picture of how and why hash value technology is impregnable or breakable and whether it can be trusted to provide probative evidence.

[617] See, eg, Nicholls Sean and Needham Kirsty, *Speedsters Rush For the Fines Exit* (2004) FairfaxDigital <http://www.smh.com.au/articles/2004/11/17/1100574541050.html?from=moreStories> at 6 May 2007.

[618] See, eg, Brown RFD Roger, 'So You Think Traffic Offences Are Simple? Camera-Detected Offences in NSW' (2006) 30 (5) *Criminal Law Journal* 302, 303. See also, Starkoff's David, *MD5 and the Law* (2005) <http://www.dbs.id.au/blog/law/md5-speed-cameras.html> at 2 May 2007.

[619] Ibid.

[620] See, eg, Robet L Levy and Patricia L Casey, *Electronic Evidence and the Large Document Case: Common Evidence Problems* (2003) Haynes and Boone LLP <http"//www.haynesboone.com/FILES/tbl_s12PublicationsHotTopic/PublicationPDF60/1057/06_01_2003_Levy-Casey.pdf> at 23 April 2007. See also, Eoghan Casey, above n 428, 173-174.

[621] Tony Morris, *MD5 and Speed Camera* (2006) < http://tmorris.net/> at 19 April 2008.

The second point is that the hash value's impregnability is controversial. The controversy stems from a difference in opinions concerning the impregnability of the hash value technology. As mentioned above, law enforcement officers rely largely on hash value to authenticate digital evidence and, therefore, it is important to assess the current state of the hash value impregnability.

There are two different attitudes towards hash value. The majority of forensic scientists argue that the hash value technology is very accurate, secure and is considered unbreakable. Kruse and Heiser, argue that the MD5 hash function is as accurate, if not more accurate than DNA testing.[622] According to Eric '…MD5 can still be relied upon by the forensic community to do an excellent job at identifying even the smallest change in electronic data'.[623] Bruce Schneier, a renowned computer security expert, stated:

> …that it's easy to take a message and compute the hash value, but it's impossible to take a hash value and re-create the original message. (By "impossible," I mean "can't be done in any reasonable amount of time.") Two, they're collision-free… This means that it's impossible to find two messages that hash to the same hash value... [624]

According to this group of scientists, the level of algorithm that is utilised to produce MD5 hash function is impregnable to attack with the current technology, because computers are not yet powerful enough to break it successfully.

On the other hand, a group of experts from Shandong University in China and the Israel Institute of Technology announced that they have developed new methods which are able to break the MD5 hash value.[625] This means that creating two different documents that have the same hash value keys is possible, and therefore, experts can alter the mirror copy by creating an identical hash value.[626] This group, however, did not divulge the methods used to break the MD5 hash value, but they developed a theoretical

[622] Kruse and Heiser, above n 437, 89.

[623] Eric, above n 601, 39.

[624] Schneier, above n 601.

[625] Wang and Hongbo Yu, above n 608, 20. See also, Eli Biham et al, Collisions of SHA-0 and Reduced SHA-1, Paper presented at the 24thAnnual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005) 38. Xiaoyun Wang et al, *Collisions for Hash Functions MD4, MD4 Haval-128 and RIPEMD* (2004) International Association for Cryptologic Research <http://eprint.iacr.org/2004/199.pdf> at 6 May 2007.

[626] Ibid.

conception.[627] Schneier opined '…no one is going to be breaking digital signature or reading encrypted messages anytime soon with these techniques. The electronic world is no less secure after these announcements than it was before'.[628] While this opinion does not deny that hash value technology is not unbreakable, it does provide the sort of overview that helps identify the technology's potential weakness, its obsolescence. Hash value technology is prone to become obsolete in a relatively short period of time due to newly emerging technology and, therefore, the role of hash value in authenticating digital evidence should be subject to judicial review to decide whether the hash value algorithm adequately sustains data integrity. In a similar manner, the metadata information should be subject to judicial review in relation to its integrity.

6.3 Admissibility of Digital Evidence

Evidence law encompasses three key concepts: burden of proof, relevance, and admissibility. On one hand, 'the burden of proof concept means the necessity or duty of affirmatively proving or disproving a particular fact or facts in dispute on an issue raised between the parties in a case'.[629] Meanwhile, relevance means 'evidence having the tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence'.[630] Therefore, relevance has been described as the password for all evidence[631] because it affects the assessment of the probative value of evidence in the proceeding.[632] In the context of cybercrimes, the two concepts are applied to digital and physical evidence alike, because in the former the prosecutors are the ones who carry the legal burden of proving all facts essential to their case. This role will not be affected by the nature of evidence, such as a physical or digital document. In a similar manner, the relevance of evidence is assessed by a judge regardless of the nature of evidence.

Evidence admissibility, on the other hand, is actually a two-step process, legislative, i.e. a law addressing admissibility, and judicial, i.e. judges admit reliable evidence. It begins

[627] See, eg, Kaminsky Dan, *MD5 To Be Considered Harmful Someday* (2004) <http://www.doxpara.com/md5_someday.pdf> at 17 May 2007. See also, Tony Morris, *MD5 and Speed Camera* (2006) <http://tmorris.net> at 19 April 2008.

[628] Schneier, above n 599.

[629] Jeremy Gans and Andrew Palmer, *Australian Principles of Evidence* (2004) 29.

[630] Ibid 132.

[631] Robert Woody, *The Law and the Practice of Human Services* (1984) 13.

[632] *Uniform Evidence Legislation* s 55(1).

with legal provisions that lay down the type of evidence which may or may not be accepted. In the second step, the accepted evidence will be subject to scrutiny by a judge to determine its probative value. The various types of physical evidence, such as fingerprints, weapons, or blood are fully scrutinised by courts to assure admissibility; on the other hand, digital evidence is neither comprehensively addressed by legislation nor fully evaluated by the judiciary. This situation varies a lot from one country to another; hard drives, Internet files, and e-mail as courtroom evidence are increasingly coming into more frequent use in courts in Australia and the USA, whereas in Jordan, its admissibility is yet to be scrutinised. However, Jordanian legislation addresses various aspects of digital evidence.

This section is divided into two main subsections. The first surveys and analyses laws passed to address digital evidence admissibility in a courtroom. The second section examines the judiciary's role in admitting digital evidence.

Legislatures have addressed specific aspects of digital evidence despite that fact that there are various types of digital evidence that are subject to discovery in cybercrime investigations. This subsection is divided into three parts. The first distinguishes between the different types of digital evidence, and the second surveys the legal responses of Jordan, Australia, and the USA, and the final part analyses the legal responses.

6.3.1 Digital Evidence Types

The US Department of Justice (DOJ) categorises digital evidence into two forms;[633] meanwhile forensic experts categorise digital evidence into three forms.[634] According to the DOJ's manual, the first is computer generated evidence, such as log files, cookies, metadata, IP addresses, and so on.[635] This evidence comes in multiple formats, data and programmes, including e-mail, websites, chatting programmes, etc.[636] It needs particular multimedia devices to be presented to the court, such as streaming video and audio. The

[633] Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002) United States Department of Justice < http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm> at 28 October 2004.

[634] Erin E. Kenneally, 'Digital Logs-Proof Matters' (2004) 1 *Digital Investigation* 94, 95. See also, Orin Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 *Columbia Law Review* 279.

[635] Computer Crime and Intellectual Property Section, above n 633.

[636] Ibid.

second is computer stored evidence, such as digital photos and Word files.[637] This form can be printed out as a hard copy or visually displayed on a computer screen. Some legal scholars, however, divide digital evidence into three forms, computer generated evidence, computer stored, and hybrid.[638] They differentiate between them from different points of view. Orin used a human being's involvement in the process of producing digital evidence as a guiding principle to differentiate between computer generated and computer stored evidence.[639] He pointed out that while the latter requires some person to interfere with the computer programmes to create the digital evidence, such as word processing files, the former is generated without human interference from the time the programme operates until it generates the evidence, such as metadata, cookies, and so on.[640] The third category is evidence that is a mixture of both computer generated and computer stored evidence.[641]

Digital evidence should be differentiated on the basis of the level of volatility and integrity. As discussed earlier, cybertrails take three different forms, and each form has its own particular aspects. These aspects can provide a good basis to distinguish between two types of digital evidence. The first type is generated directly by computers and the second is generated by human commands. Computer generated evidence is virtually visible, but is not printable, such as log files, the history of web site visits, and metadata. This form requires special forensic tools to collect, examine and present in courts, because it is fragile and needs intensive, careful treatment. While this type of evidence might provide more accurate data, because there is no human interference during its establishment, it should be scrutinised more carefully to ascertain that there is no contamination at any stage of the evidence collection and examination process. The second type is visible and printable, such as e-mails, Word files, Excel spreadsheets or PowerPoint slides, and digital pictures. This form of digital evidence can be printed out exactly as it appears.

This classification is important for two reasons. First, it shows the extent to which current legislation is able to address digital evidence. Second, it makes it easier for a legislature to comprehend and address the whole while also understanding what is

[637] Ibid.
[638]Kenneally, above n 634.
[639]Kerr, above n 634.
[640] Ibid.
[641] Ibid.

distinctive about each form. Jordanian legislation, for example, neither classifies digital evidence nor addresses evidence forms; however, different laws have addressed particular types of digital evidence. The *Electronic Transaction Law* 2001 explicitly addressed three specific types of digital evidence, electronic records, contracts and electronic signatures. These types can be either computer generated or computer stored evidence.

6.3.2 Survey of Legal Responses

Due to the increasing use of computers, and the subsequent need to admit different forms of digital evidence, legislatures have begun to recognise the importance of digital evidence and its admissibility. In many countries, such as Australia and the USA, different forms of digital evidence are frequently presented to courts and the frequency is expected to increase as Internet usage continues to grow. Legislatures, therefore, have been attempting to keep up with changes in technology by constantly enacting new laws or revising already existing laws. The situation in Jordan is similar, but not exactly the same, as the digital evidence usage, and frequency of cybercrime prosecutions is lower than in both Australia and the USA.

a) Jordan

Similar to cybercrime criminalisation, digital evidence admissibility is scattered in a variety of statutes, the *Electronic Transaction Law* 2001, *Credit Information Law* 2003, *Banking Law* 2000, *Evidence Law* 1952 and *Criminal Procedure Law* 1961. Although these laws recognise all types of digital evidence, each describes specific situations in which digital evidence might be admitted at trial.

The *Electronic Transactions Law* 2001, which is considered a special statute that applies to transactions conducted by electronic means, addressed particular types of digital evidence that courts may admit.[642] It stipulates: 'Electronic, records, contracts, messages and signatures shall be deemed to produce the same legal effect as written documents…' Accordingly, digital records, contracts, and signatures are the only three

[642] *Electronic Transaction Law 2001* (7) (a).

types of digital evidence which are admissible. Article 2 lays down what is considered digital evidence within the meaning of the Act. It defines electronic record as a contract or message generated, sent, received, or stored by electronic means. Also, it defines electronic contract as an agreement that is formed by electronic means; meanwhile, electronic signature is any letters, characters, numbers or other symbols in digital form that a person has created or adopted in order to sign a document.

In the context of credit information disputes, the *Credit Information Law* addressed both computer generated and computer stored evidence. According to article 31 (a), the parties are able to support their claims by providing computer generated evidence and electronic data. In a similar manner, Article 92 (b) of the *Banking Law* authorises the parties in banking disputes to present evidence including electronic data and computer generated evidence.

The existing rules of the *Evidence Act* 1952 and *Criminal Procedure Law* 1961, which together regulate methods of proof and physical evidence, can be applied in a limited fashion to digital evidence. The *Evidence Law* 1952 treated e-mails, and computer printouts, i.e. computer stored evidence, as original documents and, therefore, admissible unless they are uncertified or unauthenticated.[643] The *Criminal Procedure Law* on the other hand, did not address the admissibility of digital evidence. It enacted one very broad provision on this topic. Article 147/2 provided judges with discretionary power to admit any relevant evidence which it deems to have probative value.

b) Australia

In Australia, legislatures have responded positively to the growing importance of digital evidence and some courts (for example, Supreme Courts in New South Wales and Victoria) have issued practice notes encouraging litigants and lawyers to use technology in civil litigation.[644] Certainly, this practice was adopted after it was decided that digital evidence could be admissible. The law of evidence in Australia, however, is a mixture of common law and statutes that establish the rules concerning evidence admissibility. As a consequence, there are differences in addressing digital evidence.

[643] *Evidence Law 1952*, amended by the *Evidence Law 2005* s 13 (3) (a) and (c)

[644] Ainslie Lamb, and John Littrich, *Lawyers in Australia* (2007) 114.

At the federal level and in some States, courts apply the Commonwealth *Evidence Act* 1995 and the *Uniform Evidence Act* 1995. Federal courts including courts in the Australian Capital Territory apply the Commonwealth *Evidence Act*; meanwhile, New South Wales (NSW) and Tasmania apply the *Uniform Evidence Act.* These statutes are substantially the same, but not identical.[645] However, they are identical in terms of digital evidence admissibility. The Commonwealth *Evidence Law* 1995 encompasses three basic principles as part of its goal to ensure that digital evidence is admissible.[646]

First, it has broadly defined 'document' to encompass digital evidence. It defines document as any record of information, including '... (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else…'.[647] Second, this definition needs to be coupled with that contained in section 48 of the legislation, which provides a mechanism in which specific methods must be used to render the document's content. One of these methods, which is particularly useful for digital evidence, is to use a device to retrieve the stored information, such as a computer.[648] As a result, digital evidence would be classed as a document, because it needs a qualified person, i.e. forensic experts and a particular device to render its content. Third, Section 51 abolished the 'best evidence rule'. This rule had two negative aspects: (1) it required that the original version of the document should be produced unless an exception applies, such as the original has been lost; and [649] (2) if the copy is admitted, then it will have a low probative value, because it is difficult to prove that the content of the document has not been tempered with.[650] Thus, the best evidence rule used to enable a party in litigation

[645]See, Australian Law Reform Commission, *The Uniform Evidence Act 1995* (2004).

[646] Ibid.

[647] *Evidence Act 1995* (Cth) div 1 S 3.

[648] *Evidence Act 1995* (Cth) s 48.

[649] Some of these exceptions are: (1) the court is satisfied that the original document has been lost or damaged. (2) The original document is in the possession or control of the opponent of the party wishing to rely on the document. (3) The document is in the possession of a third party who lawfully refuses to produce it after service of a subpoena for production. (4) Though it is known to be in existence, the production of the original is, for practical purposes, impossible. (5) The production of the original would be highly inconvenient, physically impossible. See, Cameron Ben, 'Admissibility of Electronic Evidence in Australia' (Paper presented at the Using Electronic Evidence in Australia Courts, Sydney, 2000) 12. See also, Arenson Kenneth J and Bagaric Mirko, *Rules of Evidence in Australia: Text & Cases* (2005) 357.

[650] Philip Argy et al, *Electronic Evidence, Document Retention and Privacy* (Paper presented at the Australian Corporate Lawyers' Association (ACLA) NSW Annual Conference, Sydney, 30-31 March 2006).

to request another party to produce the original document. In the realm of digital evidence, this would cause a problem for forensic investigators, because the latter creates a duplicate mirror copy of the original storage device to perform their forensic investigation processing.[651] This duplication is necessary to ensure the integrity of the original copy. Therefore, abolishing the best evidence rule is appropriate as an original document is no longer required and digital copy is admitted into evidence in lieu of an original copy.[652]

In Victoria, Queensland, and South Australia, the *Evidence Act* specifically states that evidence derived from computers will be admissible, subject to certain conditions of reliability. For example, Section 45C of the South Australian *Evidence Act* 1929 permits the judiciary to rely on its own knowledge or on an expert report ('third parties') to assess the nature and reliability of the device that produced the evidence. Furthermore, Section 59B of the same Act is the primary section dealing with the admissibility of digital evidence. It provides that for digital evidence to be admissible in court it must be subject to the court being satisfied that:

1) The computer is correctly programmed and regularly used to produce the same kind of output.
2) The data from which the output is produced is prepared on the basis of information that would normally be admissible as evidence of the statements or representations contained in the output.
3) There is no reason to suspect any departure from the system, or any error in the preparation of the data.
4) The computer has not malfunctioned so as to affect the accuracy of the output.
5) There have been no alterations to the computer that might affect the accuracy of the output.
6) Records have been kept of alterations to the computer.
7) There is no reasonable cause to believe that the accuracy or validity of the output has been adversely affected by the use of any improper process or procedure or by inadequate.

Accordingly, digital evidence is admissible, inasmuch as it meets the requirements set forth in Section 59B.

c) USA

The Federal Rule of Evidence (FRE) provides sufficient grounds for admitting digital evidence at trial. While digital evidence is not explicitly addressed, its coverage can be

[651] Ibid.
[652] Ibid.

inferred, to a high degree of certainty, from the language of the FRE. Several rules under the FRE can be applied to make digital evidence admissible.

First, Rule number 1001 defines evidence content as ‘writing’ and ‘recording’ that consists of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting…mechanical or electronic recording, or other form of data compilation’.[653] The advantage of this wide definition is that it covers the two different forms of digital evidence. Second, Rule number 1003 permits courts to admit a mirror copy to the same extent as an original copy. Third, Rule number 901 provides illustrative examples of evidence authentication.[654] For example, digital evidence can be authenticated by the testimony of witnesses, such as computing experts who testify that the digital data or programmes which are used to process and produce such evidence are trustworthy and the status of presented evidence is the same as when it was collected.

d) Comparative Legal Analysis

Jordanian laws lack comprehensiveness and breadth of scope. On one hand, the *Electronic Transactions Law* 2001 and *Evidence Law* 1952 lack comprehensiveness and demonstrate incomplete understanding of the digital evidence because the *Electronic Transactions Law* 2001 only admitted electronic contracts and messages that are generated, sent, received or stored electronically. Meanwhile, the *Evidence Law* only admitted e-mail and computer stored evidence. As a result, many types of computer generated evidence, such as log files, metadata, and hash value are beyond the ambit of the *Electronic Transactions Law* 2001 or the *Evidence Law*, because they are neither electronic contracts, nor messages in the meaning of the *Electronic Transactions Law* 2001. On the other hand, while the *Credit Information Law* 2003, and *Banking Law* 2000 admitted the two types of digital evidence (i.e. computer generated and computer stored evidence), their scope and application are narrow, because they are applicable to a limited range of cases, namely, credit information and banking disputes.

In a different manner, while the Jordanian *Criminal Procedure Law* 1961 does not explicitly address certain forms of digital evidence, it permits judges to exercise broad discretion and admit evidence at trial. The broad language of the Article 147/2 grants judges the ability to consider the admissibility of digital evidence. Although this sounds

[653] Martin A Schwartz, and John E Kirklin, *Section 1983 Litigation* (6th ed, 1997) 221.
[654] Ibid.

good in theory, actual implementation and practice are affected by the fact that judges and prosecutors lack the necessary knowledge and training in the field of cyber law and, consequently, they will be hesitant to accept digital evidence. Furthermore, none of the above mentioned legislation addresses the admission of the exact duplicate copy, i.e. a mirror copy, and its probative value.

By contrast, Australian laws amply provide the basis for accepting digital evidence or an exact copy by broadening the definition of what constitutes a 'document' (so as to include different types of digital evidence) and providing judges with guidance for validating digital evidence, such as Section 59B of the South Australian *Evidence Act*. In a similar manner, the FRE lays down rules regarding evidence admissibility. Rule 901, for example, is similar to the Section 59B. It amply illustrates how digital evidence admissibility can be assessed.

The review and analysis of Jordanian laws demonstrate the inadequacies which need to be addressed if legislation is to achieve its objective of admitting digital evidence. The inadequacies are both legislative and non-legislative, in both technology and litigation support, and also education and training. From a legislative point of view, digital evidence admissibility is scattered over a wide range of statutes which lack uniformity and comprehensiveness. Thus, the *Evidence Law* 1952 must be amended to properly accommodate all the forms of digital evidence. It should be revised to recognise computer generated evidence and the exact copy is admitted into evidence in lieu of an original copy. From a non-legislative point of view, courtrooms must be equipped with advanced technological tools and facilities, because they are necessary for digital evidence recognition and presentation. Education and training are needed so that lawmakers and judges fully understand digital evidence.

In Jordan the court system and the judges' knowledge on technological issues including digital evidence features are immature, and are far from meeting the USA or the Australian level. This is because of the rarity of studies addressing cybercrime issues and lack of opportunity to adjudicate cases involving digital evidence.

In the following section the role of judges in accepting and evaluating digital evidence will be examined.

6.3.3 The Role of Judges in Evaluating Digital Evidence.

6.3.3.1 Inquisitorial v Adversarial Legal System

There are two major legal systems in the modern world, namely the adversarial or common law system which was developed in England, and the inquisitorial system which is commonly known as the civil law system, which developed on the continent of Europe. The extent to which judges can be involved in evaluating and assessing digital evidence varies in each system.

Criminal justice systems in most countries have been in a state of flux due to extensive social, economic, and political changes aimed at improving the efficiency and effectiveness of judicial proceedings.[655] For example, some countries have gone through a complete transition from an inquisitorial to an adversarial legal system, Italy, for example.[656] Other countries, such as Jordan, have abandoned Islamic criminal law in favour of an inquisitorial system.[657] In Australia and the USA, the common law prevails because they were colonised by English settlers.[658] The judicial system in both countries

[655] See, Aire, Freiberg, 'Non-Adversarial Approaches to Criminal Justice' (2007) 16 (4) *Journal of Judicial Administration* 205, 205.

[656] Ibid.

[657] The Jordanian judicial system is somewhat unique because it encompasses a combination of both civil and religious courts. Jordan's courts implement an inquisitorial legal system in criminal matters and Shariah law is applied only to personal concerns. The court structure is divided into three divisions: civil, religious, and special courts. The civil courts are four divisions: Courts of First Instance, Courts of Appeal, the Court of Cassation and the High Court of Justice. The Courts of First Instance are subdivided according to their specialty into two sections: the Magistrate's Courts hear minor civil and criminal cases, such as misdemeanour cases, and First Instance Courts hear serious crimes, such as murders and rapes. Decisions of these courts are subject to review by the Courts of Appeal. The Jordanian High Court exercises supervisory jurisdiction over the proceedings and decisions of the inferior courts established by the *Jordanian Constitution.* It is Jordan's highest court and has both original jurisdiction, such as cases against the state, and appellate jurisdiction. The appellate jurisdiction extends to reviewing the decisions of both the civil and special courts. Religious courts are two types: Shariah courts and non-Muslim tribunals. Shariah courts in Jordan are divided into two sections: Shariah courts and the Appeal Court. Shariah courts adjudicate personal status matters, including disputes in relation to Islamic property (Waqf), inheritance, and child custody. Decisions of these courts are subject to review by the Shariah Courts of Appeal. In a similar manner, the non-Muslim tribunals are allowed to adjudicate in all matters of personal status except criminal cases. Special courts (also known as State Security Courts) are courts exercising jurisdiction over all crimes against the country's national security, such as armed insurrection, financial crimes, drug trafficking, slandering the royal family, crimes involving the possession of weapons and explosives, and conspiracy. Decisions of these courts are subject to review by the Court of Cassation. See, Jordanian *Criminal Procedure Law* div 8 sec 2 260 (1). Jordanian *Shariah Procedure Law* s 2. See also, Jordanian Courts, the Ministry of Justice Official Website <http://www.moj.gov.jo> at 3 May 2008.

[658] See, eg, Max Rheinstein, Common Law and Civil Law: An Elementary Comparison, Rev J UPR (1952-1953) 91.

is almost the same,[659] because they share a common legal inheritance as former British colonies and both countries are federations. The colonial heritage is manifest in the implementation of the adversarial legal system and courts structure.[660]

Although there are significant differences between the inquisitorial and adversarial systems, they converge in a very specific situation.[661] Historically, the inquisitorial system has been established predominantly based on codes, statutes, and legislation.[662] Meanwhile, the adversarial legal system has been based on judicial decisions, i.e. case law and precedents,[663] and, therefore, adversarial judges enjoy more discretion than their civil law counterparts and exert somewhat more judicial authority.[664] For example, judges of the inquisitorial legal system merely apply the laws created by legislatures for particular cases; while judges of the adversarial system take fact patterns, look to applicable statutes and have broad discretion to apply a measure of judicial authority in deriving the final decision of the court.[665] In the adversarial system, the discretion of the judges is fettered by judicial precedent, whilst in the inquisitorial the judge is unfettered by previous decision, and therefore judges are free to accept or reject the views of their superiors, but practically they feel impelled to adhere to judicial precedents that have been set down by the superior courts, because they know that their decisions are subject to appeal before the superior courts.[666]

6.3.3.2 Judges' Role in Accepting Digital Evidence

In his article 'Towards a Law and Technology Theory' Cockfield has identified two distinct approaches used by courts when dealing with technological changes that

[659] Gary D Meyers and Nerida Gilbert, *Primary Sources: A 'Not-So-Anonymou' Review of US Legal Research Materials and Sources* (2003) Research for Lawyers< http://www.research-one.com.au/primary+sources+a+not-so-anonymous+review+of+us+l.aspx> at 1 May 2008.

[660] For example, in both countries a similar court system exists. The Australian High Court and the United States Supreme Court are the highest courts. These courts have both original jurisdiction, such as cases against the state or disputes between residents of different states, and appellate jurisdiction. The appellate jurisdiction extends to reviewing the decisions of federal courts and state and territory Supreme Courts of appeal. Ibid. See also, Legal Information Access Centre (LIAC) <http://www.austlii.edu.au/au/other/liac/hot_topic/hottopic/2002/3/2.html> at 5 May 2008.

[661] Kristi Kernutt, Civil Law v. Common Law Systems: Are They So Different? *Oregon Review of International Law* 1 (1999) 31.

[662] See, Peter De Cruz, *Comparative Law in a Changing World* (3rd ed, 2007) 46.

[663] Ibid 48.

[664] Ibid.

[665] Kernutt, above n 661.

[666] See, eg, Rheinstein, above n 658, 96.

challenge traditional laws. One is a rigid and backward-looking response, and the other is a more forward-looking and flexible analysis.[667] He opined that:

> some legal analysts employ a forward-looking approach that considers how the law can best protect interests and values when they are threatened by technological developments…legal analysis can also be more 'conservative' in the sense that it emphasises the need to follow traditional doctrine without fully taking into account how the interplay between law and technological developments can undermine interests and values.[668]

In Jordan, Australia, and the USA, the authority of the courts to accept evidence varies and to a large degree is restrained by the limits described in their legal system.

a) Jordan

While the law precisely defines offences and punishments, it gives the judiciary the power to assess and admit evidence on a case-by-case basis. The inquisitorial legal system of Jordan grants judges in criminal cases more leeway to exercise discretion than the adversarial system does. The *Criminal Procedure Law* 1961 provides judges with the right to invite and question experts to permit the admission of evidence. Article 162/2 of the *Criminal Procedure Law* 1961 states: 'A judge has the authority and discretion to order the litigants to disclose any evidence and/or call any witness necessary for the hearing'. Furthermore, Article 147/2 of the same Act stipulates that '[t]he presentation of evidence in criminal proceedings is unfettered by the ordinary rules of evidence and a judge adjudicates according to his own discretion'. Accordingly, judges have the authority to take steps to investigate crimes and order the parties to release evidence. In addition, the *Criminal Procedure Law* 1961 provides judges with the ability to evaluate evidence without being restrained by the law of evidence which lists only six methods of proof: written document, testimony, judicial evidence, confession, oath, and experience, thereby allowing judges to accept evidence beyond the ambit of this law of evidence.

From the above articles, someone might conclude that a judge's conception and personal knowledge play a vital role in the case of admitting digital evidence. However, the major concern in this field, as mentioned earlier, is the problem of insufficient

[667] See, Cockfield, Arthur J., 'Towards a Law and Technology Theory' (2004) 30 (1) *Manitoba Law Journal* 383, 399

[668] Ibid.

literacy in computers and in information technology, not only among judges, but also among lawyers and prosecutors. Judges, who did not grow up with computers and do not understand the technology and the issues it raises, find that their discretionary power is nullified. In addition, the courts system in Jordan is ill equipped to deal with digital evidence, even at a basic level, as there is neither a level of standardisation for the evaluation of digital evidence, nor a common set of rules for the presentation of such evidence.

b) *Australian and the US*

Under the adversarial legal system, the judge plays the role of a neutral referee and, therefore, his discretion is limited to consideration of the evidence submitted by the parties. He does not conduct his own investigation, so he decides what the parties ask him to decide, and decides only on the basis of the evidence and information presented to the court.[669] Thus, within the adversarial legal system, judges are restrained by the rules of law governing evidence, which determine what evidence is to be admissible in court. The evidence admitted to the court must fulfil two main requirements. The first one is that the evidence must be relevant to the case;[670] and the second, that it must have a significant probative value. However, as discussed in the above section, digital evidence is admissible by the law of evidence, and therefore, the judges are able to assess and admit digital evidence without legal complications.

6.4 Conclusion

In less than one decade, communications technology and personal computers have become not only a part of the conduct of criminal activities, but also part of the evidence in their criminal prosecution. While, investigators, lawyers, prosecutors, and judges, sooner or later, will be confronted with criminal issues involving digital evidence, unique features of digital evidence make the classical laws of evidence inappropriate to some degree.

[669] Ibid.

[670] Article S56 of the *Evidence Act 1995* stipulates, ‘Evidence that is relevant is admissible, and evidence that is not relevant is not’.

Digital evidence is delicate and can be easily contaminated during processing and handling, thereby increasing legal complexity and a tendency towards litigation. New complex scenarios have emerged in which defendants and prosecutors have to do battle over evidence integrity. However, up-to-data metadata and hash value will continue to be the most important keys that enable forensic investigators and prosecutors to both defend and prove digital evidence integrity in a court of law. Therefore, prosecutors and judges should be provided with the latest and most reliable information about hash value and evidence integrity techniques.

Although the most striking feature of Jordanian legislation on digital evidence admissibility is that it is scattered over a wide range of statutes, the lack of comprehensiveness is evident. These laws are either too narrow, restricting judges to accept digital evidence in a particular type of dispute or too broad, for example, *Criminal Procedure Law* 1961 grants judges a wide discretion to accept evidence. This broadness constitutes both the strength and weakness of the *Criminal Procedure Law* 1961. The judge will be able to evaluate and accept digital evidence, but lack of precise provisions and guidance will make the judge much less confident to accept digital evidence. Therefore, judges should be provided with appropriate guidance and training on how to deal with digital evidence in the courtroom.

By contrast, the Australian and the USA legislatures amended the rules of evidence to include digital evidence. The amendment was necessary to bring the classical rules of evidence, such as the Best Evidence Rule into line with information technology developments. Drawing on their experience, the Jordanian legislature must address digital evidence, including the mirror copy, volatility, integrity, and admissibility. It must detail all types of digital evidence and how prosecutors and judges assess them. In addition, courts should be fitted with appropriate visual or computerised equipments that are necessary for displaying or illustrating digital evidence.

7 SEARCHING & SEIZING DIGITAL EVIDENCE WITH A WARRANT

Introduction

There is a significant chasm between Jordan, Australia and the USA in relation to their responses to computer searches and seizures.[671] On the one hand, most law enforcement officers, judges, lawyers, and prosecutors in Jordan are not aware of the extent to which the digital world possibly impacts on search and seizure concepts or of their approach to computer searches. This is because of the significant shortage of published Arabic research on this topic as well as the rarity with which cybercrimes cases are investigated and brought before the Jordanian courts.

On the other hand, Western courts, supported by the majority of legal scholars, have identified that some corners of conventional search warrant concepts, which have been designed to address the search for physical objects, are not effective in addressing cybercrime searches.[672] Therefore, the USA Department of Justice (DOJ) issued *Federal Guidelines for Searching and Seizing Computers.* The purpose of the Guidelines is to provide law enforcement with updated principles and optimal practice in relation to digital searches.[673] In a different but equally effective manner, Australian federal lawmakers amended the *Crimes Act* 1914, in which several provisions concerning searches and seizures of computers, entitled *Law Enforcement Powers Relating to Electronically Stored Data,* have been introduced.

The objective of this chapter is to identify and demonstrate how principles for searching private premises can be applied or amended to succeed in achieving a high level of judicial approval in cybercrime searches. It addresses the fundamental principles and

[671] Legal scholars have distinguished between two different search and seizure circumstances. First are those conducted with a search warrant and, second, are those conducted without a search warrant (the latter will be addressed in the next chapter).

[672] See, eg, Indira Carr, 'Anonymity, the Internet and Criminal Law Issues' in C Nicoll, J E J Prins, and M J M Van Dellen (eds), *Digital Anonymity and The Law: Tensions and Dimensions* (2003) 185, 197. See also, Shinder and Ed Tittel, above n 210, 588. See also, Orin S Kerr, 'Digital Evidence and the New Criminal Procedure' in Jack M. Balkin et al, (eds), *Cybercrime: Digital Cops and Laws in a Networked Environment* (2007) 221, 237.

[673] See, Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, above n 633.

rules of search and seizure set forth under the Jordanian *Criminal Procedure Law* 1961 as applied to searches for evidence stored in digital formats. It deals with the traditional legal concepts of search and seizure as established in the Jordanian *Criminal Procedure Law* compared with Australian and the US patterns. It then explores the fundamental differences between conventional and digital searches and the extent to which the present search and seizure rules are compatible with the digital environment. It critically analyses the conventional rules of search and seizure in the context of digital search and assesses their impact in conducting an effective search and seizure operation.

The classical search and seizure procedures have been crafted to deal with search and seizure of physical objects. The proliferation of personal computers, high capacity digital storage media and high speed network connectivity, confronts law enforcement officers with situations in which applying classical procedures of search and seizure to digital environment could seriously jeopardise evidence admissibility and individual privacy simultaneously.

Accessing computer systems, data files, and networks to obtain digital evidence constitutes interference with privacy of individual and poses a serious threat to individuals' privacy. While a few countries have constitutionally maintained and entrenched individual privacy in the course of search and seizure procedures, others have done this explicitly or implicitly in their statutes. Jordan, Australia and the USA have each addressed search and seizure procedures differently.

Less demanding than Australian and the US laws, Article 10 of the *Jordanian Constitution* stipulates that 'Dwelling houses shall be inviolable and shall not be entered except in the circumstances and in the manner prescribed by law'.[674] The Jordanian *Criminal Procedure Law* 1961, *Terrorism Prevention Law* 2006 [675] and the *Custom Law* 1998 [676] are the main laws which articulate search and seizure requirements. The Jordanian *Terrorism Prevention Law* 2006 and the *Custom Law* 1998 permit the issuance and execution of warrants for certain offences and circumstances mainly related to terrorism and smuggling charges. For example, in the case of suspected terrorist activities, Article 4/A/3 of the *Terrorism Prevention Law* 2006 empowers

[674] *Jordanian Constitution Act 1952* div 2 (10).

[675] *Terrorism Prevention Law 2006* (4) (A) (3) (4).

[676] *Custom Law 1998* (179) (A) (C).

General Prosecutors (GPs) to respond effectively by issuing a search warrant. However as cybercrime falls beyond the scope of the *Terrorism Prevention Law* 2006 and the *Custom Law* 1998, these laws will not be addressed by this research.

In Australia, while a Bill of Rights is not entrenched, the old common law principles offer individuals robust protection against unreasonable search.[677] However, several laws authorise the issue of search warrants. The *Crimes Act* 1914 has been amended to bring it into line with information technology developments, particularly search and seizure issues under the title 'Law Enforcement Powers Relating to Electronically Stored Data'. In addition, and more particularly, the *Spam (Consequential Amendments) Act* 2003 has empowered law enforcement to execute search and seizure of computer systems, whether owned by the suspect or by the recipient of the spam.[678]

In the USA, the constitution and classical statutes were intensively analysed for the purpose of reaching a comprehensive protection of data privacy as well as presenting admissible digital evidence, seeking a reasonable balance between protecting individual privacy and executing successful cybercrime investigations. The Fourth Amendment is the key with respect to search warrant requirements. It stipulates that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

To identity and examine the search warrant requirements and their applicability to digital searches, this chapter will first discuss the basic principles of search warrants and how these can be applied to cybercrimes. The basic principles include definitions, cyber search warrant terminology, thresholds for issuing a warrant, scope of a search warrant, and procedures for obtaining a search warrant. The chapter will then proceed to describe in detail the execution of a search warrant in cybercrime, including who should accompany the officers executing the search warrant and what should be searched and seized under the search warrant. Second, the chapter will review the search warrant requirements that were designed to address issues unique to physical object searches,

[677] See, Keith Tronc, Cliff Crawford, and Doug Smith, *Search and Seizure in Australia and New Zealand* (1996) 13.

[678] *Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation* (2004) Electronic Frontiers Australia < http://www.efa.org.au/Publish/efasubm-ssbc-search2004.html> at 9 December 2004.

including probable cause, search warrant particularity, and search location. It compares and contrasts the law and judicial applications relating to the search and seizure of digital materials in Jordan, Australia and the USA.

7.1 Definition of a Cyber Search Warrant

Normally, when a crime is committed, police officers and investigators start with the evidence. They enter private premises, search items, seize evidence, arrest, interrogate, and detain suspects. Before entering and searching, however, police officers must obtain permission known as a search warrant from a designated competent authority.[679] The search warrant should be sought and instructed upon the commission of a crime and after an accusation against a person has been substantiated or when strong evidence suggests that the search will substantially discover specified items that are important to an ongoing investigation.[680] It is a coercive power authorised by the law for the sake of the public interest and as an exception to the legitimate rights of citizens to preserve their privacy in order to discover evidence of crime.[681] Therefore, it is not enough to obtain a search warrant for an imminent crime or in case of mere suspicion.

7.1.1 Search Warrant Definition

The definition of a search warrant helps explain the scope and boundaries of investigation procedures. Therefore, the doors are open for legal scholars and judges to define a search warrant. One scholar, for example, has defined a search warrant as ‘a search in a private place for discovering hidden things important to the investigation being made’.[682] Gino defined it as ‘a written document that represents judicial authorisation for peace officers to enter and search a specific place for specific items and to seize those items that are evidence to the offence, if they are found’.[683] Another definition is a ‘search warrant is a document to search a private place for evidence’.[684]

[679] See, eg, Graham Parker, *An Introduction to Criminal Law* (1977) 357.

[680] See, eg, James R Acker and David C Brody, *Criminal Procedure: A Contemporary Perspective* (2nd ed, 2004).

[681] قدري عبدالفتاح الشهاوي, *Search Disciplines in the Egyptian Law: Comparative Study* (Alaeldin Mansour Maghaireh trans, 2005) [trans of:ضوابط التفتيش في التشريع المصري والمقارن].

[682] أمل عبدالرحمن عثمان, *Criminal Procedure Law Explanation* (Alaeldin Mansour Maghaireh trans, 1975) [Trans of: شرح قانون الاجراءات الجنائية].

[683] Gino Arcaro, *Basic Police Powers: Arrest and Search Procedures* (3rd ed, 2003) 222.

[684] Ibid.

In the USA, Freedman has defined a search warrant as 'an order signed by a judge or a magistrate that authorises police officers to search for specific objects or materials at a clearly defined location at a specific time'.[685] Freedman's definition highlights the three important aspects of a search warrant, specificity of the items to be sized, the location, and the time of the search execution, although not its general purpose. The Supreme Court defined a search warrant as 'government action that violates an individual's reasonable or legitimate expectation of privacy'.[686] The definition focuses only on the ramifications of the invalid search warrant, the violation of individuals' privacy.

The definitions provided above should not be considered inclusive or comprehensive enough to account for all circumstances. They do not make a distinction between search warrants and electronic interruption and surveillance. In addition, they consider the warrant authorises the search for and seizure of tangible items. Therefore, cybercrime search warrants should be defined quite separately.

7.1.2 Cybercrime Search Warrant Definition

In the context of cybercrime investigations, no legal scholar or judicial body has defined a cybercrime search warrant. Although different legal issues related to cybercrimes search warrants have been addressed, such as search execution practice, search location, and so forth, no specific attention has been given to its definition. The essence of a definition of cybercrime search lies in the particularity of the search and its unique nature. The definition submitted here is that a cybercrime search warrant is 'an order, signed or authorised by a Judge or a General Prosecutor that authorises a Cybercrime Unit's executing officers to search on-site or off-site for digital media for specific data at a clearly defined digital location'.

The suggested definition shows the unique nature of cybercrime and has three positive features. First, the search could be authorised without need for a signature. This is an important requirement as cybercrime needs immediate action because evidence is extremely fragile and easily tampered with. Thus, a cybercrime search warrant can be

[685] Freedman Edwards H, 'Search and Seizure of Computer Equipment' (1999) 8 (3) *Information System Security* 10, 11.
[686] Orin S Kerr, 'Search and Seizure in a Digital World' (2005) 119 *Harvard Law Review* 531, 549.

obtained by phone, telex, facsimile, e-mail, or other electronic means. Second, the search must be conducted by highly experienced officers who are Cybercrime Unit personnel and can handle the evidence properly. Third, the definition protects individuals' privacy by restricting the boundaries of the search. It requires the officers preparing the search warrant to specify the file format or extension (such as doc, gif, mpg, txt, exe, html, mp3, and others) or to nominate a keyword search or file names, or to search an Internet application (such as IRC logs, e-mail messages, and data found on the Internet). Nonetheless, this specificity does not preclude a certain level of generality, in case a precise description is not attainable.

7.1.3 Cyber Search Warrant Terminology

Another issue which should be considered is the terminology that should be used exclusively to refer to cybercrime search warrants. In the context of a traditional search, the terminology 'search warrant' is used to refer to all sorts of searches. Conversely, in the context of cybercrime, several terminologies refer to cybercrime search warrants are being used. 'Digital search warrants',[687] 'computer-related search warrants',[688] and 'electronic search warrants',[689] for example, are often used interchangeably. Any of them can be used to describe a cybercrime investigation and to distinguish between a conventional search warrant and a cybercrime warrant. However, it is suggested that the preferred terminology should be 'computer search warrant' as, in some cases the search warrant is prepared to search for both physical items and computer data and 'cyber search warrant' only for searching for intangible items.

[687] See, Kerr Orin S, 'Search Warrants in an Era of Digital Evidence' (2005) 75 *Mississippi Law Journal* 85, 94.

[688] See, David E Clark, *Computers, Search Warrants, and the Private Papers Exemption* (2008) SelectedWorks <http://works.bepress.com/david_clark/1/> at March 2008.

[689] See, Clayton Northouse, 'Providing Security and Protecting Liberty' in Clayton Northouse (ed), *Protecting What Matters* (2006) 3, 11.

7.2 Privacy Protection

Individual privacy is maintained historically by respecting private premises.[690] However, confidentiality, privacy, or secrecy can be preserved in different places and containers, such as in private property, boxes, drawers, and so on, and in different conventional formats, such as hardcopy documents, or unconventional formats, such as digital documents. Indeed, nowadays, most people are switching to digital formats to save their confidential data, including e-mails, personal records, medical information, and other confidential data. Consequently, information technology has deepened the concern over privacy,[691] because the ability of law enforcement agencies to collect, classify, exchange and process personal information has significantly increased. As a result, restrictions associated with search warrant issuance must be adhered to.

Search warrant restrictions, such as scope, location and reasonable cause requirements, are meant to protect individual privacy from unreasonable search and seizure.[692] Restrictions force investigators to search and seize only the items listed in the search warrant and ensure that the items identified in the warrant are properly related to the crime committed. Conventional search warrant issuance imposes obligations upon investigators who prepare the affidavit and execute the warrant. These obligations are either embedded in legislation or outlined by judicial authorities. In *Parker v Churchill,* Burchett J said:

> … what is required by law is that the justice of the peace should stand between the police and the citizen, to give real attention to the question whether the information proffered by the police does justify the intrusion they desire to make into the privacy of the citizen and the inviolate security of his personal and business affairs.[693]

[690] Many countries' constitution, including Jordan, and the USA declare and acknowledge the right of individuals to privacy and free from unreasonable searches and unlawful seizure. Article Ten of the *Jordanian Constitution* and The Fourth Amendment of the *USA Constitution* for example, have been crafted to protect individuals from invasion into their personal life and warrantless search.

[691] See, eg, P A Nixon et al, 'Security, Privacy and Trust Issues in Smart Environments' in Diane J Cook, and Sajal K Das (eds), *Smart Environments: Technologies, Protocols, and Applications* (2005) 249, 256.

[692] Debra Littlejohn Shinder, and Michael Cross, *Scene of the Cybercrime* (2nd ed, 2008) 216.

[693] Queensland Law Reform Commission, *The Role of Justice of the Peace in Queensland*, Report No 51 (1998) 50.

The ultimate objective of these obligations and conditions is to protect the freedom of individuals in their homes or premises from illegal searches and seizures. Indeed, search warrant regimes create a balance between privacy protection and crime detection requirements.[694] As one commentator has pointed out 'search warrants are necessary in modern society; but courts strive to balance the competing interests of the citizen to the inviolability of his home or premises and of the state to prevent the commission of crime or to obtain evidence in aid of the prosecution of offenders'.[695] In order to find a balance between privacy protection and crime detection, legislators have set out several conditions to be fulfilled before the court or the GP issues a conventional search warrant. These conditions concern the threshold for search warrant issuance, the substantial search rules, and the subject matter of the search.

7.3 Threshold for Issuing a Cyber Search Warrant

Search warrants are prepared and issued for investigating different types of felonies and misdemeanours.[696] Investigating officers must obtain a warrant to search a cyber location and seize digital evidence. This warrant must be obtained after the officers present an affidavit to a competent authority[697] or obtain oral permission from a GP, who authorises the search.[698] However, a high threshold has to be met before a magistrate or GP authorises a search warrant. Although there is no particular system or specific guidance for issuing cyber search warrant, a conventional search warrant may be obtained by a police officer to search for digital evidence. Conventional search warrant issuance entails meeting three conditions. The authorities responsible for issuing search warrants might not authorise a search warrant unless they are satisfied by the information provided and the supporting evidence that is laid before them that the three elements are met.

[694] See, eg, Robert Hayes, and Micheal Eburn, *Criminal Law and Procedure in New South Wales* (2nd ed, 2006) 507.

[695] Standing Committee on Justice and Community Safety, Legislative Assembly for the Australian Capital Territory, *Incorporating the Duties of a Scrutiny of Bills and Subordinate Legislation Committee* (1999).

[696] *Cf Hart v. Commissioner of Australian Federal Police* (2002) 392 FCR 384. The court said '…the purpose of search and seizure provisions is to provide for the gathering of information to determine whether offences have been committed ...'

[697] See, eg, Parker, above n 679, 357. In Jordan, the competent authority which issues the search warrant is the General Prosecutorial Department.

[698] *Criminal Procedure Law 1961* div 2 s 4 (33).

a) Jordan

Division 4 of the *Criminal Procedure Law* 1961 sets out a statutory framework governing powers of search and seizure. It lists the following requirements for obtaining search warrant.

First, a crime must have been committed.[699] Thus, a GP must have reasonable grounds for believing that a crime has been committed and is not merely imminent.[700] Furthermore, the search should be for evidence-gathering, rather than crime prevention.[701] An exception, however, can be found in a case where the crime is against the national security of Jordan,[702] such as cyberterrorism. Article 108 of the *Criminal Law* 1960 considers an attempt to commit a crime against the peace and national security as a complete crime. Therefore, a warrant can be issued to search a computer based on mere allegations of a national security threat.

Second, the crime committed must be a felony or criminal misdemeanour.[703] The *Criminal Law* of Jordan classifies offences into three categories:

1) Felonies, punishable by three years or more of imprisonment, or by death.[704]

2) Misdemeanours, punishable by a minimum of one week in prison to three years, or by a fine not exceeding 200 JD.[705]

3) Petty misdemeanours, punishable by a minimum of 24 hours to one week in prison or by a fine.[706] Hence, to issue a search warrant, a cybercrime must be categorised as felonies or misdemeanours.

Third, an allegation or suspicion of wrongdoing has been made against a particular person.[707] The investigating officers must show sufficient evidence that the person whose premises are to be searched is either likely to be an offender or possesses

[699] كامل السعيد, *Explanation of the Criminal Procedure Law: Analytical Comparative Study* (Alaeldin Maghaireh trans, 2005) [trans of:شرح قانون اصول المحاكمات الجزائية : دراسة تحليلة تاصيلية مقارنه].
[700] Ibid.
[701] Ibid. See also, Jordanian High Court No: 842 1998.
[702] *Jordanian Criminal Law (1961)* div 2 s (1) (108).
[703] قدري عبدالفتاح الشهاوي, above n 681. See also, أمل عبدالرحمن عثمان, above n 682.
[704] *Criminal Law (1960)* div 2 s 1 (14).
[705] *Criminal Law (1960)* div 2 s 1 (15).
[706] *Criminal Law (1960)* div 2 s 1 (16).
[707] كامل السعيد, above n 699, 450.

evidential materials necessary to an ongoing investigation.[708] Sufficient evidence includes the exact location of the place to be searched and evidence to be seized.[709]

b) Australia

In Australia, a search warrant must be obtained from a magistrate or judge.[710] Investigating officers must obtain a search warrant from a magistrate before searching private property. The *Crimes Act* 1914 sets out a statutory framework governing powers of search and seizure. Section 3E lists the following requirements for obtaining a search warrant.

1) Investigating officers must demonstrate that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential materials on the premises.[711]

2) The investigating officers must show sufficient evidence that the person whose premises are to be searched possesses evidential materials.[712]

3) Investigating officers are required to state the offence to which the warrant relates, describe the premises, and the kind of evidential materials to be searched, the time at which the warrant expires and warrant execution time.[713]

c) USA

In a similar manner, investigating officers in the USA must obtain a warrant from a neutral or disinterested judge before entering private property.[714] The Fourth Amendment sets out the constitutional framework within which search warrants are issued. In making a request for a search warrant, investigating officers are required to maintain the following conditions:

1) Investigating officers must demonstrate that there is a probable cause to believe that the premises to be searched contained evidence.[715]

[708] Ibid.

[709] قدري عبدالفتاح الشهاوي, above n 681.

[710] *Police Powers* <http://www.lawhandbook.sa.gov.au/ch10s07s05.php> available at 13 October 2008.

[711] *Crimes Act 1914* S 3E (1).

[712] *Crimes Act 1914* S 3E (2).

[713] *Crimes Act 1914* S 3E (5).

[714] See, eg, Acker and Brody, above n 680, 76. See also, Stephens and Glenn, above n 533, 74. See also, Michael F Brown, *Criminal Investigation: Law and Practice* (2nd ed, 2001) 31.

[715] Michael J Palmiotto, *Criminal Investigation* (3rd ed, 2004) 35. See also, Warren J Sonne, *Criminal Investigation for the Professional Investigator* (2006) 13.

2) Officers must describe the area to be searched, and list the items that they expect to seize.[716]

3) Investigating officers are required to state the name of the officer serving the warrant, the offence to which the warrant relates, a description of the premises, and the kind of evidential materials to be searched for, the time at which the warrant expires, and warrant execution time.[717]

Each of the above legal systems has addressed the search warrant's requirements of probable cause, and scope of the search. In the realm of cyber searches, investigating officers must adhere to the requirements outlined above. But at the same time, the search warrant must be drafted and executed in a way that adequately addresses the particular needs of cybercrime and digital evidence. Therefore, these requirements must be considered by the officer drafting and executing the search.

7.3.1 Probable Cause

Probable cause is the threshold level of suspicion that justifies the issuance of a search warrant.[718] It can be defined as reasonable grounds for belief in the existence of facts that induce police officers to believe that a person is committing a crime, or has committed, or is about to commit, a crime.[719] These things must be established in the affidavit to support the issuance of the search warrant.[720] Investigators must provide sufficient evidence or facts that support the belief that the evidence connected to the criminal activity which is the subject of investigation will be discovered in the house of the suspect. The GP in Jordan and the magistrate in Australia and the USA who grants the warrant must assess the probable cause to determine whether issuing a search warrant is reasonable and necessary for the benefit of an ongoing investigation.

[716] Ibid.

[717] See, Ronald F Becker, *Criminal Investigation* (2nd ed, 2005) 83. See also, Palmiotto, above n 715. See also, Scott, above n 292, 532.

[718] Thomas K Clancy 'The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer' (2006) 75 *Mississippi Law Journal* 193, 193-242. See also, Shinder and Ed Tittel, above n 210, 216.

[719] See, Dennis J Stevens, *An Introduction to American Policing* (2008) 101. See also, Ken Wallentine, *Street Legal: A Guide to Pre-Trial Criminal Procedure for Police, Prosecutors, and Defenders* (2007) 68.

[720] See, eg, Middleton, above n 530, 229. See also, Susan Kreston, 'Computer Search and Seizure Issues in Internet Crimes against Children Cases' (2004) 30 *Rutgers Computer & Tech* 327, 330.

In cybercrime, establishing the reasonable grounds that have induced police officers to believe that a person has committed, or is about to commit a crime, is quite different from establishing grounds for conventional searches. In conventional searches, police officers find no problem in establishing a factual nexus between the items described in the warrant and the physical place to be searched.[721] For example, if police officers received reliable information containing a well-founded indication that a murder crime is being committed, or has been committed, they will be able to prepare an affidavit setting out the crime location and the items to be searched on the basis of which the GP or magistrate will grant the warrant. But if the police officers receive in a similar manner reliable information concerning a cybercrime, investigators must determine the computer's role in the alleged crime[722] and show particularised facts manifesting how evidentiary materials which are intangible are linked to the crime physical location.[723]

The Internet Service Provider (ISP) plays a significant role in providing information to officers establishing a factual nexus between the items described in the warrant and the physical place to be searched.[724] For example, in DoS attacks, investigators will obtain information from the ISP concerning the Internet Protocol (IP) address that identifies the attacker's connection.[725] Upon receiving the IP address, officers will have sufficient proof to establish a probable cause basis for the issuance of the warrant.[726]

However, the nature of cyberspace which knows no physical boundaries cripples investigators' ability to easily establish a factual nexus between the items described in the warrant and the physical place to be searched.[727] This is what is known as the problem of the association between the IP[728] address (for example, 123.45.678.7)[729] of the alleged perpetrator of a crime and his physical location.[730]

[721] Ibid.

[722] See, eg, Becker, above n 717, 446.

[723] See, Terrence Berg, 'Practical Issues in Searching and Seizing Computers' (2005) 7 *Journal of Practical and Clinical Law* 27, 32. See generally, Monique Mattei Ferraro and Eoghan Casey, *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science* (2005) 151.

[724] Ibid.

[725] See Section 3.2.1for more information about DoS and IP addresses.

[726] Obtaining a wrong IP address will lead to searching the wrong physical location. See, Ferraro and Casey, above n 723, 157.

[727] See, eg, Department of Law and Public Safety, *Computer Evidence Search and Seizure Manual* (2000) State of New Jersy < http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf> at 7 October 2004.

[728] See Section 4.4.1 for more information about IP address and crimes associated with it.

[729] An IP address is considered as non-content information and as a result officers can obtain IP addresses without a warrant because it is not protected under the Fourth Amendment. The courts held that there is

The IP address plays a critical role in locating the physical address of the suspects in a wide range of cybercrimes.[731] For example, the IP address was critical in identifying a person who allegedly posted personal details and sexually suggestive comments on the Internet about a woman in the USA.[732] However, this role varies between dynamic and static IP addresses both of which are automatically assigned by Internet Service Providers (ISPs) to their subscribers.[733] For example, subscribers using Dial-Up connection for Internet access are assigned dynamic IP address.[734] The Dynamic IP address offers the users anonymity by providing a temporary IP address to the user's device each time it connects to the Internet.[735] The IP address is terminated and will be assigned to a new user when the first user disconnects from the Internet.[736] In several scenarios, the short life time and mobility of the dynamic IP addresses make capturing the suspect's IP address and his physical location impossible[737] and disable investigators from tracking the physical location of the suspect. For example, if a suspect downloaded child pornography and then disconnected while investigators were conducting an online investigation, the IP address which leads to his physical location will be lost and assigned to a different user. However, a probable cause can be established if the suspect is still online.

A static IP address, on the other hand, is a unique number permanently assigned to a computer device connected to the Internet located in a fixed physical place.[738] For example, subscribers using Broadband Internet access and public bodies such as

no reasonable expectation of privacy in subscriber information provided to a commercial ISP. See, *United States V. Hamvrick*, 55 F 2d 504 (1999). See also, *United States v. Kennedy,* 81 F 2d 1103, 1110 (Kan, 2000). A suspect's account information can be obtained from the ISP, such as subscriber name, a telephone number …etc. This information can be obtained from the ISP based on a subpoena. In the Perez case the FBI located the suspect's physical location after identifying his IP address obtained from the ISP 'Time Warner Cable'. See, *United States v. Perez*, 485 F 3d 735, 738 (5th Cir, 2007).

[730] See, eg, Ferraro and Casey, above n 723, 152.

[731] See, eg, Shinder and Ed Tittel, above n 210, 198. See also, Anthony Reyes et al, *Cyber Crime Investigations : Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (2007) 202.

[732] See, Daniel J Solove, Marc Rotenberg, and Paul M Schwartz, *Privacy, Information, and Technology* (2006) 114.

[733] See especially, Shivendra Panwar et al, *TCP/IP Essentials: a Lab-Based Approach* (2004) 172. See also, Fadia Ankit, *Unofficial Guide to Ethical Hacking* (2002) 74.

[734] See, eg, Ankit, ibid.

[735] Ibid.

[736] See, eg, Matt Bishop, *Computer Security: Art and Science* (2003) 367.

[737] Ibid.

[738] See, eg, Ankit, above n 733. See also, Beryl A Howell, 'Real-World Problems of Virtual Crime' in Jack M Balkin et al (eds), *Cybercrime: Digital Cops and Laws in a Networked Environment (*2007) 87, 103.

schools, universities, libraries, are assigned static IP addresses. These addresses can lead to the names and physical locations of the subscribers. Nevertheless, in several scenarios, there will be a problem in establishing a nexus between the static IP address and the physical location to be searched.[739] The suspect can access the Internet from locations associated with a static IP address, such as from a public library, to communicate with his victim. In such a scenario, unless the suspect divulges information about the computer used, it is hard, if not impossible, for the police to locate the particular suspect and computer used to commit the crime. The investigator will be able to locate the physical location, but the probable cause to search all computers associated with the static IP address would be invalid.

Probable cause has been addressed by different legal systems.

a) Jordan

Reasonableness or probable cause has not been expressly incorporated into the law. However, the *Criminal Procedure Law* 1961 provides a very simple threshold for issuing a search warrant. Articles 46 and 48/2 of the Act obligate a GP to issue a search warrant if there is a fair probability that the place to be searched houses a criminal, or a suspect, or an accomplice or even a person harbouring evidence of a crime, or an occupant of the home who has requested the search.

At the time of writing, no documented court cases have addressed the issue of IP address and probable cause. Scholars, however, have addressed probable cause in relation to conventional searches. They argue that the officer must be able to show that the defendant committed a crime and that an accusation against him is substantiated and, more importantly, that the search will reveal contraband or incriminating evidence.[740]

[739] See, Ralph D Clifford, *Cybercrime: the Investigation, Prosecution and Defence of a Computer-Related Crime* (2nd ed, 2006) 130.

[740] See, قدري عبدالفتاح الشهاوي , above n 681. See also,عصام الطوالبة Computer Search and Seizure Procedures (Alaeldin Mansour Maghaireh trans, 2003) [trans of اجراءات البحث و التفتيش في الكمبيوتر] 58-65, See also صلاح الدين جمال الدين, *the Validity of Search Procedures* (Alaeldin Maghaireh trans, 2005) [trans of: الطعن في اجراءات التفتيش] 25.

b) Australia

The Australian perspective is reflected both in legislative provisions governing search warrants and in judicial expositions. Section 3E of the *Crimes Act* 1914 provides: 'An issuing officer may issue a warrant to search premises if the officer is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises'. To obtain a search warrant, this Section clearly indicates that officers must demonstrate reasonable grounds to believe that the search will uncover evidence of a crime.

There has been much argument, however, over the definition and exposition of the 'reasonable grounds'. Courts have significantly contributed to the development of the meaning of 'reasonable grounds'. Justice Downes, the President of the Administrative Appeal Tribunal, has said that 'reasonable grounds means grounds based on reason, as distinct from something "irrational" absurd or ridiculous'.[741] In *George v. Rockett*, the High Court of Australia defined reasonable grounds as 'an inclination of the mind towards assenting to, rather than rejecting, a proposition and the grounds which can reasonably induce that inclination of the mind may, depending on the circumstances, leave something to surmise or conjecture'.[742] From these definitions it becomes clear that reasonable grounds arise either through information provided to the officers or through the latters' personal knowledge.

In a similar manner to Jordan, there is no case law in Australia that addresses the issue of IP address and probable cause. However, exploring the judicial view of the USA may be helpful in predicating how Australia will rule on this issue.

c) USA

The Fourth Amendment provides protection against unreasonable searches.[743] It imposes on law enforcement officers the requirement that the searches be based on 'probable cause'.[744] The 'probable cause' benchmark has, in several cases, been established as being that 'a person of reasonable caution could believe that the search may reveal evidence of a crime; it does not demand any showing that such a belief be

[741] *McKinnon v. Secretary, Department of Treasury* (2006) 229 ALR 187, 1549.
[742] *George v. Rockett* (1990) 170 CLR 104.
[743] See, eg, Stephens and Glenn, above n 533, 9.
[744] Ibid.

correct or more likely true than false'.[745] This benchmark is intended to help law enforcement officers to prepare search warrant affidavits. The Ohio Court of Appeals and the Supreme Court of Ohio affirmed this benchmark. In *Beck v. Ohio* the court stated:

> …officers had probable cause to make it--whether at that moment the facts and circumstances within their knowledge and of which they had reasonably trustworthy information were sufficient to warrant a prudent man in believing that the petitioner had committed or was committing an offence.[746]

Thus, the reasonable belief of a prudent man is being used as a parameter in the USA to evaluate the reasonableness and legitimacy of the probable cause which arise during crime investigation and require the issue of a search warrant.[747]

The officers' experience plays a significant role in establishing a strong probable cause. Thus, it is helpful to begin a search warrant affidavit with an introductory paragraph that briefly describes the officer's training and experience in the area or subject matter of the investigation.[748] Although the experience of the investigators preparing the affidavit is significant in this area, some courts consider the officer's expert opinion alone is not enough to establish a strong probable cause. For example, in *United States v. Schultz*, the court noted '...an officer's expert opinion that drug traffickers often keep records in their residences', and stated 'but that alone will not be enough to establish a nexus between the illegal trafficking and the residence to establish probable cause for a search'.[749] Establishing a probable cause requires, in addition to the officer's experienced opinion, a nexus between criminal activity and the item to be seized, and between the item to be seized and the place to be searched.

In the context of cyber search warrants, New York's Court of Appeals has ruled that the mere access or subscribing to a child pornography site is insufficient to establish probable cause to search the suspect's premises.[750] However, different crimes require

[745] *Carroll v. United States*, 267 US 132, 162 (Wash, 1925). *United States v. Olson*, 03-CR-51-S, (Wis, 2003). See also, Jamison M K, 'New Developments in Search & Seizure law' (2006) The *Army Lawyer*, 23.

[746] *Beck V. Ohio* 379 US 2d 223 144, 145 (1964).

[747] See, eg, Hayes and Eburn, above n 694, 500. See also, Shinder and Ed Tittel, above n 210, 155.

[748] See, eg, Kreston, above n 718.

[749] *United States v. Schultz* 14 F. 3d 1093, 1097 (6th Cir, 1994).

[750] *United States v. Perez,* 247 2d 2, 75 461,481 (NY 2003).

different ways of preparing the warrant. For example, in child pornography a probable cause can be established based on information and images collected by the undercover investigator posing as a minor online, or by informant reports about the receipt of child pornography image files to law enforcement agents, who then begin an investigation.[751] In this example, the investigator's experience and facts provided create a reasonable belief that criminal activity had taken place, justifying the issuance of a search warrant.

d) Comparative Legal Analysis

Laws obligate law enforcement officers to draft a search warrant based on probable cause or reasonable grounds. Police officers must have 'probable cause' as the threshold to justify the issue of a conventional search warrant. The same threshold must be reached to draft a cyber search warrant.

The Jordanian threshold, set by Articles 46 and 48/2, to issue a search warrant is simple and serves justice, because the search warrant is obtainable if any one of the three following circumstances is applicable: first, a visual observation by the officer; second, information provided by other citizens about the crime; third, an occupant of the property requests a search. This is applicable to cyber search warrants without any problems. For example, an undercover investigator posing as a minor will be able to obtain a cyber search warrant because of his visual observation of the crime. In addition, investigators will be able to avoid the problem of IP addressing, because the law does not require investigators to provide factual evidence linking the items to be seized and the place to be searched. However, the threshold of probable cause set by Jordan provides investigators with streamlined controls on how to prepare a search warrant, it ignores privacy issues.

In contrast, the Australian and US threshold is more complex. The reasonable belief of a prudent man is being used in both Australia and the USA to evaluate the reasonableness and legitimacy of the 'probable cause' requirement for issuance of a search warrant.[752] In addition, factual evidence linking criminal activity and the item to be seized, and between the item to be seized and the place to be searched, is an important factor in drafting a warrant. Indeed, because the reasonable belief of a prudent man is unfettered by a fixed parameter and varies with each case and officer's experience, courts require

[751] Kreston, above n 720.

[752] See, eg, Hayes and Eburn, above n 694, 500.

factual evidence supporting the affidavit. In different scenarios, obtaining factual evidence is impossible, because of the problem of the IP addressing system.

The requirement of obtaining factual evidence linking the items to be seized and the place to be searched hinders the investigation process, particularly, when officers are able to obtain evidence remotely without the need for physical access to the suspect's property.

7.3.2 Subject of the Search Warrants

Search warrants have traditionally been used to search and seize tangible things, being the fruit of the crime, the object of the crime, or the instrumentality of the crime, such as illegal drugs, stolen property, cash, and weapons. The officers enter the nominated premises, search evidence by entering rooms, opening drawers and looking around and then seizing tangible objects.

In the cyber world, when the data is contraband, evidence, or instrumentalities of crime, the subject of the search will be intangible items, such as data, images, files, and so on.[753] Investigators enter a real home or other building and search and seize data or they seize hardware, such as hard disks, and then make a mirror copy. The investigator acquires evidence by entering digital commands through a keyboard,[754] or using forensic tools to retrieve the requested contents from the mirror copy and sends it to an output device, such as a monitor, printer,[755] or a peripheral to display the evidence.

a) Jordan

The current laws of Jordan authorise the search and seizure of tangible things. On the one hand, Article Ten of the *Jordanian Constitution* protects individuals from illegitimate search in their houses and vicinities, such as gardens or other tangible places associated with the premises. In addition, it protects against illegitimate search of physical places used for residential purposes, such as hotels, condominiums, private apartments, whether owned or rented. The invisible digital contents are not addressed by the law and are not recognised as a commodity in their own right. On the other hand, the

[753] See, eg, John Rittinghouse and Bill Hancock, *Cybersecurity Operations Handbook* (2003) 1205.
[754] Kerr, above n 686, 538-540.
[755] Ibid.

Criminal Procedure Law 1961 identifies that the subject of the search warrant is either a physical place[756] in which a person lives and maintains privacy, confidentiality, and secrecy, or an individual.[757] In addition, Articles 33 and 34/1 authorise General Prosecutors and police officers to seize visible items and hard copy documents. Meanwhile, Article 88 authorises GPs to seize letters, parcels and other mail items.

b) Australia

By contrast, Australian parliaments have enacted specific provisions to address issues raised by digital searches. The new search powers permit Australian law enforcement officers executing a search warrant to search not only tangible items but also intangible materials. Section 3L of the *Crimes Act* 1914*,* titled 'use of electronic equipment at premises', permits executing officers to operate electronic equipment to seize data on electronic devices.[758] Section 3C defines data as any information in any form, or any programme.

c) USA

US statutes and courts recognise the search and seizure of data stored on electronic devices. The *Electronic Communications Privacy Act of 1986* (ECPA) for example, authorises law enforcement officers to access and seize digital data stored by a provider of electronic communications service.[759] The United States Supreme Court stated in *United States v. New York TEL.CO* that 'we recognised in *Katz v. United States,* which held that telephone conversations were protected by Fourth Amendment, that Rule 41[760] is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions…'[761] In *United States v. Biasucci*, the Second Circuit Court held that the fruits of video surveillance are 'property' that may be seized using a Rule 41 search warrant.[762] Accordingly, data stored in electronic form is 'property' that may properly be searched and seized using a Rule 41 warrant.[763]

[756] *Criminal Procedure Law 1961* div 4 S 1 (3) (81).
[757] *Criminal Procedure Law 1961* div 4 S 1 (3) (81), (86/1).
[758] *Crimes Act 1914* S 3L.
[759] *Electronic Communications Privacy Act*, 18 USC §§ 2073 (1986).
[760] According to Rule 41(2) (a) "property" includes documents, books, papers, any other tangible objects, and information.
[761] *United States v. New York Tel.Co*, 434 U.S. 159 (1977).
[762] Rittinghouse and Hancock, above n 751.
[763] Ibid.

d) Comparative Legal Analysis

The law of search and seizure in Jordan is inadequate to address the specific concerns raised by the subject of the search in digital context. The lack of recognition of intangible data as a commodity makes the current law of search and seizure incapable of dealing with digital evidence. According to the current provisions, law enforcement officers can only seize visible and tangible objects. To meet this problem, the Australian legislature has recognised the problem by enacting Section 3L, providing law enforcement officers with resources they need to search and seize intangible evidence. The USA Supreme Court expanded the definition of property to include digital items. So, Jordanian law should be amended to expressly authorise the search and seizure of intangible materials.

7.3.3 Scope of the Search Warrants

Search warrants must precisely describe the scope of the search and the items to be seized.[764] Law enforcement officers, according to the general rule of searching and seizing evidence, must search for those evidentiary materials that are described in the search warrant and only seize what is authorised by the warrant.[765] Therefore, the search warrant is the map that provides investigators with the guidelines necessary to execute a precise and rapid search.

Cyber search warrants may be issued to secure two different categories of evidentiary materials: hardware and software. Computers are composed of two vital components: the hardware component, such as screens, hard drives, motherboards, and so on, and digital component, such as programmes and data. While none of the two components can work separately, they are completely different entities and require totally different approaches in search and seizure procedures. When the data is contraband, evidence, or an instrumentality of the crime, the digital part is the main focus of the search, because it contains the evidence, while the other part is a compartment or container. Therefore, when a computer system is hacked, the hardware itself will not be contraband, or evidence or an instrumentality of the crime, but is considered to be merely a storage

[764] See, Becker, above n 717, 434. See also, Scott, above n 293, 25-9.
[765] See eg, Middleton, above n 530, 226.

place for evidence of the crime, and investigators should not obtain a warrant to seize the hardware, but to create a mirror copy. This is an important point because, practically, seizing computer hardware is not problematic if one computer is identified in the crime scene.[766] The problem arises when the object to be seized is a complicated network, such as several computers connected to a common Local Area Network (LAN) in one office or in a commercial business area. Although seizing the entire networks, and network infrastructure, PC-workstations and peripherals, is feasible and a search warrant to seize the entire system is obtainable, seizing the entire network deprives businesses and people, who are not associated with the offence, of the entire computer system and, therefore, will cripple their business operations as well as invade privacy.[767]

The general notion of particularity,[768] also known as the principle of specificity,[769] means the search warrant should be issued for a particular crime, to search a particular place, and to seize particular items.[770] The *Crimes Act* 1914 and the Fourth Amendment established principles that would soon restructure a search warrant particularity. First, the search warrant must specify the particular areas to be searched.[771] Second, the search warrant must describe the particular object to be searched and things to be seized.[772]

In cybercrime searches, particularity is more complicated and problematic; particularly in relation to the scope of data to be searched. Investigators encounter incriminating data intermingled with thousands of files with no connection to the investigation and which cannot practicably be separated at the site of the search.[773] These files either belong to the person who is the subject of the investigation or to other persons and are neither contraband nor evidence of criminal activity,[774] or they might be privileged files, such as lawyers' files. Under any of these circumstances, the core of the problem is that

[766]See, Computer Crime and Intellectual Property Section Criminal Division, above n 633, 43.

[767] See, Middleton, above n 530, 207. See also, Brenner, and Frederiksen, above n 596. See also, Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[768] See, eg, Becker, above n 717, 446.

[769] See generally, New Zealand Law Report Commission, *Search and Surveillance Power*, Report No 0113-2334; 97 (2007) 120.

[770] See, Amy Evans and Martin F Murphy 'The Fourth Amendment in the Digital Age: Some Basics on Computer Searches' (2003) 20 (10) *Computer and Internet Lawyer* 4, 6. See also, Peter Gillies, *The Law of Criminal Investigation* (1982) 232.

[771] See, Raphael Winick, 'Searches and Seizures of Computer and Computer Data' (1994) 8 *Harvard Journal of Law & Technology*, 75, 85. See also, Acker and Brody, above n 680, 164.

[772] Ibid.

[773] See generally, New Zealand Law Report Commission, above n 769, 176.

[774] See, eg, Winick, above n 771,105.

the scope of the search goes beyond the limits drawn in the search warrant.[775] This happens when a valid search warrant fails to include all the documents the subject of the search because the investigators are not aware that these documents are outside the scope of the search or because the separation between incriminating data and unrelated documents is impractical.[776] Indeed, forensics investigators usually make a mirror copy of the hard drive and conduct a thorough examination off-site. A mirror copy could include innocent and confidential information with no connection to the ongoing investigation. This problem is comparable with the traditional problem of separating the wheat from the chaff at the physical location of the search.[777] Courts and scholars, therefore, are increasingly confronting the question of the search's proper boundaries or particularity. They offer two different perspectives on the issue.

First: Pro-particularity Approach

The first approach rejects the use of broad language in preparing the search warrant. The search warrant should be drawn as specifically as possible and officers must not open files or folders randomly. Thus, the search warrant must be specific as to the files or data to be searched.[778] This approach was obvious in different courts' cases that quashed mirror copy searches, and delivered judgment in favour of conducting specific searches.[779] The USA Court of Appeals for the Ninth Circuit, for example, declined to validate a warrant authorising blanket removal of all computer storage removable media for later examination.[780] Other courts have considered the phrase 'including but not limited to' which is mentioned in search warrants[781] as failing to satisfy the particularity requirement.[782] Nevertheless, courts which adopted this approach admitted that a comprehensive search is permissible in specific circumstances associated with the search of commercial premises which conduct illegal business operations beyond the

[775] See, Brenner and Frederiksen, above n 596.

[776] See, eg, Aaron Lowenstein, *Search and Seizure on Steroids: United States v. Comprehensive Drug Testing and Its Consequences for Private Information Stored on Commercial Electronic Databases*, (2007) Selected Works <http://works.bepress.com/aaron_lowenstein/1/ >at 22 November 2007.

[777] See, eg, Eoghan Casey, above n 428, 110.

[778] See eg, Jonathan M Jacobson, *Antitrust Law Developments* (2007) 740.

[779]See, Clifford, above n 739, 230. See also, Carla Rhoden, 'Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond' (2003) 30 *American of Criminal Law*, 120.

[780] *United States v. Hill* 459 .F 3d 1, 27 (9th Cir, 2006).

[781] See, *In the Matter of Search Warrant for K-Sports Imports Inc* 163 F 594 (Cal, 1995).

[782] See, Moore, above 597, 75. See also, Rhoden, above n 779, 115.

scope of the business' registration.[783] For example, if an affidavit shows that the entire business which is the subject of a search is merely a scheme to defraud and all the computers harbour evidence then unrestricted search is valid.[784] Such a warrant authorises law enforcement to search computers and digital records located at the crime scene as long as police officers believe that the computers are likely to house evidence of criminal activity.[785]

Second: Anti-particularity Approach

A majority of scholars support an anti-particularity approach to cyber searches.[786] Franklin supports comprehensive and unlimited search warrants if there is plenty of time and uncertainty about what evidence is being sought. However, he further advised that a limited search warrant is desirable if the evidence can be precisely located.[787] Ivan suggests that a search warrant should include any computers and computer removable media found in the premises the subject of the search.[788] In his affidavit, Detective Askew presented a comprehensive affidavit stating that 'this application is to search any computer media found therein…'[789] He backed his argument with the fact that the search specificity would incur additional time and financial cost during the search execution. Furthermore, restraining the search would preclude investigators from conducting complete and fruitful searches; this is because cybercriminals are more professional and skilled in concealing incriminating evidence than criminals of traditional crimes.[790] For example, by using encryption technology, evidence could be hidden inside any of the numerous images, videos, files and documents, and suspiciously modified in such a way that a narrow search will likely omit incriminating items.[791] And most importantly, the search for incriminating evidence requires the executing officer to retrieve deleted files, and therefore, the mirror copy search is significant for retrieving relevant data.

[783] Rhoden, ibid 118.

[784] Ibid.

[785] Ibid 119.

[786] See, Clifford, above n 739, 230.

[787] See, Carl Franklin, *the Investigator's Guide to Computer Crime* (2006) 162.

[788] Clifford, above n 739, 134

[789] *United States v Grimmett*, 439 F.3d 1236 (9th Cir, 2006).

[790] See, J J McLean, 'Homicide and Child Pornography' in Eoghan Casey (ed), *Handbook of Computer Crime Investigation* (2002) 361, 373.

[791] See Section 5.3.2 for more information about Encryption.

a) *Jordan*

No provisions in laws specifically deal with cyber searches and mirror copy.[792] In addition, no court decisions or scholarly work identify and analyse the issue. Therefore, it is highly likely that conventional search warrant procedures would be applied to cyber searches, because they grant GPs broad authority to make a mirror copy and seize any items necessary for ongoing investigations. Indeed, the *Criminal Procedure Law* 1961 entitles GPs and executing officers to search and seize anything (tangible) that might relate to any offence.[793] The same rules were applied in 1970 in the *Chic Fashions* case and in *Pringle v. Bremner & Stirgling*.[794] In these cases, the investigator seized not only the stolen goods which had been listed on the search warrant, but also any other goods which he believed on reasonable ground to have been stolen and to be material evidence.[795]

b) *Australia*

In Australia, the *Crimes Act* 1914 Section 3F (1) (c) draws the limits of the search scope. It stipulates that the warrant should be issued to search the premises for the kinds of evidential material specified in. Section 3C defines 'evidential material' as 'a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form'. From the definition and Section 3F it can be concluded that executing officers are obliged to search and seize the items listed on the search warrant, including data. Nevertheless, executing officers are entitled to make a mirror copy as Sections 3F, 3K and 3L provide executing officers with a variety of options:

1) Bringing to the warrant premises forensic equipment to examine or process data in order to determine whether it may be seized.[796]

2) Removing from the premises data to examine or process elsewhere in order to determine whether it may be seized.[797]

[792]The author browsed and probed more than one hundred thousand Jordanian court decisions looking for judicial exposition regarding search particularity and related issues, however, no single case was found. Furthermore, two prominent Jordanian websites publishing court decisions were browsed, www.Adelah.com.info and www.Qunaun.com. Also, E-mail from the lawyer Firas Al-qotha to Alaeldin Maghaireh, 5 May 2007.

[793] *Criminal Procedure Law 1961* div 4 S 1 (3) (87).

[794] See, eg, L H Leigh, 'Recent Developments in the Law of Search and Seizure' (1970) 33 *The Modern Law Review* 272, 272-3

[795] Ibid.

[796] *Crimes Act 1914* (Cth) div 2 S 3K (1).

3) Operating electronic equipment at the premises, copying the data found thereby on to a device brought to the premises and removing that device from the premises.[798]

4) Operating electronic equipment at the premises and then seizing it.[799]

5) Operating electronic equipment at the premises, using facilities at the premises to create documents there-from and then seizing them.[800]

6) Securing electronic equipment at the premises so that it may be operated with the assistance of an expert.[801]

These provisions empower executing officers to rummage through data first and then make a mirror copy and seize specified evidential material. In *Kennedy v. Baker,* for example, the Australian Federal Court permitted the executing officer to conduct and remove the hard drive image from the premises.[802] The Explanatory Memorandum to the *Cybercrime Bill* 2001 explained subsection 3L. It stated that:

> It would enable law enforcement officers executing a search warrant to copy data held on any electronic equipment or associated devices at search premises to a storage device where there are reasonable grounds for suspecting that the data contains evidential material. This will permit officers to copy all data held on a computer hard drive or data storage device if some of the data contains evidential material or if there are reasonable grounds to suspect the data contains evidential material… The existing provision only allows evidential material to be copied (Crimes Act, paragraph 3L (2) (c)). Electronic equipment, such as a computer hard drive, can hold large amounts of data. It is often not practicable for officers to search all the data for evidential material while at the search premises and to then copy only the evidential material which is found. The proposed provision would allow officers to copy all the data on a piece of electronic equipment (by imaging a computer hard drive for example) in situations where an initial search of the data uncovers some evidential material or where the officer believes on reasonable grounds that the equipment might contain evidential material.[803]

This explanation inspired the Judge in *Kennedy v. Baker* to argue that data stored in the hard drive of a personal computer is a single thing regardless of whether it contains different parts, such as files and documents. He further emphasised that a computer's

[797] *Crimes Act 1914* (Cth) div 2 S 3K (2).
[798] *Crimes Act 1914* (Cth) div 2 S 3L (1A) (a).
[799] *Crimes Act 1914* (Cth) div 2 S 3L (2) (a).
[800] *Crimes Act 1914* (Cth) div 2 S 3L (2) (b).
[801]*Crimes Act 1914* (Cth) div 2 s 3L (4) (6).
[802] See, *Kennedy v. Baker* (2004) FCA 562.
[803] Explanatory Memoranda, *Cybercrimes Bill 2001* (Cth) 16.

hard drive contains a single magnetic medium albeit that the computer can be operated to access selectively certain parts of that data, such as particular files or documents. Therefore, he said:

> …I take the view that the ordinary meaning conveyed by the text of part 3L (1A) (a) is that if the executing officer or constable assisting believes on reasonable grounds that data from a particular source accessed by operating a computer might constitute evidential material, he or she may copy the data from that source to a disk, tape or other associated device brought to the premises. A computer hard drive is, in my view, a single source of data within that meaning….I reject the contention that…Mr Baker was not authorised by subs 3L (1A) of the *Crimes Act* to copy all of the data held on the examined hard drive, thus creating the imaged hard drive, and to take the imaged hard drive from the Premises.[804]

c) USA

The Fourth Amendment and the *Privacy Protection Act* (PPA) protect materials and defend individuals against broad search and seizure. The Fourth Amendment established principles that soon restructured search warrant particularity. First, the search warrant must specify the particular areas to be searched.[805] Second the search warrant must describe the particular object to be searched and things to be seized.[806] The PPA protects digital materials which are prepared for publication on the web, as well as documentary materials from searches and seizures unless they are contraband, instrumentalities, or fruit of crime.

Because cyberspace is significantly different from the real world in terms of the ability of the officers and forensic tools to distinguish between incriminating materials and protected materials, the PPA application would pose considerable hurdles to search and seizure procedures in cyberspace. Therefore, the Sixth Circuit in *Guest v. Leis* has explicitly ruled that the incidental seizure of PPA-protected material commingled on a suspect's computer with evidence of a crime does not give rise to PPA liability, because 'when police execute a search warrant for documents on a computer, it will often be difficult or impossible (particularly without the co-operation of the owner) to separate the offending materials from other "innocent" material on the computer' at the site of

[804] *Kennedy v. Baker*, above n 802.
[805] See, Winick, above n 771, 85. See also, James R Acker and Brody, above n 680, 164.
[806] Ibid.

the search'.[807] In another similar decision, the Tenth Court has suggested that 'if the executing officer comes across evidence intermingled with irrelevant documents that cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents'.[808]

This approach, however, while it facilitates law enforcement preparing and executing a search warrant, is permissible only in particular situations. Different courts have held that the search and seizure of 'any and all computer hardware,' and 'any and all computer software' is permissible in certain circumstances such as where:

1) A more precise description is not feasible;[809]

2) The suspect made it difficult to describe particularly the items to be seized.[810]

3) The items to be seized are voluminous.[811]

Therefore, the Tenth Court in *United States v. Cary* has suggested in some circumstances that investigators 'must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant'.[812] In another case for example, where the defendant was accused of possession of child pornography, the Ninth Circuit Court held that the detective must examine only files containing extensions indicating pictures, such as JPEG and GIF.[813] In a recent decision, however, the same Court broke new ground in deciding that law enforcement officers are permitted to execute non-restrictive searches if they observe the following rules:

a) They waive reliance upon the plain view doctrine which allows them to seize evidence which they observe is not within the scope of their search warrant:

[807]See, Computer Crime and Intellectual Property Section Criminal Division, above n 633, 50.
[808] See, *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir, 1999). See also, *United States v. Tamura*, 694 F.2d at 596-97.
[809] See, *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir, 1986). See also, *United States v. Lacy*, 119 F.3d 742 (9th Cir, 1997).
[810] See, *United States v. Bentley*, 825 F.2d 1110 (7th Cir, 1987).
[811] *United States v. Johnson* 06-4002-17-CR-C-NKL (2007).
[812] *United States v. Carey*, above n 808.
[813] See, *United states v. Grimmett*, above n 787.

b) The collected data is segregated or reduced by specialised personnel or an independent third party:

c) The warrant discloses the actual risks of destruction of information and describe prior efforts to seize the information:

d) The search protocol must be designed to uncover only the information for which it has probable cause and only that information may be examined by the investigative agents; and

e) Law enforcement officers must destroy or return unrelated data.[814]

Furthermore, the Tenth Circuit Court proposed that in the off-site investigation, computer examiners should be required to 'employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory'.[815] Some courts have gone further than this and have restricted the issuance of search warrants upon providing the court with particular search methods aimed at protecting the intermingled files.[816] For example, the Tenth Circuit Court proposed that in the off-site investigation, computer examiners should be required to 'employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory'.[817] The same court in *United States v. Brooks* has refused, however, to restrain executing officers from implementing or describing particularised computer search methods to the defendant.[818]

[814] *United State v. Comprehensive Drug Testing*, F.3d 2009 WL 2605378 (9th Cir, 2009).

[815] See, *United States v. Carey*, above n 808, 1276.

[816] In *United States v. Camlimlim*, the court had issued a warrant requiring the government to use search methods that would avoid exposing documents not included on the warrant, such as surveying file directories, opening files and cursorily reading the first few pages to determine their contents, scanning storage space for intentionally deleted data, and performing key word searches to locate relevant documents. See, Lowenstein, above n 776, 13.

[817] See, *United States v. Carey*, above n 808.

[818] See, *United States v. Brooks*, 427 F 3d 1246, 1252 (10th Cir, 2005). See also, *United States v. Dennis* 100 A.F.T.R.2d (2007). The court denied the defendants motion to suppress evidence seized pursuant to the search warrant, because the executing officer had not applied particular search methods. See also, in *United States v. Hill,* where the court rejected the use of specific search methods because it found that 'Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer'. *United States v. Hill* 459 F 3d 1, 27 (9th Cir, 2006).

d) Comparative Legal Analysis

Drawing the borders of the search in advance is a daunting task because, among other things, obtaining definite details of evidence is beyond the officers' knowledge and evidence can be concealed, encrypted or disguised. Thus, preventing investigators from searching the entire data and opening files would pose considerable hurdles to searches and seizures in cyberspace, and obstruct police investigations. Therefore, the second approach, which permits law enforcement officers to make a mirror copy, is more common and is frequently used by forensics investigators.

In Jordan, in the absence of provisions expressly dealing with cyber searches, the broad language of the *Criminal Procedure Law* 1961 might allow officers to create a mirror copy and conduct an unrestricted search. Police officers exercise broad latitude in executing the search warrant. They are not restricted or bounded by particularity principles which restrict officers to precisely search and seize items. They are granted autonomy to seize not only the items listed on the warrant, but also any other items they believe on reasonable ground to be material evidence. This provides investigators with a flexible avenue in executing the search; even if it does not recognise the unique nature and characteristics of digital evidence.

Developed countries, such as Australia, have amended their laws relating to cyber searches to permit mirror copy searches. Sections 3F, 3K and 3L of the *Crimes Act* 1914 entitle the executing officer to rummage through the data using forensic tools to determine the items that should be seized and authorises the executing officer to create a mirror copy. Therefore, the *Criminal Procedure Law* must be amended by adding a text explicitly allowing law enforcement officers and GPs to conduct exhaustive digital searches. At the same time, the search warrant must be detailed and clearly direct law enforcement officers to the incriminating data to avoid rummaging through innocent data. But if a more precise description is impossible, or the suspect makes it difficult to describe the items to be seized, or the items are voluminous, the USA perspective can be adopted because it provides executing officers with a clearer image respecting computer search and seizure procedures, as well as recognising the nature of digital evidence by limiting the search as far as possible to evidential materials.

7.4 Execution of the Cyber Search Warrants

Conventional search warrant execution refers to carrying out the search warrant by conducting the entry and search of the specified place.[819] Traditional search warrant execution can be divided into three stages. The first stage begins with knocking and notifying,[820] then observing and marking the place to be searched in order to determine which is the most effective and efficient pattern of search to apply to the crime scene environment.[821] For example, a 'zone' search would be chosen for a small space zone, such as a bedroom, while a 'grid' search might be chosen for a large open outdoor area, such as a backyard.[822] The second stage involves a more thorough search, such as rummaging and moving items, opening and emptying closed containers.[823] The final stage, which culminates in seizure of items, is the most intrusive level of search, such as emptying every drawer in the scene and searching thoroughly through anything marked in the first stage.[824]

By contrast, the cyber search warrant execution refers to the process of executing data processing by conducting forensic analysis. This search is divided into two major phases: the pre-digital search and the digital search.

The pre-digital phase is conducted on-site, and therefore, mimics the first stage of the traditional search procedures.[825] This phase can be further divided into two sub-steps:

The first sub-step often commences with the first stage of the traditional search procedures, which begins with notifying and observing the physical location to be searched, then nominating the right search mechanism and, finally, identifying the digital devices specified in the warrant. Also, it involves procedures associated with the

[819] Arcaro, above n 683, 232.

[820] According to 3H (1) of the *Crimes Act* 1914, the executing officer must hand the occupier a copy of the search warrant.

[821] Arcaro, above n 683.

[822]Greg Dagnan, *Searching in Stages to Prevent Destruction of Evidence at Crime Scenes* (2007) <http://www.crime-scene-investigator.net/SearchingStages.html> at 15 September 2007. See specially, Ross Gardner, *Practical Crime Scene Processing and Investigation* (2005) 125.

[823] Ibid.

[824] Ibid.

[825] See, *Crimes and Criminal Procedures* 18 USC § 3109. See also, *Crimes Act 1914* div 5 s 3ZS.

place of the search, the suspect, and other routine procedures, such as documentation,[826] recording[827] and video shots.[828] Such procedures are imperative to prove that the first responders did not contaminate the crime scene in any way, providing evidence in its original state,[829] as well as for chain of custody purposes, to track the evidence collection process from its original sources to the courtroom presentation.[830]

The second sub-step involves particular procedures associated with the computer as a piece of hardware, such as labelling all the connections and wires attached to the computer and cutting off the power which is recommended by a number of forensic investigators.[831] This procedure should happen only after saving and shutting down any programmes that might be running in RAM.[832] (The RAM temporarily holds information that is currently running and travelling between the hard disk and Internet and switching off the power supply improperly will damage any unsaved data running in RAM).[833] Significant consideration should be given to the type of the operating system used, for example, Windows XP, Linux, UNIX, and Macintosh, as each of these systems uses a different mechanism for storing and running files stored in RAM.[834] For example, in a Windows Operating System, the data in RAM is immediately lost once the power is removed from the computer.[835] Labelling all the cables attached to the computer seized is vital because it 'facilitates the reconnection of the cables when the computer is reassembled and restarted'.[836]

[826] The crime scene documentation process normally involves six steps: 1) documentation of major events relating to the search efforts that are taken by investigators to insure that an organised search is accomplished; 2) documentation of the general appearance of the crime scene as first observed; 3) photographing and recording the scene.4) documentation of physical evidence (computer) locations, size, measurement, etc. 5) documentation of the recognition, collection, marking, and packaging of physical evidence for administrative and chain of custody purposes; and 6) documentation of the recognition, collection, marking, and packaging of lifts made of latent prints discovered at the scene. See generally, *Crime Scene Response Guidelines: Documentation Procedures* <http://www.crime-scene-investigator.net/respon4.html> at 15 September 2007.

[827] These procedures - documentation, photographing, and recording - are part of every step in the search execution. Reyes suggests that a voice recorder is important to be used before moving onto each step of the search execution. See generally, Anthony Reyes et al, above n 731, 145.

[828] See, eg, Dagnan, above n 819. See also, Ferraro and Eoghan, above n 723, 116.

[829] See, eg, Eoghan Casey, above n 428, 629.

[830] See generally, Jay Siegel, *Forensic Science: The Basic* (2007) 43.

[831] See specially, Reyes Anthony et al, above 731, 147- 149. See also, Moore, above n 597, 86.

[832] Ibid.

[833] See, eg, Scott Mueller's, *Upgrading and Repairing PCs* (14th ed, 2002) 417. See also, Jeff Dodd, 'Memories Are Made of This: Several Types of Memory Play a Role in PCs ' (2002) 6 (7) *Smart Computing* 12.

[834] Ibid.

[835] Jack Belzer, at el, *Encyclopedia of Computer Science and Technology* (1987) 161.

[836] Moore, above n 597, 86.

The second phase of cyber search is digital. This stage requires no physical motion in the execution, because it works entirely with the data. It embodies unique procedures conducted by forensic officers off-site.[837] Indeed, it is handled by different personnel at different times using different methods to recover and discover invisible or intangible evidence from the hardware devices that were seized in the first stage. Investigators must be reasonably familiar with computers and be able to distinguish database programmes, electronic mail files, telephone lists, and stored visual or audio files from each other. Evidentiary materials searched for in this stage can be the fruit of crime (such as the history files on the defendant's computer showing the dates and times of hacked access to specific pages) or the object of the crime (such as child pornography photos, spoofed website making tools, and so on).

Although the two stages of search are apparently separate, each impinges on the other. Procedures executed in the pre-digital phase may indirectly effect the digital search step in a negative way. The notifying procedure, for example, which is used for informing the suspect or other residents of the search warrant execution, must be narrowly applied in order to prevent the suspect from having any opportunity to destroy, contaminate, or hide incriminating evidence.[838] Therefore, when applying the announcement procedure, the first responder must firstly secure the crime scene or the place to be searched physically and digitally.

The physical step is to keep the suspect away from the crime scene or the place to be searched and to prevent anyone from approaching or accessing the computer via a wireless connection or any other means of transmitting data from one location to another, such as over a network.[839] This can be done by unhooking any phone connections, inspecting the computer for booby-traps[840] and isolating the computer from

[837] Kerr, above n 687, 91.

[838] Clifford, above n 739, 135.

[839] See specifically, Eoghan, above n 428, 627. See also, Moore, above n 597, 83-85.

[840] In the real world booby traps are an explosive material designed to kill or cause severe casualties. The same term is used in the cyber world to refer to malicious codes inflicting system damage. See generally, Ingrid Detter Delupis, *The Law of War* (2nd ed, 2000) 221. In computers, booby traps are phoney icons on the desktop created to destroy files when someone (investigators or an unwanted user) clicks on it. For example, if a suspect created an icon named 'kiddie porn' an investigator might be tempted to click on it. If the investigator clicks on the icon, it will overwrite the targeted files, encrypt the hard disk, or perform other actions that make investigation impossible. See, Shinder and Ed Tittel, above n 210, 331. Also, booby traps take another form, such as creating a very short program that would cause the computer to demand a password periodically, and if the correct password is not entered within ten seconds, would

any network connections.[841] In a scenario where there is more than one terminal, Kevin O'Shea, co-author of *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*, has suggested some clues that might be useful in identifying the physical location of the digital media that has the highest probability of containing the evidentiary information described in the warrant.[842] For example, in a hacking investigation, where a couple of computers were found in the suspect family's house scattered between his bedroom and the lounge.[843] The investigator must first secure the one that was found in the suspect's bedroom. However, while it is hard to speculate about the intangible location of digital evidence, because the computers are networked together, he pointed out that the type of crime the subject of the investigation may guide the investigators to the right digital container.[844] For example, in a case of an obsessive child pornography collector, the evidence can be speculatively found in a huge container, such as hard drive or removable disks.[845] Nevertheless, investigators must not rely on such indications and all the digital media found should be examined.

It might be possible that evidence contamination can be achieved wirelessly while the officers are present at the crime scene.[846] The danger of wireless network connections lies in the ability of any other user to control and destroy incriminating evidence remotely by deleting files and programmes or maliciously planting incriminating evidence. For example, piggybacking[847] is new generation of cybercrime that exploits wireless connection technology to obtain someone's wireless connection log.[848] This technique can be used by the suspect himself to access and destroy evidence.[849]

trigger the automatic destruction of the computer's files. See, Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[841] See, Reyes Anthony et al, above n 731, 142. See also, Middleton, above n 530, 17.

[842] Reyes Anthony et al, ibid.

[843] Ibid.

[844] Ibid.

[845] Ibid, 145.

[846] See generally, Gregory Kipper, *Wireless Crime and Forensic Investigation* (2007) 58.

[847] War-driving, War-biking and Walk-driving are piggybacking methods used to gain illegal access by wireless computer connection. War-driving is illegal access into a wireless Internet connection by driving around a specific area looking for a wireless network to gain access and compromise the information contained on the network. War-biking and Walk-driving are the same technique, but in the former the bicycle is used and in the latter the hacker walks around the specific area using a laptop looking for a wireless network to gain illicit access. See generally, Kipper, above n 846, 17-21.

[848] Ibid.

[849]See, eg, James Michael Byrne and Donald J Rebovic (eds), *The New Technology of Crime, Law and Social Control* (2007) 29. See also, Stacey L Edgar, *Morality and Machines: Perspectives on Computer Ethics* (2nd ed, 1997) 211.

Therefore, investigators must take into their consideration evidence contamination by wireless means and apply appropriate procedures to secure the crime scene and/or the place the subject of the search.

a) Jordan

In Jordan, the Director of Public Prosecutions (DPP) is the only authority entitled to prepare and execute search warrants.[850] Public prosecutors within each district may opt to carry out the search warrant personally, or assign the task to police officers and law enforcement investigators who are exclusively listed in Article 9 of the *Jordanian Criminal Procedure Law*.[851] The designated officers and investigators must obey and adhere to the public prosecutor's instructions about the warrant execution procedures, its scope and its time, and the warrant must be performed according to the rules of law.[852]

In regard to the pre-digital phase, GPs have been vested with the power to issue and conduct search warrants without notifying in advance the defendant or the suspect of the search.[853] However, the warrant does require the defendant's presence during the time of the search warrant execution or a representative, such as a lawyer, or two witnesses, or a local notary. One of them must attend the search execution.[854] He has also been vested with a broad discretion in deciding what appropriate procedures and measures must be taken to ensure proper search and seizure operation. For example, the GPs can assign the search procedures to experts.[855] In regards to the digital phase, no provisions in the law address the particular procedures that should be applied for in computer searches and seizures.

b) Australia

The Australian *Crimes Act* 1914 addresses notification procedures by obliging the officer executing a search warrant to announce that s/he is authorised to enter the

[850] *Criminal Procedure Law 1961* div 2 s 4 (43). In Australia, a search warrant may be issued only by a Justice of the Peace based on judicial discretion. See, Gillies, above n 770, 222.

[851] The officers who are exclusively listed in Article 9 are: 1) governors; 2) police commissioner; 3) police officers; 4) detectives; 5) local notaries; and 6) any officer entitled to prepare and execute search warrants.

[852] *Criminal Procedure Law 1961* div 2 s 4 (33) (48/1) (89/1).

[853] *Criminal Procedure Law 1961* div 4 S 1 (3) (84).

[854] The Court of Cassation, قرار محكمة تمييز جزاء رقم 1999/430 (هيئة عامة 1999/8/28).

[855] *Criminal Procedure Law 1961* div 3 S 4 (39).

premises to search.[856] Furthermore, Section 3H clearly orders the executing officer to hand over a copy of the search warrant to the occupier of the premises or another person who apparently represents the occupier and is present at the premises.[857] The search warrant copy made available to the occupier must include detailed information about the search, such as the name and description of the issuing officer and the details as to the date or place of its issuance.[858] It also obliges the executing officer to identify him/herself to the person present at the place to be searched.[859] However, with reasonable grounds, officers have been vested with the power to enter premises without announcement.[860] Even more, under new legislation to go before Federal Parliament, police officers will be given unprecedented 'sneak and peek' powers to search homes and computers without notification.[861]

In the digital phase of the search, the Australian *Crimes Act* 1914 explicitly authorises the officers executing the search warrant to bring to the premises equipment necessary for protecting, examining or processing any data found at the premises in order to determine whether it may be seized under the warrant. [862]

c) USA

In the USA, Section 213 of the *PATROT Act* authorises the executing officers to perform what is called a 'sneak and peek' search. As defined by Charles Doyle, such 'a search authorises officers to secretly enter (physically or electronically), conduct a search, observe, take measures, conduct exams, take pictures, copy documents, download or transmit, and depart without any tangible evidence or leaving notice of their presence'.[863] This search warrant gives authorities the right to search, observe, copy, download or transmit computer files without taking any tangible evidence or leaving notification or notifying the occupier of the premises, or another person who

[856] *Crimes Act 1914* div 5 S 3ZS (1) (A).

[857] *Crimes Act 1914* S 3H (1).

[858] See, eg, *Oke v. Commissioner of the Australian Federal Police* (2007) (FCA27).

[859] *Crimes Act 1914* P 1AA div 2 S 3H (4).

[860] *Crimes Act 1914* div 5 S 3ZS (2) stipulates: 'A constable is not required to comply with subsection (1) if he or she believes on reasonable grounds that immediate entry to the premises is required to ensure: (a) the safety of a person (including a constable); or (b) that the effective execution of the warrant or the arrest is not frustrated'.

[861] Tom Allard, 'New Secret Search Powers', *the Sydney Morning Herald* (Sydney), August 1, 2007, 1.

[862] *Crimes Act* 1914 S 3k (1).

[863] Charles Doyle, 'Terrorism: Section by Section Analysis of the USA PATRIOT ACT' in Alphonse B Ewing and Charles Doyle (eds), *The USA Patriot Act Reader* (2005) 1, 14.

apparently represents the occupier at the premises.[864] However, the issue of a 'sneak and peek' search warrant must be backed by a reasonable belief that knocking and announcing will lead the suspect to destroy, or hide evidence, or obstruct investigation.[865]

d) Comparative Legal Analysis

It is clear that applying the traditional procedures of knocking and notifying to the place the subject of the search may jeopardise the integrity of the evidence that is going to be discovered, because digital evidence can be quickly and easily destroyed even by something as simple as pressing a Hotkey.[866] The success of a search execution often relies on taking the suspect by surprise or using sneak tactics so they do not hide or destroy evidence. Therefore, the need for issuing a 'sneak and peek' search warrant, instead of a classical search warrant involving knocking and notifying, is self-evident in cybercrime investigation more than any other sort of investigation.

Jordan's and Australia's positions suffice for executing a search warrant without notifying in advance the suspect. Neither of them, however, authorises the executing officer to conduct a 'sneak and peek' search. Jordanian law explicitly requires the attendance of two witnesses or a notary during the search execution. Australian law is more complex and is not suitable for executing a sneak warrant, because handing a copy of the warrant to the suspect significantly conflicts with sneak and peek procedures, unless there are reasonable grounds, such as the need to conduct an effective search; in which case the officer may enter the place subject of the search without announcement. Australia is in the process of reforming its laws to allow a US style 'sneak and peek' feature. It would also be a useful step for Jordan to apply 'sneak and peek' to cybercrime investigation.

[864] See, eg, Kerr, above n 687, 429. See also, Middleton, above n 530, 219.

[865] See, Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[866] A Hotkey is a combination of keys, such as Shift-Ctrl-A, that allows a user to launch applications using the keyboard. See, Computer Crime and Intellectual Property Section Criminal Division, above n 633, 56.

7.5 Who Should Accompany the Officers Executing the Search?

Cybercrime searches have a unique nature and different phases. The pre-digital phase is conducted on-site, and the digital phase is primarily conducted off-site. They require both conventional and digital tools to accomplish their goals together with investigative teams, such as technicians, evidence custodians, forensic examiners and forensic analysts. They assist in carrying out the conventional and digital procedures and conduct searches off-site. Therefore, they can be divided into two groups: the first group is the first responders who perform basic procedures, such as securing the physical location. The second group is the professional investigators who are trained to conduct cybercrime as well as traditional searches, because investigators have to deal with physical places, real suspects, and a variety of investigative tools, such as video and audio tapes, hardware, cameras, technical equipment, etc.

a) Jordan

In the absence of any provisions concerning cyber searches, conventional search warrant execution requirements must be observed when dealing with cybercrime. According to the *Criminal Procedure Law* 1961, conventional search execution requires the attendance of two groups of people. These are, first, police officers who execute the warrant and, second, civilian witnesses accompanying them for the purpose of witnessing the search.

The first group is composed of professional investigators and forensic experts led by a GP. The GP supervises the officers' compliance with the law. If the case needs expertise, the GP can nominate the right experts to provide assistance in executing the search.[867] The experts declare in writing (under oath) that they will carry out their task faithfully and impartially.[868]

The second group is precisely identified in the search warrant's provisions as persons who must accompany the officers executing the search warrant.[869] Two witnesses who are blood relatives of the defendant or, if not available, a notary, must accompany the

[867] *Criminal Procedure Law 1961* div 3 S 4 (39/2).
[868] *Criminal Procedure Law 1961* div 3 S 4 (41/1).
[869] *Criminal Procedure Law 1961* div 3 S 4 (36/2).

officers and witness the execution procedures.[870] The purpose is to offer the defendant protection and an opportunity to suppress the collected evidence, if the executing officer misuse his authority. The designated accompanying persons must sign in at the end of the search report; otherwise the search will be invalid.[871] The Court of Cassation has handed down judgment in favour of their attendance.[872] Conducting a search without the presence of any of these persons who are mentioned makes the search unlawful unless the defendant is present.[873]

b) Australia

In Australia, meanwhile, the occupier of the premises is entitled to be present during the search,[874] and the executing officers are vested with the power to terminate his presence if s/he impedes the search.[875] In addition, the executing officer can order a specified person to provide any information or assistance that is reasonable and necessary to allow him to access, copy, or convert the data into documentary form.[876]

c) USA

In the USA, neither the Fourth Amendment to the USA Constitution nor Article 18 U.S.C. § 3105 require the presence of the defendant during the search. Under the current law, the executing officer has authority to hire experts in various fields, including computer forensics, to assist in the search.[877] Also, the executing officer can accompany the victim, or a personal representative of the victim, to the premises if he provides persuasive reason to support the victim's presence.[878]

d) Comparative Legal Analysis

In cyber searches, the Jordanian GP's supervision in searches is limited to searches carried out on-site. The off-site searches are carried out by the experts who have an advanced knowledge in forensic investigation. S/he prepares the necessary report to the GP.

[870] *Criminal Procedure Law 1961* div 4 S 1 (83/2/3).

[871] The Court of Cassation, قرار محكمة تمييز جزاء رقم 1999/430 (هيئة عامة 1999/8/28).

[872] The Court of Cassation, قرار محكمة تمييز جزاء رقم 1997/697 (هيئة خماسية1997/12/22).

[873] Ibid.

[874] *Crimes Act 1914* div 2 s 3 pt (1).

[875] *Crimes Act 1914* div 2 s 3 pt (2).

[876] *Crimes Act* 1914 div 2 s 3LA (1) (A) (B) (C).

[877] See, Clifford, above n 739, 156.

[878] Ibid 158.

The second group in attendance, on the other hand, poses a problematic question as to how off-site attendance can be achieved. The two witnesses can attend and observe the physical searches and sign the initial report, but their attendance and observation is unattainable off-site, because digital analysis off-site takes time to accomplish and it is unpractical to allow witnesses to attend this digital analysis. Therefore, the *Criminal Procedure Law* 1961 requirement conflicts with the special needs of cyber searches and hinders remote searches as well. The attendance of two witnesses or a local notary is impractical in remote searches. By contrast, Australian's and the USA's perspectives provide the executing officers a more flexible approach to execute cybercrimes warrants by not demanding the presence of witnesses during the execution of a search.

7.6 Search Location

Computers are becoming an integral part of people's life.[879] On one hand, individuals, organisations, and public and private sectors rely on computers for daily work. For example, communications, financial transactions, such as online banking and shopping, social activities, such as dating and facebook websites, education and entertainment, and many other daily activities are processed by computers. On the other hand, people are used to seeing law enforcement officers leaving private premises and organisations carrying off computers hardware, CD's, floppy disks, and so on, to be further examined off-site. As a result, various individuals and organisations are significantly influenced by the search and seizure procedures, because digital assets are an integral part of their business operations and interrupting or depriving the business of computer systems may cause serious harm.

The essence of where the search is to be conducted is that most of individuals, organisations, and businesses rely on computers for daily work. This situation makes it harder for law enforcement officers to conduct a search on-site for long hours or perform a search off-site. In fact, it has always been said that corporations and businesses resist the removal of computers off-site, because of fear of intellectual

[879] The Jordanian government, in an effort to boost computer literacy, has initiated an unprecedented project called 'computer for every student'. This project offers a monthly payment plan, allowing university students to buy laptops at a competitive price: approximately 400 thousand laptops tax-free will be on-sale. The project also offers home owners the chance to buy a PC. See, 'Computer for Every Student', *Alrai Daily Newspaper* (Amman), 18 January 2008.

property and institutional data exposure as well as work interruption.[880] Also, conducting a search on-site for long hours causes work interruption and privacy intrusion.[881] Thus, the search location creates a dilemma between conducting the search and seizure on-site or off-site.

The balance that should be struck between on-site searches on the one hand, and the need to move the computer off-site on the other hand, will be described, and the legal perspective of each view will be examined.

7.6.1 Searching Computers On-site v. Off-site

Searching a computer on-site occurs when the executing officers look through a computer screen to see what information it may hold in relation to the search warrant.[882] There is also the possibility that the search on-site may go further by opening files and folders and viewing file properties and printing out documents.[883] For example, in cyberstalking offences, stalkers often use e-mail and chat rooms to harass their victims. If a search warrant were issued to search the offender's computer, the evidence in such a case would be held in his computer's RAM.[884] Therefore, investigators must perform and complete the search on-site, because RAM is a temporary and volatile storage device, and cutting off the power supply to remove the data off-site will erase all the information located on the RAM.[885] On the other hand, off-site search occurs when investigators remove computers, including documents, files, and programmes, to an off-site laboratory for a thorough search to seize evidence and then return any irrelevant materials.[886]

Forensic experts, scholars, and investigators have addressed the issue of whether computer searches should be conducted on-site or off-site. From a technical point of view, they argue that digital evidence recovery and analysis processes may impose technical and logistical restrictions on the officers executing the search and make an on-

[880] See, Jeff Lendino, '*Practical Guidance for Conducting Electronic Discovery*' Ontrack Data Recovery <http://www.ontrack.com> at 29 June, 2007

[881] Ibid.

[882] See, eg, Kerr, above n 687, 549 . Kerr uses 'exposure-based approach'. Under this approach the search occurs when data stored on hard disk drives is observed or exposed to human observation.

[883] Ibid.

[884] Anthony Reyes et al, above n 731, 169.

[885] See, Belzer, above n 835.

[886] See, Brenner and Frederiksen, above n 596.

site search impossible or impractical.[887] Hence, the majority of forensic experts and DOJ guidelines recommend that computer searches and acquisition of data must be performed off-site.[888] They argue that the conditions in the laboratory, such as temperature, time flexibility, expert support, and other technical issues, such as overcoming password protected systems, are better controlled in the laboratory than in the search location.[889] On the other hand, Bernner argues that cyber searches should not be conducted off-site.[890] From a practical point of view, she explained that computer searches using Automated Search Techniques, such as a key-word search, will take less time and effort to perform on digital containers compared with hardcopy files search.[891] She said:

> The benefits of electronic search techniques are that they are fast, accurate, and within the narrow scope of their capabilities. If the officers are searching for very specific information and know one or two exact phrases or words to search for, a comprehensive electronic search can be conducted in a matter of hours…[892]

She added that the off-site search would cripple businesses and generally causes interruption as long as the investigation continues.[893]

[887] However, Brenner and Frederiksen argue that if the computer to be searched is a personal one, such as a laptop, or PC with a small storage capacity, the off-site search will be unreasonable, because current forensic tools are able to locate the evidence in a reasonable period of time. See especially, Brenner and Frederiksen, above n 596, 72.

[888] The DOJ search guideline stated 'Attempting to search files on-site may even risk damaging the evidence itself in some cases. Agents executing a search may learn on-site that the computer employs an uncommon operating system that the on-site technical specialist does not fully understand. Because an inartful attempt to conduct a search may destroy evidence, the best strategy may be to remove the hardware so that a government expert in that particular operating system can examine the computer later. Off-site searches also may be necessary if agents have reason to believe that the computer has been 'booby trapped' by a savvy criminal. Technically adept users may know how to trip-wire their computers with self-destruct programs that could erase vital evidence if the system were examined by anyone other than an expert...In these cases, it is best to seize the equipment and permit an off-site expert to disarm the program before any search occurs'. See, Computer Crime and Intellectual Property Section Criminal Division, above n 633. See also, Peter Toren, *Intellectual Property and Computer Crimes* (2003) 8-27.

[889] See, eg, Franklin, above n 787, 162. See also, Anthony Reyes et al, above n 731, 169. See also, Kipper, above n 846, 100. See also, Bill Nelson et al, *Guide to Computer Forensic and Investigations* (2nd ed, 2006) 160. See also, Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[890] See, Brenner and Frederiksen, above n 596, 59.

[891] Ibid.

[892] Ibid.

[893] Ibid.

a) Jordan

General prosecutors and executing officers enjoy a wide measure of discretion in the execution of search warrants. The Court of Cassation held that the GP and executing officers play a master role in investigating crimes and executing search warrants.[894] Hence, they are the only authority which determines whether the search should be conducted on-site or off-site. However, the *Criminal Procedure Law* 1961 permits the GP to hire an expert to assist in investigation and decision-making. Thus, it is highly likely that the GP will apply the experts' opinion on whether computers system should be searched on-site or off-site.

b) Australia

In Australia, the *Crimes Act* 1914 amendment, Law Enforcement Powers Relating to Electronically Stored Data, addresses the issue. Subsection 3K (2) (a) permits the executing officers to move computers from premises to the forensic laboratory for further search, examination, and analysis. The Act places limits, however, on the power of law enforcement to move objects off-site and seize documents. Subsection 3K (2) (A) (i) allows search off-site under two specific circumstances: first, when the on-site search is less practicable, because it is time-consuming and very expensive and second, when that the search needs specialist assistance which is not available at on-site. The Explanatory Memorandum at pp 14-15 provides some more guidance as to what parameters the executing officers should depend on to move the computers off-site for examination. It states:

> The proposed amendment would allow a thing to be moved from the search premises to another place for examination or processing, without the occupier's consent, where it is significantly more practicable than processing the thing at the search premises and where there are reasonable grounds to believe that the thing contains or constitutes evidential material. In determining whether it is significantly more practicable to process or examine the thing at another place, the executing officer or constable assisting must have regard to the timeliness and cost of processing or examining the thing at another place rather than on site and to the availability of expert assistance. In other words, the proposed amendment would permit a thing to be moved to another place if it is significantly faster or less costly to process or examine the thing at that other place or easier to obtain expert assistance to process or examine the thing at the other place.[895]

[894] The Court of Cassation, قرار محكمة تمييز جزاء رقم 2004/725.

[895] Explanatory Memoranda, Cybercrimes Bill 2001 (Cth) 14-15.

It is clear that the investigators must assess the possibility of conducting the search on-site and seizing only related items, or move the object, such as a hard drive, or makes a mirror copy at the forensic lab to conduct the second phase of the search, i.e. the digital phase.[896]

c) USA

Courts have upheld off-site searches to be reasonable under the Fourth Amendment relying on the premise that on-site search is unfeasible. The courts have held that conducting a search for property listed in the warrant after moving it to another site for further examination is a legal search as long as conducting that search on-site would be impractical. In *United States v. Sissler,* for example, the court held that the police were not obliged to inspect the computer and disks at the site of the search, because they were password protected which takes time and effort to crack as well as an expert to perform the examination off-site.[897] In another case, *United States v. Hill,* the court held that the police were not required to bring with them equipment capable of reading computer storage media and experts to operate them.[898] The Court established two reasons why the search off-site is more reasonable than the on-site search.[899] It stated that the on-site search poses two significant problems.[900] The first is the risk of damaging or destroying evidence or compromising the integrity of the evidence if the examination is carried out at the place to be searched.[901] The second problem was long time required to search files at the scene as it will take many hours and perhaps days to accomplish.[902]

The 2001 Guidelines, on the other hand, explain the circumstances under which seizure and search off-site of computer hardware containing evidence are justified:

[896] For example the New Zealand Commission Law proposed five factors to be considered in determining whether the search off-site is justified or on-site search must be performed. These factors are: 1) whether other options are practicable in the circumstances; 2) whether the evidence is not able to be accessed without using off-site equipment or expertise; 3) the risk of damaging or destroying evidence if the examination or analysis is carried out at the place to be searched; 4) whether using off-site equipment or expertise is necessary to preserve the evidential integrity of the item; and 5) the length of time it would take and the level of intrusiveness of the search if the examination or analysis were carried out at the place where the search occurs. See generally, New Zealand Law Report Commission, above n 769, 207.

[897] *United States v. Sissler,* No. 90-CR-12, WL 239001 (W.D Mich, 1991).

[898] *United States v. Hill*, 459 F.3d 966, (9th Cir 2006).

[899] Ibid.

[900] Ibid.

[901] Ibid.

[902] Ibid.

> As a practical matter, circumstances will often require investigators to seize equipment and search its contents off-site. First, it may take days or weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information. Agents cannot reasonably be expected to spend more than a few hours searching for materials on-site, and in some circumstances (such as executing a search at a suspect's home) even a few hours may be unreasonable. Given that personal computers sold in the year 2000 usually can store the equivalent of ten million pages of information and networks can store hundreds of times that (and these capacities double nearly every year), it may be practically impossible for agents to search quickly through a computer for specific data, a particular file, or a broad set of files while on-site. Even if the agents know specific information about the files they seek, the data may be mislabelled, encrypted, stored in hidden directories, or embedded in 'slack space' that a simple file listing will ignore. Recovering the evidence may require painstaking analysis by an expert in the controlled environment of a forensics laboratory.[903]

The DOJ guideline explicitly encourages law enforcement officers to move and conduct the search off-site even though they know in advance the files they seek. Therefore, in their affidavit for a search warrant, US executing officers must provide detailed information of where the search will be conducted and why it should be conducted off-site.[904] For example, in *United States v. Comprehensive Drug Testing, INC,* the warrant stated: 'If the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data'.[905]

d) Comparative Legal Analysis

The problem of the location search is more severe in areas where the computers, including data, form the backbone of the businesses operations, such as banks and insurance companies. The problem occurs when computer hardware, including data, are removed and transferred off-site for intensive search.

Scholars and pundits have addressed the question whether to search computers on the premises or off-site. They have approached the problem in different ways. The majority who supported off-site searches based their arguments mainly on technical grounds. This argument may be challenged on the ground that law enforcement officers are able

[903] Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[904] See, Rhoden, above n 779, 124.

[905] *United States v. Comprehensive Drug Testing, INC,* 473 F. 3d 915, 963 (9th Cir, 2006).

to make a mirror copy of the entire contents of the computers on-site and examine them carefully off-site without removing computer hardware from the work site. A mirror copy search would alleviate the problem of seizing the entire computer and causing work interruption. In addition, in several scenarios, on-site searches suffice. For example, unless they are password protected or encrypted, some files can be swiftly identified by opening and printing them out. Child pornography often takes a specific format and can be visibly identified, such as JPEG files.

Brenner, who supported on-site search, backed her argument by showing the power of Automated Search Techniques. This argument may be challenged on the ground that the Automated Search, although efficient, is limited because the key word search is only effective if the officer searches for specific information, such as names, numbers, or phrases; otherwise, the search yields a high number of false hits.[906] In addition, the problems of encryption, deleted files, and password protected files tend to limit the capability of the Automated Search Techniques.

Because none of the above-mentioned viewpoints is entirely accepted, the option in the matter is left to the law enforcement officers to decide in a case-by-case manner.

In Jordan, the current procedures ignore the nature of digital evidence and the harm that could be inflicted on businesses or a third party, because no limits have been set to control the officers' discretion. The *Criminal Procedure Law* 1961 considers the executing officer as the master who assesses the appropriate measures for executing the search warrant. Executing officers exercise absolute discretion in determining whether a computer search should be conducted on-site or off-site. Though unrestricted discretionary power is a half century old, it is applicable to cyber searches. The application of this principle to cyber searches, however, may cause a problem if the GP chooses to move all the equipment off-site without knowing anything about it or making an assessment of whether on-site search is possible or not. In Australia and the USA, the decision to investigate on-site or off-site is discretionary and depends upon the circumstances of a case. The *Crimes Act* 1914 and court decisions expressly permit the executing officers to move computers off-site if necessary. However, their discretionary

[906] False hits are documents that have the same words of a particular search, but have no evidentiary value and are beyond the scope of the warrant. For more information see, Clancy, above n 718, 211.

power is not unrestricted. The *Crimes Act* 1914 and the JOD's guidelines specified particular circumstances under which the search off-site is conducted.

Thus, the matter should not be left without guidance on this critical issue. Although Jordanian investigators should be given the necessary power to transfer the mirror copy or any other items from the search premises for further examination, this power should be restrained to situation where it is not reasonably practicable to conduct the digital search at the place where the search occurs. Law enforcement officers should request in the search warrant that a part of the search will be carried out off-site. This request must be justified on reasonable grounds, such as the search on-site is not feasible and no other practical alternative exists.[907]

7.7 Conclusion

The effectiveness and the efficiency of cybercrimes investigation processes depend significantly on a precise criminal procedure law that identifies the unique nature of cybercrime searches. Although criminal investigation procedures, including arrest, interrogation, and detention have not been affected by the unique nature of cybercrime, traditional search and seizure rules are found to be defective or inappropriate in the cyber world. Some of the conventional search warrant procedures, however, are efficient to meet cyber search requirements, such as the threshold for issuing and obtaining search warrant.

Cyberspace and the digital revolution have directly influenced the different perspectives of search and seizure procedures. Australia and the USA have responded to cybercrimes in a more effective manner and, therefore, Australia amended particular provisions of *Crimes Act* 1914 to meet cyberspace's particularity; meanwhile, the USA issued guidelines for search and seizure of computers. Furthermore, the judicial expositions in both countries, specifically in relation to search warrant execution, probable cause, particularity and search location, have contributed in shaping the search and seizure regime in the cyber world. Meanwhile, Jordanian legislation has witnessed no changes, because of either rarity of cybercrimes or lack of critical skills to make the distinction

[907] This justification was introduced in *United States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir, 1982).

between real world and cyber world searches. Either way, the experience of Australia and the USA in this area is important to inspire the Jordanian counterpart.

Important sections of the search procedures must be amended or appropriate provisions be added to the *Criminal Procedure Law* 1961 to meet cyberspace's unique environment. The conventional search warrant makes no difference between searching and seizing physical items, and data, and it ignores the unique nature of cyber search. These discrepancies should be made to avoid the problem of intermingled documents and guide law enforcement to the right approach. Also, the probable cause made out in cybercrimes and the actual nexus between the physical place to be searched and IP addresses requires law enforcement officers experienced and qualified in cybercrimes. Therefore, guidelines should be established for this purpose.

The search scope and location in cyber world is controversial. Forensic experts urge more flexible approach permitting an off-site search. The nature of cyberspace makes the particularity requirements and on-site search in cybercrimes impractical and, therefore, a flexible approach that grants executing officers more leeway on what and where to search must be adopted. However, a mirror copy search is recommended for computers shared by many users, such as in organisations, to lesson the harmful consequences of the physical search.

8 SEARCHING AND SEIZING DIGITAL EVIDENCE WITHOUT A WARRANT

Introduction

Similar to the collection of physical evidence, the process for collecting digital evidence must comply with the laws and judicial precedents that control the process of physical evidence collection. The main concern of these laws and judicial decisions is to protect individual privacy as well as to collect evidence properly. Thus, while the laws have crafted legal instruments - subpoenas and search warrants are the most common legal instruments - permit entering private properties and obtaining evidence, the same laws established a number of exceptions that permit enforcement officers to enter private property in order to obtain evidence in specific circumstances.

Although these exceptions constitute a serious infringement of privacy rights, they are crucial in situations where obtaining a search warrant is very difficult or impracticable. Indeed, without such exceptions it would be impractical, if not impossible, for law enforcement officers to administer justice in a fair, timely and efficient manner. Therefore, while legislation maintains privacy rights, it also typically provides law enforcement officers with exceptional power for search and seizure without the need for formal prior authorisation through the issue of an official search warrant.[908]

There are specific exceptions when obtaining a warrant is impracticable and would obstruct crime prevention and, thus, law enforcement officers are authorised by statutes and judicial precedents to enter private premises, to search for and seize incriminating evidence, without the need for formal prior authorisation through the issue of an official search warrant. In Jordan, Australia and the USA, search warrant exceptions are well established in traditional searches and have been confirmed and applied in law enforcement practice and judicial precedents. Yet each country's approach to warrantless search is different. The application of these exceptions to digital content is still ambiguous, because prosecutors and judges, particularly in Jordan, lack the knowledge and experience necessary to determine whether these exceptions are

[908] Tronc, Crawford, and Smith, above n 677, 47.

applicable to digital content, and how law enforcement officers should handle these exceptions in the field of cybercrime. Furthermore, there are no judicial precedents, professional or academic opinions on these issues to date.[909] By contrast, Australian and US experience in this area is expanding at an increasing rate.

The objective of this chapter is to demonstrate that different aspects of the current Jordanian exceptions for warrantless search are very limited and narrowly defined to circumstances that may not be applicable to digital searches. It deals with the traditional legal concepts of warrantless searches and seizures as established in the *Criminal Procedure Law* 1961. In the following section, the aspects of warrantless search exceptions will be identified and discussed in both traditional and digital search contexts. It then proceeds with an examination and assessment of each exception and its applicability and compatibility with searches and seizures of digital evidence.

8.1 Exceptions That Allow Searching and Seizing without a Warrant

In specific circumstances, the public interest in justice in a society outweighs personal privacy rights. The need for a swift and efficient system of search and seizure is globally recognised. International Human Rights Law for example, recognises that individual privacy rights are not absolute and must be balanced with a government's interest in detecting and combating crimes.[910] Although the *Jordanian Constitution* enshrines the privacy of dwellings, it allows a limited exception in which law enforcement officers may enter private properties without a search warrant, in specific circumstances prescribed by the law, to protect life and property, preserve evidence, to search for evidence or to make an arrest.

[909] On more than one occasion, the Minister of Justice has enunciated that the judicial body lacks the necessary experience and skills to adjudicate on the issues arising from information technology. Therefore, the Ministry of Justice established a programme to send judges abroad to obtain Master degrees from the USA and other English speaking countries. See, eg, *Judges to Obtain Master Degree from the United States* (2008) Ammonnews <http://www.ammonnews.net/arabicDemo/article.php?issue=&articleID=8331>at 5 February 2008.

[910] See, eg, Bronitt and Gani, above n 409, 161.

This section examines search warrant exceptions which have been stipulated in the *Criminal Procedure Law* 1961, the Australian *Crimes Act* 1914, and USA judicial precedents on search and seizure of electronic devices. It assesses whether the exceptions which have been addressed by the *Criminal Procedure Law* 1961 are applicable to digital searches. The exceptions that are examined here are categorised as: exigent circumstances, consent searches, plain view searches, and search incident to a lawful arrest. They are examined in considerable detail by providing a general description of traditional procedures and then comparing these to the digital context.

a) Jordan

In Jordan, the *Criminal Procedure Law* 1961 is the keystone that allows exceptions against warrantless search. These exceptions were created in an attempt to balance the protection of privacy with the need for swift enforcement action to prevent a crime or to preserve incriminating evidence. Since its creation in 1961, a very rapid and significant development in information technology combined with new criminal trends and their modus operandi have emerged. In addition, unique and unusual evidence is constantly encountered at the new crime scenes, which make the 1961 Act less responsive to the diverse needs and circumstances of cybercrimes.

Provision 93 of the *Criminal Procedure Law* provides law enforcement officers with the right to search private premises without obtaining a search warrant. It authorises officers to enter and search any house or place without a search warrant if any of the following circumstances occur:

1) If the police officer has a reasonable suspicion that there is a crime being committed or has just been committed.[911]

2) If the dwelling owner is calling for a help.[912]

3) If a resident is calling for help and the officer has a reasonable suspicion that there is a crime is being committed or has just been committed.[913]

[911] *Criminal Procedure Law 1961*(93/1).
[912] *Criminal Procedure Law 1961*(93/2).
[913] *Criminal Procedure Law 1961*(93/3).

4) If the police officer is pursuing a suspect and the latter entered a house, the police officer may search that house and the suspect.[914]

The *Criminal Procedure Law* 1961 set forth only four situations where enforcement officers are able to enter a house or place without a search warrant. Law enforcement officers, however, are not the only authority to conduct warrantless searches; other governmental agencies also have been given the power to perform searches and seizures, which are essential to the achievement of their jobs, without the need for formal prior authorisation through the issue of official search warrants. For example, the *Customs Law* 1998 authorises custom officers to carry out inspections, examine any luggage, or to 'stop and frisk search' travellers.[915] Prison security guards are also authorised to perform searches and seizures inside prisons.[916] Nevertheless, provision 93 of the *Criminal Procedure Law* 1961 is the basis which provides law enforcement officers with the opportunity to perform warrantless searches and seizures of private property.

b) Australia

The Australian *Crimes Act* 1914 has been amended to be in line with the current practices with respect to search warrants (see previous chapter). Similar to the Jordanian *Criminal Procedure Law*, but in a more detailed way, the *Crimes Act* 1914 Divisions 3, 3A and 4, addresses warrantless searches and seizures.

1) Division 3, entitled 'Stopping and Searching Conveyance',[917] addresses searches without a warrant in emergency situations. Under section 3T, on reasonable ground, law enforcement officers have the power to search without a warrant a vehicle of any sort.

2) Division 3A empowers law enforcement officers to stop, question and search persons in relation to terrorist acts without a warrant. Section 3UD authorises law enforcement officers to conduct an ordinary search or a

[914] *Criminal Procedure Law 1961*(93/4).
[915] *Customs Law 1998* para 12 s 2 179 (a) (d).
[916] *Prisons Law 1953* (16).
[917] According to the *Crimes Act* 1914 Part I conveyance includes an aircraft, vehicle or vessel. Part IAA defines conveyance in relation to a search of person, as a conveyance operated or occupied by a person at anytime within 24 hours before the search commenced.

frisk search of the person,[918] a search of anything that is or that the officers suspects on reasonable grounds to be under the suspect's immediate control.[919]

3) Division 4, entitled 'Arrest and related matters', addresses warrantless searches incident to a lawful arrest. Section 3ZB empowers law enforcement officers to enter premises to arrest offenders[920] and search the premises for the person in order to prevent the concealment, loss or destruction of evidence relating to the offence.[921] Also, sections 3ZE and 3ZF respectively empower officers to conduct a frisk and an ordinary search of an arrested person. Section 3ZG permits searching the arrested person's premises and seizing things in plain view.

Unlike Jordan, judicial precedents in Australia also play a significant role in crafting solutions to problems arising in searches and seizures of digital evidence.

c) USA

In the USA, courts have gradually established new standards for the application of the Fourth Amendment to the digital environment.[922] In the 1960s, the courts established strict requirements for search warrants. For example, in *Terry v. Ohio,* the court stated that 'the police must, whenever practicable, obtain advance judicial approval of searches and seizures through a warrant procedure'.[923] This approach protects the rights of the criminal more than it grants the police the power needed to crack down offences.[924] In the 1970s, the trend was to provide the police with more appropriate tools and powers to tackle crimes. Harris has opined: 'The USA also strictly imposes more restrictions on law enforcement practices through the exclusion of evidence than does any other nation…slowly and carefully, the court is ceding to the police more authority and flexibility to do their jobs effectively'.[925] Therefore, a balanced standard

[918] *Crimes Act 1914* (Cth) div 3A s 3UD (1) (b) (i).
[919] *Crimes Act 1914* (Cth) div 3A s 3UD (1) (b) (ii).
[920] *Crimes Act 1914* (Cth) div 4 s 3ZB (1) (b).
[921] *Crimes Act 1914* (Cth) div 4 s 3ZB (3) (b).
[922] See, eg, Scott, above n 292, 530-531.
[923] *Terry v. Ohio*, 392 U.S. 1, 20 (1968).
[924] See, Franklin, above n 787, 206.
[925] Daniel M Harris, 'The Supreme Court's Search and Seizure Decisions of the 1982 Term: The Emergence of a New Theory of the Fourth Amendment' (1984) 36:41 *The Baylor Law Review*, 41.

was adopted to protect individual privacy and to give law enforcement power to investigate crimes. For example, in *Katz v. United States*, Franklin J. commented that '…the warrant is required where practical, but that the issue of practicality will often be measured with a very narrow yardstick…if circumstances justify and if the courts have established a clear "exception" then no warrant is required'.[926] In the post-September 11th period, law enforcement power to combat crimes and secure evidence, as well as to conduct warrantless searches and seizures, has been reinforced. Stephens and Glenn, opine that '…searches and seizures conducted outside the judicial process…[are] subject to only a few jealously and carefully drawn exceptions …the list of exceptions now seems to include much of what is characterised as routine police activity'.[927] Accordingly, search warrant exceptions seem to have become the norm and have drifted beyond the limits of what the Fourth Amendment allowed.

d) Comparative Legal Analysis

Provision 93 of the Jordanian *Criminal Procedure Law* 1961 is the only provision for warrantless searches and seizures. In the first exception to the requirement for a warrant, the need for formal prior authorisation through the issue of an official search warrant is not necessary when an exigent circumstance is present. Exceptions two and three presume that a search warrant is not necessary if the owner of property or a person who owns or has authority or control over the property searched requests the search. There is a distinction between the two exceptions. In the second exception, the officer does not have to have a reasonable suspicion in order to conduct the search if the owner agrees to allow the property to be searched. In the third exception, the officer must have a reasonable suspicion of criminal activity if a resident but not the owner of the property consents. Exception four presumes that a search warrant is not necessary when a search accompanies an arrest. Although these four exceptions apply without complications to the needs of classical crimes and physical places such as dwellings, cybercrimes and digital evidence pose serious challenges to the application of provision 93.

Although the *Crimes Act* 1914 widened the scope of the power to execute search warrants to permit the search and seizure of digital evidence effectively,[928] power to

[926] Ibid 207.

[927] Stephens and Glenn, above n 533, 84.

[928] See, Bronitt and Gani, above n 409, 160. See also, Chapter 7 for more information about search and seizure with a warrant.

execute searches without a warrant was not amended accordingly. Division 3 and 3A permit warrantless searches in narrowly defined cases. Division 3, for example, only addresses exigent circumstances in a limited framework and in a particular context associated with transportation searches, and Division 3A is only applicable to terrorist offences. Unlike Jordan, however, Australian courts play a significant role in applying some of those circumstances to digital content. The USA's approach, by contrast, is more advanced and highly efficient. Search exceptions were created and developed through judicial precedents and warrantless searches and seizures were mainly guided by the precedents of other court decisions made in similar cases.

With the advent of information technology, legislation and courts are confronted with challenging cases associated with cybercrime and digital evidence. The *Criminal Procedure Law* 1961 does not contain provisions in relation to warrantless searches and seizures of digital evidence. Law enforcement officers and public prosecutors, therefore, must abide by the law that governs warrantless search of traditional objects. This is like putting the wrong key in a lock which it does not open. Meanwhile, in Australia and the USA, courts actively addressed warrantless searches and seizures of digital evidence, so that their decisions might be seen as a useful model for Jordan. Even with this, the application of the search warrant exceptions to cybercrime and digital evidence can still be described as a legal minefield.

The exceptions to the use of a warrant addressed in the *Criminal Procedure Law* 1961 will be examined below and discussed in detail in the context of current experience, practices, and developments associated with cybercrime and digital evidence searches and seizures.

8.1.1 Exigent circumstances

In the criminal procedure context, an exigent circumstance means 'an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property or to forestall the imminent escape of a suspect or destruction of evidence'.[929] Another definition, presented by Conser, Russell and Paynich, defines this circumstance

[929] John Feridico, *Criminal Procedure for the Criminal Justice Professional* (9th ed, 2005) 615.

as ‘conditions that create a need for immediate action to prevent the destruction of evidence’.[930] According to Hatonn, the author of *First Step: Whether Long or Short - The Road Matters Not if the First Step is Never Taken,* ‘exigent circumstances means the evidence is about to be destroyed or taken away, and therefore there is not enough time to obtain a warrant’.[931] These definitions highlight the basic features of exigent circumstances: imminent threat to life or property; imminent escape of a suspect or destruction of evidence; and application only in serious and urgent emergencies. In either case, exigent circumstances must be established by demonstrating specific facts showing that urgency and necessity exists to authorise warrantless search and seizure.[932] These facts are examined by courts to determine the existence of exigent circumstances.[933] Among other things, the courts examine law enforcement officers' experience and their training and common sense, as these are the important factors that are taken into account when determining the exigent circumstance.[934]

Exigent circumstances can exist in digital context. The same exigent circumstances of physical evidence can be extended to apply to digital evidence. However, unlike most other evidence, digital data can usually be destroyed or contaminated by the click of a button. For example, in a case of a natural disaster, such as flooding, the exigent circumstance permits the agent to seize the computer hardware component, but this circumstance, according to Hugh, gives him no authorisation to conduct a digital search.[935] To conduct an in-depth digital search, a warrant must be issued because computer forensics searches take a long period of time to be completed usually and, therefore, off-site investigators have enough time to obtain a search warrant.[936] This point of view is the core of the exigent circumstance exception argument in digital environments.

[930] James A Conser, Gregory D Russell and Rebecca Paynich, *Law Enforcement in the United States* (2nd ed, 2005) 157.

[931] Gyeorgos C Hatonn, *First Step: Whether Long or Short - The Road Matters Not if the First Step is Never Taken* (1995) 50.

[932] See, eg, Ronald J Bacigal, *Criminal Law and Procedure: An Introduction* (2nd ed, 2002) 207.

[933] See, eg, Northwestern University School of Law, ‘Arresting a Suspect in a Third Party's Home: What is Reasonable?’ (1981) 72 *the Journal of Criminal Law & Criminology* 293, 313.

[934] Ibid.

[935] See, eg, Scott above n 293, 25-13.

[936] Ivan Orton, ‘The Investigation and Prosecution of a Cybercrime’ in Ralph D. Clifford (ed), ‘*Cybercrime: the Investigation, Prosecution and Defense of a Computer-Related Crime*’ (2nd ed, 2006) 97, 145. See also, Scott, above n 292.

Legal systems acknowledge the need for a swift response to urgent situations encountered by law enforcement officers. Jordan, Australia and the US each approach the identification of exigent circumstances exception differently.

a) Jordan

In Jordan, provision 93/1 of the *Criminal Procedure Law* 1961 addresses indirectly the exigent circumstances exception. It clearly stipulates the right of law enforcement officers to enter and perform an unlimited search of any property, including dwelling houses, by force if necessary, without a warrant when they have probable cause to believe that a crime is about to be committed, is being committed, or has just been committed. Under any of these exigent circumstances, officers can search for evidence or preserve evidence without a search warrant.

Although Jordan's *Criminal Procedure Law* does not enunciate the purposes of a warrantless search under the exigent circumstances exception, it provides law enforcement officers with the necessary power to enter, and perform a search without a warrant under three certain circumstances, namely, (1) a crime is about to be committed; (2) a crime is being committed; and (3) a crime has just been committed. However, Kamal Al-saeed, a prominent Jordanian legal scholar, argued that these three circumstances are illustrative only and not intended to be exclusive or exhaustive.[937] The same scholar has criticised the *Criminal Procedure Law* for granting officers broad power in exigent circumstances.[938] He has opined that the exigent circumstances should not permit officers to perform a search, but only to seize or perform any action necessary to alleviate the exigent circumstances.[939] However, Al-saeed's argument was originally made in the context of traditional searches.

In the digital context, Jordanian courts have not yet examined this doctrine; however, exploring the view of Australia and the USA may be helpful in predicating how Jordan's courts will rule on this issue.

[937] كامل السعيد, above n 699, 400.
[938] Ibid.
[939] Ibid.

b) Australia

In Australia, by contrast, the *Crimes Act* 1914 addresses two kinds of urgent circumstances that justify searches without the need for formal prior authorisation through the issue of an official search warrant. The first is to prevent the evidence from being concealed, lost or destroyed. For example, section 3T (1) (b) of the *Crimes Act* 1914 authorises law enforcement officers to perform warrantless searches on reasonable grounds, in order to prevent a thing from being concealed, lost or destroyed.[940] The second arises from compelling or serious and urgent circumstances.[941] For example, in *The Queen v. Michael Malloy*, Crispin J stated:

> I am prepared to assume for present purposes that there is a common law power of search and seizure in exigent circumstances. Such a power might enable a police officer coming unexpectedly upon a situation involving a grave and imminent threat to public safety to intervene and save lives without acting unlawfully and thus exposing himself or herself to an action for trespass. Nonetheless, the search of a person's private property and the seizure of his or her belongings constitutes a serious invasion of privacy and any common law power to so infringe the rights of others could be justified only by compelling circumstances.[942]

This decision offers a very different view of the exigent circumstances exception. It did not delineate exigent circumstances scenarios, but any compelling circumstances might permit search without a warrant. Furthermore, the court's opinion extended the application of the exigent circumstances to search private premises and not only conveyances as mentioned in the law.

c) USA

In the USA, exigent circumstances have long been held as a potential exception to search warrant requirements.[943] The courts have had numerous opportunities to consider exigent circumstances in both searches and seizures of physical and digital evidence. In *Cupp v. Murphy* (1973), investigators inspected and took a sample of scrapings of dried blood under the suspect's fingernails without the latter's permission, because they did not have enough time to obtain a warrant, and during the time needed to obtain a

[940] *Crimes Act 1914* (Cth) S 3T (1) (b).
[941] *Crimes Act 1914* (Cth) S 3T (1) (c).
[942] *The Queen v. Michael Malloy* (1999) 118 ACTSC.
[943] See, Moore, above n 597, 113.

warrant, the suspect could have washed his hands.[944] The court upheld the officers' action.[945] In digital searches, in *United States v. David* the fragile nature of digital evidence led the court to authorise the search of a Personal Digital Assistant (PDA) under the exigent circumstances doctrine.[946]

Courts examined exigent circumstances thoroughly and requirements have been developed for the successful use of the exigent circumstances doctrine. These requirements are as follows:[947]

1) The degree of urgency involved.
2) The amount of time necessary to obtain a warrant.
3) Whether or not the evidence is about to be removed or destroyed.
4) The possibility of danger at the site.
5) Information indicating the possessors of the contraband know the police are on their trail.
6) The ready destructibility of the contraband or how easy the evidence is to destroy.

Furthermore, courts review the totality of the circumstances, including the severity of the crime being investigated,[948] as well as the officer's perception of the exigent circumstance in light of their experience and training,[949] to assess the magnitude of the potential danger.[950] The courts also examine whether law enforcement officers have had enough time to obtain a search warrant before the evidence is moved or destroyed.[951] Accordingly, in many cases, courts have suppressed the evidence recovered during a

[944] See, George F Cole and Christopher E Smith, *Criminal Justice in America* (4th ed, 2005) 135.

[945] Ibid.

[946] Ibid 114.

[947] *United States v. Reed*, 935 F.2d 641 (4th Cir, 1991). (Cited from *United States v. Taylor*, 650 F.2d 526 (4th Cir. 1981).

[948] See, Scott, above n 293, 25-13.

[949] See, *United States v. Jonathon Dean*, 234 F. 780, 782 (4th Cir, 2007).

[950] See, *Mora v. Gaithersburg Police Dept*, 519 F. 3D 216 (4th Cir. 2008). 'The Court held that in circumstance that suggests a grave threat and true emergency, law enforcement is entitled to take whatever preventive action is needed to defuse it'.

[951] See, *People v. Camilleri* 220 Cal.App.3d 1199, 1206 (1990). See also, *United States v. Todd Andrews*, 442 F. 3d 966 (7th Cir, 2006). 'When reviewing a warrantless search to determine if exigent circumstances exist, a court conducts an objective review, analysing whether the government has met its burden to demonstrate that a reasonable officer has a reasonable belief that there is a compelling need to act and no time to obtain a warrant'.

search that was executed pursuant to exigent circumstances, because the investigators had enough time to obtain a warrant but failed to do so.[952]

d) Comparative Legal Analysis

Although the use of the exigent circumstance doctrine in cybercrime searches is permitted, a controversy erupted over the scope of the search and whether the exigent circumstances doctrine allows officers to conduct a thorough digital search or only the seizure of the physical part.[953] Hugh's argument is that, in some scenarios, exigent circumstances, it is quite reasonable but not in cybercrime investigations where it is not likely to be accepted, because exigent circumstances in cybercrime and digital evidence needs more than the seizure of the physical items. For example, where a police officer investigating a drug related crime finds a laptop which the suspect was going to destroy, the seizure without a warrant would protect the laptop including its digital content. In this example, the officer is able to preserve the laptop by seizing the hardware parts and he must then obtain a search warrant to conduct a digital search. But if the officer while investigating a victim's system discovers that a hacker or intruder has logged onto the system, perhaps to destroy evidence, the officer must perform a limited search to preserve the data in its current state. It can be seen that in the two scenarios, this exception should not allow investigators to exercise a comprehensive or a thorough computer search,[954] but simply prevent the imminent destruction of evidence and preserve data.

While Jordan and Australia have not developed the application of the exigent circumstances doctrine to digital evidence, the US courts recognised the authority of law enforcement officers to seize electronic storage devices in circumstances in which there is an immediate danger of losing data, or to prevent the imminent destruction of electronic devices (hardware components). The same approach can be adopted by Jordan, because the three circumstances that permit the search in exigent circumstance mentioned in the law are illustrative only and not intended to be exclusive or exhaustive. Therefore, the traditional practice of law enforcement in an exigent circumstance can be extended and applied to search digital evidence in which there is an immediate danger of losing data, or to prevent the imminent destruction of hardware

[952] See, eg, *United States v. Young*, 909 F.2d 442, 446 (11th Cir.1990).
[953] See Hugh's and Al-saeed's argument page 222 and 223.
[954] See, eg, Franklin, above n 787, 212.

components. The main purpose of the warrantless search is to preserve evidence of a discovered crime. Law enforcement officers, therefore, should be given the authority to seize and search electronic storage devices and evidence in circumstances in which there is an immediate danger of losing data, or to prevent the imminent destruction of hardware devices.

8.1.2 Consent

According to *Black's Law Dictionary* 'consent' means 'voluntary agreement by a person in the possession and exercise of sufficient mentality to make an intelligent choice to do something proposed by another'.[955] This definition of consent is clear in that it includes the essential characteristics of consent. Thus, consent must include (1) free choice; (2) ability to make a decision; (3) communication by one person to another.

In many jurisdictions, consent to search is a well recognised exception to the search warrant requirements. Residents, occupants or owners of the premises can agree to waive the protection afforded by the constitution or any statute and permit a warrantless search.[956] Under this exception, officers may seek to obtain explicit or implied consent. The consent can be for limited searching of a specific object or may be for unlimited searching of premises.[957] In addition, the consent should be obtained voluntarily from a particular individual who has authority to approve the search.[958] These main pillars of the consent are: (1) the nature of the consent, for example, explicit or implied; (2) the scope of the consent, for example, limited or unlimited; (3) the time of the consent, for example, before or after the search; and (4) the status of the person who grants the consent. Each of these is important in the consideration of the validity of the search.

[955] Henry Campbell Black et al, *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern* (7th ed, 1991) 210.

[956] See, eg, Jeremy D Calsyn et al, 'Warrantless Searches and Seizures' (1998) 86 (5) *Georgetown Law Journal* 1214, 1247. See also, Acker and Brody, above n 680, 182. هلالي عبداللاه احمد, *Searching Computer Systems and Suspect's Rights: Comparative Study* (Alaeldin Maghaireh, trans 1997) 161 [trans of: دراسة : تفتيش نظم الحاسب الالي و ضمانات المتهم المعلومات مقارنة].

[957] See, eg, Acker and Brody, above n 680.

[958] See, Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (2005) 153. See also, Acker and Brody, above n 680, 184. Matthew S. Cook, Third-Party Consent Under the United States and Utah Constitutions: Should Utah Adopt the Federal Standard? (1999) 1 *Brigham Young University Law Review* 381, 387.

Statutes and judicial decisions in Jordan, Australia and the USA address these issues differently.

a) Jordan

Even though the *Criminal Procedure Law* 1961 does not use the word ‘consent’, provisions 93/2 and 3 permit a warrantless search of premises upon request from the owner or the occupier of the premises. If the owner or the occupier of any building requests help, officers may enter and search the property without the need for formal prior authorisation through the issue of an official search warrant. This provision should not be interpreted as a green light to conduct consent searches, because the word ‘consent’ has a different meaning from that of ‘request’. According to *Black’s Law Dictionary* definition of consent, search consent is granted after negotiation between the consenting party and police officers, and the former makes a clear decision of consent. Meanwhile, ‘request’ means to ask for something and does not involve negotiation. Once the requesting party seeks help, however, officers have the right to search and seize evidential materials.

No judicial precedent has been rendered by the Jordanian courts with respect to the nature of the consent given for a search. When there is no national precedent, however, Jordanian courts may consider the Egyptian judicial precedents when making decisions because both legal systems are based upon Civil and Shariah laws. Jordanian legal scholars have, therefore, examined the Egyptian judicial precedents concerning the nature of the consent in terms of a traditional search.[959] According to Egyptian judicial principles in this matter, the validity of the consent is determined by examining all of the surrounding facts and circumstances of the case, such as the age of the person giving the consent.[960] The consent must be explicit and freely given,[961] so any threat, intimidation, or coercion, whether explicit or implied, will invalidate the consent.[962] Furthermore, the consent must be obtained before the search is conducted.[963]

[959] See كامل السعيد, above n 699, 395. See also, هلالي عبداللاه احمد, above n 956.

[960] Ibid.

[961] See, حسين علم, *the Law of Criminal Procedures* (Alaeldin Maghaireh, trans) 134-135 [trans of قانون الاجراءات الجنائية].

[962] See, eg, ,صلاح الدين جمال الدين, above n 740, 271.

[963] See, حسين علم, above 961. See also, ibid صلاح الدين جمال الدين.

b) Australia

By contrast, two specific provisions of the *Crimes Act* 1914 address consent to search: (1) written consent is required during a search warrant execution in order to take a photograph of the premises or of things at the premises incidental to the execution;[964] (2) written consent is required to conduct a strip search.[965] The Australian Law Reform Commission's Report, 'Criminal Investigation: An Interim Report,' recommended that:

> All searches and seizures be unlawful unless made pursuant either to a court order or warrant, or, if made without a warrant, in accordance ... (b) at the invitation, or with the consent, of the person occupying the premises or in charge of the vehicle in question,…the Commission considers, on balance that an appropriate solution is for searches on consent to be permitted, provided that such consent is entirely voluntary and is made after being informed of the right to refuse consent.[966]

The report highlights the importance of a consent search, providing an outline of the main features of a consent search.

Australian courts have had an opportunity to examine the consent search exception in terms of traditional searches. Generally speaking, the courts have held that a person may grant law enforcement officers the right to search premises. For example, in the joint judgment of Gaudron and McHugh JJ in *Plenty v. Dillon,* their Honours said: 'The common law has a number of exceptions to the general rule that a person is a trespasser unless that person enters premises with the consent, express or implied, of the occupier…'.[967] From this judgment, it is clear that the consent must be voluntarily given without express or implied coercion, intimidation, or threat. The suspect's voluntary consent to a search makes the warrantless search and the evidence discovered admissible in a court of law.[968] In addition, the Supreme Court of NSW has said voluntary consent must be informed consent.[969] Informed consent means that the consenting party has knowledge of his right to refuse to give consent.[970] For example, the officer must explain to the defendant that anything seized may be produced in

[964] *Crimes Act 1914* (Cth) div 2 s 3J (1) (a) (b).
[965] *Crimes Act 1914* (Cth) div 4 s 3ZH (3).
[966] The Law Reform Commission, *Criminal Investigation: An Interim Report*, Report No 2 (1975) 92, 97.
[967] *Plenty v. Dillon* (1991)171 CLR 635.
[968] See, eg, *Dpp v Leonard* (2001) NSWSC 797.
[969] Ibid.
[970] Ibid.

evidence to ensure that the consenting party is aware of his rights.[971] Law enforcement officers must inform the person, the subject of the search, of the right to refuse consent unless the consenting party is legally trained, or himself a police officer or other person known to be familiar with the search consent, and understands what is going to happen and the consent ramifications.[972]

c) USA

In the USA, consent to a warrantless search has received a great deal of juridical attention. The courts have had the opportunity to examine the nature and scope of the consent in both traditional and digital searches. In traditional searches, the consent exception is approached in a similar way to that found in Australia. For example, the consent must be obtained prior to the conduct of any search.[973] Also, the validity of consent is determined from the totality of all the circumstances[974] identified by the US courts to determine the validity of the consent search. The Supreme Court has listed factors to be examined before deciding the validity of a warrantless search conducted upon consent.[975]

1) The age of the person giving the consent;

2) The person's education, intelligence, and mental condition;

3) The person's physical condition;

4) Whether the person was under arrest; and

5) Whether he had been advised of his right to refuse consent.

In the digital context, in *Williford v. Texas,* the court upheld the search of the defendant's computer as a result of his consent to the search.[976] The defendant complained that the search and seizure of his computer was illegal.[977] He contended that his consent to the search and seizure was tainted and, as there was no warrant, there was

[971] Ibid.
[972] Ibid.
[973] Stephens and Glenn, above n 533, 84.
[974] Clancy, above n 718, 253. See also Franklin, above n 787, 216.
[975] Calsyn et al, above n 956, 1249. See also, Stephens and Glenn, above n 533, 85. See also, Toren, above n 888, 8-36.
[976] *Williford v. State of Texas*, 127 S.W 3d 310, 313 (Tex, 2004).
[977] Ibid.

no probable cause.[978] The court dismissed the appeal on the ground that the seizure was proper.[979]

d) Comparative Legal Analysis

The *Criminal Procedure Law* 1961 does not recognise consent search, but it addresses request search. The requesting party may ask the requested officers to conduct physical or digital searches. From the general meaning of provisions 93/2&3, officers upon request from a person authorised to search premises without a warrant, including any computer systems found in the premises. Therefore, unlike consent search, police officers cannot negotiate with the requesting party to obtain consent to search computer systems. Once the requesting party makes the request, officers have the power to conduct a full search. However, the general principles of consent search which have been addressed by Egyptian judicial precedents and accepted by Jordanian scholars can be applied to search and seize computers and digital evidence. For example, consent search of computers should be conducted in accordance with a voluntary consent which must be obtained before the search.

In Australia, consent search has been addressed by the Law Reform Commission and court decisions. Law enforcement officers are able to obtain consent to search computers and digital evidence. Although, an implicit consent is valid according to the Australian courts, it is recommended here that a written or recorded consent should be obtained. This is preferable to ensure that the consent is valid and to prevent the consenting party from withdrawing or denying his consent. For example, if the suspect gives the officer his password and the latter accessed the system using the given password, the search would be valid unless the consenting party denied the given consent.

Factors which are applied by the USA Supreme Court are also applicable to digital searches. Jordan and Australia apply the same factors to consent searches. For example, the age of the person giving the consent in a traditional search must be the same age as for the digital search. The person's education, intelligence, and mental condition are important factors to determine the validity of the search. If consent to search computer systems was obtained from an uneducated person, for example, the search and seizure

[978] Ibid.
[979] Ibid.

procedures should be invalid, because the consenting person has no knowledge about the search consequences.

The scope of the consent and third party consent, however, constitute the major unresolved concerns pertaining to digital searches. In the following section, the scope of the consent and third party consent are discussed.

8.1.2.1 Scope of Consent

The scope of the consent is an important factor to be considered because it has been considered as equivalent to exceeding the scope of a search warrant.[980] A suspect has the right to delimit the scope of the search to which he consents.[981] Indeed, the consent search is a negotiable process that is entirely between law enforcement officers and the suspect, so a limited consent it can be expanded and vice versa.[982] The scope of the consent in the context of a digital search differs from traditional search, because digital data's unique nature and characteristics have no peer in the real world.[983] It is well recognised that the digital world contains a variety of objects, such as files, e-mail messages, graphics, and so on, which need a considerable amount of time and effort to be investigated. Although these files are often protected by passwords to prevent unauthorised use, there is a high risk of evidence contamination because it is fragile and can be damaged easily. So, it is important for law enforcement officers to abide by the scope of the search as set forth in the consent.

Scope of consent takes two forms. First is the extension of the physical search to search digital devices. For example, consent given to search an apartment is extended to search a personal computer located in the apartment. Second is the extension of the digital search to a search of other devices or files not specified in the initial consent (specific digital to unlimited search). For example, consent given to examine a CD is extended to search a PC's hard drive or consent given to search for JEPG files is extended to search for MP3 files.

[980] *United States v. Cotten*, 669, P.2d 680 (1994).

[981] See, eg, *Floria, petitioner v. Luz Piedad Jimeno et al,* 114 L. Ed. 2d 297 (1991).

[982] See, eg, *United States v. Lemmons,* 282 F.3d 920 (7th Cir 2002).

[983] See Section 6.2 for more information about the unique nature of digital data.

a) Jordan

No specific provision, legal precedent or regulation appears to guide enforcement officers in either obtaining or extending consensual search for a physical object to search and seizure of electronic devices, including intangible data. The absence of such rules and regulations makes the scope of consent is imprecise. Provision 93/2 & 3, which address a warrantless search upon request from the owner or occupant of the premises, does not elaborate the right of the requesting party in delineating the scope of the search. Law enforcement officers, therefore, may conduct unrestricted searches.[984] Although there are no documented courts cases that have addressed this issue,[985] it is a possibility in the future. Exploring the judicial view of Australia and the USA, however, may be helpful in predicating how Jordan's legislature and courts will rule on this issue.

b) Australia

In Australia, the *Crimes Act* 1914 addresses the scope of consent in particular cases. It addresses only the scope of consent when an officer conducting a search with a warrant intends to widen his search. Section 3J prevents officers from taking photographs or video recordings of the premises or of things at the premises not incidental to the execution of the warrant without a written consent.[986] Although Australian Law Reform Commission recommended consent search, it did not address its scope.[987] Tronc, Crawford, and Smith, the authors of *Search and Seizure in Australia and New Zealand*, however, have argued that the consensual search will be lawful if the search is confined to the scope of consent.[988] As a result, the consenting person can limit the scope of his consent and officers must confine their search to the places delineated by the consent.

c) USA

In the USA, by contrast, the scope of the search is an important factor in consensual searches.[989] It can be inferred from the courts' considerations of consent searches that they use two criteria to determine the scope of the consent.

[984] *Jordanian Criminal Procedure Law 1961* (93) (2) (3).
[985] See footnote number 792.
[986] *Crimes Act 1914* div 2 s 3J (2).
[987] See, The Law Reform Commission, above n 966.
[988] See, Tronc, Crawford, and Smith, above n 677, 86.
[989] See generally, Ferdico, above n 521, 389.

First is the totality of all the circumstances.[990] The courts examine the person's education, understanding, intelligence, and mental condition, because they are important factors in deciding whether the person understands the differences between the physical and digital searches and the risk that may be associated with the digital searches.[991] For example, in *United States v. Snow,* the court held that a person who consents to the search of a car should reasonably expect that readily-opened, closed containers discovered inside the car will be opened and examined.[992]

Second, the courts examine what is 'objectively reasonable'.[993] The Supreme Court has explained this as what the typical reasonable person would have understood by the information exchanged between the officer and the person consenting to the search.[994] In the *United States v. Lemmons,* for example, the court held that the defendant's invitation of the officer to his trailer to look at different things including the computer, and turning the latter on for the officer to access and search files, constituted an unlimited consent.[995] In a similar decision, the Tenth Court found that the consent given to search a computer using particular forensic tools extends to searching the same computer using a manual search engine, i.e. a different forensic approach.[996] In a different manner, in *United States v. Blas* (1990) the court found that the defendant's consent to examine the pager he was carrying did not extend to consent to search the contents of the pager.[997] Therefore, to avoid confusion and the possible invalidation of consent, Moore (2003) and Berg (2005) have suggested that law enforcement officers must present a written consent form delineating the scope of the consent.[998] Moore suggested the following information o be included in the consent form:

1) The area to be searched,

2) What it is the investigator is intending to search for, and

[990] See, Middleton, above n 530, 178.
[991] Ibid.
[992] *United States v. George Snow*, 44 F.3d 133, 135 (2nd Cir, 1995).
[993] *United States v. Brooks* , above n 818. See also, Scott, above n 292, 538.
[994] Ibid.
[995] *United States v. Lemmons,* 282 F.3d 920 (7th Cir, 2002).
[996] *United States v. Brooks*, above n 818,1249. FBI agent obtained consent to search a computer using disk that would automatically search for image files. The defendant argued that his consent was therefore limited to the specific software-driven pre-search the agent initially described, and the images obtained during by manual search should have been suppressed.
[997] Lisa Key Decker, 'The Search and Seizure of Electronic Pagers: a Federal Case Law Review', 10 *Criminal Justice Policy Review,* 343, 348.
[998] See, Berg, above 723, 36. See also, Moore, above n 597, 109.

3) The investigator’s desire to search within any computer or technological device found within the area.

Meanwhile, Berg suggested that the consenting party:

1) has access and control over the computer and all of the data contained on the computer

2) is not aware of any areas within the computer to which that party is not allowed access.

3) grants authorisation to the officers to search the entire contents of the computer.

d) Comparative Legal Analysis

In the absence of any judicial precedent on this matter, or any specific legislative definition or direction, Jordanian enforcement officers are not restrained from rummaging through electronic devices in search of evidence. While the requesting party permits the search, he has not been given authority to confine it. Meanwhile, the Australian *Crimes Act* 1914 addresses the scope of the consent only in relation to the execution of search with a warrant. Consent to search without a warrant and its scope are not addressed. However, the argument about the scope of the consent presented by Tronc, Crawford, and Smith is logical, because the search is entirely built upon consent and, therefore, the consenting person can limit his consent. This argument also can be applied to cybercrime investigation searches and digital evidence and, therefore, the owner of a computer system or an authorised person can limit the scope of the digital searches. In a similar manner, he can also limit the physical search by means which are not to be extended to digital searches.

In the USA, by contrast, while the general concept is that officers must abide by the terms of consent, different courts have handed down contradictory rulings on the scope of consent. Some courts have approved the first form of consent, i.e. extension of a physical search to search a digital device (see, for example, *United States v. Lemmons*). Other courts have rejected the extension of a physical search to search for digital evidence (see, for example, *United States v. Blas*). The contradiction between the two decisions can be avoided only by adopting Moore’s and Berg’s suggestions. These suggestions are beneficial for both forms of consent, because they precisely show the search limits, and how the officers will carry out the search. Also, they protect the right of the defendant and give credibility to the consent procedures by delineating the outer boundaries of the consent.

8.1.2.2 Third-Party Consent

Third party consent is a relatively new exception to the search warrant requirements.[999] It means that, 'under certain circumstances, individuals other than the householder against whom evidence is sought may validly consent to a search of shared premises'.[1000] The creation and development of this exception and certain limitations and exceptions to it, signals the consistent path of restricting individual privacy rights while expanding the scope of law enforcement power.[1001]

In the context of cybercrime investigation, third party consent is very important, because technologies, particularly computers, networks and Internet, are shared between multiple users, such as family members, roommates and workplaces.[1002] Investigators usually encounter one or more computers located on private property where each computer can be accessed by multiple users or from different locations.[1003] Furthermore, the third party consent doctrine is vital in workplaces. Employers who control or administer their employees may consent to searches and seizure of evidence. Therefore, third party consent in cybercrime investigations takes two categories: private household members and workplace consents.

[999] The seminal case in the USA is *United States v. Matlock* 415 U.S. 164 (1974) where the Supreme Court stated the general proposition that 'the voluntary consent of any joint occupant of a residence to search the premises jointly occupied is valid against the co-occupant'. It also added that 'the consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared'. This was subsequently confirmed in the *Illinois v. Rodriguez* 497 U.S. 177 (1990). Recently, in *Georgia. v. Randolph*, 457 US 103 (2006), the court stated that 'voluntary consent of an occupant who shares, or is reasonably believed to share, a premise with the suspect while the latter is absent is a valid warrantless search'.

[1000] Renee E Williams, 'Third Party Consent Searches After *Georgia v. Randolph:* Dueling Approaches to the Dueling Roomates' (2008) 87 *Boston University Law Review* 937-938.

[1001] Ibid.

[1002] See, eg, Toren, above n 888.

[1003] Ibid.

8.1.2.2.1 Household Consent

Operating systems, such as Windows, allow users to create private zones protected by passwords as well as permitting files to be shared by multiple users without restrictions.[1004] In addition, computer networks and the Internet provide users with the capability to access remote computers and retrieve information from networked computers. Therefore, third party consent in cybercrime investigations typically takes two forms: local and remote consents.

First: Local Consent

Local consent refers to the geographical proximity between a third party who has the right to make voluntary consent, and a defendant living in the same geographical proximity with the third party. In other words, the third party and the defendant live in the same vicinity. For enforcement officers, local consent encompasses two steps. The first step is to enter the premises, negotiate with a person other than the householder against whom evidence is sought, and obtain consent to physically search hardware drives, CDs, DVDs, laptops, flash memory, floppy disks, and so on. This step is valid as long as the consenting party has equal rights of possession and control of the property that is the subject of the search, with the defendant. The second step is to obtain a more specific consent to operate the equipment located inside the premises and to search the digital contents. The second consent obtained is valid only when the digital contents are accessible either directly, such as where no password is needed to access the system, or indirectly because the system is password protected but the consenting party possesses the password and has access to the files. For example, where spouses live together and share a computer, then he or she may approve a warrantless search, and the consent should be upheld as long as they share the same password.[1005] But if the computer is exclusively used by a spouse in such a manner as to prevent his or her partner from accessing the whole computer or particular files then the consent is invalid for that restricted part.[1006]

[1004] See generally, Linda Volonino, Reynaldo Anzaldua, and Jana Godwin, *Computer Forensics: Principles and Practices* (2007) 206-216.

[1005] Orton, above n 936, 141.

[1006] Ibid.

Second: Remote Consent

Remote consent is unique and is only associated with digital searches. Internet and networks make the remote search practicable. For example, to operate effectively and smoothly, each computer network, such as a Local Area Network (LAN), needs continuous maintenance as well as supervision.[1007] So, every network has a system administrator or system operator responsible for operating, maintaining, and developing the system.[1008] This position grants system administrators root level access,[1009] which effectively gives them complete control over the entire system they control[1010] enabling them to monitor computer users (including their Internet access).[1011]

The extent of the power of the third party to access a defendant's computer is important in determining the third party's ability to consent the search.[1012] However, the third party consent exception is markedly different in Jordan, Australia and the USA according to national legislation and judicial precedents.

a) Jordan

In Jordan, third party consent is not mentioned anywhere in the *Criminal Procedure Law* 1961. Instead, law enforcement officers are authorised to enter and search any private premises without a search warrant if they are accompanied by a local notary or two native witnesses.[1013] The attendance of the local notary or the two witnesses - in the absence of a suspect - is vital to the validity of the search.[1014] Their attendance is to observe and witness the search, but not to consent to or refuse the search. Third party consent, therefore, is not required before the officers may proceed with the search and seizure procedures. With one exception, no judicial precedent directly addresses third party consent. The only court decision focused on third party attendance is the Court of

[1007] See, eg, Marion G Ceruti, 'Web-to-Information-Base Access Solution' in John P Slone (ed), *Local Area Network Handbook* (1999) 433, 458.

[1008] See, *System administrator* Wikipedia <http://en.wikipedia.org/wiki/System_administrator> at 13 September 2007.

[1009] 'Root access is a descriptive term meaning that the user is recognised as a system administrator and consequently obtains the authority to change passwords or destroy data authority that normal users do not have'. Reid Skibell, *Cybercrimes & Misdemeanors: A Revaluation of the Computer Fraud and Abuse Act*, (2003) 18 *Berkeley Technology Law Journal*, 909, 925.

[1010] See, Bruce Cantrell, *Electronic Privacy in the Private Sector Workplace* (2007) <http://www.giac.org/resources/whitepaper/law/147.php> at 5 September 2007. See, also Computer Crime and Intellectual Property Section Criminal Division, above n 633.

[1011] See, eg, Schell, and Martin, above n 45, 179-180.

[1012] See, Franklin, above n 787, 226.

[1013] *Criminal Procedure Law 1961* (94).

[1014] See, eg, قدري عبدالفتاح الشهاوي, above n 681, 157.

Cassation decision number 697/97.[1015] The court's decision invalidated a search because it was conducted without the attendance of a local notary or two witnesses (who must be the defendant's relatives, such as family members or relatives).[1016] While the attendance of third party is vital, it is not parallel to third party consent. Exploring the judicial view of the USA, however, may be helpful in predicating how Jordan's legislature and courts will rule on this issue.

b) Australia

In the absence of any judicial precedent on which to rely, the Australian Law Reform Commission recommended that consent to a search can be made voluntarily by a person occupying the premises or in charge of the vehicle in question.[1017] Hence, consent is invalid unless given by a person with actual authority to do so. This obligates enforcement officers to make the necessary inquiries to ensure that the consenting third party has the legal authority to consent. The Commission did not suggest an appropriate mechanism to ascertain the third party's authority to consent to the search.

c) USA

In the USA, as a general premise, third party consent is valid as long as the consenting party has equal rights of possession and control of the property that is the subject of the search with the defendant.[1018] Or there is a relationship between the consenting third party and the defendant.[1019] However, the question arises, how can law enforcement officers determine whether the third party consent is legitimate? Lee Cook argues that there are four circumstances in which the third party consent should be allowed to legitimise the search.[1020] These are:

1) The third party has been victimised by the defendant's conduct;[1021]

2) The third party is involved in the criminal activity;[1022]

[1015] The Court of Cassation, قرار محكمة تمييز جزاء رقم 1997/697 (هيئة عامة /1997).
[1016] Ibid.
[1017] The Law Reform Commission, above n 966, 92.
[1018] See, eg, Virginia Lee Cook, Third-Party Consent Searches: An Alternative Analysis' (1973) 41 (1) *The University of Chicago Law Review* 121, 123. See also, Stephens and Glenn, above n 533, 88. See also, Cook, above n 958, 389.
[1019] Lee Cook, ibid 128. See also, Calsyn et al, above n 956, 1254.
[1020] Cook, ibid 140-141.
[1021] Ibid.
[1022] Ibid.

3) The defendant has abandoned the property;[1023] and

4) Where obtaining the consent of all occupants of all premises is impractical, a single consent will suffice.[1024]

It can be seen that these four circumstances circumscribe third party consent and, therefore, hinder investigations, because they exclude family members, roommates, or anyone sharing the same dwelling, unless the consenting person has been victimised by the defendant's conduct or is an accomplice of the defendant in the commission of the criminal offence.

The USA Supreme Court has applied two different tests to determine the validity of third party consent.[1025] Both assess the officers' perceptions of the facts at the time of the search. The first is known as 'an actual authority' examination, and the second is 'an apparent authority' examination.[1026]

The actual authority test is used to evaluate the validity of the third party consent by examining whether the officer executing the search had a reasonable belief that the consenting third party had equal rights to possess and control the property that was the subject of the search.[1027] For example, in the *United States v. Matlock,*[1028] the court relying on the actual authority test held that the defendant's father, spouse and son could grant consent to search.

The apparent authority examination, on the other hand, was used in *Illinois v Rodriguez* where the Supreme Court stated that if a third party lacked actual authority to consent, the third party's consent could be valid if the police, at the time of entry, reasonably believed the consenting party possessed common authority over the premises.[1029]

The courts do not rely on one single test. They first examine the actual authority to determine the validity of the consent; otherwise they examine the apparent authority.

[1023] Ibid.
[1024] Ibid.
[1025] See generally, Renee Williams, above n 1000, 937. See also, Cook, above n 958, 395
[1026] Ibid.
[1027] *United States v. Mattlock*, 476 F.2d 1038 (7th Cir, 1973).
[1028] In 1970 Mattlock was arrested for robbing a Federal Deposit Insurance Corporation (FDIC) insured bank in Wisconsin. The woman whom the defendant, Mattlock, was residing within a single bedroom consented to officers to searching the bedroom that she and the defendant jointly occupied. See generally, *United States v. Mattlock*, 476 F.2d 1038 (7th Cir, 1973).
[1029] *Illinois v Rodriguez,* 497 U.S. 177, 188-189 (1990). See generally, Cook, above n 958.

For instance, in *United States v. Ray Andrus,* the District Court concluded that the defendant's father, Dr Andrus, who gave officers consent, lacked actual authority, because he did not know how to use the computer, had never used the computer, and did not know the user name that would allow him to access his son's computer.[1030] Thus, the court proceeded to consider the apparent authority.[1031] It based its conclusion on the fact that the defendant's father had apparent authority on the following factual findings:

> (1) the e-mail address bandrus@kc.rr.com, an address associated with Dr. Bailey Andrus, was used to register with Regpay and procure child pornography; (2) Dr. Andrus told the agents he paid the household's internet access bill; (3) the agents knew several individuals lived in the household; (4) Ray Andrus' bedroom door was not locked, leading a reasonable officer to believe other members of the household could have had access to it; and (5) the computer itself was in plain view of anyone who entered the room and it appeared available for anyone's use.[1032]

Local consent is obvious in this case, because the officers approached the defendant's father and obtained consent to access the premises and then obtained further consent to search the defendant's computer. Although, the defendant's father, Dr Andrus, did not have a password for the computer, he paid for the internet access. This was enough to indicate that the defendant's father possessed actual authority, because paying the bills shows control over the Internet connection.

d) Comparative Legal Analysis

The general rules of third party consent are also applicable to digital searches. Third party consent is valid only if obtained voluntarily and given by a competent person. But digital searches have created a new form of third party consent. For the first time, consent can be obtained from a person who has no common authority over the physical place to be searched, but has common authority over the computer to be searched. The common authority can be demonstrated by the ability of the third party to legally access the defendant's system. In addition, the remote access third party consent offers enforcement officers an efficient way to obtain consent from a third party without leaving their offices.

[1030] Ibid.
[1031] Ibid.
[1032] Ibid.

The Jordanian *Criminal Procedure Law* 1961 does not permit the conduct of any forms of third party consent. Pursuant to the conditions set forth in the *Criminal Procedure Law*, the attendance of a local notary or two native witnesses suffices to validate a warrantless search. A third party who shares common control or authority of the premises to be searched, or a system operator, lacks authority to consent to the search of a computer. Although this situation facilitates the warrantless search execution, because officers are not required to negotiate with third parties to obtain consent, it has three drawbacks. First, it unfairly jeopardises third parties' privacy. Second, the local notary or the two native witnesses may lack sufficient understanding and knowledge of computer systems and, therefore, will be unable to observe the search execution properly. Third, the attendance of a local notary or the two native witnesses is impracticable in remote searches, because the latter requires swift action and inviting them would delay the urgently needed search and seizure.

By contrast, in Australia and the USA, besides the knowing and willingness requirements, third party consent search is valid only if the third party giving consent has actual or apparent authority over the computer to be searched.

The application of the actual or apparent authority to local consent in digital search would be as follows. The key to actual authority is that the consenting third party has equal rights of possession and control of the property and, more importantly, possesses the password and has access to the system, which is the subject of the search. Apparent authority, on the other hand, is not applicable to search a password protected system unless the consenting third party possesses the password. For example, a defendant's parents, sometimes, have authority and control over the place to be searched, but do not have the password to get access to their child's computer or they are not computer literate. In such a case, they lack actual authority, i.e. equal rights of access, to consent.[1033] If the computer is not password-protected and the parents are computer literate, however, the investigators will have a reasonable belief that one or both of the parents have apparent authority to consent. The search will be considered valid[1034] because of the apparent authority of the parents.[1035]

[1033] See, *People v. Blair*, 748 N.E.2d 318 (2001).

[1034] Contra, Berg, above n 723, 35. See also, Clifford, above n 739.

[1035] *United States v. Ray Andrus,* 483 F.3d 711 (10th Cir, 2007).

In cases of remote consent, the actual authority is demonstrated by the ability of the system operator to legally access the defendant's system, but if the defendant's computer is inaccessible to the system operator, the later will lack actual authority to consent. The apparent authority in remote consent cannot be demonstrated unless the operator shows common authority over the defendant's computer.

8.1.2.2.2 Workplace Consent

Digital technology and the Internet are increasingly being seen, particularly in the developed world, as an integral part of workplace performance and productivity (in both the private and public sectors). Businesses are fostered by the pervasiveness of information technology, e-commerce and the emergence of new tools with networking and processing capabilities.[1036] The downside of this is the negative effect of cybercrimes.[1037] According to a recent Australian Institute of Criminology report on crime, approximately half of the organisations that responded to the study had experienced at least one type of cybercrime.[1038] Insider abuse of computer systems, such as by disgruntled employees, was the third most common type of breach.[1039] This increased over the four year study period, from 26% in 2003 to 32% in 2006.[1040] Similarly, the average loss per cybercrime for US companies escalated to $350,000 in 2007 from $168,000 in 2006.[1041] From these statistics it is evident that workplace computer stations are either the victims of cybercrimes or the tools of the cybercrime.[1042] Therefore, a workplace's computers and networks are a critical part of the crime scene in cybercrime investigation and law enforcement officers can take advantage of workplace expertise to conduct searches, and more importantly, to conduct warrantless searches.

[1036] See generally, Peter Grabosky, 'The Global Cyber-Crime Problem: The Socio-Economic Impact' in Roderic Broadhurst and Peter Grabosky (ed), *Cyber-Crime: The Challenge in Asia* (2005) 29, 31.
[1037] See, eg, ibid 45-46.
[1038]See, Jack Dearden and Samantha Bricknell, Australian Crime: Facts & Figures 2007 (2008) Australian Institute of Criminology <http://www.aic.gov.au/publications/facts/2007/facts_and_figures_2007.pdf> at 1 June 2008.
[1039] Ibid.
[1040] Ibid.
[1041]See, *Computer Crime and Security Survey* (2007) Computer Security Institute < http://www.gocsi.com/forms/csi_survey.jhtml> at 4 June 2008. For a complete picture of cybercrime statistics see generally, Smith, Grabosky and Urbas, above n 25, 13-25.
[1042] David Wall argues that cybercrimes may not be individually as serious as many of the statistics claim, but their seriousness lies in their globalised aggregate value. David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007) 18.

In Jordan, Australia, and the USA, no specific statutory provisions pertain to workplace searches. In the USA, only a few court decisions on the subject have been reported and there are no judicial precedents on workplace warrantless searches in Jordan or in Australia. Therefore, the author will simply address the US perspective and then examine whether it is optimal for Jordan.

In a workplace search a distinction must be made between private and public workplaces. Middleton has opined that 'the legality of warrantless workplace searches depends on often subtle factual distinctions, such as whether the workplace is public sector or private sector, whether employment policies exist that authorise a search, and whether the search is work related'.[1043] There are some marked differences between the purposes of a search conducted by employers and by law enforcement officers. The former's purpose is mainly to make sure that the agency operates in an effective and efficient manner,[1044] while the latter's purpose is only to gather evidence of a criminal offence.

First: Private Sector Workplace Consent

Private workplaces employers can conduct different types of searches.[1045] The first is non-investigatory searches, such as searching a desk or filing cabinet to obtain documents, or computers to retrieve a needed data file.[1046] The second is work-related misconduct searches, such as for corruption investigations.[1047] A third type is what is known as a 'mixed-motive' search, aimed at simultaneously discovering evidence of work-related misconduct[1048] as well as evidence of a crime committed by the employee.[1049] In each of these types of searches, the employer may pass the incriminating information and consent to law enforcement officers to search and seize an employee's computer.

[1043] Middleton, above n 530,192.

[1044] Robert Sprague, 'Employee Privacy in Virtual Workplaces' in Pavel Zemliansky, and Kirk St. Amant (eds), *Handbook of Research on Virtual Workplaces and The New Nature of Business Practices* (2008) 183, 184.

[1045] See, eg, Paul R Koster, 'Workplace Searches by Public Employers and the Fourth Amendment' (2007) 39 *Urban Lawyer* 75.

[1046] Henry M Wrobleski and Karen M Hess, *Introduction to Law Enforcement and Criminal Justice* (8th ed, 2006) 264.

[1047] See, eg, Bryan R Lemons, 'Public Privacy: Warrantless Workplace Searches of Public Employee' (2004) 7 *Journal of Labour and Employment* 1. See also, Koster, above n 1045, 75.

[1048] See, eg, Sprague, above n 1044, 184.

[1049] See, Koster, above n 1045, 78.

The underlying question is whether and to what extent private employers consent to the government searching and seizing an employee's computer is valid. To answer the question it will be necessary to examine the balance between the employee's right to privacy and the employer's need to know that the workplace's policies are appropriately applied.[1050]

Hackerott and Rosen have argued that the balancing act between the rights of the employee and the employer can be made easier if the groundwork is clearly laid early in the employment relationship.[1051] For example, if the company's privacy policy clearly articulates the places and items that the company has the right to search, and it has a policy of routinely searching employees' computers, the search within the scope of the policy would be permitted.[1052] Conversely, if the company's policy does not authorise the employer to search an employee's work area and protects the employee's privacy, the court may conclude that the employee has a reasonable expectation of privacy in the use of his computer.[1053]

Kerr argued that a private sector search is equivalent to a search involving an individual's home and, therefore, requires a search warrant to search and seize a computer. However, he added that employers can consent to searches of employees' workplace computers in specific circumstances. He concluded that:

> under the Fourth Amendment, private-sector employees have traditionally enjoyed Fourth Amendment protection in the contents of their offices, including in their office computers. The police can't just barge in to your office and rifle through your desktop computer. Instead, the police need either to get a warrant or to go to your employer and ask for the employer's permission to conduct the search...[1054]

The argument is consistent with the *Electronic Communications Privacy Act* of 1986 (ECPA), as well as with the Fourth Circuit Court decision in *United States v. Simons.* On one hand, the ECPA, which is the only federal statute that offers protection for

[1050] See, eg, ibid. See also, Lisa Guerin, *The essential guide to workplace investigations* (1st ed, 2007) 247.

[1051] See, eg, Cynthia L Hackerott and Lori Rosen, *HR How-to: Internal Investigations: Everything you Need to Know to Conduct an Internal Investigation in the Workplace* (2003) 60.

[1052] See, eg, Euqene Ferraro, *Undercover Investigation for the Workplace* (2000) 227.

[1053] See, Toren, above n 888, 8-50.

[1054] See, Orin Kerr, *Ninth Circuit Mostly Eliminates Private-Sector Workplace Privacy Rights in Computers* (2006) Orinkerr.com: Law, the Legal Academy, and the Legal Profession <http://www.orinkerr.com/2006/08/09/ninth-circuit-mostly-eliminates-private-sector-workplace-privacy-rights-in-computers/#comments> at 20 July, 2008.

employees in office computer privacy, does not protect employee privacy in the workplace if actual or implied consent exist.[1055] The Fourth Circuit, on the other hand, held that the employer's Internet usage policy, which prohibited employees from browsing non-work related sites and permitted the employer to conduct electronic audits to ensure compliance with this policy, dissolved any expectation of privacy.[1056] The dissolution of expectation of privacy means that employer can consent to searches.

In a recent decision, the Ninth Circuit Court of Appeal in its decision in *United States v. Jeffrey Ziegler* confirmed the above argument. The court ruled that:

> Social norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability. Thus, in the ordinary case, a workplace computer simply "do[es] not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance... For these reasons, the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to his use of his employer's computers.[1057]

The court concluded that Ziegler's employer exercised common authority over 'his' office and workplace computer.[1058] The common authority validates consent to search Ziegler's workplace computer.[1059] The social norms, according to the Ninth Circuit Court diminish the employee's reasonable expectation of privacy.

In sum, it can be said that conducting a warrantless search of a private workplace after obtaining the consent of an employer who exercises common authority over the workplace area is an admissible search.

[1055] See, eg, Thomas W Dillon and Daphyne S Thomas, 'Knowledge of Privacy, Personal Use, and Administrative Oversight of Office Computers and E-mail in the Workplace' (2006) *Information Technology Learning and Performance Journal* 23, 24.

[1056] *United States v. Mark L. Simons*, 206 F. 3d 392 (4th Cir, 2000).

[1057] *United States v. Jeffrey Ziegler*, 456 F. 3d 1138, 1145 (9th Cir, 2006). Ziegler was convicted by a lower court of various criminal charges arising from his use of his workplace compute to view and download child pornography.

[1058] Ibid.

[1059] Ibid.

Second: Public Sector Workplace Consent

In public sector workplaces, employees regularly access the internet for personal use, such as sending and receiving e-mails, and saving private files. The Supreme Court in the USA has suggested that employees enjoy a reasonable expectation of privacy with respect to the use of their computers. Indeed, the general standard for a reasonable expectation of privacy in public workplace was set by the USA Supreme Court in its seminal decision of 31 March 1987 in *O'Connor v. Ortega.* The Supreme Court stated that the 'offices of government employees, and a fortiori the drawers and files within those offices, are covered by the Fourth Amendment…therefore, search and seizure by government employers or supervisors…are subject to the restraints of the Fourth Amendment'.[1060] However, scholars have stressed that public workplace expectation of privacy should be addressed on a case-by-case basis.[1061]

In a similar manner to the private sector workplace, the office's polices, regulations, instructions and practices may reduce an employee's expectation of privacy.[1062] In *United States v. Simons*, the Fourth Circuit held 'that a government employee lacked a reasonable expectation of privacy in electronic files on his office computer, in light of the employer's policy which states that employees were to use the Internet for official government business only'.[1063] Thus, if the employer has a policy to inspect and monitor Internet activity, the employee has no privacy regarding information on the computer.[1064] Public employers can consent to a law enforcement search if the employees are aware of the agency's rules which grant supervisors access to the employees' computers to investigate suspected employee wrongdoing.[1065] For example, in *Leventhal v. Knapek* the court upheld the warrantless search of a public sector workplace, holding that the search was justified in terms of the employer's legitimate need for control.[1066] The courts set criteria to decide whether an employee has a reasonable expectation of privacy in his computer as follows:[1067] First, is the workplace area in question assigned solely to the employee or do others have access to the space?

[1060] *O'Connor v. Ortega* 480 U.S 709, 718 (1987).
[1061] Stephens, and Glenn, above n 533, 154.
[1062] See, Clancy, above n 718, 222.
[1063] *United States v. Simons*, above n 1053.
[1064] *United States v Slanina*, 283 F.3d 670 (5th Cir, 2002).
[1065] See, Brenner and Frederiksen, above n 596. See also, Kerr, above n 1054, 576. Clifford, above n 739, 140. See also, Rittinghouse and Hancock, above n 753, 370. See also, Cantrell, above n 1010.
[1066] *Leventhal v. Knapek,* 266 F3d 64 (2nd Cir, 2001).
[1067] Ibid

Second, does the nature of the employment require a close working relationship with others? Third, do office regulations place employees on notice that certain areas are subject to search? Fourth, is the property searched in public or private? According to these criteria, employees have a reasonable expectation of privacy in their offices, including computers, when the access to a personal office and computer does not appear to be frequent, widespread, or extensive.

Workplace Searches in Jordan & Australia

The Jordanian *Criminal Procedure Law* 1961 and Australian *Crimes Act* 1914, respectively, do not address private or public sector workplace searches.

In Jordan, the problem is more complicated, because third party consent is not recognised by the law. Instead, it requires a local notary or two native witnesses to be present during the search execution. This requirement causes difficulty to the search process.[1068] Therefore, law enforcement officers should be able to conduct workplace searches with the help of the employers who legally authorised the search of employees' computers.

In Australia, third party consent is recognised, and therefore an employer's consent to law enforcement to search and seize evidence would be governed by consent of the employer as a third party as long as the employees are aware of the agency's rules that grant supervisors the right to access the employee's computers.

According to the USA perspective, however, the parallel between employer's and third party consent in certain respects is self-evident. The third party consent general concept is that the consent should be obtained voluntarily from an individual other than the defendant who has authority to approve the search. In workplace searches, by contrast, the general theme is that employers (government or private) who have common authority over their employees' computers have authority to consent to law enforcement searches of employees' computers. Therefore, there should be no problem in applying the general rules of third party consent to workplace searches.

[1068] See Section 8.2.2.2. (a) for more information about the difficulties caused by the requirement.

8.1.3 Plain view

The plain view doctrine is an American legal concept derived from three landmark decisions, *Coolidge v. New Hampshire* (1971), *Arizona v. Hicks* (1987), and *Horton v. California* (1990).[1069] Some scholars name this doctrine 'plain view observation'.[1070] It means that 'anything in plain view of an officer, who has a right to be where he or she is, may be seized'.[1071] According to Arcaro, the author of *Basic Police Powers: Arrest and Search Procedures,* plain view means 'unexpectedly finding evidence, without having prior knowledge that the item was in the place and without physically searching the place to find the item'.[1072] From these definitions the plain view doctrine allows investigators to observe[1073] or to seize but not to search evidence of a crime, even though the crime is not the one for which the investigator was authorised to investigate or to seize evidence.[1074] The plain view doctrine occurs during the execution of a search warrant or arrest, when contraband not described in the search warrant is observed and seized. For example, if a computer pursuant to a warrant is being searched for DDoS attack, and a single child pornography image is accidentally discovered, the agent may seize the image without rummaging the entire hard disk. Indeed, the plain view doctrine allows seizure beyond the scope of the search warrant and is, therefore, considered as an exception to the general rules of search and seizure.[1075]

In cybercrime investigation, the core problem with the plain view doctrine is the unique aspects of computers and forensic tools. Computers store enormous amounts of information, such as intermingled documents, files, folders, programmes and databases. These files and folders are either active files, or latent data.[1076] Forensic tools are able to scrutinise data thoroughly to retrieve hidden and deleted data. Therefore, the application of the plain view doctrine to computers raises some problems. According to the classical rule of plain view, investigators have power to seize but not to search evidence. In other words, the seizure occurs as a result of visual observation at the time of the search

[1069] See, eg, Robert Moore, 'To View or not to View: Examining the Plain View Doctrine and Digital Evidence' (2004) 29 *American Journal of Criminal Justice*, 61.
[1070] See, Ferdico, above n 521.
[1071] Carl J Franklin, *Constitutional Law for the Criminal Justice Professional* (1999) 137.
[1072] Arcaro, above n 683, 266.
[1073] See generally, Ferdico, above n 521, 412.
[1074] See, eg, *United States v. Derrick Jackson*, 131 F. 3d 1105, 1108 (4th Cir, 1997).
[1075] Ibid.
[1076] See Section 6.2 for more information about active and latent data.

warrant's execution. By applying this rule to computer searches, investigators executing search warrants should only seize the active data,[1077] because these data are visible information that need no particular skills or forensic tools to display them and are usually not passworded or otherwise protected from view. Meanwhile, seizure of latent data and closed files in plain view raises an unresolved legal question about whether or not it is possible for officers to seize deleted data and closed files pursuant to the plain view exception. The problem occurs because visual observation is limited to what can be physically seen on the computer screen, such as images, or opened files.[1078] Hidden, unopened or deleted files are not apparent immediately,[1079] as forensic tools are required to retrieve and display this sort of information. These forensic tools do not allow investigators to see the file content, but only file name extensions, such as jpg, doc, html and, to view such files, officers must open, download, or run specific applications.[1080] In this regard, Brenner opined:

> In the cyberworld... there is no analogue of real world sight... searches of computer--files are method--specific. As long as the officer is using a text--based search program, the contents of non--textual files, such as JPEG files, will be opaque to him, clearly not in plain view...As the officer uses the software program to search text files, the contents of all text files on the computer's hard drive are in the officer's sight, but the contents of the non--textual files, the JPEG files, are not…the JPEG files are of course visible to the officer, but they are analogous to a closed and locked box. In order to view the contents of the locked box, an officer would have to obtain the implements to unlock and then open the box. Unlocking and opening the box would...be a search, and so, outside the scope of the plain view doctrine.[1081]

Legal scholars have approached the plain view doctrine with quite a different set of considerations. Brenner, Frederiksen and Kerr have suggested limiting the application of the plain view doctrine with respect to computer searches. They argue that a computer search using a general key word or file type that widens the search scope to examine each individual file on the hard drive should not be allowed.[1082] Kerr has added that investigators must use targeted search tools that limit the operation of the plain

[1077] See, eg, Toren, above n 888, 8-45.
[1078] Ibid.
[1079] See, eg, Moore, above n 1069.
[1080] Ibid.
[1081] Brenner and Frederiksen, above n 596.
[1082] See, Brenner and Frederiksen, above n 596. See also, Kerr, above n 687, 576. Clifford, above n 739, 147.

view doctrine.[1083] He has suggested three approaches that might limit the plain view doctrine in computer searches.

The first approach focuses on the circumstances of the search where the investigator's intent and the forensic tools determine the validity of the plain view doctrine.[1084] If the investigator's intention is to look for evidence described by the warrant, the discovered materials are admissible evidence, but if the investigator ignores the warrant and starts a different search, the discovered material is not admissible.[1085] In addition, forensic tools can play role in narrowing the plain view exception through using particular tools.[1086] For example, cyberforensics tools might be designated to investigate specific types of cybercrimes, such as intrusion software forensic programmes which are different from cyberstalking forensic tools.

The second approach focuses on the seriousness of the offence.[1087] According to this approach, the plain view evidence can only be admissible if it was associated with serious crimes, perhaps only terrorist offences.[1088]

The third approach demands the termination of the plain view doctrine in computer searches, arguing that the plain view doctrine unduly extends the scope of the search and is difficult to apply in the digital context.[1089]

The restrictive recommendations suggested by Kerr are not practicable in most instances, as he himself explained. The first suggestion, concerning police intent, is somewhat difficult to apply in practice since the police intent may be difficult to know and forensic tools,[1090] such as Paraben Software, are used for different types of searches ranging from e-mails to password recovery.[1091] Similarly, the second suggestion is indefinite and ambiguous since it is difficult to draw the line between serious and less serious offences. The third suggestion discards the plain view doctrine altogether for computer searches. While such a recommendation is appealing from the point of view

[1083] See, Kerr, above n 687.
[1084] Ibid.
[1085] Ibid.
[1086] Ibid 577.
[1087] Ibid.
[1088] Ibid 580.
[1089] Ibid 582.
[1090] Ibid.
[1091] See generally, Volonino, Anzaldua, and Godwin, above n 1004, 179.

of privacy advocates, it would undermine law enforcement efforts in tackling cybercrimes.

Taking a different approach, Moore has defended the use of the plain view doctrine in a digital context.[1092] He suggested that the plain view doctrine in digital searches requires three additional parameters:

1) Access to the source of the evidence be obtained legally. To fulfil this requirement, he recommended that law enforcement officers draft a search warrant that contains a section discussing the nature of the electronic storage media and the need to examine the entire contents of computer.[1093]

2) The apparent illegal nature of the evidence is immediately known.[1094] This requirement is contingent upon the investigators' experience and training. For example, files named 'Boys.gif' are suspicious files potentially containing child pornography materials.[1095]

3) The officer not to abandon the original search. This requirement depends on the existence of objective procedures that corroborate an officer's action.[1096]

According to national legislation and judicial precedents, the plain view exception is markedly different in Jordan, Australia and the USA.

a) Jordan

Although, the plain view doctrine is not explicitly recognised in the Jordanian *Criminal Procedure Law* 1961, two provisions, 82 & 87, of the Act specifically allow officers to search and seize items in plain view. Provision 82 authorises the General Prosecutor to conduct a comprehensive search of the entire site to find whatever it is that might be evidence of a crime.[1097] Provision 87 allows law enforcement officers to seize anything that is deemed to be necessary for ongoing investigation.

[1092] See, Moore, above n 1069, 71.

[1093] Ibid.

[1094] Ibid.

[1095] See, eg, Dorothy E. Denning and William E. Baugh Jr, 'Hiding Crimes in Cyberspace' in Peter Ludlow (ed), *Crypto Anarchy, Cyberstates, and Pirate Utopia* (2001) 115, 126.

[1096] Moore, above n 1069.

[1097] *Criminal Procedure Law* 1961 (82).

Currently, no judicial precedent rendered by Jordan courts clarifies how officers should deal with computer searches, so exploring the judicial view of Australia and the USA may be helpful in predicating how Jordan's legislature and courts will rule on this issue.

b) Australia

In Australia, the *Crimes Act* 1914 recognises the plain view doctrine. Section 3ZG empowers law enforcement officers to seize on reasonable grounds evidential materials, including electronic forms, if it is in plain view. Division 4, 3ZG stipulates that '[a] constable who arrests a person at premises for an offence, or who is present at such an arrest, may seize things in plain view at those premises that the constable believes on reasonable grounds to be: (a) evidential material in relation to that or another offence; or (b) seizable items'. Accordingly, law enforcement personnel are authorised to seize unexpected evidence inadvertently presented in the plain view.

c) USA

In the USA, the plain view doctrine has long been used to justify seizure of incriminating things presented in the plain view of police.[1098] For example, in *United States v. Cray,* the District Court for Eastern Virginia stated that:

> Agents authorised by warrant to search a home or office for documents containing certain specific information are entitled to examine all files located at the site to look for the specified information. So it is not surprising, then, that in the course of conducting a lawful search pursuant to a search warrant, law enforcement agents often discover evidence of criminal activity other than that which is the subject of the warrant. If an agent sees, in plain view, evidence of criminal activity other than that for which she is searching, this does not constitute an unreasonable search.[1099]

In an earlier decision, the Supreme Court developed two elements that make evidence obtained by the plain view doctrine admissible.[1100]

1) The incriminating nature of the item in plain view must be immediately apparent.

[1098] See generally, Robert Stering, *Police Officer's Handbook: An Introductory Guide* (2004) 83. See also, Brenner and Frederiksen, above n 596, 39-89. See also, Franklin, above n 1071, 137.

[1099] *United States v. Cray* 78 F.Supp.2d 524, 528-29 (E.D. Va. 1999).

[1100] *Horton v. California*, 495 U.S. 128, 136-37 (1990). See also, *United States v. Patrick Carey*, 172 F. 3d 1268 (10th Cir 1999).

2) The officer must be lawfully located in a position from which he or she can plainly see the item. Thus, seizures of items in plain view incident to the exercise of a search warrant, an arrest, or a valid exception to the warrant requirements are valid..

These elements have become key determinants in the USA in validating the plain view doctrine either in traditional searches or cybercrime and digital evidence. Nevertheless, the application of the Supreme Court's elements to digital searches can cause some problems, particularly the first element (which requires that the object be immediately apparent). The second element can be applied to physical and digital searches simultaneously without causing particular difficulties. For example, concerning the second element of seizures of items in plain view, incidental to the exercise of a lawful search, an officer legally searching for evidence of DoS attack can seize pornography images displayed on the computer's screen.

The USA courts, however, have adopted two different viewpoints about whether a warrant authorising a search of a computer for a specific crime would permit the officer to search images files that appear to contain evidence of other criminal activity. The first viewpoint is illustrated by the judgment of the Tenth Circuit Court in *United States v. Carey*.[1101] That court invalidated a plain view search of child pornography images on the ground that the investigator who obtained a warrant to search for drug trafficking evidence, temporarily abandoned his original search when he discovered sexually suggestive files that contained child pornography images.[1102] The investigator then spent five hours searching and downloading child pornography files.[1103]

The second viewpoint provides more leeway for investigators to open closed files in the course of conducting a search under the plain view doctrine. In *United States v. Cray,* the Eastern District of Virginia held that:

> It is not surprising that in the course of conducting a lawful search pursuant to a search warrant, law enforcement agents often discover evidence of criminal activity other than that which is the subject of the warrant. If an agent sees, in plain view, evidence of criminal activity other than that for which she is searching, this does not constitute an unreasonable search under the Fourth Amendment.[1104]

[1101] *United States v. Carey,* above n 808, 1268.
[1102] Ibid.
[1103] Ibid 1272.
[1104] *United States v. Montgomery Gray*, 78 F. Supp. 2d 524, 528 (1999).

The court based its judgment on the ground that in computer searches it is not immediately apparent whether or not an object retrieved is within the scope of a search warrant and therefore officers must examine the object to determine that.[1105] The court stated that digital documents, unlike illegal drugs or other contraband, may not appear incriminating on the surface.[1106] As a result, in any search for records or documents, innocuous records must be examined to determine whether they fall into the category of those papers covered by the search warrant.[1107] Thus, an agent authorised by a warrant to search computers or networks for files containing certain specific information is entitled to examine all files located at the hard disk to look for the specified information.[1108]

d) Comparative Legal Analysis

Jordanian law does not provide much direction on whether to seize incriminating digital evidence discovered inadvertently. Although the two provisions are not equivalent to the plain view doctrine, they function as an appropriate mechanism to seize evidence if it is positioned in plain view. However, the current provisions are only meant to apply to physical searches and seizures.

Australian law, in contrast, recognises the plain view doctrine in digital searches. The *Crimes Act* 1914 explicitly states that incriminating digital evidence discovered in plain view while conducting a lawful search can be seized. It explicitly authorises officers to seize digital evidence not described in a warrant and presenting itself in plain view of police.

In the USA, the courts have modelled two different types of decisions, restrictive and non-restrictive. The restrictive view protects criminals and aborts justice because it restrains investigators from opening files they see as suspicious. The second view takes into consideration the unique nature of digital contents by allowing investigators to open files to discover evidence of criminal activity other than that described in the warrant. From these conflicting viewpoints, it is evident that the courts interpret the plain view

[1105] Ibid.
[1106] Ibid.
[1107] Ibid.
[1108] Ibid.

doctrine in different ways and that these differences will continue to pose problems for forensic investigators.

The unrestrictive plain view doctrine can play a significant role in computer searches. This is because electronic storage devices are increasing in capacity and becoming typical places where illegal and incriminating objects are stored. While, forensic software tools are increasing in capability to rummage through thousands of files, images and documents, the likelihood is increasing of encountering incriminating objects not described in the search warrant. Therefore, the unrestricted plain view doctrine serves the interest of justice. Jordanian law enforcement officers sooner or later will encounter situations in which the plain view doctrine helps to seize incriminating data. Requirements to obtain a warrant prior to seizing items in such circumstances would unduly hamper efficient and effective investigations and often be impractical. Therefore, it is optimal for Jordan to amend its law to authorise this non-restrictive approach of plain view.

8.1.4 Incident to a Lawful Arrest

According to Clancy, arrest 'involves a police officer chasing and graphing a known suspect, informing him of his Miranda rights that he is under arrest, searching him and hauling that person to the police station'.[1109] This definition shows that searching the suspect is a fundamental procedure of arrest, but this arrest must be a lawful one. For example, if a police officer sees a robber on the run, he may arrest the robber and search him for evidence without a warrant. A warrantless search is permissible if it is executed incidentally to a lawful arrest. This gives police officers the absolute right to search premises and seize evidence if they observed the crime being committed or they believe on reasonable grounds that the suspected person committed the crime.[1110] For example, if shortly after a murder occurred, an officer found a man carrying a briefcase around

[1109] 'A common definition of arrest states that it occurs in any one of three ways: 1) touching a person; 2) any act indicating an intention to take the person into custody, which subjects the individual to the actual control and will of the person making the arrest; 3) consent by the person to be arrested'. For more definitions of arrest and discussion, see Thomas Clancy, 'What Constitute an Arrest within the Meaning of the Fourth Amendment'? (2003) 48 *Villanova Law Review* 129,130-137.

[1110] See, eg, Larry J Siegel and Joseph J Senna, *Introduction to Criminal Justice* (10th ed, 2005) 252. See also, Tronc, Crawford, and Smith, above n 677, 111. See also, Calsyn et al, above n 956, 1227. See also, كامل السعيد, above n 699, 460. See also, قدري عبدالفتاح الشهاوي, above n 681, 92.

the crime scene with blood on his clothes, a search of the suspect's person and of the briefcase and his immediate surrounding would be a proper search incident to a lawful arrest without a warrant.

The purpose of the search that is an incident of a lawful arrest is twofold. First, it is to preserve evidence of a crime.[1111] Police officers are authorised to search a suspect and areas within the suspect's immediate control, including containers found in his possession, such as a laptop, a cellular phone or a palm, and preserve incriminating items.[1112] Second, it is to protect an individual or a group of people, or the suspects or the officers from possible danger by removing any objects nearby that may cause harm.[1113] Furthermore, two rules must be observed when conducting a warrantless search that is incidental to a lawful arrest. First, the search must be conducted at the time of or immediately following a lawful arrest.[1114] Hence, any search that is conducted after the arrest or if the arrest was unlawful is invalid. Second, the police may search only the suspect and the area within the suspect's immediate control.[1115]

Nowadays, it is common for law enforcement officers to find electronic devices in the possession of a person who is arrested, because of the ubiquity and pervasiveness of laptops[1116] and other portable electronic devices, such as mobile phones, and PDAs. In Jordan, Australia, and the USA, search as an incident to a lawful arrest is well established in traditional searches and has been confirmed and applied in law enforcement practice and judicial precedents. Yet each country's approach to the concept of search incident to a lawful arrest is different. Jordan's courts have not yet handled the search incident to a lawful arrest without a warrant of digital devices. Therefore, exploring the judicial view of the USA may helpful in predicating how Jordan's legislature and courts will rule on this issue.

[1111] See, eg, David Feldman, *the Law Relating to Entry, Search, & Seizure* (1986) 227.
[1112] See, Computer Crime and Intellectual Property Section Criminal Division, above n 633. See also, هلالي عبداللاه احمد, above n 956, 156.
[1113] See, Feldman, above n 1111. See also, Clancy above n 718. Moore, above n 1069, 94.
[1114] Siegel and Senna, above n 1107.
[1115] Ibid.
[1116] In 2000, for example, a standard laptop's storage capacity was 1.5 Gigabyte hard disk compared with more than 250 Gigabyte nowadays, and the size is increasing dramatically.

a) Jordan

The power of search and seizure incident to a lawful arrest exception is identified somewhat narrowly in the Jordanian *Criminal Procedure Law* 1961. Two provisions are of particular concern to the search incidental to arrest doctrine. The first provision addresses the search of properties incidentally to the arrest of the arrestee's person, and the second is the frisk search of a person who is arrested. First, provision 93/4 of the *Criminal Procedure Law* 1961 authorises law enforcement officers to search premises where the suspect might be hiding for the purpose of finding the suspect. In addition, it authorises officers to search properties to preserve evidence relevant to the crime or to protect an individual or a group of people, or the suspects or the officers from possible danger, by removing any objects nearby that may cause harm and arrest the culprit without a warrant. The second provision 97/1 authorises the search of a person's body, clothes, or belongings to preserve evidence of a crime. The frisk search must be performed immediately at or after the arrest.

b) Australia

In Australian, the High Court in *Wheare v Police* had occasion to consider search incident to a lawful arrest and stated: '…a constable is entitled to enter on private property to effect an arrest within the limits of his common law power to arrest without warrant, although he would be a trespasser if he entered or remained on the property for any other purpose'.[1117] Australian law enforcement officers, therefore, have been vested by the common law with the power to arrest a person where they have reasonable grounds for suspecting that an offence has been committed and that he or she is the person who committed it.[1118] The *Crimes Act* 1914 then thoroughly defines the parameters of a search incident to a lawful arrest.[1119] Section 3UD states that 'police officers on reasonable grounds have the right to search and seize items that might be connected to the offence committed or any other items that might be used against the police or other persons'.[1120] It authorises officers to perform either an ordinary search or a frisk search of a person[1121] and his immediate surrounding area.

[1117] *Wheare v. Police* (2008) SASC 13.
[1118] Ibid.
[1119] *Crimes Act 1914* (Cth).
[1120] See, Tronc, Crawford and Smith, above n 677.
[1121] *Crimes Act 1914* s 3UD (1) (b) (i).

c) USA

By contrast, in the USA, the rules of search incident to a lawful arrest have been elaborated by the courts' decisions. Courts validated the warrantless search of a person arrested and his immediate surrounding area, because of the urgent need to remove weapons that the person might seek to use in order to resist arrest or escape, and the need to prevent the concealment or destruction of evidence.[1122]

In *United Sates v. Rafael,* troopers arrested Rafael. In a search of Rafael incidental to his arrest, officers found two mobile phones on his person and seized them and then one officer downloaded the memory of one phone and someone else the memory of the other.[1123] Rafael contended that the two mobile phones were illegally searched without a warrant and that the search was remote in time or place from the arrest.[1124] The court held that:

> under the circumstances of this case, the government has met its burden to show that the troopers' search of the cell phones by accessing stored numbers was justified as a search incident to arrest…it is imperative that law enforcement officers have the authority to immediately "search" or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence.[1125]

In its decision, the court relied on the Fifth Circuit judgment in *United States v Finley* in which law enforcement officers arrested Finley on drug charges and searched his person and found a cell phone.[1126] During the questioning, another agent searched through the phone's call records and text messages.[1127] The court upheld the retrieval of call records and text messages from the cell phone as search incident to arrest.[1128] Nevertheless, some scholars disagree with the court's conclusion. Toren, Moore, and Middleton have argued that the unique nature and characteristics of digital data require a different approach.[1129] They have rejected the suggestion that the officer may inspect the entire contents of a suspect's electronic device as the courts uniformly held that the agent may inspect the entire contents of a suspect's wallet, address book, or search the content of a

[1122] *Chimel v. California*, 395 2d 685 US 753, 763 (Supreme Court of the United States, 1969).
[1123] *United States v. Rafael Mercado-Nava*, 486 F. Supp 2d 1271, 1274 (Kan, 2007).
[1124] Ibid 1275.
[1125] Ibid 1278.
[1126] *United States v. Finley* 477 F. 3d 250, 254 (5th Cir, 2007).
[1127] Ibid.
[1128] Ibid 260.
[1129] See, eg, Toren, above n 888, 46. See also, Moore above n 958, 158. Middleton, above n 530, 189.

briefcase without a warrant.[1130] They have emphasised that such a comparison is a flawed, because it ignores the invasive nature of digital search.[1131]

d) Comparative Legal Analysis

The rules of traditional search incident to a lawful arrest are applicable to searches of digital devices. In regard to the purpose of the search, the search incident to lawful arrest is critical in digital searches to preserve evidence, because digital evidence is fragile and delicate, liable to damage, and susceptible to alteration or concealment. In regard to the time and scope of the search, digital searches incidental to a lawful arrest are often associated with suspects who hold personal and portable electronic devices. As a result, legislatures, scholars and judges alike agree that in deciding what is incidental to lawful arrest, officers may immediately search the arrestee and the area within the arrestee's immediate control, including computers found in his possession. However, scholars have debated whether a search incident to a lawful arrest allows officers to conduct a thorough search of the digital contents.

Jordanian law permits search incidental to a lawful arrest without a warrant. The officers can conduct an ordinary search or a frisk search of the person, including portable computers. In a similar manner, the *Crimes Act* 1914 and some of the US courts decisions permit a thorough search of the suspect's person and the area within the suspect's immediate control, including digital devices. The courts upheld the search of digital contents incidental to a lawful arrest. However, disagreement erupted over the scope of the search as a thorough search of digital devices was criticised by scholars, because it ignores individuals' right to privacy and the risk associated with on-site digital searches.

A thorough search of digital devices incidental to a lawful arrest on-site is not recommended, and a warrant must be obtained to conduct a thorough search off-site by forensics investigators to avoid evidence contamination and privacy invasion.

[1130] Ibid.
[1131] Ibid.

8.2 Conclusion

Constitutions draw attention to the fact that individual and dwelling privacy rights are not absolute and are subject to reasonable searches. Therefore, legislatures, courts and scholars all recognise the permissibility of searches without a warrant in exceptional circumstances. These exceptions fulfil the need of law enforcement agencies to have swift and effective search powers in some specific circumstances without the need for formal prior authorisation through the issue of an official search warrant.

The Jordanian *Criminal Procedure Law* 1961 and the Australian *Crimes Act* 1914 address a number of search warrant exceptions. These exceptions are exigent circumstances, consent, plain view, and searches incident to a lawful arrest. Unlike Jordan and Australia, in the USA it is court decisions that have significantly contributed to expanding and re-defining the boundaries of the search warrant exceptions in relation to cybercrime and digital evidence searches.

In regard to exigent circumstance, the *Criminal Procedure Law* 1961 and the *Crimes Act* 1914 provide officers with the power to conduct a search and seizure of evidential materials. However, some scholars have criticised the undue search power, arguing that the exigent circumstance doctrine allows officers to take actions necessary to alleviate the exigent circumstances but it should not allow investigators to conduct a thorough search. Officers must obtain a search warrant to do that. The US court decisions in digital searches show that the doctrine can be applied to search and seizure of digital evidence when there is an immediate danger of losing data, or to prevent the imminent destruction of electronic devices and hardware components. Because digital searches practice jeopardises digital content, and because the digital search requires highly sophisticated investigation skills, and well-equipped professionals, it is recommended that in the case of an exigent circumstance, officers must not perform a search, but seize the hardware devices and obtain a warrant to conduct digital search off-site. However, officers should be able to search electronic storage devices and evidence in exigent circumstances in which there is an immediate danger of losing data, or to prevent the imminent destruction of electronic devices and hardware components.

Consent is not expressly stated in the *Criminal Procedure Law* 1961 but the latter addresses a search on request of the owner or the occupier. The request search is not equivalent to a consent search. Law enforcement officers cannot approach a defendant's property unless the defendant himself asks them to do so. Meanwhile, in Australia and the USA, law enforcement officers can always search a property if the owner or the occupier of the property gives consent to the search. Law enforcement officers have the opportunity to obtain consent from a person with authority to grant such consent to search private premises including electronic devices. This opportunity is clearly demonstrated in judicial decisions, which indicate that consensual search practices and principles are almost the same in both traditional and digital searches, but that the scope of the search and third party consent in a digital search should be treated differently from traditional searches to reflect the nature and characteristics of digital searches.

The plain view doctrine is foreign to the *Criminal Procedure Law* 1961 but is to be inferred from its general statutory provisions relating to the search warrant exceptions. Australian law explicitly authorises officers to seize digital evidence not described in a warrant yet presenting itself in plain view. Even with these provisions, cybercrime and digital searches create a unique situation which requires a different approach from that used in traditional searches to seize digital evidence positioned in plain view. The USA courts have reached two different conclusions about whether a warrant authorising a search of a computer for a specific crime would permit the officer to search for image files that appear to contain evidence of other criminal activity. The first prohibits officers from opening and seizing files containing evidence of other criminal activity. The second view allows investigators to open files to discover evidence of criminal activity other than that described in the warrant. The latter view serves the interest of justice because electronic storage devices are increasing in capacity and in the likelihood of encountering incriminating objects not described in the search warrant.

Search incidents to a lawful arrest are important in cybercrime and digital searches due to the pervasive use of portable electronic devices. The purpose of the search is to preserve evidence. Jordanian and Australian laws permit two types of searches, ordinary and frisk searches. In the absence of legal provisions or judicial positions on the issue of digital searches, law enforcement officers may treat digital devices with the same familiarity as physical items. In the USA, the courts have upheld the search for digital contents incidental to a lawful arrest although scholars have debated whether search incident to arrest allows officers to conduct a thorough search of the digital contents. Some scholars have rejected the search arguing that the unique nature and characteristics of digital data require treatment different from tangible items. The search of digital contents incidental to a lawful arrest should be confined to the physical device only and not to the digital contents. The argument is quite compelling not only for privacy aspects, but for the risks associated with comprehensive on-site searches. A warrant must be obtained to conduct a thorough search by forensics investigators to avoid evidence contamination and privacy invasion. Therefore, law enforcement officers can physically search and seize the electronic devices and conduct a thorough digital search off-site, which must be supported by a warrant.

Finally, while information technology use is continually increasing and law enforcement agencies use more advanced and sophisticated investigation tools, the current *Criminal Procedure Law* 1961 is inappropriate to address search warrant exceptions. In addition, law enforcement needs relating to cybercrime and digital evidence are different from those relating to traditional circumstances and, therefore, Jordanian law must be amended to bring it into line with the unique nature of digital searches.

9 CROSS-BORDER SEARCHES AND SEIZURES

Introduction

The absence of physical borders in cyberspace undermines cybercrime investigation. While cybercriminals are able to cross-borders and commit cybercrimes without leaving their desks, law enforcement agencies are encumbered by physical borders. Ritter considers the absence of geographic boundaries to be one of the greatest challenges in cybercrime investigation.[1132] This is because law enforcement agencies over the years have exercised their power over crimes committed in the territories located within their own jurisdiction. But with the advent of information technologies and the Internet a novel environment has been created where law enforcement's investigative powers could no longer be performed effectively without mutual assistance from other states. As stated by Silvia Sanusian, Assistant Professor in Law of International Business Transactions, University of Buenos Aries, 'the advent of the Internet has radically shattered the traditional correspondence between territoriality and legally relevant acts and events, destroying the links between geographical location and the...legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena'.[1133] However, even though the co-operation between law enforcement agencies is increasing, this has not been accompanied by a similar development in a legal perspective.[1134]

When a cybercrime is originated abroad and evidence is located in another jurisdiction, local procedures would be fruitless unless accompanied by appropriate international assistance. The previous two chapters showed that the application of traditional search and seizure procedures to cybercrime and digital evidence poses significant challenges and difficulties for law enforcement officers. Thus, Australia and the USA have

[1132] See eg, Nancy Ritter, *Digital Evidence: How Law Enforcement Can Level The Playing Field With Criminals* (2006) National Institute of Justice <http://www.ojp.usdoj.gov/nij/journals/254/digital_evidence.html> at 12 October 2006.

[1133] Silvia S Sanusian, 'Argentina' in Dennis Campbell (ed), *The Internet: Laws and Regulatory Regimes* (2006) 45, 47.

[1134] See, eg, Katrina Michael and Gregory Rose, '*Human Tracking technology in Mutual Legal Assistance and Police Inter-State Co-operation in International Crimes*' University of Wollongong <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1559&context=infopapers> at 23 July 2008.

amended their local laws to meet the new requirements of digital evidence. However, the efficiency and effectiveness of the new amendments are confined by their physical borders. With respect to search for and seizure of digital evidence located in foreign nations, the situation is even more difficult not only for Jordan but also for Australian and US enforcement officers because international practices in the area of search and seizure of digital evidence are not fully harmonised at the international level.

The objective of this chapter is to clarify the legal position and compare Jordan with other jurisdictions where international cybercrime investigation practices have been more fully developed. It compares Jordan with Australia and the US on aspects of international co-operation in cybercrime investigation, and identifies jurisdictional hurdles that hinder cross-border searches and seizures and the ways in which law enforcement officers approach cross-border searches. The key features of the Convention on Cybercrime will be discussed, including the provisions relating to cross-border search and seizure procedures.

The legal instruments available for performing cross-border searches and seizures are very limited and consist mainly of either Mutual Legal Assistance Treaties (MLATs), letters rogatory or domestic legislations.

9.1 Trans-Jurisdictional Hurdles

Jurisdiction refers to the power that each country has to make its own laws and enforce them.[1135] This power is exercised in the legislative, judicial, and executive spheres.[1136] The legislative sphere, or 'jurisdiction to prescribe', includes the power of a state to enact substantive and procedural laws applicable to particular individuals and circumstances.[1137] The judicial sphere relates to the power of a state to subject persons or things to the procedures of its courts or administrative tribunals, whether in civil or in criminal proceedings.[1138] The executive sphere refers to the ability of a state to

[1135] See, Shinder and Ed Tittel, above n 210, 626. See also, Susan W. Brenner and Bert-Jaap Koops, 'Approaches to Cybercrime Jurisdiction' (2004) 4 *Journal of High Technology Law* 3, 5.
[1136] See, eg, Ilias Bantekas, and Susan Nash, *International Criminal Law* (2nd ed, 2003) 143.
[1137] Juan Miguel Goenechea and Agustin Gonzalez Garcia, 'Spain' in Dennis Campbell (ed), *The Internet: Laws and Regulatory Regimes* (2006) 539, 566.
[1138] Ibid.

implement its laws and enforce judicial decisions.[1139] These three types of jurisdiction are generally recognised in international law[1140] and each is necessary for cybercrime investigation. Jurisdiction to prescribe is required to enact legislation which allows for the search and seizure of computer data. Judicial jurisdiction is required to judge and convict cybercriminals. Executive power is vital to carry out investigations and enforce judicial decisions.

In contrast to the way a state's extraterritorial legislative jurisdiction is limited to a particular person in a particular situation,[1141] the scope of its executive power to conduct search and seizure is limited by the state's physical and political boundaries.[1142] For example, if an Australian computer hacker hacked into the computers of the City Bank in Jordan and obtained the password necessary to effect a wire transfer from that bank to another bank account in the USA,[1143] then the criminal act was perpetrated in Australia though the harmful consequences of the crime happened in Jordan. The question that needs be asked is: can Jordanian officers search the suspect's computer or the service provider's server which is located in Australia and seize evidence?

The practical procedures of search for and seizure of digital evidence are almost identical, whether incriminating evidence is located within the national jurisdiction on the defendant's computer hard drive or on a foreign Internet Service Provider's server. The widespread accessibility of the Internet, coupled with the ease of use and power of forensic tools, provides opportunities to view and retrieve intangible objects stored on foreign servers, networks or the Internet.[1144] In other words, law enforcement officers

[1139] Bantekas, and Nash, above n 1136.

[1140] Darrel C Menthe, *Jurisdiction in Cyberspace: A Theory of International Space* (1998) Michigan Telecommunications and Technology Law Review < http://www.mttlr.org/volfour/menthe_art.html>at 16 August 2008.

[1141] Johnson and Post argue that states should not seek to apply territorially based regulations to online activities, because the state's inability to enforce its regulations against law-violators not located within its territory renders any attempt to regulate futile and illegitimate. See, David R Johnson and David G Post, 'Law and Borders -The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review,* 1367.

[1142] Maier agues 'the idea that sovereign authority is limited by territorial boundaries is far from dead'. Harold G Maier, 'Jurisdictional Rules in Customary International Law' in Karl Matthias Meessen (ed), *Extraterritorial Jurisdiction in Theory and Practice* (1996) 64, 65. See also, Ralf Michaels, 'Territorial Jurisdiction After Territoriality' in Pieter J Slot et al, (ed), *Globalisation and Jurisdiction* (2004) 105, 107. See also, Patricia L Bellia, 'Chasing Bits Across Borders' (2001) *The University of Chicago Legal Forum* 35, 47.

[1143] For more examples concerning this particular form of hacking see, James Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering* (1999), 70-71.

[1144] See eg, Jack L Goldsmith, 'The Internet and Legitimacy of Remote Cross-Border Searches' (2001) *The University of Chicago Legal Forum*, 103.

may be able to hack into any foreign computer systems to gather evidence.[1145] Therefore, the Jordanian officers in the above example might be able to access and review data and seize digital evidence located in Australia without encountering technical problems or notifying the Australian counterpart. Nevertheless, the mere search, by itself, would usually not suffice to support a successful prosecution and, therefore, Jordan will need the co-operation of the Australian counterpart to extradite the accused or to assist in the prosecution. Furthermore, unilateral foreign search and seizure of data violates the foreign state's (i.e. Australia's) sovereignty.[1146] As a result, countries are highly unlikely to conduct cross-border searches without notifying the concerned party through proper legal avenues.[1147]

Search and seizure of digital evidence stored on foreign servers should be legally treated as a physical object search and, therefore, law enforcement officers must consider the local law applicable where the evidence is located as well as any legal agreement in effect that covers the issue. In their book *Cyber Criminals on Trial*, Smith, Grabosky and Urbas identify a number of challenges facing law enforcement officers investigating cross-border cybercrime.[1148] Two of these challenges are, for the most part, jurisdictional concerns. The first challenge experienced by enforcement officers who receive a request for assistance is the ambiguity concerning whether the conduct in question is unlawful in their own jurisdiction.[1149] While in the above example the situation is very simple, because hacking is a crime in Australia, in more complex scenarios where the offence was not against the laws of Australia, or the offence was considered not to be prosecutable due to insufficient evidence, the assistance may be declined. The second challenge arises when incriminating data and files are stored on a

[1145] For example, FBI agents investigating cybercrime cases were able to hack and download evidence off a suspect's computer networks in Russia. See, *Russian Hacker Gets 3 Years in Jail*, msnbc < http://www.msnbc.msn.com/id/3078748/> at 4 August 2008.

[1146] A States' sovereignty in cyberspace is a controversial subject. Jack Goldsmith, argues that 'unilateral extraterritorial enforcement measures should not be viewed as an illegitimate invasion of another nation's sovereignty. Cross-border searches and seizures should be viewed instead as part of the inevitably messy process of working out new customary principles of sovereignty to accommodate a new and important, but also potentially dangerous, technology'. Goldsmith, above n 1144, 118. He also, argues that unilateral regulation of the internet is legitimate". See, Jack Goldsmith, 'Unilateral Regulation of the Internet: A Modest Defence' (2000) 11 *European Journal of International* 135.

[1147]Goldsmith, above n 1144.

[1148] Smith, Grabosky and Urbas, above n 25.

[1149] Ibid.

remote server located in one or more other jurisdictions.[1150] The issue is even more complicated, involving not only one but many sets of national laws. In such a case, seeking incriminating evidence located in one or more foreign countries, getting access to and collecting the data is a bewildering and complicated process. This challenge may also be sufficient reason to refuse law enforcement cooperation.

9.1.1 Factors Contributing to the Success or Failure of Cross-border Searches

Three important factors should be considered when approaching cross-border searches, namely political, cultural and legal factors.

a) Political

Scholars argue that a good relationship between the countries concerned is going to benefit cross-border criminal investigations. For example, informal police-to-police co-operation flourishes in a friendly political atmosphere. In this context, Smith, Grabosky, and Urbas opined:

> …If relations with one's counterparts in another country are not close, one is less likely to go the extra mile. Even where a treaty places an obligation on parties to cooperate…when authorities in another country are disinclined to cooperate, for whatever reason, investigations can be complex and legally murky.[1151]

The political factor, i.e., the presence or absence of political will, significantly contributes to the success or failure of any cross-border investigation.[1152] For example, the 1996 attack on Citibank in New York by Russian hackers[1153] clearly demonstrated the problems of co-operation within an unstable political relationship between Russia and the USA. The Russian counterpart showed no interest in cooperating with the FBI.

[1150] Smith, Grabosky and Urbas, above n 25, 48. See also, Roderic Broadhurst, 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29 (3) *An International Journal of Police Strategies & Management* 408, 412.

[1151] Smith, Grabosky and Urbas, above n 25, 57.

[1152] See, eg, M M Richard, ' International Assistance in Combating Crime' in Brice Ruyver, Gert Vermeulen, and Tom Beken (eds), *Strategies of the EU and the US in Combating Transnational Organized Crime* (2002) 227, 229.

[1153] In 1996, the Russian hackers were able to transfer $10 Million across 40 transactions from Citibank to accounts in Finland, Russia, Germany, the Netherlands, the United States, Israel and Switzerland. See generally, Dan Blake, 'Russian Hackers Caught After Stealing $10 Million', *Denver Post* 1995, 7.

The latter responded unilaterally and in an unprecedented way. The FBI set up a bogus computer security company in Seattle, and then lured the Russian hackers, Alexei Ivanov [1154] and Vasiliy Gorshkov, to do some well-paid security work as hackers. For the job interview, undercover FBI agents installed keystroke logging, a programme that records what is typed on a keyboard on the laptop provided by the FBI,[1155] and asked Ivanov and Gorshkov to demonstrate their hacking skills. The hackers happily complied and logged in to their home server back in Russia.[1156] Following their arrest, FBI agents used the recorded information to access the hackers' computer situated in Russia and download evidence.[1157]

Good political relationships between the concerned parties coupled with regular implementation of any relevant treaty enhance the Mutual Legal Assistance (MLA) process. M.M Richard, Senior Counsel for Enforcement Matters, US Mission to the EU, opined that 'experience has shown that countries tend to give priority attention to requests from bilateral partners where special relationships have grown between those responsible for implementation over multilateral requests'.[1158] Thus, cross-jurisdictional search and seizure can sometimes be affected in the absence of a good political relationship but a good relationship and willingness to help each other in cross-border investigation is usually a requirement prerequisite. Fortunately, political relationships between Jordan, Australia, and the USA are fundamentally in good shape.

b) Cultural

Cultural factors are of crucial importance in cross-border investigations. Widely differing cultural perspectives are may hinder coordination and co-operation on criminal

[1154] Alexei Ivanov was a 20 year old computer programmer from Chelyabinsk, Russia. See generally, Art Jahnke, *Alexey Ivanov and Vasiliy Gorshkov: Russian Hacker Roulette* (2005) CSO Security and Risk <http://www.csoonline.com/article/219964/Alexey_Ivanov_and_Vasiliy_Gorshkov_Russian_Hacker_Roulette?contentId=219964&slug=&> at 2 August 2008.

[1155] See generally, Richard Gissel (ed), *Digital Underworld: Computer Crime and Resulting Issues* (2005) 128. See also, Susan W Brenner and Joseph J Schwerha, 'Cybercrime Havens: Challenges and Solutions' (2007) 17 *Business Law Today.* See also, Jahnke, above n 1154.

[1156] Ibid.

[1157] Ibid.

[1158] M M Richard, above n 1152, 237.

assistance and cross-border investigation.[1159] Mike Kennedy, the president of Eurojust, opined:

> Increasingly, we are finding that there are cases linked to Member states which are not just adjacent to each other in geographical terms but also linked, possibly through the internet, right across the European Union. Because the legal systems are so different, particularly the four common law countries…from those based on the Napoleonic Code or other codes…there are many rubbing points. This is simply in the systems themselves. There is a cultural difference …we need to bridge these gaps and these barriers to be able to deal satisfactorily with cases.[1160]

Each nation has its own notion about what constitutes criminality, the appropriateness of punishment, proportionality of punishments[1161] and investigative priorities.[1162] This is obvious in some views of cybercrime investigation policy. For example, countries such as Australia and the USA pay maximum attention to fighting child pornography but pay no attention to pornography production and distribution. This situation is totally opposite to that in Jordan, where child pornography is not on the national agenda because of the lack of resources and the need to attend other prevalent crimes, such as the production, distribution and possession of pornography. Arguably, such cultural factors may be of less affect in cybercrime investigations because there are few discrepancies in cultural policy concerning cybercrime criminalisation. Indeed, a significant degree of consensus exists regarding certain types of cyber offences.[1163]

c) Legal

Cyberspace has no geographic boundaries,[1164] so cybercrime often crosses multiple-jurisdictional boundaries with differing laws and procedures.[1165] Law enforcement officers must engage in a complicated jurisdictional quarrel to obtain evidence.

[1159] See, eg, Miriam F Miquelon-Weismann, ‘The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects For Procedural Due Process’ (2005) 23 *The John Marshall Journal of Computer & Information Law* 329, 354.

[1160] Home Affairs Committee, Great Britain: Parliament: House of Commons, *Justice and Home Affairs Issues at European Union Level* (2007) 46.

[1161] Ibid.

[1162] See Section 5.2.1 for more information about cybercrime investigation priorities.

[1163] See chapters 3 & 4 for more information about cybercrime criminalisation.

[1164] Al Aldesco, ‘Demise of Anonymity: A Constitutional Challenges to the Convention of Cybercrime’ (2002) 23 *Loyola of Los Angeles Entertainment Law Review* 81, 82. See also, Smith, Grabosky and Urbas, above n 25, 12.

[1165] See, eg, Ian Walden, 'Crime and Security in Cyberspace' (2005) 18 (1) *Cambridge Review of International Affairs* April 2005, 56.

Sometimes, evidence cannot be obtained, because of data protection and privacy rights concerns,[1166] or the lack of legal instruments authorising transnational cooperation.

Substantive legal factors, such as the existence of a common criminalisation policy, are still essential. For example, the failed prosecution for the release of the 'I love you' virus by a Philippine student demonstrated the importance of a common criminalisation policy.[1167] The Philippine student was able to walk free from court in the Philippines, despite the fact that the political relationship between the Philippines and the USA was quite positive, because of the absence in the criminal code at the time in the Philippines of the crime of the creation and distribution of computer viruses.[1168] However, different legal instruments in particular serve to facilitate law enforcement co-operation in the fight against transnational crimes. MLA, letters rogatory and domestic legislation are particular legal instruments that seek to resolve problems of cross-border criminal investigation and create effective co-operation among countries.

The three mentioned above – political, cultural and legal - factors have always existed and have a close relationship in any form of transnational cooperation. Political and cultural differences preclude concerned parties from adopting common criminalisation policies. For example, freedom of religion is protected by the constitution of the USA, while conversion from Islam to another religion is considered a serious crime in most parts of the Islamic world. Hence, creating a website to promote atheism and fight religious influence is not an offence in the USA, but a crime in Jordan.[1169] If that website is hosted by an American Internet Service Provider and the webmaster lives in the USA, the latter will not respond to an assistance request issued by Jordan. The existence of the political will to assist and cultural consistency, as well as robust legal instruments, are each vital for successful cross-border investigation. Nevertheless, the existence of robust legal mechanisms for obtaining evidence in foreign nations reflects both the political will to cooperate and bridge cultural differences.

[1166] M M Richard, above n 1152, 228.

[1167] See Sections 1.4.1/3.1 and 3.2.2.1 for more information about 'I LOVE YOU BUG'.

[1168] Smith, Grabosky and Urbas, above n 25, 55.

[1169] *Criminal Law 1960* (278).

9.2 Legal Mechanisms to Obtain Evidence Situated in a Foreign State

Over the past decade, it has become critical for law enforcement agencies and officers involved in any cybercrime investigation to understand the legal mechanisms by which evidence may be obtained from foreign nations. In the absence of particular legal provisions concerning searches and seizures of digital evidence, the traditional legal avenues for searching and collecting evidence remain pre-eminent. They are MLA and letters rogatory as well as domestic legislation. These will each be examined in this chapter. The sole international legal instrument on cybercrime, the Convention on Cybercrime, will also be examined and discussed. Then the perspectives of Jordan, Australia, and the USA will be explored and analysed.

9.2.1 Mutual Legal Assistance (MLA)

The use of MLA instruments which allow the exchange of evidence between jurisdictions is commonly and increasingly used to cooperate in transnational prosecutions.[1170] Michael and Rose define MLA as a 'mechanism by which lawyers and the courts of one jurisdiction can request assistance from another.'[1171] Another definition 'is the process whereby one state provides assistance to another in the investigation and prosecution of criminal offences'.[1172] The two definitions seem to emphasise two different but equally important aspects of MLA. According to Rose, the MLA can be carried out in a more simplified way, and would be less susceptible to the political factor because it can be requested by lawyers or courts. According to the second definition, it can be formalised through bilateral state-to-state agreement.[1173] For example, the USA has bilateral Mutual Legal Assistance Treaties (MLATs) with more

[1170] See, eg, Jody R Westby, *International Guide to Combating Cybercrime* (2003) 44. See also, Bantekas, and Nash, above n 1136, 231.

[1171] Michael and Rose, above n 1134.

[1172] William C Gilmore, *Mutual Assistance in Criminal and Business Regulatory Matters* (1995) xii.

[1173] See Bantekas, and Nash, above n 1136.

than 80 countries around the world,[1174] and multilateral agreements, such as the Council of Europe Convention on MLA in Criminal Matters (which came into force in 1962).[1175]

9.2.1.1 Bilateral Mutual Legal Assistance Treaty

Bilateral MLAT is a popular legal mechanism which obliges two parties to assist each other in various criminal investigations by obtaining evidence located in one country for the benefit of the requesting party.[1176] For example, Article 15 of the bilateral MLAT between the government of Australia and the USA stipulates 'The Requested State shall execute a request for the search, seizure, and delivery of any article to the Requesting State if the request includes the information justifying such action under the laws of the Requested State'.[1177] MLAT is one of the most important legal tools that can be utilised to obtain evidence located in a foreign country. It deals with the legal complexities associated with the problems of coordinating law enforcement, including dual criminality[1178] and other transnational co-operation requirements.[1179]

Countries seem to prefer not to have a bilateral MLAT limited to a narrow range of offences or procedures[1180] and, therefore, there is no bilateral MLAT specifically to address cybercrime investigations assistance. The classical forms of mutual legal assistance, which were originally established to address traditional crimes, are currently used to provide assistance in searching for and gathering digital evidence across borders. It provides several advantages including that investigation assistance may be provided even in the absence of common criminalisation policies and that a designated authority will serve as a direct point of contact for receiving and transmitting requests

[1174] See, U.S State Department, *Mutual Legal Assistance (MLA) and Other Agreements* <http://travel.state.gov/law/info/judicial/judicial_690.html> at 20 September 2008.

[1175] *European Convention on Mutual Assistance in Criminal Matters*, opened for signature 20th April, 1959, CETS No. 030 (entered into force 12 June 1962).

[1176] See, eg, Jeffrey G Bullwinkel, 'International Co-operation in Combating Cyber-Crime in Asia: Existing Mechanisms and New Approaches' in Roderic G Broadhurst, and Peter N Grabosky (eds), *Cyber-Crime: The Challenge in Asia* (2005) 269, 276.

[1177] *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters,* opened for signature 30 April 1997, No 19, art 15 (1) (entered into force 30 September 1999).

[1178] According to Westby, dual criminality means the act under investigation must be criminalised under both concerned parties' laws and punishable by a minimum term in prison, usually one year. See, Westby, above n 1167. See also, Bullwinkel, above n 1173.

[1179] Alan Ellis and Robert L Pisanit 'The United States Treaties on Mutual Assistance in Criminal Matters: A Comparative Analysis' (1985) 19 *International Lawyer* 189, 191. See also, Westby, above n 1167, 45. M M Richard, above n 1152, 235.

[1180] See M M Richard, ibid 238.

for assistance.[1181] Nevertheless, the classical form of mutual assistance seems much less capable of handling digital evidence searches because digital evidence is highly volatile[1182] and has a correspondingly high risk of contamination or destruction at the touch of a keyboard.[1183] Cybercrime searches require swift and decisive action to which, often, the normal search and seizure procedures addressed by MLAT are not well suited. For example, Article 15/3 of the MLAT between Australia and the USA stipulates that 'the Central Authority of the Requested State may require that the Requesting State agree to terms and conditions deemed necessary to protect the articles to be transferred'.[1184] Although this Article requires the requested State to process the request in accordance with the procedures set forth in its law, it delays quick and immediate response. Indeed, the MLATs have been consistently criticised as being 'cumbersome and time consuming'.[1185] Richard opined that:

> In fact, our experience has shown that even well drafted international instruments that are poorly implemented can be less effective than poorly drafted ones that are implemented with a view by the parties of providing the widest possible range of co-operation allowed under the instrument.[1186]

The practical application of the treaty is fraught with complications due to the bureaucratic system it goes through and poor implementation.

9.2.1.2 Multilateral Mutual Legal Assistance

Several countries and international organisations have made efforts to improve cybercrime law enforcement co-operation by adopting measures especially concerning extradition and mutual legal assistance procedures and other forms of co-operation such as common training. For example, the Council of Europe (CoE), Asian-Pacific

[1181] Bullwinkel, above n 1176.

[1182] See Section 6.2 for more information about digital evidence volatility.

[1183] See, eg, Susan W Brenner, 'The Council of Europe's Convention on Cybercrime' in Jack M. Balkin, et al (eds), *Cybercrime: Digital Cops in a Networked Environment* (2007) 207, 213.

[1184] *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters,* opined for signature 30 April 1997, No 19, art 15 (3) (entered into force 30 September 1999).

[1185] See, Gregor Urbas and Peter Grabosky, 'Cybercrime and Jurisdiction in Australia' in Bert-Jaap Koops and Susan W Brenner (ed), *Cybercrime and Jurisdiction* (2006) 47, 65. See also, Bantekas, and Nash, above n 1136, 232. Westby, above n 1167. Susan Brenner and Joseph J Schwerha IV 'Introduction-Cybercrime: A Note on International Issues' (2004) 6 *Information System Frontiers* 111, 112.

[1186] Richard, above n 1152, 228.

Economic Co-operation (APEC), the G8[1187] and the United Nations (UN) have each developed cross-border mutual assistance responses to cybercrime. The CoE Convention on Cybercrime is the first and only multilateral MLAT specially aimed at cybercrime and open to non-member countries to ratify.[1188] The USA is a signatory to the Convention, while Jordan and Australia can sign up and become parties.

Convention on Cybercrime

The foreign ministers of the Council of Europe, on November 8, 2001 adopted the Convention on Cybercrime.[1189] At its adoption date, the Convention was signed by 26 of the 46 member states of the CoE, along with the CoE's partner states Canada, Japan, South Africa and the USA, who participated in its elaboration but who are not member states of the CoE.[1190] On July 1, 2004 the convention came into force for Albania, Croatia, Estonia, Hungry and Lithuania.[1191] As of August 28, 2008, the Convention has been signed by 45 states and ratified by 23 countries.[1192]

The European Convention on Cybercrime consists of forty-eight articles in four chapters, namely, use of terms, measures to be taken at the national level, international cooperation, and final provisions.[1193] It is the first and sole international treaty focused only on problems arising from cybercrime.[1194] The Convention aims at harmonising the member states' provisions on cybercrime and strengthening international cooperation.[1195] Accordingly, it adopts a three-pronged approach, encompassing provisions relating to the harmonisation of substantive cybercrime law, domestic

[1187] The G8 stands for the 'Group of Eight Nations' the USA, Japan, United Kingdom, Italy, Russia, Germany, France, and Canada.

[1188] Council of Europe, *Convention on Cybercrime CETS NO: 185*, < <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>at> 28 August 2008

[1189] Ibid. See also, Kristin Archick, 'Cybercrime: the Council of Europe Convention*'* in John V Blane (ed), *Cybercrime and Cyberterrorism: Current Issues* (2003) 1, 2.

[1190] Ibid.

[1191] Council of Europe, *Chart of Signatures and Ratifications*, < http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=11&DF=9/28/2008&CL=ENG> at 28 August 2008.

[1192] Council of Europe, *Convention on Cybercrime CETS NO: 185*, < <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>at> 28 August 2008.

[1193] Council of Europe, *Convention on Cybercrime CETS NO: 185* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=11&DF=9/28/2008&CL=ENG> at 24 August 2008.

[1194] Ibid.

[1195] Ibid.

procedural law powers for investigation and prosecution of cybercrime, and mutual legal assistance.[1196]

The first prong of the three-pronged approach is legislative.[1197] Articles 2 to 13 address substantive law issues and include criminalisation provisions.[1198] One of the Convention's key achievements is to require members to ensure that their national cybercrime laws meet the criteria set forth in the Convention with respect to four categories of cybercrime:[1199]

1) Offences against the confidentiality, integrity, and availability of computer data and systems, including hacking, illegal interception, data interference, system interference, and misuse of devices;[1200]

2) Computer-related offences including forgery and computer fraud;[1201]

3) Computer-related offences including production, dissemination, and possession of child pornography;[1202]

4) Offences related to infringement of copyright and related rights, including commercial scale distribution of pirated works.[1203]

The four categories represent the minimum list of offences necessary for a uniform criminal policy on legislation concerning cybercrime.

The second prong of the Convention, Articles 14 to 21 seeks to harmonise domestic rules of procedural law and jurisdiction among signatory countries.[1204] This requires each member country to incorporate the following procedural laws:

1) Expedited preservation of stored computer data, including any measures as may be necessary to oblige a service provider to preserve and maintain the

[1196] See, Diane Rowland, and Elizabeth Macdonald (ed), *Information Technology Law* (3rd ed, 2005) 481.
[1197] Ibid.
[1198] See, eg, Council of Europe, above n 1188.
[1199] See generally, Indira Carr, and Katherine S Williams, 'Draft Cyber-Crime Convention: Criminalization and the Council of Europe Draft Convention on Cyber-Crime' 18 *Computer Law & Security Report* (2002) 83-87.
[1200] Ibid.
[1201] Ibid.
[1202] Ibid.
[1203] Ibid.
[1204] See, eg, Council of Europe, above n 1188.

integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, and subject to an extension;[1205]

2) The ability to order a person to provide computer data under his or her control and to order a service provider to provide subscriber information under its control;[1206]

3) Search and seizure of stored computer data, ensuring that a member state can authorise the search of any computer system located in its territory and any other computer system accessible from the initial system;[1207] and

4) Real-time collection of traffic data and interception of content data.[1208] These procedures are to be applied not only to the crimes defined in accordance with the Convention but also to any crime committed by means of a computer system and to the collection of digital evidence for use in prosecuting any other crime.[1209]

The third prong pertains to mutual assistance.[1210] Although the Convention does not supersede existing bilateral mutual legal assistance treaties, it addresses a variety of areas of mutual legal assistance, including extradition,[1211] spontaneous information exchanges,[1212] designation of a central authority responsible for all incoming and outgoing legal assistance and extradition requests,[1213] expedited preservation of stored computer data located within the territory of a party,[1214] expedited disclosure of

[1205] *Convention on Cybercrime*, opened for signature 23 November, 2001, CETS No. 185, art 16 (2) (entered into force 1 July 2004).
[1206] *Convention on Cybercrime*, opened for signature 23 November, 2001, CETS No. 185, art 18 (1) (entered into force 1 July 2004).
[1207] *Convention on Cybercrime*, opened for signature 23 November, 2001, CETS No. 185, art 19 (entered into force 1 July 2004).
[1208] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 20 (entered into force 1 July 2004).
[1209]Council of Europe, *Convention on Cybercrime: Explanatory Report* < http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> at 22 August 2008.
[1210] Rowland, above n 1176.
[1211] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 24 (entered into force 1 July 2004).
[1212] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 26 (entered into force 1 July 2004).
[1213] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 27 (entered into force 1 July 2004).
[1214] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 29 (entered into force 1 July 2004).

preserved traffic data,[1215] search and seizure across-borders,[1216] and real-time collection of traffic data.[1217] These create a new regime of mutual legal assistance with respect to mechanisms particularly necessary for rapid effective co-operation in computer related criminal matters.

In relation to search and seizure across-borders, the Convention empowers member states to issue an expedited request for the preservation of data and disclosure of preserved data. According to the Explanatory Report, preservation of data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate.[1218] The Convention divides the expeditious preservation request into two stages. The first stage requires the requested party to keep the specified information safe from modification, deterioration or deletion.[1219] The data can be preserved for as long a period of time as necessary, up to a maximum of 90 days unless an extension is granted.[1220] The preservation request does not, however, prevent the owner from accessing or using the preserved data, unless the requesting country requests clearly otherwise.[1221] Second, the preserved data is not disclosed to the foreign law enforcement authorities during the preservation period, unless the requesting party expressly requests its disclosure.[1222] The request for preservation should be made by expedited methods, such as fax or e-mail and processed by a designated central authority.[1223] The central authority of the state receiving the request must respond immediately to avoid data contamination or destruction.[1224]

The Convention authorises participating countries to take unilateral action in specific situations.[1225] If the computer system to be searched is located in a foreign jurisdiction and is a publicly accessible open data space, the participating nation may without the

[1215] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 30 (entered into force 1 July 2004).

[1216] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 32 (entered into force 1 July 2004).

[1217] *Convention on Cybercrime,* opened for signature 23 November, 2001, CETS No. 185, art 33 (entered into force 1 July 2004).

[1218] Council of Europe, *Convention on Cybercrime: Explanatory Report*, above n 1209.

[1219] Ibid.

[1220] Ibid.

[1221] Ibid.

[1222] Ibid.

[1223] *Convention on Cybercrime*, opened for signature 23 November, 2001, CETS No. 185, art 25 (3) (entered into force 1 July 2004).

[1224] Council of Europe, *Convention on Cybercrime: Explanatory Report*, above n 1209.

[1225] *Convention on Cybercrime*, opened for signature 23 November, 2001, CETS No. 185, art 32 (a) (b) (entered into force 1 July 2004).

permission of the other member state access the stored computer data and obtain evidence.[1226] In a similar manner, if the computer system to be searched is password protected or restricted in some other way, the participating nation may also conduct a cross-border search without the authorisation of the other concerned member state if a lawful and voluntary consent is obtained from the person who has the lawful authority to give consent.[1227]

However, the Convention is subject to criticism for its classical and decentralised approach. The Convention did not establish a new mechanism for tackling cybercrime. Instead, it delegated the responsibility for tackling cybercrimes to member states individually.[1228] For example, each state is responsible for defining cybercrime and for investigating, prosecuting and punishing cybercriminals. This approach, according to Brenner, 'attests a traditional approach, nationally based law enforcement to nonterritorially based crime'.[1229] She suggested two alternative approaches. The first is to establish a global enforcement agency or 'global cybercrime police'[1230] which would be responsible for investigating cybercrime, and prosecuting and sanctioning cybercriminals. This is a centralised approach, in which the role of the concerned counties is limited and the agency's role is broad.[1231] However, the approach is unlikely to be successful because countries are not likely to be willing to give up their enforcement powers.[1232] The second approach is a mixed model which incorporates both centralised and decentralised elements.[1233] The prosecution and sanctioning of cybercriminals would remain the responsibility of discrete states, but the processes of investigating cybercrime and apprehending cybercriminals would be delegated to the global agency.[1234] The agency would have a wider role than Interpol, which only coordinates investigations among law enforcement officers from various countries.[1235]

[1226] Council of Europe, *Convention on Cybercrime: Explanatory Report*, above n 1209.
[1227] Ibid.
[1228] Brenner, above n 1183, 218.
[1229] Ibid.
[1230] The recent Cybercrime Conference which was held in India has called for establishing a global monitoring agency. See, Matt Chapman, *Conference Calls for Global Cyber-Crime Police* (2007) Vunuet < http://www.vnunet.com/vnunet/news/2198757/conference-calls-world>at 17 September 2008.
[1231] Ibid.
[1232] Ibid.
[1233] Brenner, above n 1183.
[1234] Ibid.
[1235] Ibid.

Also the Convention has attracted a good deal of criticism because of the complexity of its provisions and its lack of mechanisms to ensure compliance with its provisions.[1236] Accordingly, many developing countries, including Jordan, will be hesitant to implement the Convention. Therefore, in 2009 the United Nation's International Telecommunications Union commissioned a multidisciplinary international group of experts to draft model legislation to assist developing countries to draft cybercrime laws to implement the Convention. The model legislation uses language drafted in a manner that can be customised to suit the cybercrime laws of a particular country but that should eliminate confusion as to the meaning or the varying interpretations of the Convention.

Howeverd, the Convention will have little influence on crimes committed from non-member countries.[1237] Jack L Goldsmith, Professor of Law, University of Chicago Law School, suggests that state parties should impose significant sanctions on nations that fail to ratify, implement, or enforce it.[1238] Finally, the Convention did not specify how data should be preserved and then seized. It is left to each state to determine the appropriate manner of preservation.[1239]

Although the Convention established a common criminal policy among countries, i.e. its three-pronged approach, it stopped short of establishing a global agency that would investigate and prosecute cybercriminals. Consequently, developing countries, such as Jordan, will be hesitant to comply with the Convention because of the lack the necessary resources. Brenner's suggestion to establish an international investigative unit could encourage developing states to accede because it could provide the necessary resources to enable them to comply. These countries will be able to respond to the requirements of development in cybercrime so long as the developed countries keep providing them with the logistical support and funding which are necessary for tackling cybercrime.

[1236] Goldsmith, above n 1144, 107.
[1237] Ibid.
[1238] Ibid.
[1239] Council of Europe, *Convention on Cybercrime: Explanatory Report*, above n 1209.

9.2.2 Letters Rogatory

Letters rogatory are requests for assistance from the courts of one country to the courts of another country.[1240] This approach is only appropriate when the assistance requested is beyond the scope of MLAT,[1241] i.e. the country requesting the assistance is not a signatory to a multilateral or bilateral MLAT with the requested country.[1242] Thus, they are a default mechanism based upon the principle of international comity.[1243]

Letters rogatory are processed slowly because of the huge bureaucracy that it takes to issue and process them.[1244] For example, the USA Department of State (DOS) outlines the steps in the letters rogatory process as follows:[1245]

1) draft request,
2) obtain seal and signature of USA court,
3) forward request to DOS or USA embassy,
4) USA embassy prepares diplomatic note and forwards to ministry of foreign affairs,
5) ministry of foreign affairs forwards to ministry of justice,
6) ministry of justice forwards to foreign court of competent jurisdiction,
7) foreign court executes request subject to court's calendar,
8) evidence sought returned by court to ministry of foreign affairs,
9) ministry of foreign affairs returns evidence to US embassy,
10) US embassy returns evidence to DOS,
11) DOS returns evidence to US court that issued request, and
12) US court returns evidence to requesting party.

[1240] Christine A Laciak (ed), *International Antitrust Co-operation Handbook* (2004) 15.

[1241] See, eg, Bantekas, and Nash, above 1136, 46.

[1242] See, Westby, above n 1170, 46.

[1243] The principle of international comity has been defined as 'the recognition one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience'. See, Sarah Joseph, *Corporation and Transnational Human Rights Litigation* (2004) 46.

[1244] See, eg, Edward F Greene et al, *U.S Regulation of the International Securities and Derivatives Markets* (8th ed, 2005) 15-10. See also, Richards, above n 1143, 216.

[1245] See, Laciak, above n 1240, 16.

It is a time consuming process[1246] and generally takes between six months and one year to achieve.[1247] This slowness in multiple handling may be attributed to three reasons:

1) The absence of particular forms for letters rogatory;[1248]

2) The absence of an equivalent central authority among countries for overseeing and coordinating the process;[1249] and

3) The processing of letters rogatory through diplomatic channels.[1250]

Thus, scholars prefer the use of MLAT over letters rogatory regime. According to Cherif Bassiouni and David Gualtieri, MLATs have six advantages over letters rogatory.[1251] Four of these advantages contribute to the inefficiency of the letters rogatory approach in cross-border cybercrime investigation.

1) MLATs represent obligations between states, while letters rogatory function merely as a matter of comity.[1252]

2) MLATs are more efficient because requests travel through 'central authorities'; letters rogatory must pass through courts, foreign and justice ministries and embassies.[1253]

3) MLATs avoid the costs of employing foreign attorneys to pursue the assistance sought by a letter rogatory.[1254]

4) MLATs are substantially more effective in overcoming bank secrecy laws that have impeded efforts to thwart organised crime and money laundering.[1255]

[1246] M M Richard, above n 1152, 233. See also, Jonathan Drimmer, *Cross-Border Corporate Investigations and Prosecutions Involving the Department of Justice* (2008) Lexisnexis < http://law.lexisnexis.com/practiceareas/Insights - Analysis/International/Jonathan-Drimmer-on-Cross-Border-Corporate-Investigations-and-Prosecutions-Involving-the-Department-of-Justice> at 24 September 2008. See also, Greene, above n 1244.

[1247] U.S. Department of State: Bureau of Consular Affairs, *Preparation of Letters Rogatory* (2008) http://www.travel.state.gov/law/info/judicial/judicial_683.html> at 18 September 2008. See also, Dan K Webb, Robert W Tarun, and Steven F Molo, *Corporate Internal Investigation* (1993) 13-41.

[1248] Ibid.

[1249] M M Richard, above n 1152.

[1250] See, eg, Micheal Geist and Milana Homsi, *Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World* (2004) <www.michaelgeist.ca/resc/FINAL_UNB.doc> at 6 September 2008. See also, Greene, above n 1241. See also, U.S. Department of State, above n 1247.

[1251] M Cherif Bassiouni and David S Gualtieri, 'International and National Responses to the Globalization of Money Laundering' in Ernesto Ugo Savona (ed), *Responding to Money Laundering: International Perspectives* (2000) 107, 113. See also, Webb, Tarun and Molo, above n 1247, 13-42.

[1252] Bassiouni and Gualtieri, ibid.

[1253] Ibid.

[1254] Ibid.

Therefore, law enforcement officers are discouraged from using letters rogatory to obtain evidence.[1256] However, scholars consider it more likely that letters rogatory will be processed through non-traditional means, such as by e-mail.[1257] If e-mail were adopted as a primary method of letters rogatory transmission, it would be a major change that benefits cross-border cybercrime investigations. The use of non-traditional media to prepare, process, receive and transmit letters rogatory would definitely accelerate processing of letters rogatory.

9.2.3 Domestic Legislation and Responses to MLA & Letters Rogatory

Several countries have domestic laws that deal with mutual assistance in criminal matters. The objectives of these laws are to ensure that mutual assistance in criminal matters is provided in response to requests even in the absence of a formal agreement.[1258] Australia and the USA have both enacted domestic legal instruments to ensure that mutual assistance is regulated by the law. Meanwhile, Jordan has not yet enacted any law governing mutual legal assistance.

a) Jordan

Unfortunately, Jordan's participation in international co-operation to combat cybercrime is not at all apparent. The Jordanian government is neither a signatory to bilateral treaties on mutual legal assistance with Australia and the USA, nor to any multilateral treaties in criminal matters.[1259] This deficiency may be attributed to the two following factors. First, the lack of technical knowledge, training and funding causes difficulties in keeping up with the forensic investigations required to provide the assistance sought. Second, Jordan's current procedural provisions with respect to cybercrime are not strong enough to effectively handle digital evidence and are inadequate to deal with

[1255] Ibid.
[1256] See, eg, Peter Andreas and Ethan Nadelmann, *Policing the Globe: Criminalization and Crime Control in International Relations* (2006) 143.
[1257] Broadhurst and Grabosky, above n 107, 12.
[1258] See, Bullwinkel, above n 1176, 274.
[1259] See generally, التشريعات الاردنية [Trans of: *Jordanian Legislation*] National Information System < <http://www.lob.gov.jo/ui/contracts/listall.jsp> at 17 August 2008. See also, U.S. Department of State: Bureau of Consular Affairs, above n 1247.

situations involving cross-border searches. For example, there are no specific provisions for compelling ISPs who hold the information to cooperate with investigators.

The use of letters rogatory for search and seizure of property is unknown in Jordan.[1260] According to the USA Department of State, Jordanian officers are unfamiliar with the procedures of letters rogatory and reluctant to execute letters rogatory requests.[1261]

b) Australia

In addition to the MLAT between Australia and the USA,[1262] the federal legislature has enacted the *Mutual Assistance in Criminal Matters Act 1987* (MACMA) to regulate mutual legal assistance. The MACMA regulates, among other things, the taking of evidence in a foreign country,[1263] evidence collection from Australia,[1264] the production of any document or other article including articles in digital format for the purposes of a proceeding in a foreign country; [1265] and the issue of a search warrant and the seizure of anything relevant to a proceeding or investigation in a foreign country.[1266]

Part 3, entitled 'Assistance in Relation to Search and Seizure' comprises two sections. The first deals with the evidence requested by the Australian authorities and its admissibility in the national legal standard and second deals with a request by foreign countries for search and seizure of evidence located in Australia. Furthermore, Section 38N authorises the executing officers to operate electronic equipment at the premises to seize evidence.

According to the Act, the Attorney General, the Minister of Home Affairs, or a delegate can offer to and request from foreign nations a broad range of assistance.[1267] This makes the MACMA very important to countries which do not have a bilateral MLAT with Australia, such as Jordan, because Section 13 of the MACMA allows the Attorney

[1260] See generally, *Jordanian Legislation*, above n 1259.

[1261] US Department of State: Bureau of Consular Affairs, above n 1247.

[1262] *Australian Bilateral Mutual Legal Assistance Agreements*, Australian Government: Attorney-General's Department < http://www.ag.gov.au/www/agd/agd.nsf/Page/Extraditionandmutualassistance_Relationshipwithothercountries_Australianbilateralmutualassistanceagreements> at 26 September 2008.

[1263] *Mutual Assistance in Criminal Matters Act 1987*(Cth) s12 (a).

[1264] *Mutual Assistance in Criminal Matters Act 1987*(Cth) s13 (a) (b).

[1265] *Mutual Assistance in Criminal Matters Act 1987*(Cth) s12 (b).

[1266] *Mutual Assistance in Criminal Matters Act 1987*(Cth) s14 (2).

[1267] Attorney General Department, *Mutual Assistance* (2006) Australian Government < http://www.ag.gov.au/www/agd/agd.nsf/Page/Extradition_and_mutual_assistanceMutual_assistance> at 28 September 2008.

General of Australia, upon a request from Jordan, to search for and seize evidence located in Australia and transmit the collected evidence to the requesting country.

c) USA

Section 28 U.S.C § 1782[1268] is an important legal instrument to obtain evidence located in the USA. It has builds on what is called a *Subpoena Duces Tecum.*[1269] It authorises the US courts at the request, and on behalf, of a foreign jurisdiction to compel a defendant to produce evidence.[1270] It is commonly used by foreign jurisdictions to obtain evidence located in the USA.[1271] Although the use of the *Subpoena Duces Tecum* suffices to obtain most documents and other tangible evidence, MLAT is necessary for issuing a warrant authorising USA officers to conduct a search and seizure in response to a foreign request.[1272]

US law enforcement agencies significantly rely on both bilateral and multilateral mutual assistance agreements to obtain evidence located in another jurisdiction.[1273] The USA has bilateral MLATs with more than 80 countries around the world.[1274] The objectives of these treaties are mainly twofold. First, the USA wants the signatory country to provide the requested evidence.[1275] Second, the requested evidence should be provided in a form that will be admissible in USA courts.[1276] A MLAT is self-executing and the scope of evidence available pursuant to a MLAT is not substantively limited by the terms of 28 U.S.C. §1782. The US courts ruled that where a MLAT exists, the elements of §1782 do not have to be met in order to provide assistance to a foreign jurisdiction

[1268] Section 28 U.S.C §1782 provides that a federal district court 'may order' a person 'resid[ing]' or 'found' in the district to give testimony or produce documents 'for use in a proceeding in a foreign or international tribunal ... upon the application of any interested person'.

[1269] See, Michael Abbell, 'Obtaining Evidence in the U.S. in Criminal Cases Through Use of Compulsory Process' in Richard D Atkins (ed), *The Alleged Transnational Criminal* (1995) 293, 298.

[1270] Ibid.

[1271] Ibid.

[1272] Ibid.

[1273] See, eg, Ethan A Nadelmann, *Cops Across Borders: The Internationalization of U.S Criminal Law Enforcement* (1993) 315.

[1274] See, US State Department, above n 1171. On August 2006, the US ratified the Convention and it came into force on January 2007. Sean McCormack, *United States Joins Council of Europe Convention on Cybercrime* (2006) U.S. Department of Justice < http://www.state.gov/r/pa/prs/ps/2006/73353.htm>at 28 August 2008

[1275] Ibid.

[1276] Ibid.

invoking the MLAT.[1277] This point of view grants enforcement officers more scope to deal with mutual assistance requests.

d) Comparative Legal Analysis

There is a consensus among scholars that the default letters rogatory regime is inappropriate for cross-border investigation. This inappropriateness will be obvious in cybercrime investigations because it is ill-suited to the requirement of swift action. The letters rogatory regime operates slowly and is clogged with bureaucratic and diplomatic procedures. Although the use of e-mail and other forms of electronic communications may accelerate the transmission of letters rogatory, bureaucratic and diplomatic procedures are likely to continue to hinder their speed and effectiveness. Therefore, MLA is more appropriate for cross-border investigations.

The capability differences between Australia and the USA, on the one hand, and Jordan, on the other hand, are quite striking. Jordan lacks practical experience, knowledge and the legal tools to cooperate with foreign nations. Australia and the USA are actively involved in international co-operation on criminal matters in the fight against transnational crimes, including cybercrimes. The Australian MACMA and the USA Section 28 U.S.C § 1782, as well as MLAT between the two countries, are legal instruments used to obtain evidence located in a foreign state. Although these instruments provide officers with tools necessary to deal with cross-border investigation, none of them is sufficiently well adapted to the needs of particular digital evidence because they have been designed to address the search for physical objects and, therefore, are not effective in addressing cybercrime searches unless appropriate amendments are made to these instruments.

9.3 Conclusion

The absence of physical borders in cyberspace makes the investigation of cybercrime even more complicated, as procedures for obtaining evidence from abroad can be cumbersome and somewhat daunting for developing countries such as Jordan. On the

[1277] *In re Commissioner's Subpoenas*, 325 F.3d 1287, 1291 (11th Cir, 2003). See also, *United Kingdom v. United States*, 238 F.3d 1312 (11th Cir, 2001).

other hand, because of the absence of borders, investigating countries are able to hack into a foreign network, server or computer to obtain evidence. However, because of the doctrine of international comity and of the futility of unilateral action, as well as the availability of cooperative assistance to access foreign data, countries often avoid acting unilaterally. Instead, evidence situated in a foreign nation can be obtained only by means of MLA or letters rogatory.

The letters rogatory regime may be used to obtain digital evidence, however, it is not a practical tool for this purpose, because the nature and characteristics of cybercrime and digital evidence require a timely response and expedient handling. Therefore, MLA (whether in bilateral or multilateral form) is more appropriate for use in obtaining cross-border assistance. The classical forms of bilateral mutual legal assistance, which were originally established to address traditional crimes, are currently used to provide assistance in searching for and gathering digital evidence across-borders. This form is much less capable of handling cybercrime investigations because the latter require swift and decisive action and MLA is fraught with complications due to the bureaucratic system it goes through.

The Convention on Cybercrime established a MLA regime designed and optimised specifically to satisfy the particular needs of cross-border assistance in respect of cybercrime. Although the Convention accelerated international co-operation in cybercrime, it did not establish a global cybercrime police force to enforce the Convention's provisions and to investigate cross-border cybercrime. It is believed that such an agency would encourage developed countries to join the Convention and to fully implement its provisions.

10 GENERAL CONCLUSION

Introduction

The key concern of this thesis has been to review and reconceptualise substantive and procedural laws in Jordan in order to accommodate the search for and seizure of digital evidence. Cybercrime is a new phenomenon in Jordan. As far as the author knows, there are no formal published reports on cybercrime which explore the magnitude of the problem or strategies to deal with it. As is evident in proceeding chapters, there is no consolidated Jordanian cybercrime legislation in place although scattered provisions do address specific types of cybercrimes. The dearth of law is further deepened by the absence of any specific judicial precedential decisions on the issue. Therefore, the author has contrasted and critically analysed the legislation, investigation models, and judicial decisions in Australia and the USA, both of which have developed robust responses to cybercrimes. Then the results found in the Jordanian, Australian, and the US approaches on the one hand, and the particularity of cybercrime investigations on the other hand, have been analysed and synthesised together to shed light on the optimal approach to cybercrime investigation.

Chapters 3 and 4 analysed in detail the inadequacy of Jordanian substantive laws in criminalising common types of cybercrimes. Chapter 5 compared and analysed cybercrime investigation models and the challenges posed by privacy law and encryption technology. Chapter 6 demonstrated the nature of digital evidence extracted from cybercrime scenes and the legal approaches to this evidence. Then, chapters 7, 8 and 9 analysed in detail how traditional search and seizure procedures can be applied to digital evidence in cybercrime investigations.

The aim of this final chapter is to summarise the major findings of the thesis and to formulate specific recommendations for improvements in Jordanian national legislation concerning cybercrime, cybercrime investigations, collection of digital evidence and search and seizure procedures.

10.1 Criminalisation of Cybercrime

The population of Internet users is increasing rapidly. At the same time, the quantity and sophistication of cyber offences are also increasing. Therefore, Jordanian legislators must quickly craft laws that effectively respond to cyberspace offences.

In terms of criminalisation, cybercrimes comprise no more than two main types: first, new crimes invented for a technology-enabled environment like 'a new wine in a new bottle' and, second, traditional crimes committed with the use of computers, like 'an old wine in a new bottle'. In the absence of a comprehensive cybercrime law in Jordan, a handful of provisions either explicitly or implicitly criminalise some forms of cybercrimes. They can be found scattered across various laws, for example, the Jordanian *Criminal Law* 1960, *Telecommunications Law* 1995 and *Electronic Transactions Law* 2001. These provisions are either too narrow or are inappropriate to address all the forms of cybercrimes.

The *Criminal Law* 1961, which was formulated in the past century primarily to protect property and tangible objects against traditional criminals, fails to criminalise various forms of cybercrime, mainly because cybercrime is invisible, new, and the victims are almost intangible. On the other hand, the *Telecommunications Law* 1995, which was enacted before the arrival of the Internet revolution in Jordan, is inappropriate to address cybercrime, because it is so broad in scope. It treats both physical and logical attacks against electronic communications alike.

To close the loopholes in the above laws, Jordanian legislators passed the *Electronic Transactions Law* in 2001. Although most of its provisions focus on electronic transactions, Article 38 criminalises the use of computer systems to commit traditional crimes. This article, however, is too narrow because it criminalises one aspect of cybercrime. It does not apply to new crimes, such as computer hacking.

By contrast, Australia and the USA have been relatively successful in enacting legislation specifically focused on cybercrime. The Australian *Cybercrime Act* 2001 and the USA *Computer Fraud and Abuse Act* 1984 (CFAA) are the backbone of anti-hacking and cybercrime laws in these countries.

10.1.1 Cyberspace as the Target of the Crime

The most common types of cybercrime where cyberspace is the target of the crime are Transmission Control Protocol (TCP) related-crimes, cybertrespass, and cybersabotage.

In TCP related-crimes, legislators in the three countries studied avoided making any specific references to the Denial of Service Attack and the Distributed Denial of Service Attack attack, but rather aimed at setting out a broad framework addressing communications interruption and impairment. The Jordanian *Telecommunications Law* 1995, however, mainly addresses physical attack against electronic communications, because the communications installations and telecommunications traffic mentioned in the law are physical devices, such as modems, and computers. However, specific types of cybercrime, such as TCP attacks, can be prosecuted under the law because both logical and physical attacks cripple communications traffic. This is problematic because it treats alike all cybercriminals regardless of their motivations and objectives. A hacker who breaks down a website, for example, could be punished as severely as a person who attacks national infrastructure. On the other hand, the consequences of the illegal physical attack may exceed the virtual world attack as it causes injuries to people and property and the loss of human lives. Conversely, the *Cybercrime Act* 2001 and the CFAA prohibit unauthorised prevention of electronic communication traffic to or from a computer system and distinguish between minor and serious cybercrimes, imposing harsh penalties in the latter cases.

Concerning cyber-trespass, the criminal intention is either to access without permission, to exceed permission, to alter parts of or the entire computer system, or to commit further crimes. The *Telecommunications Law* 1995, the *Cybercrime Act* 2001 and the CFAA provide that a person is guilty of cybertrespass once he wilfully and knowingly accesses a computer system illegally. The *Telecommunications Law* 1995, however, does not apply if the legitimate user then exceeds her/his permission, or accesses beyond a pre-determined period of time.

Concerning cybersabotage, the application of the Jordanian *Criminal Law* 1960 to cyberspace poses a problem because it does not recognise the intangible nature of digital programmes and data. Thus, deleting or modifying data and programmes without damaging the physical medium, as a Trojan horse does, is not a crime. Also, the

Telecommunications Law 1995 provision (76) only criminalises actions specifically intended to inflict damage on the contents of a message being transmitted through a communications network, but sabotage which goes beyond destruction of a mere message, such as alteration of programmes or static data stored in a computer memory, does not fall under the above provision. However, the *Cybercrime Act* 2001 and the CFAA sufficiently and directly address all forms of cybersabotage.

10.1.2 Cyberspace as the Means of the Crime

Concerning cyber forgery, Jordanian laws and the CFAA fail to protect the forgery digital documents, such as software dependent records, because they do not recognise them as documents having legal efficacy or force. To criminalise cyber forgery, digital records should be granted legal efficacy or the use of computers to forge digital records or documents should be criminalised. Australian lawmakers provide a useful model of this in the *Crimes Act* 1914. Jordanian lawmakers should come up with adequate laws to close the loopholes that facilitate using computers to forge digital records.

Concerning cyberpornography, although the *Criminal Law* 1960 can be interpreted extensively to apply to all forms of cyber pornography, including virtual characters, to do so would contradict a core principle of criminal law, which is that criminal laws are to be construed narrowly. In addition, the expansive application ignores any distinction between adult and child pornography. Child pornography threatens the physical and psychological well-being of children. Therefore, the punishment must be proportionate to the crime. This is why the *Cybercrime Act* 2001 and the CFAA impose harsh punishments on cyber-child pornography criminals.

Concerning cyber identity theft, the *Criminal Law* 1960 specifically addresses only two forms of traditional identity theft: false identification and impersonating law officers. The definitions of these crimes do not extend to cyberspace identity theft offences, such as web spoofing, unless a physical appearance or I.D. card has been used for the deception. Meanwhile, the *Cybercrime Act* 2001 criminalises unauthorised access to computer systems with intent to commit or facilitate an offence, such as identity theft. The *Identity Theft and Assumption Deterrence Act* 1998 criminalises all forms of cyber identity theft and the use of personal information of other people to defraud online.

Concerning cyberstalking, the Jordanian *Criminal Law* 1960 only addresses physical harm and different forms of physical sexual harassment. The *Criminal Law* 1960 can be applied to cyberstalking only if the latter escalates into physical harm. It is therefore inadequate because cyberstalking does not always escalate into physical harm. The Australian *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill* 2004 criminalises cyberstalking by addressing the use of telecommunications services for menacing and harassing people. In the USA, the *Criminal and Crimes Procedure Act* criminalises the transmission of any communication in interstate or foreign commerce containing a threat to injure and harass people.

Recommendations

The author recommends the urgent establishment of a comprehensive Jordanian law that addresses cybercrime. Legislators should enact legislation defining the following actions as crimes:

- First, accessing the whole or any part of a computer system without authorisation by infringing security measures.
- Second, damaging, deleting or altering computer data without authorisation.
- Third, seriously hindering without authorisation the functioning of a computer system by inputting, transmitting, damaging, deleting, altering, or suppressing computer data.
- Fourth, inputting, altering and deleting data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic.
- Fifth, offering or making available child pornography through a computer system; distributing or transmitting child pornography through a computer system; producing child pornography for the purpose of distribution through a computer system.

- Sixth, transmitting any communication containing a threat to injure and harass people.

10.2 Cybercrime Investigation Approaches and Challenges

Promulgating a criminalising law is only part of the solution. The other half of the solution lies in streamlining and strengthening procedures concerning cybercrime investigation and eliminating impediments to it.

The continuous growth in cybercrimes is jeopardising the capability of police investigators to investigate almost any type of crime. Different types of cybercrimes are perceived as a trivial or low-value and not worthy of investigation, while others are high profile crimes. Parameters that specify which cybercrimes should be investigated and which ones should not, should consider the cost and time of investigation, level of effect, sophistication of the attack, nature of target, and significance of the target. Therefore, the 'Quality over Quantity' approach applied to traditional crimes in the mid-1970s to determine investigation priority, works to optimise cybercrime investigations too. This would enhance law enforcement investigation management, by freeing resources, such as staffing and equipment, to investigate high-profile cybercrimes only.

In Chapter 5, cybercrime investigation models developed by governmental and non-governmental organisations and among computing experts were selected and examined and compared with the Jordanian model. These models are intended to provide incontestable proof that digital evidence was not contaminated and that it remained intact during the computer forensic process. Optimality was not evident in any of these models as no benchmark was available to measure each model's robustness, nor does a single widely accepted model exist for conducting and managing cybercrime investigations. Forensic scholars, however, provide guidelines for crafting a model yielding admissible digital evidence that can be used in court proceedings. First, the model must include features that make it possible for investigators to protect the cybercrime scene from contamination, hypothesise how the attack took place, collect evidence, analyse the incident, reconstruct the crime scene, conduct a trace back investigation, perform detailed analysis, and prepare a report.

The model formulated and adopted by the Jordanian Computer Crime Unit (JCCU) lacks comprehensiveness and it omits necessary steps. Although it addresses the proper acquisition and preservation of computer evidence and its documentation, the examination process, analysis, and reporting are not mentioned anywhere in the model. Therefore, the JCCU's model should be remodelled to clarify more aspects of cybercrime investigation. Examination, analysis, and reporting processes should be incorporated into the model.

A comprehensive and robust model is part of the approach to an effective investigation. The other part is to eliminate or reduce obstacles and barriers that can be present when investigating cybercrimes. Privacy restrictions and encryption are two common obstacles that can prevent investigators from efficiently investigating cybercrimes.

In Jordan, privacy objections do not raise a legal concern for investigators, because there are no laws or regulations that address the rules of cyberspace surveillance and data collection. Although the Constitution specifically recognises a limited right to privacy protection in relation to telephonic communications, this protection does not extend to cyberspace because the latter is different from telegraphic and telephonic communications. Encryption, on the other hand, is a concern as there is no effective legal mechanism to compel a holder or third party to divulge the decryption keys. In Jordan and the USA, police investigators have no power to compel offenders or a third party to divulge encryption keys. Meanwhile, Australian police officers have been given the power to do so.

Recommendations

The author recommends the urgent establishment of criteria and guidelines that quantify and assess which cybercrimes should be investigated as priorities and whether they are investigable. The guidelines should consider the following criteria: investigation cost and time, level of effect, or what level of harm has been caused, and sophistication of the attack, nature of the target, and the target's significance.

The JCCU's model of cybercrime investigation should be remodelled to clarify more aspects of cybercrime investigation, including the examination process, analysis and reporting.

Law enforcement officers should be provided with a new legal mechanism to deal with encrypted systems to prevent suspects and third parties from hiding or refusing to reveal encryption keys.

10.3 Digital Evidence Admissibility

Enacting robust cybercrime laws and crafting effective investigation approaches are fruitless efforts unless the collected digital evidence is admissible in the criminal trial. Indeed, admissible, reliable digital evidence is essential to the success of cybercrime investigation and prosecution.

Digital evidence typically exists in different data types and resides in different locations, networks, or repositories. This makes the evidence very volatile and needy of more care and diligence in its handling to achieve the highest possible standard of integrity and admissibility. Thus, investigators must always ensure that the original version of the evidence is kept intact and must make a mirror-image copy of it. There are two digital instruments available to authenticate the mirror-image copy: Metadata and Hash value. They play a critical role in authenticating digital evidence; however, their role should be subject to regular judicial review to decide whether they adequately sustain data integrity.

Jordanian laws addressing digital evidence lack comprehensiveness and breadth of scope. The *Electronic Transaction Law* 2001 and *Evidence Law* 1952 demonstrate incomplete understanding of digital evidence. The *Electronic Transactions Law* 2001 only admits electronic contracts and messages that are generated, sent, received or stored electronically and the *Evidence Law* only admits e-mail and computer stored evidence. As a result, many types of computer generated evidence, such as log files, metadata, and hash value are beyond the ambit of Jordanian laws because they are neither electronic contracts nor messages. On the other hand, although the *Credit Information Law* 2003 and *Banking Law* 2000 admitted the two broad types of digital evidence (i.e. computer generated and computer stored evidence), their scope and application are narrow because they are applicable only to a limited range of cases, namely for credit information and banking disputes. Finally, although, the *Criminal Procedure Law* 1961 provides judges with discretionary power to admit any relevant evidence which they deem to have probative value, the judges lack the necessary knowledge and training in the field of cyber law and, consequently, they will be hesitant to accept digital evidence. By contrast, the Australian and the US legislatures amended the rules of evidence to include both computer generated and computer stored evidence.

Recommendations

The author recommends the urgent revision of current Jordanian legislation to recognise the two broad types of digital evidence and to enable the exact duplicate copy to be admitted into evidence in lieu of the original copy. In addition, courts should be fitted with appropriate visual or computerised equipment necessary for displaying or illustrating digital evidence.

10.4 Searching and Seizing Digital Evidence with a Warrant

Law enforcement officers, judges, lawyers, and prosecutors in Jordan are not fully aware of the extent to which digital information impacts on search and seizure concepts. The unique nature of digital evidence in cybercrime investigations requires the formulation and use of a specifically designed cyber search warrant. The following issues are indispensable to the newly formulated warrant. First, the search authorisation can be obtained instantly without the need for a signature. Second, the search must be conducted by highly experienced forensic officers. Third, a warrant must protect individual privacy by restricting the boundaries of the search but this specificity does not preclude a certain level of generality, in case a precise description of the subject of the search is not attainable.

The terms of the cybercrime search warrant should include restrictions on the scope and location of the search and should be premised on the existence of reasonable cause to justify the search. Restrictions force investigators to search and seize only the items listed in the search warrant and to ensure that the items identified in the warrant are properly related to the crime committed.

1) *Threshold for Issuing a Cyber Search Warrant*

Search warrant regimes should create a balance between privacy protection and crime detection requirements. Legislators have set out several conditions to be fulfilled before a court or General Prosecutor issues a search warrant. These conditions are the reasonable cause threshold for search warrant issuance, the subject matter of the search and its scope.

a) Probable cause

A problem encountered by investigators in drafting cyber search warrants is the difficulty of establishing probable cause. The statement of probable cause must contain factual evidence linking both the criminal activity with the item to be seized, and the item to be seized with the place to be searched. In some scenarios, Internet Service Providers can play a significant role in identifying the link between the items described in the warrant and the physical place to be searched by providing investigators with the Internet Protocol address identifying the suspected physical location.

The probable cause threshold set by Jordanian law is low. A warrant can be obtained if any one of the three following circumstances has occurred: a visual observation of a crime, or information provided by other citizens about the crime, or an occupant of the property's request for a search. Accordingly, it authorises investigators to obtain a search warrant without the need for a reasonable ground or factual information linking the evidence to be searched with the physical location. Similarly, to issue a search warrant, the Australian *Crimes Act* 1914 and US courts request a reasonable ground to believe that the search will uncover evidence of a crime. This threshold is applicable to a cyber search warrant without any problems. For example, an undercover investigator posing as a minor will be able to obtain a cyber search warrant because of his visual observation of the crime.

With a cybercrime warrant, however, the problem arises when the courts require factual information which forms a link between the evidence to be searched with the physical location because, in some cases, the Internet Protocol addressing system offers the user anonymity, which makes locating the suspect's physical location impossible.

Recommendations

The author does not believe that probable cause requires establishing factual information which links the items to be seized and the place to be searched, particularly when officers are able to obtain evidence remotely without the need for physical access to the suspect's property.

b) Subject of the Search Warrant

In cybercrime, the data itself is contraband, evidence or the instrument of a crime, thus the subject of the search will be for intangible items, such as data, images, files, and so on.

The current Jordanian *Criminal Procedure Law* 1961 permits officers to seize visible and tangible objects and specifies that the subject of the search warrant is either a physical place or an individual. The lack of recognition of intangible data as an object under the law of search and seizure is problematic. By contrast, Australian legislation precisely describes the subject of the search as both tangible items and 'data'. It provides law enforcement officers with the resources which they need to search for and seize intangible evidence. In addition, the US Supreme Court has expanded the definition of property to include data that may be seized under search warrant rules.

Recommendations

Jordanian law should be amended to explicitly permit the search and seizure of intangible materials. This can be achieved by inserting the word 'data' in provision 1/86 after the word 'things'.

c) Scope of the Search Warrant

Particularity or specificity is required in a search warrant, which means that the search warrant should be issued for a particular crime, to search a particular place, and to seize particular items. The common practice in cybercrime investigation scenes is that the investigators create a mirror copy of the hard disk.

Two approaches have emerged to define the scope of a digital search, i.e. restrictive and non-restrictive approaches. The first approach constrains investigators from searching the entire mirror copy and opening a variety of files, while the non-restrictive approach allows investigators to conduct an unlimited search if there is plenty of time and uncertainty about what evidence being sought and to seize evidential materials. Although the restrictive approach protects privacy, it poses considerable difficulties for investigators to sufficiently search and seize evidence because the ability of the investigators to separate between incriminating and non-suspect data is difficult.

In Jordan, none of the above approaches have so far been adopted. The broad language of the Jordanian *Criminal Procedure Law* 1961, however, might allow officers to create a mirror copy search and conduct unlimited search.

In Australia, the non-restrictive approach is adopted. The *Crimes Act* 1914 authorises investigators to rummage through data first and then make a mirror copy and seize only evidential material. In contrast, some courts in the USA have ruled that investigators must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. The Ninth Circuit Court, however, has set a new precedent to permit the non-restrictive approach in certain circumstances.

Recommendations

The Jordanian *Criminal Procedure Law* 1961 should expressly entitle investigators to create a mirror copy and to rummage through data to determine the items that should be seized. Simultaneously, the law must restrain investigators from rummaging through non-suspect data unless a more precise description is impossible, or the circumstances make it difficult to describe the items to be seized or the size of data is very large.

2) *Execution of the Cyber Search Warrants*

The execution of a cyber search warrant differs considerably from a traditional search. It involves two stages, i.e. pre-digital and digital searching. The first one mimics the first stage of the traditional search procedure, i.e. knock and announcement. The second stage involves unique procedures conducted by forensic officers off-site. Although the two stages of search are apparently separate, each impinges on the other. Procedures executed in the pre-digital phase may indirectly affect the later digital search in a negative way. For example, in some scenarios, the notifying procedure of the search warrant execution gives the suspect opportunities to destroy, contaminate or hide incriminating evidence.

In Jordan, although the *Criminal Procedure Law* 1961 authorises investigators to conduct a search without notifying the suspect in advance, it requires the defendant's presence during search execution or a representative, such as a lawyer, or two witnesses, or a local notary.

In a similar manner, the Australian *Crimes Act* 1914 obliges investigators to announce their presence and authority. It also requires investigators to hand the occupier of the premises a copy of the warrant.

In contrast, the USA *PATRIOT Act* authorises the executing officers to perform what is called a 'sneak and peek' search. This warrant authorises investigators to search, observe, copy, download or transmit computer files without notifying the occupier of the premises.

Recommendations

The knock and announcement prior to entry requirement must be narrowly applied in relation to a cyber search warrant in order to prevent the suspect from having any opportunity to destroy, contaminate or hide incriminating evidence. Indeed, the law must authorise the investigators to execute a 'sneak and peek' warrant in a cybercrime investigation when there is a factual basis for believing that announcement would result in the destruction of the evidence.

3) Who Should Accompany the Officers Executing the Search

Cybercrime searches have a unique nature which requires a specialised group of investigators technicians, evidence custodians, forensic examiners and forensic analysts.

In Jordan, the *Criminal Procedure Law* 1961 requires the attendance of two groups of people, namely, police officers executing the warrant and witnesses, i.e. two local witnesses or a local notary. The latter's attendance is, of course, impractical and even not feasible in cyber searches due to the off-site investigation and use of remote searches.

In a different manner, the Australian *Crimes Act* 1914 authorises investigators to terminate the occupier's presence if s/he impedes the search. In the USA, the presence of the occupier of the premises during the search is not a requirement.

Recommendations

The *Criminal Procedure Law* 1961 must be amended to allow enforcement officers to conduct a search in cases of cybercrimes without the attendance of two local witnesses or a local notary.

4) Search Location

Moving computer hardware off-site for criminal investigation purposes can jeopardise businesses and the individuals who depend on them. Similarly, conducting a search on-site for a long duration of time also negatively affects business and individuals' working lives.

There are basically two viewpoints about whether computer searches should be conducted on-site or off-site. The majority of scholars support the off-site search. The Jordanian *Criminal Procedure Law* 1961 provides officers with absolute discretionary power to determine the appropriate measures for executing a search warrant. There is a somewhat different approach in Australia and the US. The decision to investigate on-site or off-site is discretionary but depends on the circumstances of a case. For example, the off-site search is permissible if the search would take days or weeks to find the specific information.

Recommendations

The Jordanian investigators' discretionary powers should not be left without guidance concerning the search location. Investigators should be given the needed power to move computers off-site only when it is not reasonable and practicable to conduct the digital search on-site.

10.5 Search and Seizure without a Warrant

Although the *Jordanian Constitution* enshrines the privacy of dwellings, it allows a limited exception in which law enforcement officers may enter private properties without a search warrant in specific circumstances prescribed by the law to protect life and property, preserve evidence, or to search for evidence and to make an arrest. Thus, the Jordanian *Criminal Procedure Law 1961* addresses search warrant exceptions. Unfortunately, though, developments in information technology and the emergence of new criminal offences with new modi operandi have made the Act less responsive to the demand of digital searches.

In comparison, the Australian *Crimes Act* 1914 and US courts have developed a number of exceptions to the warrant requirements. Important legal precedents have been set in recent years which play a substantial role in applying search exceptions to digital evidence.

1) Exigent circumstances

Legal systems acknowledge that urgent circumstances require swift action to prevent imminent destruction of evidence. The core problem of the exigent circumstance exception in cybercrime is the scope of the search and whether the doctrine allows officers to conduct a thorough digital search or just the seizure of the physical components. Jordan, Australia and the USA each approach the exigent circumstances exception differently.

The Jordanian *Criminal Procedure Law* 1961 provides law enforcement officers with the necessary power to enter and perform a search without a warrant under three limited circumstances: (1) a crime is about to be committed; (2) a crime is being committed; and (3) a crime has just been committed. It does not allow search in order to prevent imminent destruction of evidence. Therefore, a Jordanian scholar has argued that the three circumstances are illustrative only and not intended to be exclusive and, therefore, investigators are authorised to act to prevent imminent destruction of evidence. He added that the exigent circumstances doctrine must not allow investigators to perform a search, but only to seize evidence. In the digital context, Jordanian courts have not yet examined this doctrine.

In Australia, the *Crimes Act* 1914 justifies searches without a warrant to prevent the evidence from being concealed, lost or destroyed. Similarly, US courts have ruled that the fragile nature of digital evidence authorises the search under the exigent circumstances doctrine.

Recommendations

Jordanian law should be amended to provide investigators with the right type of power to seize and search electronic storage devices and evidence in exigent circumstances in which there is an immediate danger of losing data, or to prevent the imminent destruction of electronic devices and hardware components.

2) Consent

Consent to search is a very important exception that is made to allow a swift search or extend a search without the need for formal prior authorisation through the issue of an official search warrant.

Jordanian law does not recognise the concept of defendant's consent to search his home. Instead, it permits a warrantless search upon a request from the owner or the occupier of the premises. This is very different to the situation in Australia and the USA, where consent to search is a well recognised exception to the usual search warrant requirements.

Recommendations

Jordanian law should provide officers with a similar power to seize and search electronic storage devices and evidence upon consent given by the owner or occupier of premises.

Although, no fundamental problem exists in applying consent to digital searches, defining the scope of the consent and who may give it constitute the unresolved concerns pertaining to digital searches.

a) Scope of Consent

In regard to the scope of consent, the question arises as to whether the police officers can go beyond the limits of search set by the consenting person. For example, can answers to these questions be implemented?

1) Can consent to search a physical place extend to searching digital devices located on the property?

2) Can consent to examination of a compact disk extend to search of a PC's hard drive, or

3) Can consent to examine JEPG files extend to MP3 files?

In Jordan and Australia, in the absence of legislative provisions and judicial precedent on this matter, law enforcement officers are not restrained from rummaging through electronic devices and extending the search beyond the specified area of the property. In the USA, courts have delivered contradictory decisions on this issue. Some courts have approved searches that exceeded the scope of consent, while others have rejected the extension of a physical search to a search for digital evidence.

Recommendations

To avoid the potential invalidation of the search, the author supports suggestions that law enforcement officers must present a written consent form delineating the scope of the consent in order to clarify in advance the boundaries of the consent search. For example, the form will show precisely the search limits, and how the officers will carry out the search and whether he is going to extend the search.

b) *Third Party Consent*

Third party consent is very important because computers, networks and the Internet are often shared between multiple users, such as family members, roommates and work colleagues. It takes two forms: local and remote consents. These forms of consent enable individuals associated with, but other than the suspect person against whom evidence is sought, to validly consent to a search of the suspect person's computer.

In Jordan, third party consent is not recognised by the law. Instead, law enforcement officers are authorised to search any private premises without a search warrant if they are companied by a local notary or two local witnesses to observe the search process.

In Australia and the USA, third party consent is valid as long as the consenting party has equal rights of possession and control of the property or has apparent authority over the computer to be searched. For example, because spouses live together and may share a computer, then one or the other may consent to a search.

Recommendations

Jordanian law should be amended to permit all forms of third party consent and not require third party attendance (i.e. by two local witnesses or a local notary) because their attendance in cybercrime is impracticable and disruptive to the search process. However, the consenting third party must have joint access or control over the defendant's computer.

c) *Workplace searches*

Workplace computers and networks are important in cybercrime investigation because of the high percentage of cybercrimes that occur in workplaces. Thus, law enforcement officers can take advantage of workplace access to conduct searches and, more importantly, to obtain consent to conduct warrantless searches.

The Jordanian *Criminal Procedure Law* 1961 and Australian *Crimes Act* 1914, respectively, do not address workplace searches. While the problem is more complicated in Jordan because third party consent is not recognised by the law, in Australia, an employer's consent would be governed by rules relating to third party consent principles.

In the USA, the workplace's policies, regulations, instructions and practices may reduce an employee's expectation of privacy and, therefore, employers can consent to investigators to search. The Courts have ruled that employers exercise common authority over employees' offices and workplace computers and that the common authority validates consent to search workplace computers.

Recommendations

Jordanian law should be amended to permit law enforcement officers to obtain consent from employers who have common authority over the employees' computers to conduct workplace searches.

3) Plain View

The plain view doctrine allows investigators to observe or to seize but not to search evidence of a crime, even though the crime is not the one that the investigator was authorised to investigate or to seize evidence for. Usually, it occurs during the execution of a search warrant or arrest, when contraband not described in the search warrant is observed and seized.

The unique aspects of digital evidence and its forensic tools, which capture every bit of digital information stored on a hard drive, including latent data and closed files, make it difficult to apply the plain view doctrine. Those data are not apparent immediately and officers must open, download, or run specific applications to observe an object's contents. Therefore, some scholars have suggested limiting the application of the plain view doctrine to digital searches; others have suggested that the doctrine should not apply in computer searches since it unduly extends the scope of the search. While the latter recommendation is appealing from the point of view of privacy advocates, it would undermine law enforcement efforts in tackling crimes.

Jordanian law does not provide much direction on whether officers may seize incriminating digital evidence discovered inadvertently. From the general meaning of Articles 82 and 87 of the Jordanian *Criminal Procedure Law* 1961, however, it can be inferred that investigators may seize an object not described in a warrant if the object itself is in plain view and its incriminating nature is immediately apparent.

Australian law explicitly authorises officers to seize digital evidence not described in a warrant if it presents itself in plain view.

In the USA, courts have taken different positions, some overruling investigators' authority to open files they see as suspicious, others upholding investigators' authority to open files and discover evidence of criminal activity other than that described in the warrant.

Recommendations

Because electronic storage devices are increasing in capacity and increasing the likelihood of encountering incriminating objects not described in the search warrant, investigators should be given the power to open suspicious files and seize evidence presenting itself in plain view.

4) Search incident to a lawful arrest

A search incidental to a lawful arrest is the most common exception to the search warrant requirements. It is based upon the necessity to preserve evidence of a crime and/or to protect the suspects, officers or others from possible danger. The search of digital devices incidental to a lawful arrest is crucial due to the fact that digital evidence is fragile and delicate, liable to damage, and susceptible to alteration or concealment. Scholars have debated whether a search incidental to arrest should allow officers to conduct a thorough search of the digital contents. Some scholars have rejected the search power arguing that the unique nature and characteristics of digital data require treatment different from tangible items and that the search should be confined to the physical device only and not to the digital contents.

Laws in Jordan and Australia authorise officers to search items or premises incident to a lawful arrest. In the absence of a judicial position on the issue, the traditional practice of search and seizure incidental to arrest would allow officers to search when they encounter a person carrying or possessing a digital device. In the USA, the courts have upheld the validity of a search of digital contents incidental to a lawful arrest.

Recommendations

The author supports the idea of confining the search and seizure incidental to arrest to the electronic device only to avoid digital evidence contamination, privacy invasion and misuse of personal data. Thus, investigators must obtain a warrant to conduct a thorough search.

10.6 Cross-border Searches and Seizures

Cyberspace has no geographic boundaries. Cybercriminals can commit cybercrimes without leaving their desks, while law enforcement agencies are encumbered by physical borders. Law enforcement investigation power in cybercrime can often not be performed effectively without assistance from other states or countries. Even though law enforcement and intelligence co-operation is increasing, it is substantially influenced by political, cultural and legal factors. The existence of the political will to assist and of cultural consistency, as well as robust legal instruments in each jurisdiction, are vital for successful cross-border investigations. A good relationship and willingness to help each other in cross-border investigations usually contributes to the success of cross-border investigations. However, cultural factors may be of less negative effect in cybercrime investigations because there are few discrepancies in cybercrime criminalisation policy.

The classical forms of mutual legal assistance, which were originally established to address traditional crimes, seem less capable of handling searches of digital evidence because digital evidence requires swift and decisive action for which the normal search and seizure procedures are not well suited. Therefore, the Convention on Cybercrime adopted new specific procedures for improving and strengthening international co-operation in cybercrime investigations. Expedited preservation of stored computer data located within the territory of a member, expedited disclosure of preserved traffic data, search and seizure across borders, and real-time collection of traffic data are new procedures for mutual legal assistance with respect to mechanisms particularly necessary for rapid effective co-operation in cybercrime investigations.

Jordan's involvement in cross-border cybercrime investigations is hindered by its lack of an adequate legal basis necessary to set up, facilitate and process mutual legal assistance. In contrast, Australia and the USA are actively involved in international co-operation on criminal matters in the fight against transnational crimes, including cybercrimes. The Australian *Mutual Assistance in Criminal Matters Act 1987* and the US Section 28 U.S.C § 1782 as well as the Mutual Legal Assistance Treaty between the two countries are legal instruments used to obtain evidence located in a foreign state.

Recommendations

The author recommends the urgent enactment of Jordanian domestic legislation on mutual assistance in criminal matters that would incorporate provisions necessary for the success of mutual legal assistance in cybercrime investigations. The statute should establish a central authority responsible for receiving and processing assistance requests and it should empower General Prosecutors to issue expedited requests for the preservation of data stored by Internet Service Providers and its disclosure on request. The data should be preserved for as long a period of time as necessary, up to a maximum of 90 days, unless an extension is granted.

10.7 Closing Comments

The Author hopes that recommendations made in this research will support efforts to strengthen law enforcement efficiency in the investigation of cybercrimes. He also hopes that the research findings will provide a useful source for Jordanian General Prosecutors, lawyers, judges and students of law and that the findings will encourage law-makers and regulators to enact a comprehensive cybercrime law and enhance investigations and international co-operation to counter cybercrimes. Also, the author hopes that the research will pave the way for more research in the area. Cybercrime investigation and digital evidence studies are still in their infancy, particularly in Jordan, and to date there has been little interdisciplinary research. Shariah law and cybercrime, the behaviour of Middle Eastern hackers, cyber-sectarian and the geographical aspects of cybercrime (i.e. within the Arab world) are very rarely examined.

Bibliography:

Articles/Books/Reports

Abbell, Michael, 'Obtaining Evidence in the U.S. in Criminal Cases Through Use of Compulsory Process' in Richard D. Atkins (ed), *The Alleged Transnational Criminal* (1995).

Acker, James R., and David C. Brody "*Criminal Procedure: A Contemporary Perspective*" (2nd ed, 2004).

Advanced Networking Management Lab, *Distributed Denial of Service Attacks (DDoS) Resources* (2001) Indiana University <http://www.anml.iu.edu/ddos/types.html> at 20 December 2005.

Ahmad, Mohib, *Dr. Mohammad Haneef to Be Released* (2007) Indian Muslim Blog < http://indianmuslims.in/dr-mohammad-haneef-to-be-released/> at 25 March 2008.

Akman, L E, B Akkan and N Baykal, *Optimization of an Online Course with Web Usage Mining* (Paper presented at the Conference on Artificial Intelligence and Applications, Innsbruck, Austria, February 2004).

Al Aldesco, 'Demise of Anonymity: A Constitutional Challenges to the Convention of Cybercrime' (2002) 23 *Loyola of Los Angeles Entertainment Law Review* 81.

Allard, Tom, 'New Secret Search Powers', *the Sydney Morning Herald* (Sydney), August 1, 2007.

Andert, Stephen and Donald K. Burleson, *Web Stalkers: Protect Yourself from Internet Criminals & Psychopaths* (2005) 93.

Andreas, Peter and Ethan Nadelmann, *Policing the Globe: Criminalization and Crime Control in International Relations* (2006).

Ankit, Fadia, *Unofficial Guide to Ethical Hacking* (2002).

Anonymous, *Maximum Security* (2001).

Anson, Steve, and Steve Bunting, *Mastering Windows Network Forensics and Investigation* (2007).

Arcaro, Gino, *Basic Police Powers: Arrest and Search Procedures* (3rd ed, 2003).

Archick, Kristin, 'Cybercrime: the Council of Europe Convention' in John V. Blane (ed) *Cybercrime and Cyberterrorism: Current Issues* (2003).

Arenson, Kenneth J and Bagaric Mirko, *Rules of Evidence in Australia: Text & Cases* (2005).

Argy, Philip et al, 'Electronic Evidence, Document Retention and Privacy' (Paper presented at the Australian Corporate Lawyers' Association (ACLA) NSW Annual Conference, Sydney, 30-31 March 2006).

Arnold, Bruce, 'Identity Theft' (2005) 38 *Security Solutions* 55.

Arquilla, John and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (2001).

Arrieta, S, *Hacker Categorized* (2000) MSC Institute of Technology <http://msc.edu.ph/wired/netspeak-15a.html> at 2 September 2005.

Attorney General Department, *Mutual Assistance* (2006) Australian Government < http://www.ag.gov.au/www/agd/agd.nsf/Page/Extradition_and_mutual_assistanceMutual_assistance> at 28 September 2008.

Australian Bilateral Mutual Legal Assistance Agreements, Australian Government: Attorney-General's Department < http://www.ag.gov.au/www/agd/agd.nsf/Page/Extraditionandmutualassistance_Relationshipwithothercountries_Australianbilateralmutualassistanceagreements> at 26 September 2008.

Australian High Tech Crimes Centre, *Computer Intrusion and Denial-of-Service* AHTCC <http://www.ahtcc.gov.au/tech_crimes_types/computer_intrusion.htm> at 15 March 2008.

Australian High Tech Crime, *Online Fraud*, AHTCC <http://www.ahtcc.gov.au/tech_crimes_types/fraud.htm> at 15 March 2008.

Baase, Sara, *A Gift of Fire: Social, Legal, and Ethical Issues For Computer and the Internet* (2nd ed, 2003).

Bacigal, Ronald J, *Criminal Law and Procedure: An Introduction* (2nd ed, 2002).

Bahadur, Gary, William Chan and Chris Weber, *Privacy Defended: Protecting Yourself Online* (2002).

Baird, Bruce J, Lindsay L Baird and Jr and Ronald P Ranauro, 'The Moral Cracker?' (1987) 6 (6) *Computer & Security* 471.

Baltatu, Madalina et al, 'Security Issues in Control, Management and Routing Protocols' (2000) 34 (6) *Computer Networks* 881.

Bantekas, Ilias, and Susan Nash, *International Criminal Law* (2nd ed, 2003).

Barrett, Neil, *Digital Crime: Policing the Cybernation* (1997).

Barua, Yogesh and Denzle P Dayal, *Cyber Crimes: Notorious Aspect of the Humans and the Net Spam Attacks, Cyber Stalking and Abuse* (2001).

Baryamureeba, Venansius and Florence Tushabe, *The Enhanced Digital Investigation Process Model* (2004) Institute of Computer Science, Makerere University <http://www.forensicfocus.com/enhanced-digital-investigation-model> at 22 September 2006.

Bassiouni, M. Cherif and David S. Gualtieri, 'International and National Responses to the Globalization of Money Laundering' in Ernesto Ugo Savona (ed) *Responding to Money Laundering: International Perspectives* (2000).

Becker, Ronald F, *Criminal Investigation* (2nd ed, 2005).

Bell, R. E, 'The Prosecution of Computer Crime' (2002) 9 *Journal of Financial Crime.*

Bellia, Patricia L., 'Chasing Bits Across Borders' (2001) *the University of Chicago Legal Forum* 35.

Bellovin, Steven M, *Security Problems in the TCP/IP Protocol Suite* (1989) <http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html> at 4 January 2006.

Belzer, Jack at el, *Encyclopedia of Computer Science and Technology* (1987).

Berg, Terrence, 'Practical Issues in Searching and Seizing Computers ' (2005) 7 *Journal of Practical and Clinical Law* 27.

Best Practice for Computer Forensics (2006) Scientific Working Group on Digital Evidence <http://www.ncfs.org/swgde/documents/swgde2006/Best_Practices for Computer Forensics%July06.pdf> at 22 November 2006.

Biham, Eli et al. Collisions of SHA-0 and Reduced SHA-1 (Paper presented at the 24thAnnual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005).

Black, Henry Campbell et al, *Black's Law Dictionary: Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern* (7th ed, 1991).

Blake, Dan, 'Russian Hackers Caught After Stealing $10 Million', *Denver Post* 1995.

Boaz, Ganor, *Defining Terrorism: Is One Man's Terrorist Another Man's Freedom* Fighter? International Institute for Counter-Terrorism <http://www.ict.org.il/Articles/define.htm> at 27 April 2006.

Bocij, Paul, Mark Griffith and Leroy Mcfarlane, 'Cyberstalking: A New Challenge for Criminal Law' (2002) 122 *The Criminal Lawyer* 3.

Bocij, Paul, *Victims of Cyberstalking : An Exploratory Study of Harassment Perpetrated Via the Internet* (2003) <http://www.firstmonday.dk/issues/issue8_10/bocij/index.html> at 5 March 2006.

Branigan, Steven, *High-Tech Crimes Revealed* (2005).

Breeding Brand New Viruses (2006) Computer Crime Research Center <http://www.crime research.org/news/17.01.2006/1764/> at 23 January 2006.

Brenner, Susan and Barbara Frederiksen 'Computer Searches and Seizures: Some Unresolved Issues ' (2001 / 2002) *Michigan Telecommunication and Technology Law Review* 28.

Brenner, Susan and Joseph J Schwerha IV ‘Introduction-Cybercrime: A Note on International Issues’ (2004) 6 *Information System Frontiers.*

Brenner, Susan, *Quotes*, <http://thinkexist.com/quotes/susan_brenner/> at 12 April 2008.

Brenner, Susan W and Bert-Jaap Koops, Approaches to Cybercrime Jurisdiction, (2004) 4 *Journal of High Technology Law* 3.

Brenner, Susan W and Joseph J Schwerha, ‘Cybercrime Havens: Challenges and Solutions’ (2007) 17 *Business Law Today.*

Brenner, Susan W, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' (2001) 8 (2) *E Law- Murdoch University Electronic Journal of Law* < http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html> at January 2005.

Brenner, Susan W, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 *Virginia Journal of Law and Technology 13.*

Brenner, Susan W., ‘The Council of Europe’s Convention on Cybercrime’ in Jack M. Balkin, et al (eds), *Cybercrime: Digital Cops in a Networked Environment* (2007).

Brill, Alan E, Mark Pollitt and Carrier M Whitcomb, 'The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications' (2006) Journal of Digital Practice 3.

Bristol, James E, III, ‘Free Expression in Motion Pictures: Children Sexuality and a Satisfied Society’ (2007) 25 *Cardozo Arts & Entertainment* 333.

Broadhurst, Roderic and Peter Grabosky, ‘Computer-Related Crime in Asia: Emergent Issues’ in Roderic Broadhurst, and Peter N Grabosky (ed) *Cyber-Crime: The Challenge in Asia* (2005).

Broadhurst, Roderic, 'Developments in the Global Law Enforcement of Cyber-Crime' (2006) 29 (3) *An International Journal of Police Strategies & Management* 408.

Bronitt, Simon and Miriam Gani, ‘Cyber-Crime in the 21st Century: Windows on Australian Law’ in Roderic Broadhurst and Peter Grabosky (ed), *Cyber-Crime: The Challenge in Asia* (2005).

Brown, Christopher, *Computer evidence: collection & preservation* (1st ed, 2006).

Brown, Michael F, *Criminal Investigation: Law and Practice* (2nd ed, 2001).

Bullwinkel, Jeffery G, ‘International Co-operation in Combating Cyber-Crime in Asia: Existing Mechanism and New Approaches’ in Roderic G Broadhurst and Peter N Grabosky (ed), *Cyber-Crime: The Challenge in Asia* (2005).

Byrne, James Michael and Donald J Rebovic (eds), *The New Technology of Crime, Law and Social Control* (2007).

Byte Wikipedia <http://en.wikipedia.org/wiki/Byte> at 26 September 2007.

Buffer <http://www.webopedia.com/TERM/b/buffer.html> at 9 May 2006.

Caloyannides, Michael A, *Privacy Protection and Computer Forensics* (2004).

Calsyn, Jeremy D et al, Warrantless Searches and Seizures’ (1998) 86 (5) *Georgetown Law Journal* 1214.

Cameron, Ben, 'Admissibility of Electronic Evidence in Australia' (Paper presented at the Using Electronic Evidence in Australia Courts, Sydney, 2000).

Cantrell, Bruce, *Electronic Privacy in the Private Sector Workplace* (2007) Global Information Assurance Certification <http://www.giac.org/resources/whitepaper/law/147.php> at 5 September 2007.

Carolyn, Penfold, 'Child Pornography Laws: the Luck of the Locale' (2005) 30 (3) *Alternative Law Journal* 123.

Carr, Indira, and Katherine S Williams, ‘Draft Cyber-Crime Convention: Criminalization and the Council of Europe Draft Convention on Cyber-Crime’ 18 *Computer Law & Security Report* (2002) 83.

Carr, Indira, ‘Anonymity, the Internet and Criminal Law Issues’ in C Nicoll, J.E.J Prins, and M.J.M. Van Dellen (eds), *Digital Anonymity and The Law: Tensions and Dimensions* (2003).

Carter, Arthur J and Audrey Perry, 'Computer Crimes' (2004) 41 *American Criminal Law Review 313.*

Carter, David L, *Computer Crime Categories: How Techno-criminals Operate* (1995) National Security Institute <http://nsi.org/library/compsec/crimecom.html> at 2 September 2005.

Carrier, Brian, and Eugene H Spafford, 'Getting Physical with the Digital Investigation Process' (2003) 2 (2) *International Journal of Digital Evidence.*

Carrier, Brain D, and Euguen H Spafford, 'Categories of Digital Investigation Analysis Techniques Based on the Computer History Model' (2006) 3 *Digital Investigation* 121.

Carrier, Brain D and Joe Grand, *A Hardware-based Memory Acquisition Procedure for Digital Investigation* (2004) Digital Investigation/Forensic and Evidence Research <http://www.digital-evidence.org/papers/tribble-preprint.pdf> at 2 June 2007.

Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2nd ed, 2004).

Casey, Eoghan, ‘ Reconstruction Digital Evidence’ in W Jerry Chisum and Brent E Turvey (eds), *Crime Reconstruction* (2006).

Casey, Eoghan, 'Investigating Sophisticated Security Breaches' (2006) 49 (2) *Communications of the ACM* 48.

Casad, Joe, *Teach Yourself TCP/IP in 24 Hours* (3rd ed, 2004).

Casiraya, Lawrence, *Philippines Cybercrime Bill to Cover Cell Phones* (2005) Computer Crime Research Center <http://www.crime-research.org/news/05.01.2005/878/> at 21 November 2006.

Cert, *Advisory CA-1999-02 Trojan Horses* (1999) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1999-02.html> at 19 January 2006.

Ceruti, Marion G, 'Web-to-Information-Base Access Solution' in John, P Slone (ed), *Local Area Network Handbook* (1999).

Chapman, Matt, *Conference Calls for Global Cyber-Crime Police* (2007) Vunuet < http://www.vnunet.com/vnunet/news/2198757/conference-calls-world>at 17 September 2008.

Chatterjee, Bela Bonita, 'Last of the Rainmacs: Thinking about Pornography in Cyberspace" in David Wall (ed) *Crime and the Internet: cybercrime and cyberfears* (2001).

Chirillo, Tavani Q, *Information Technology and citizen's rights* (2002).

Ciardhuain, Seamus O, 'An Extended Model of Cybercrime Investigation ' (2004) 3 (1) *International Journal of Digital Evidence* .

Cid Carlos, 'Recent Development in Cryptographic Hash Functions: Security Implications and Future Directions' (2006) 11(2) Information Security Technical Report 100.

Clancy, Thomas K, 'The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer' (2006) 75 *Mississippi Law Journal* 193.

Clancy, Thomas, What Constitute an Arrest within the Meaning of the Fourth Amendment? (2003) 48 *Villanova Law Review* 129.

Clark, David E, *Computers, Search Warrants, and the Private Papers Exemption* (2008) SelectedWorks <http://works.bepress.com/david_clark/1/> at March 2008.

Clark, Drew, *Privacy Experts Urge Vigilance Against Surveillance* (2003) The Computer Freedom & Privacy <http://www.cfp2003.org/cfp2003/njtd1.html> at 3 December 2006.

Clifford, Ralph, *Cybercrime: the Investigation, Prosecution and Defence of a Computer-Related Crime* (2nd ed, 2006).

Coates, Sam, *Rader Gets 175 Years for BTK Slayings* (2005) The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/18/AR2005081800201.html> at 3 April 2007.

Cobely, Cathy, *Sex Offenders: Law, Policy and Practice* (2nd ed, 2005).

Cockfield, Arthur J., 'Towards a Law and Technology Theory ' (2004) 30 (1) *Manitoba Law Journal* 383, 399.

Cochran, Doug et al, *Rules of Evidence: A Practical Approach* (2007).

Cohen Adam I and Lender David J, *Electronic Discovery: Law and Practice* (2004).

Cole, George F and Christopher E Smith, *Criminal Justice in America* (4th ed, 2005).

Comer, Douglas, *Q & A on TCP Segment Size* (2003) Purdue University <http://www.netbook.cs.purdue.edu/othrpags/qanda110.htm> at 16 May 2006.

Computer Crime and Intellectual Property Section, *Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations* (2002) US Department of Justice < http://www.justice.gov/criminal/cybercrime/s&smanual2002.htm> at 10 May 2007.

Computer Crime and Security Survey (2007) Computer Security Institute < http://www.gocsi.com/forms/csi_survey.jhtml> at 1 June 2008.

Computer Crime & Security Survey (2006) The Australian High Tech Crime Centre (AHTCC) <http://www.auscert.org.au/images/ACCSS2006.pdf> at 3 January 2007.

Computer Emergency Team, *Denial of Service Attacks* (2001) <http://www.cert.org/tech_tips/denial_of_service.html> at 24 November 2005.

Computer Emergency Response Team, *CERT Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks* (2000) Computer Emergency Response Team <http://www.cert.org/advisories/CA-2000-21.html> at 24 November 2005.

Computer Emergency Response Team, *CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks* (2000) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1996-21.html> at 24 November 2005.

Computer Forensic Software Tools Downloads, Forensic Computing Ltd < http://www.forensic-computing.ltd.uk/tools.htm#forensic_windows> at 1 March 2009.

'Computer for Every Student', *Alrai Daily Newspaper* (Amman), 18 January 2008.

Computer Security Definitions <http://www.computerhope.com/jargon/z/zombie.htm> at 12 December 2005.

Conser, James A, Gregory D Russell and Rebecca Paynich, *Law Enforcement in the United States* (2nd ed, 2005).

Conway, Maura, 'Cyberterrorism: Academic Perspectives' (Paper presented at the 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, 28-29 June 2004).

Cook, Matthew S, Third-Party Consent Under the United States and Utah Constitutions: Should Utah Adopt the Federal Standard? (1999) 1 *Brigham Young University Law Review* 381.

Cook, Virginia Lee, Third-Party Consent Searches: An Alternative Analysis' (1973) 41 (1) *The University of Chicago Law Review* 121.

Cotroneo, D et al, 'An Architecture for Security-Oriented Perfective Maintenance of Legacy Software' (2003) 45 *Information and Software Technology* 619.

Council of Europe, *Chart of Signatures and Ratifications* < http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=11&DF=9/28/2008&CL=ENG> at 28 August 2008.

Council of Europe, Convention on Cybercrime CETS NO: 185, < <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>at> 28 August 2008.

Council of Europe, *Convention on Cybercrime: Explanatory Report* < http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> at 22 August 2008.

Council of Europe, *Convention on Cybercrime: Frequently Asked Questions and Answers*, Computer Crime & Intellectual Property Section (DoJ) < http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm> at 8 September 2008.

Craig, *Ball, Computer Forensic For Lawyers Who Can't Set the Clock on Their VCR* (2005) <http://www.craigball.com/cf_vcr.pdf> at 4 June 2007, 11.

Craiger, Philip, *Computer Forensic Procedures and Methods,* National Center for Forensic Science < http://ncfs.org/craiger.forensics.methods.procedures.final.pdf> at 5 May 2008.

Crime Scene Response Guidelines: Documentation Procedures Crime Scene Investigation <http://www.crime-scene-investigator.net/respon4.html> at 15 September 2007.

Criscuolo, Paul J, *Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht* (2000) Computer Incident Advisory Capability - Department of Energy <http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf> at 1 December 2005.

Crime definition, Webster's Ninth New Collegiate Dictionary < http://dict.sztaki.hu/webster/webster> at 22 August 2005.

Crompton, Malcolm, *Inquiry Into the Law Enforcement Implications of New Technology* (2001) Parliament of Australia <http://www.aph.gov.au/senate/committee/acc_ctte/completed_inquiries/1999-02/itlaw/submissions/sub27.doc> at 22 November 2006.

Crypto Politics, Electronic Frontiers Australia http://www/efa.org.au/Issues/Crypto2.html#usa at 6 November 2006, 199.

Cryptography Wikipedia <http://en.wikipedia.org/wiki/Cryptography> at 17 October 2006.

Cypherix Strong Encryption <http://www.cypherix.co.uk/cryptainerle/faqs.htm> at 11 October 2006.

'Cybercrime Costs Huge Losses for British Business says survey.' *Xinhua News Agency* 24 February 2004.

Cybercrime Inquiry (2004) Australian Bankers' Association Inc < http://www.bankers.asn.au/ArticleDocuments/CybercrimeInquiryFinal.doc> at 3 September 2005.

Dagnan, Greg, *Searching in Stages to Prevent Destruction of Evidence at Crime Scenes* (2007) <http://www.crime-scene-investigator.net/SearchingStages.html> at 15 September 2007.

Dave, B, *Simple TCP Spoofing Attack* (1997) <http://www.tech-forums.net/computer/topic/1807.html> at 6 January 2006.

Dearden, Jack and Samantha Bricknell, Australian Crime: Facts & Figures 2007 (2008) Australian Institute of Criminology <http://www.aic.gov.au/publications/facts/2007/facts_and_figures_2007.pdf> at 1 June 2008.

DeCew, Judith Wagner, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (1997).

Decker, Lisa Key, 'The Search and Seizure of Electronic Pagers: a Federal Case Law Review', 10 *Criminal Justice Policy Review*, 343.

De Cruz, Peter, *Comparative Law in a Changing World* (3rd ed, 2007).

Definitions of Communications Protocol on the Web, Google Search <http://www.google.com.au/search?hl=en&lr=&oi=defmore&defl=en&q=define:communications+protocol> at 23 November 2005.

Delupis, Ingrid Detter, *The Law of War* (2nd ed, 2000).

Denning, Dorothy, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services* (2000) Georgetown University <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> at 26 April 2006.

Denning Dorothy, 'Cyberwarriors' (2001) 23 (2) *Harvard International Review* 70.

Denning, Dorothy E and William E. Baugh Jr, ‘Hiding Crimes in Cyberspace’ in Peter Ludlow (ed), *Crypto Anarchy, Cyberstates, and Pirate Utopia* (2001).

Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002) Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice. < http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm> at 28 October 2004.

Department of Law and Public Safety, *Computer Evidence Search and Seizure Manual* (2000) State of New Jersy < http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf> at 7 October 2004.

Desmond, Rosemary, 'Qld: Angry Hacker Jailed Over Sewage Dumping', *AAP General News* 31 October 2001.

Deutch, Miguel, 'Computer Legislation: Israel's New Codified Approach' (1996) 14 *The John Marshall Journal of Computer & Information Law* 461.

Dhillon, Joginder S and Robert I Smith, 'Defensive Information Operation and Domestic Law: Limitations on Government Investigative Techniques' (2001) 50 *The Air Force Law Review* 135.

Dillon, Thomas W and Daphyne S Thomas, ‘Knowledge of Privacy, Personal Use, and Administrative Oversight of Office Computers and E-mail in the Workplace’ (2006) *Information Technology Learning and Performance Journal* 23.

Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation (2003) The National Center for Forensic Science <http://www.ncfs.org/DE_courtroomdraft.pdf> at 10 June 2007.

Dodd, Jeff, 'Memories Are Made Of This: Several Types of Memory Play a Role In PCs ' (2002) 6 (7) *Smart Computing* 12.

Douligeris, Christos, and Aikaterini Mitrokotsa, 'DDoS Attacks and Defence Mechanisms: Classification and State-of-the-Art' (2004) 44 (5) *Computer Networks* 643.

Downing, Richard W, *Drafting Procedural Laws: Empowering Law Enforcement with the Legal Tools Needed to Investigate and Deter Cybercrime* (2002) <http://www.cybersecuritycooperation.org/moredocuments/Drafting%20Cybercrime%20Laws/Procedural%20LawsText.pdf> at 22 November 2006.

Doyle, Carolyn and Mirko Bagaric, Privacy Law in Australia (2005).

Doyle, Charles, 'Terrorism: Section by Section Analysis of the USA PATRIOT ACT' in Alphonse B Ewing and Charles Doyle (eds), *The USA Patriot Act Reader* (2005).

Drimmer, Jonathan, ' *Cross-Border Corporate Investigations and Prosecutions Involving the Department of Justice'* (2008) Lexisnexis < http://law.lexisnexis.com/practiceareas/Insights--Analysis/International/Jonathan-Drimmer-on-Cross-Border-Corporate-Investigations-and-Prosecutions-Involving-the-Department-of-Justice> at 24 September 2008.

Dugan, Sean, 'Enterprise Computing: Cybersabotage' (1995) *InfoWorld* .

Easton, Susan. M, *The Problem of Pornography: Regulation and the Right to Free Speech* (1994).

Edgar, Stacey L, *Morality and Machines: Perspectives on Computer Ethics* (2nd ed, 1997).

Edwards, Mark Joseph, *Understanding TCP/IP* (1997) Windows IT Library <http://www.windowsitlibrary.com/Content/121/01/2.html> at 26 November 2005.

Ellis, Alan and Robert L Pisanit 'The United States Treaties on Mutual Assistance in Criminal Matters: A Comparative Analysis' (1985) 19 *International Lawyer.*

E-mail from Nigel Phair to Alaeldin Maghaireh, 7 October 2006.

Erbschole, Michael, *Trojans, Worms, and Spyware* (2005).

Eriksson, Mattias, *An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions*, UMEA University <http://www.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf> at 6 January 2006.

E Social Science Dictionary <http://www.elissetche.org/dico/P.htm> at 3 July 2006.

Etzioni, Amitai, 'Implications of Select New Technologies for Individual Rights and Public Safety' (2002) 15 *Harvard Journal of Law & Technology* 258.

Evans, Amy and Martin F Murphy, 'the Fourth Amendment in the Digital Age: Some Basics on Computer Searches' (2003) 20 (10) *Computer and Internet Lawyer* 4.

Experts Call White House Anti-Terrorism Efforts Ineffective (2003) Computer Freedom & Privacy <http://www.cfp2003.org/cfp2003/njtd1.html. > at 2 December 2006.

Explanatory Memoranda, Cybercrimes Bill 2001 (Cth) 16.

Farlex, *Modem*, The Free Dictionary <http://computing-dictionary.thefreedictionary.com/Computer+modem> at 24 November 2005.

Fast Guide to DSL <http://whatis.techtarget.com/definition/0,sid9_gci213915,00.html#adsl> at 3 May 2006.

FBI's Carnivore System Disrupted Anti-Terror Probe (2002) Electronic Privacy Information Centre <http://www.epic.org/privacy/carnivore/5_02_release.html> at 24 November 2006.

Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data* (2005) Federal Trade Commission <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf > at 12 February 2006.

Federal Trade Commission, *Provisions of New Fair and Accurate Credit Transactions Act Will Help Reduce Identity Theft and Help Victims Recover* (2004) Federal Trade Commission <http://www.ftc.gov/opa/2004/06/factaidt.shtm> at 23 April 2007.

Federal Trade Commission, *Take Charge: Fighting Back against Identity Theft* Federal Trade Commission <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#How> at 23 February 2006.

Feldman, David, *The Law Relating to Entry, Search, & Seizure* (1986).

Felten, Edward W et al, 'Web Spoofing: An Internet Con Game' (Paper presented at the 20th National Information Systems Security Conference, Baltimore, Maryland October 1997).

Ferdico, John N, *Criminal Procedure for the Criminal Justice Professional* (9th ed, 2005).

Ferraro, Euqene, *Undercover Investigation for the Workplace* (2000).

Ferraro, Monique Mattei, and Eoghan Casey, *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science* (2005).

Finch, Emily, ‘What a Tangled Web we Weave: Identity Theft and the Internet’ in Yvonne Jewkes (ed), *Dot.cons: Crime, Deviance and Identity on the Internet* (2002).

Forester, Tom and Perry Morrison, *Computer Ethics* (2nd ed, 1994).

Franklin, Carl, *The Investigator's Guide to Computer Crime* (2006).

Franklin, Carl J, *Constitutional Law for the Criminal Justice Professional* (1999).

Freedman, Edwards H, 'Search and Seizure of Computer Equipment' (1999) 8 (3) *Information System Security* 10.

Free on-Line Dictionary of Computing, <http://foldoc.org/foldoc.cgi?query=connection+oriented> at 25 November 2005.

Freiberg, Aire, 'Non-Adversarial Approaches to Criminal Justice' (2007) 16 (4) *Journal of Judicial Administration* 205.

Friedman, Matt, *Canada Frees Up Crypto* (1998) WIRED <http://www.wired.com/news/politics/0,1283,15362,00.html> at 1 October 2006.

Furnell, Steven, *Cybercrime: Vandalizing the Information Society* (2002).

Galloway, John and Simeon J Simoff, 'Network Data Mining : Methods and Techniques for Discovering Deep Linkage Between Attributes' (Paper presented at the 3rd Asia-Pacific Conference on Conceptual Modelling , Hobart, Australia, 2006).

Gans, Jeremy and Andrew Palmer, *Australian Principles of Evidence* (2004).

Gardner, Ross, *Practical Crime Scene Processing and Investigation* (2005).

Garretson, Cara, *Vulnerable Security Algorithms Raise Concers* (2005) Network World <http://www.networkworld.com/news/2005/110105-nist-crypto.html> at 7 May 2007.

Geist, Micheal and Milana Homsi, *Outsourcing our Privacy?: Privacy and Security in a Borderless Commercial World* <www.michaelgeist.ca/resc/FINAL_UNB.doc> at 6 September 2008.

Gerald, Kovacich L, 'Hackers: Freedom Fighters of the 21st Century' (1999) 18 (7) *Computers & Security* 573.

Ghosh, Ajoy et al, *Guidelines for the Management of IT Evidence* (2003) 12.

Ghosh, Ajoy, ‘Guidelines for the Management of IT Evidence’ (Working Paper No 29, APEC, 2004).

Gillies, Peter, *The Law of Criminal Investigation* (1982).

Gilmore, William C, *Mutual Assistance in Criminal and Business Regulatory Matters* (1995).

Gino, Arcaro, Basic Police Powers: Arrest and Search Procedures (3rd ed, 2003).
Gissel, Richard (ed), *Digital Underworld: Computer Crime and Resulting Issues* (2005).

Godwin, Mike, *Cyber Rights: Defending Free Speech in the Digital Age* (2003).

Goenechea, Juan Miguel and Agustin Gonzalez Garcia, ‘Spain’ in Dennis Campbell (ed), *The Internet: Laws and Regulatory Regimes* (2006).

Goldsmith, Jack L, ‘The Internet and Legitimacy of Remote Cross-Border Searches’ (2001) *The University of Chicago Legal Forum* 103.

Goldsmith, Jack, *The Internet and the Legitimacy of Remote Cross-Border Searches* (2001) Social Science Research Network < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732> at 14 August 2008.

Goldsmith, Jack, Unilateral Regulation of the Internet: A Modest Defence, (2000) 11 *European Journal of International* 135.

Goldstein, Seth L, *The Sexual Exploitation of Children: A Practical Guide to Assessment, Investigation, and Intervention* (2nd ed, 1998).

Gold, Steve, 'UK - Court Acquits Teenage Hacker', *Newsbytes News Network* (London), 17 March 1993.

Goodman, Marc D, 'Why the Police Don't Care about Computer Crime' (1997) 10 *Harvard journal of law and technology* 465.

Gordon, Lawrence et al, 'CSI/FBI Computer Crime and Security Survey' (2005).

Grabosky, Peter, *Electronic Crime (2007).*

Grabosky, Peter and Russel G Smith, *Crime in the Digital Age: Countering Telecommunications and Cyberspace Illegalities* (1998).

Grabosky, Peter N, Russell G Smith and Gillian Dempsey, *Electronic Theft: Unlawful Acquisition in Cyberspace* (2001).

Grabosky, Peter, ‘The Global Cyber-Crime Problem: The Socio-Economic Impact’ in Roderic Broadhurst and Peter Grabosky (ed), *Cyber-Crime: The Challenge in Asia* (2005).

Greenawalt, Kent, 'Wiretapping and Bugging: Striking a Balance between Privacy and Law Enforcement ' (1966-1967) 50 *Judicature*.

Greene, Edward F et al, *U.S Regulation of the International Securities and Derivatives Markets* (8th ed, 2005).

Green, Ian, *DNS Spoofing by The Man In The Middle* (2005) SysAdmin, Audit, Network, Security Institute <http://www.sans.org/rr/whitepapers/dns/1567.php> at 9 January 2006.

Grimes, Roger A, *Honeypots for Windows* (2005).

Grimes, Roger A, *Malicious Mobile Code: Virus Protection for Windows* (2001).

Groothuis, Douglas R, *The Soul in Cyberspace* (1997).

Grossman, Lev, "*Attack of the Love Bug*", Time Europe, May 15, 2000, http://www.time.com/time/europe/magazine/2000/0515/cover.html>at 20 November 2005.

Guerin, Lisa, *The Essential Guide to Workplace Investigations* (1st ed, 2007).

Gupta, Rashi, *Windows 2000 Security* (2000).

Hackerott, Cynthia L and Lori Rosen, *HR How-to*: *Internal Investigations: Everything you Need to Know to Conduct an Internal Investigation in the Workplace* (2003).

Halper, Mark, 'Former Hacker Makes New Career in Computer Security', *Sunday Business* (London), 16 June 2002.

Hancock, Bill, 'Site Spoofing Becomes More Popular' (2000) 19 (7) *Computer & Security* 581.

Hancock, Douglas H, 'To What Extent Should Computer Related Crimes Be The Subject Of Specific Legislative Attention' (2001) 12 *Albany Law Journal of Science & Technology* 97.

Harrington, Jan L, *Network Security: A Practical Approach* (2005).

Harris, B, and R Hunt, 'TCP/IP Security Threats and Attack Methods' (1999) 22 *Computer Communication* 885.

Harris, Daniel M, 'The Supreme Court's Search and Seizure Decisions of the 1982 Term: The Emergence of a New Theory of the Fourth Amendment' (1984) 36:41 *The Baylor Law Review.*

Hash Function, <http://www.fileformat.info/tool/hash.htm> at 21 April 2008.

Hatonn, Gyeorgos C, *First Step: Whether Long or Short-The Road Matters Not if the First Step is Never Taken* (1995).

Hayat, Muhammad, Privacy and Islam: From Qura'n to Data Protection in Pakistan, 2007, *Information &Technology Law* 16.

Hayes, Robert, and Micheal Eburn, *Criminal Law and Procedure in New South Wales* (2nd ed, 2006).

Hemphill, Barbara, 'Who Are You? (Preventing Identity Theft)' (2003) *the National Public Accountant.*

Henry, Jonathan, 'Computer Based Media' in Peter White (ed), *Crime Scene to Court: The Essentials of Forensic Science* (2nd ed, 2004).

Henry, Paul A, *a Brief Look at the Evolution of Killer Worms* (2003) CyberGuard Corporation <http://www.csoonline.com/whitepapers/050504_cyberguard/EvolutionoftheKillerWorms.pdf> at 22 January 2006.

Hess, Patrick, *Cyberterrorism and Information War* (2002).

Hinde Stephen, 'Smurfing, Swamping, Spamming, Spoofing, Squatting, Slandering, Surfing, Scamming and Other Mischiefs of the World Wide Web' (2000) 19(4) *Computers & Security* 312.

Hoar, Sean B., 'Identity Theft: The Crime of the New Millennium' (2001) 80 *Oregon Law Review* 1423.

Holahan, Catherine, and Staff Writer, *Computer Viruses at Epidemic Proportion* (2004) <http://www.highbeam.com/library/doc3.asp?DOCID=1P1:91913140&num=5&ctrlInfo =Round18%3AProd%3ASR%3AResult&ao=1&FreePremium=BOTH> at 8 December 2005.

Holley, Brain, Henry Schimke and Erin Ebeler, *Caesar Shift Cipher and General Shift Cipher* University of Nebraska-Lincoln <http://cse.unl.edu/~bholley/Cypher%20Tutorial.html> at 17 October 2006.

Holmes, Stephen T and Ronald M. Holmes, *Sex Crimes: Patterns and Behavior* (3rd, ed 2007).

Holy Qur'an 24: 27 – *The Message of THE QUR'AN* translated and explained by *Muhammad Asad* (1980) Gibraltar

Home Affairs Committee, Great Britain: Parliament: House of Commons, *Justice and Home Affairs Issues at European Union Level* (2007).

Hosse, Jayne, Stephen Clift and Simon Carter, 'Combating Tourist Sexual Exploitation of Children' in Stephen Clift, and Simon Carter (eds), *Tourism and Sex: Culture, Commerce and Coercion* (2000).

Howell, Beryl A, 'Real-World Problems of Virtual Crime' in Jack M. Balkin et al (eds), *Cybercrime: Digital Cops and Laws in a Networked Environment* (2007).

Http://groups.google.com.sa/group/mslamhaker?hl=ar>at 11 November 2008.

Hudson, David L Jr, '*New Cyberstalking Law Challenged Over 'Annoy' Language'* (2006) First Amendment Center < http://www.firstamendmentcenter.org/news.aspx?id=16535> at 7 May.

Human Rights Liberties Protected, *The Jordan Times* (Amman), Monday, February 18th, 2008.

Human Rights Watch, *Shutting out the Critics* (2007) Human Rights Watch <http://hrw.org/reports/2007/jordan1207/jordan1207web.pdf> at 20 February 2008.

Hunsucker, Keith, *Right to Be, Right to See: Practical Fourth Amendment Application for Law Enforcement Officers* (2003) The Police Chief <http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=95&issue_id=092003> at 18 December 2006.

Hussain, Alefiya, John Heidemann and Christos Papadopoulos, 'Distinguishing between single and multi-source attacks using signal processing' (2004) 46 (4) *Computer Networks* 479.

Ieong, Ricci, 'FORZ Digital Forensics Investigation Framework that Incorporate Legal Issues' (2006) 29 *Digital Investigation* 30.

Information about Legal and Illegal Pornography: Child Porn Offending The Internet Safety Group <http://www.netsafe.org.nz/legal/child_porn2.aspx> at 6 October 2007.

Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation (2004) Electronic Frontiers Australia < http://www.efa.org.au/Publish/efasubm-ssbc-search2004.html> at 9 December 2004.

Internet Protocol Spoofing, Wikipedia <http://en.wikipedia.org/wiki/IP_spoofing> at 7 January 2006.

Internet Scam Guide, Official New York Web Site <http://www.nyc.gov/html/dca/downloads/pdf/internet.pdf> at 28 February 2006.

Interview with the Investigators 1St Lieutenant Ayman Bani Hani, (Jordanian Computer Crime Prevention Unit, Criminal Forensics Department, May 2005).

IP Spoofing Attacks and Hijacked Terminal Connections (1995) Computer Emergency Response Team <http://www.cert.org/advisories/CA-1995-01.html> at 8 January 2006.

Iqbal, Mohammad, 'Defining Cybeterrorism' (2004) 22 *The John Marshall Journal of Computer & Information Law* 397.408.

Jackson, K M, J Hruska, and Donn B parker, *Computer Security References Book* (1992).

Jahnke, Art, Alexey Ivanov and Vasiliy Gorshkov: *Russian Hacker Roulette* (2005) CSO Security and Risk http://www.csoonline.com/article/219964/Alexey_Ivanov_and_Vasiliy_Gorshkov_Russian_Hacker_Roulette?contentId=219964&slug=&> at 2 August 2008.

Jamison, M.K, 'New Developments in Search & Seizure law ' (2006) *The Army Lawyer* 23.

Jamsa, Kris A., and Lars Klander, *Hacker Proof: The Ultimate Guide to Network Security* (2nd ed, 2002) 292.

Janczewski, Lech J and Andrew M Colarik, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* (2005).

Jenkins, Philip, *Beyond tolerance*: *child pornography on the Internet* (2001).

Jeremy Andrews, *Understanding TCP Reset Attacks* (2005) <http://kerneltrap.org/node/3072> at 23 November 2005.

Johnson, David R and David G Post, Law and Borders—The Rise of Law in Cyberspace, (1996) 48 *Stanford Law Review* 1367.

Johnston, Tim, *Australian Judge Dismisses Terrorism Case* (2007) The New York Times <http://www.nytimes.com/2007/11/13/world/asia/13australia.html?ex=1352610000&en=f77331cefcf2e3ef&ei=5088&partner=rssnyt&emc=rss> at 25 March 2008.

Jonathan, M Jacobson, *Antitrust Law Developments* (2007).

Jordanian Cybercrime Investigation Unit, Computer & Cyber Crime Digital Evidence Guideline, Unpublished.

Jordanian Legislation [Trans of: التشريعات الاردنية National Information System < <http://www.lob.gov.jo/ui/contracts/listall.jsp> at 17 August 2008.

Joseph, Harold, 'The Threats on the Web' (1997) 1997(6) *Computer Fraud & Security* 7.

Joseph, Sarah, *Corporation and Transnational Human Rights Litigation* (2004).

Jordanian Courts, the Ministry of Justice Official Website <http://www.moj.gov.jo> at 3 May 2008.

Joseph, Janice, ' Cyberstalking: An International Perspective' in Yvonne Jewkes (ed), *Dot.cons Crime, Deviance and Identity on the Internet* (2003).

Judges to Obtain Master Degree from the United States (2008) Ammonnews <http://www.ammonnews.net/arabicDemo/article.php?issue=&articleID=8331>at 5 February 2008.

Kaminsky, Dan, *MD5 To Be Considered Harmful Someday* (2004) <http://www.doxpara.com/md5_someday.pdf> at 17 May 2007.

Kanaley, Reid, 'Computer Hackers Wrestle with Often Ambiguous Morals of Cyberspace', Knight Ridder/Tribune News Service 23 August 1995.

Kay, Russel, 'Computer Forensics', *Computerworld* April 17 2006, 49.

Keenan, Kevin M., *Invasion of Privacy: A Reference Handbook* (2005).

Kenneally, Erin, *Computer Forensic* (2002) The Magazine of Usenix & Sage, <http://www.usenix.org/publications/login/2002-08/pdfs/kenneally.pdf> at 5 October 2006.

Kenneally, Erin E, 'Digital Logs-Proof Matters' (2004) 1 *Digital Investigation* 94.

Kennedy, Ryan P, 'Ashcroft v. Free Speech Coalition: Can We Roast the Pig Without Burning Down the House in Regulating "Virtual" Child Pornography?' (2004) 37 Akron *Law Review* 379.

Kernutt, Kristi, Civil Law v. Common Law Systems: Are They So Different? Pangea1 (1999).

Kerr, Orin S, 'Digital Evidence and the New Criminal Procedure' (2005) 105 *Columbia Law Review* 279.

Kerr, Orin S, 'Digital Evidence and the New Criminal Procedure' in Jack M Balkin, et al (eds) *Cybercrime: Digital Cops and Laws in a Networked Environment* (2007).

Kerr, Orin S, *Ninth Circuit Mostly Eliminates Private-Sector Workplace Privacy Rights in Computers* (2006) Orinkerr.com: Law, the Legal Academy, and the Legal Profession <http://www.orinkerr.com/2006/08/09/ninth-circuit-mostly-eliminates-private-sector-workplace-privacy-rights-in-computers/#comments> at 20 July, 2008.

Kerr, Orin S, 'Searches and Seizures in a Digital World ' (2005) 119(2) *Harvard Law Review* 531.

Kerr Orin S, 'Search Warrants in an Era of Digital Evidence' (2005) 75 *Mississippi Law Journal* 85, 549.

Kim, Tai-hoon, and Seung-youn Lee, ' Design Procedures of IT Systems Security Countermeasures' in Osvaldo Gervasi, et al (eds), *Computational Science and Its Applications ICCSA* (2005).

King, Chula G, and W Timothy O'keefe., 'Online Identity Theft and Business' (2004) 74(4) *The CPA Journal* 50.

King of Cards (2005) Jordan Business <http://www.zawya.com/printstory.cfm?storyid=ZAWYA20051107090132&SecIndustries/pagE-Banking&l=000000051113> at 26 February 2006.

Kipper, Gregory, *Wireless Crime and Forensic Investigation* (2007).

Kizza, Joseph Migga, *Computer Network Security* (2005).

Kolko, David J, and Elissa J Brown, ' Child Sexual Abuse' in Robert T. Ammerman and Michel Hersen (ed), *Case Studies in Family Violence* (2nd ed, 2000).

Koster, Paul R, Workplace Searches by Public Employers and the Fourth Amendment, (2007) 39 *Urban Lawyer* 75.

Kovara, Joe, and Ray Kaplan, ‘Implementing Kerberos in Distributed Systems’ in Harold F. Tipton, and Micki Krause (eds), *Information Security Management Handbook* (6th ed, 2007).

Kreston, Susan, 'Computer Search and Seizure Issues in Internet Crimes against Children Cases' (2004) 30 *Rutgers Computer & Technology Law Journal* 327.

Kruse, Warren G and Jay G Heiser, *Computer Forensic: Incident Response Essentials* (2002).

Kuzma, Lynn M., ‘Security Versus Liberty: 9/11 and the American Public’ in William J Crotty (ed), *The Politics of Terror: The U.S. Response to 9/11* (2004).

Laciak, Christine A (ed), *International Antitrust Co-operation Handbook* (2004).

Lamb, Ainslie, and John Littrich, *Lawyers in Australia* (2007).

Lamplugh, Diana, and Paul Infield, 'Harmonising Anti-Stalking Laws' (2003) 34 *George Washington International Law Review* 853.

Lange, Michele C. S. and Kristin M. Nimsger, *Electronic and Discovery: What Every Lawyer Should Know* (2004).

Larkin, Daniel, *FBI Works To Protect Global Citizens From Online Crime* (2006) Internet Crime Complaint Centre (IC3) Federal Bureau of Investigation < http://dhaka.usembassy.gov/uploads/images/-feh04ECK4GeURwNBFPPqA/pre2apr02_06.pdf >at 14 December 2006.

Laundering Money: Obscuring the Link between the Criminal and the Crime', UN Chronicle 6/22/1998 1998.

Lawyer, David S, *Plug-and-Play-HOWTO* (2005) The Linux Documentation Project <http://www.tldp.org/HOWTO/Plug-and-Play-HOWTO.html> at 20 January 2006.

Lee, Debra, *Malware* (2004) Search Security <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci762187,00.html> at 18 October 2005.

Legal Information Access Centre (LIAC) http://www.austlii.edu.au/au/other/liac/hot_topic/hottopic/2002/3/2.html> at 5 May 2008.

Leigh, L. H, ‘Recent Developments in the Law of Search and Seizure’ (1970) 33 *The Modern Law Review.*

Lehey, Greg, *The term "hacker"* (2002) LEMIS <http://www.lemis.com/hacker.html> at 20 August 2005.

Levine, Diane E and Gary C Kessler, ‘Denial of Service Attacks’ in Seymour Bosworth and M E Kabay (eds), *Computer Security Handbook* (4th ed, 2002).

Levy, Robet L and Casey Patricia L, *Electronic Evidence and the Large Document Case: Common Evidence Problems* (2003) Haynes and Boone LLP <http"//www.haynesboone.com/FILES/tbl_s12PublicationsHotTopic/PublicationPDF60/1057/06_01_2003_Levy-Casey.pdf> at 23 April 2007.

Lemons, Bryan R, ‘Public Privacy: Warrantless Workplace Searches of Public Employee’ (2004) 7 *Journal of Labour and Employment.*

Lendino, *Jeff, ‘Practical Guidance for Conducting Electronic Discovery’* <http://www.ontrack.com> at 29 June, 2007.

Lesson: All about Datagrams <http://java.sun.com/docs/books/tutorial/networking/datagrams/index.html> at 26 November 2005.

Levy, Steven, *Hackers: Heroes of the Computer Revolution* (1st ed, 1984).

Lewis, James a, *Security and Surveillance* (2002) The Internet Society's 12th Annual INET Conference <http://www.inet2002.org/CD-ROM/lu65rw2n/papers/g10-b.pdf> at 3 November 2006.

Lilley, Peter, *Hacked, Attacked, and Abused: Digital crime exposed* (2002).

List of Treaties Open to the Non-European Non-Member States of the Council of Europe, Council of Europe < http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=12&CL=ENG> at 31 August 2008.

Lo, Joseph, *Trojan Horse Attacks* (2004) <http://www.irchelp.org/irchelp/security/trojan.html> at 29 January 2006.

Loshin, Pete, *TCP/IP Clearly Explained* (2nd ed, 1997).

Lowenstein, Aaron, *Search and Seizure on Steroids: United States v. Comprehensive Drug Testing and Its Consequences for Private Information Stored on Commercial Electronic Databases*, (2007) Selected Works <http://works.bepress.com/aaron_lowenstein/1/ >at 22 November.

Lynch, Jennifer, 'Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks' (2005) 20 *Berkeley Technology Law Journal* 259.

MacVean, Allyson, 'Understanding Sexual Predators on the Internet: Towards a Greater Knowledge' in Allyson MacVean and Peter Spindler (eds), *Policing Paedophiles on the Internet* (1st ed, 2003).

Madsen, Wayne, *Cryptography and Liberty: an International Survey of Encryption Policy* (1998) Global Internet Liberty Gampaign <http://www.gilc.org/crypto/crypto-survey.html> at 19 October 2006.

Maghaireh, Alaeldin Mansour, 'Combating Cyberterrorism: The Response from Australia and New Zealand' in James Veitch (ed), *International Terrorism: New Zealand Perspectives* (2005).

Maghaireh, Alaeldin Mansour, 'Shariah Law, Cyber-Sectarian Conflict & Cybercrime: How Can Islamic Criminal Law Respond to Cybercrime' (2008) 2 *International Journal of Cyber Criminology* .

Mahnaimi, Uzi and Tom Walker, 'Al-Qaeda Woos Recruits with Nuclear Bomb Website', *The Sunday Times* 6 November 2005.

Maier, Harold, G, 'Jurisdiction Rule in Customary International Law' in Karl Matthias Meessen (ed), *Extraterritorial Jurisdiction in Theory and Practice* (1996).

Malinowski, Chris, 'the Digital Investigative Unit: Staffing, Training, and Issues' in Thomas Alfred Johnson (ed), *Forensic Computer Crime Investigatio*n (2006).

Mallery, John, 'Cyberforensics: The Ultimate Investigative Tool: The Right Way and The Wrong Way to Run a Computer Investigation' (2005) *Security Technology and Design*.

Mccombs, Barrie, 'Phoney Phishing and Pharming' (2005) 10 (3) *Canadian Journal of Rural Medicine* 186.

McCormack, Sean, *United States Joins Council of Europe Convention on Cybercrime* (2006) U.S. Department of Justice < http://www.state.gov/r/pa/prs/ps/2006/73353.htm>at 28 August 2008.

McKenzie, Shane, *Partnership Policing of Electronic Crime: An Evaluation of Public and Private Police Investigative Relationship* (PhD Thesis, Melbourne University, 2006).

McLean, J.J., 'Homicide and Child Pornography' in Eoghan Casey (ed), *Handbook of Computer Crime Investigation* (2002).

Mctaggart, Craig, 'A Layered Approach to Internet Legal Analysis.' (2003) 48 (4) *McGill Law Journal* 571.

Mena, Jesus, *Investigative Data Mining For Security and Criminal Detection* (2003).

Menthe, Darrel C, *Jurisdiction in Cyberspace: A Theory of International Space* (1998) Michigan Telecommunications and Technology Law Review < http://www.mttlr.org/volfour/menthe_art.html>at 16 August 2008.

Meyers, Gary D and Nerida Gilbert, *Primary Sources: A "Not-So-Anonymous" Review of US Legal Research Materials and Sources* (2003) Research for Lawyers < http://www.research-one.com.au/primary+sources+a+not-so-anonymous+review+of+us+l.aspx> at 1 May 2008.

Meyer, Gordon R, 'Hackers, Phreakers, and Pirates: The Semantics of the Computer Underground' in Grover Maurice Godwin (ed), *Criminal Psychology and Forensic Technology: a Collaborative Approach to Effective Profiling* (2001).

Meyers, Matthew, and Marcus Rogers, 'Digital Evidence Forensics: Meeting the Challenges of Scientific Evidence' in Mark Pollitt and Suject Shenoi (eds), *Advances in Digital Forensics* (2005) 43.

Michael, Katrina and Gregory Rose, '*Human Tracking technology in Mutual Legal Assistance and Police Inter-State Co-operation in International Crimes'* <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1559&context=infopapers> at 23 July 2008.

Michaels, Ralf, 'Territorial Jurisdiction after Territoriality' in Pieter J. Slot et al (ed), *Globalisation and Jurisdiction* (2004).

Middleton, Bruce, *Cyber Crime Investigator's Field Guide* (2005).

Milutinovic, Veljko, *Infrastructure for Electronic Business on the Internet: Lessons Learned* (2001).

Milhon, Jude, *Hackers Lose a Patron Saint* (2003) WIRED <http://www.wired.com/news/technology/0,1282,59711,00.html> at 20 September 2005.

Milhorn, Thomas, *Cybercrime: How to Avoid Becoming a Victim* (2007).

Mohay, George et al, *Computer and Intrusion Forensics* (2003).

Moore, Robert, *Cybercrime: Investigating High-Technology Computer Crime'* (2005).

Moore, Robert Emest, *Search and Seizure of Digital Evidence: An Examination of Constitutional and Procedural Issues* (PhD Thesis, the University of Southern Mississippi, 2003).

Moore, Robert, 'To View or not to View: Examining the Plain View Doctrine and Digital Evidence' (2004) 29 *American Journal of Criminal Justice* 61.

More Nuke Information and Patches <http://www.irchelp.org/irchelp/nuke/info.html#icmpflood> at 1 December 2005

Morris, Tony, *MD5 and Speed Camera* (2006) < http://tmorris.net/> at 19 April 2008.

Morrison, Perry and Tom Forester, *Computer Ethics* (1994).

Mota, Sue Ann, *The U.S. Supreme Court Addresses the Child Pornography Prevention Act and Child Online Protection Act in Ashroft v. Free Speech Coalition and Ashcroft v. American Civil Liberties Union* (2002) Indiana University <http://www.law.indiana.edu/fclj/pubs/v55/no1/mota.pdf> at 18 February 2006.

Moyes, Gordon, *Is there a Paedophile in Cabinet* (2003) Moyes Gordon Website <http://www.gordonmoyes.com/2003/06/03/is-there-a-paedophile-in-cabinet> at 26 June 2008.

Mueller's, Scott, *Upgrading and Repairing PCs* (14th ed, 2002).

Nadelmann, Ethan A, *Cops across Borders: the Internationalization of U.S Criminal Law Enforcement* (1993).

National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* (2001) Department of Justice <http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf> at 11 October 2006.

Nelson, Bill et al, '*Cyberterror: Prospects and Implications*' (Defense Intelligence Agency, 1999).

Nelson, Bill et al, *Guide to Computer Forensic and Investigations* (2nd ed, 2006).

Nemerofsky, Jeff, 'The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?' (2000) 6 (23) *Richmond Journal of Law & Technology*.

New Zealand Law Report Commission, Search and Surveillance Power, Report No 0113-2334; 97(2007).

Nincic, Miroslav, 'Information Warfare & Democratic Accountability' in Emily O. Goldman (ed), *National Security in the Information Age* (2004).

Nissenbaum, Helen, *Protecting Privacy in an Information Age: The Problem of Privacy in Public* (1998) Online Ethic Center <http://www.onlineethics.org/com/nissenbaum/privacy.html> at 18 November 2006.

Nixon, P A et al, ‘Security, Privacy and Trust Issues in Smart Environments’ in Diane J Cook, and Sajal K Das (eds), *Smart Environments: Technologies, Protocols, and Applications* (2005).

Norris, Ed, ‘ Protecting against Hacker Attacks’ in Sanjiv Purba (ed), *Architectures for E-Business Systems: Building the Foundation for Tomorrow’s Success* (2001).

North, Geoffrey A., 'Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance' (2002) 28 *Rutgers Computer & Technology Law Journal* 155.

Northouse, Clayton, ‘Providing Security and Protecting Liberty’ in Clayton Northouse (ed), *Protecting What Matters* (2006).

Northwestern University School of Law, Arresting a Suspect in a Third Party’s Home: What is Reasonable? (1981) 72 *the Journal of Criminal Law & Criminology*.

O’Brien, Kevin A, ‘Information Age Terrorism and Warfare’ in David Martin Jones (ed), *Globalisation and the New Terror* (2004).

O’Brien, Michael J, *Computer Crime* <http://www.mobrien.com/computer_crime1.htm> at 18 August 2005.

O'Connor, Tom, *Cybercrime: the Internet as Crime Scene* (2005) North Carolina Wesleyan College <http://faculty.ncwc.edu/toconnor/315/315lect12.htm> at 11 April 2006.

O’Halloran, Joe, 'FBI arrests young Turk and Moroccan for Zotob' (2005) (5) *Network Security* 1.

O'Neill, Sean and Yaakovlapppin, 'Extremist Islamist has Returned - via Internet', *The Times* 21 October 2005.

Oppliger, Rolf, *Internet and Intranet Security* (1998).

Orton, Pa Ivan, ‘the Investigation and Prosecution of a Cybercrime’ in Ralph D. Clifford (ed), *Cybercrime: the Investigation, prosecution and Defense of a Computer-Related Crime* (2nd ed, 2006).

Osborne, Cynthia S and Thomas N Wise, 'Paraphilias' in Richard Balon, and Taylor Segraves (eds), *Handbook of Sexual Dysfunction* (2005).

Panwar, Shivendra et al, *TCP/IP Essentials: a Lab-Based Approach* (2004).

Palmiotto, Michael J, *Criminal Investigation* (3rd ed, 2004).

Papapavlou, George, 'Legal Aspects of New Information Technologies' (Working Paper No DG XIII-E1, National Institute of Standards and Technology, 1992).

Parker Donn B, 'Computer Crime' in K M Jackson and J Hruska (eds), *Computer Security: Reference Book* (1992).

Parker, Donn B, *Categories of Hackers* (1996) VirginiaTech <http://courses.cs.vt.edu/~cs3604/lib/Hacking/Parker.html#1> at 30 August 2005.

Parker, Donn, *Crime by Computer* (1976).

Parker, Graham, *An Introduction to Criminal Law* (1977).

Patzakis, John*, Maintaining the Digital Chain of Custody* Infosecurity Europe <http://www.infosec.co.uk/files/quidance_software_04_12_03.pdf> at 2 June 2007.

Penny, Steven, Reasonable Expectation of Privacy and Novel Search Technologies: An Economic Approach, (2007) 97 *the Journal of Criminal Law & Criminology.*

People Republic of China a Global Survey of Cybercrime Legislation <http://www.cybercrimelaw.net/countries/china.html> at 22 November 2005.

Petroni Jr Nick L et al, 'FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory' (2006) 3 (4) *Digital Investigation* 197.

Peysakhovich, Sofya, 'Virtual Child Pornography: Why American and British Laws are at Odds With Each Other' (2004) 14 *Albany Law Journal of Science & Technology* 799.

Philippsohn, Steven 'Trends In Cybercrime: An Overview of Current Financial Crimes on the Internet' (2001) 20 (1) *Computers & Security* 53.

Ping Wikipedia <http://en.wikipedia.org/wiki/Ping> at 20 December 2005.

Pipkin, Donald L, *Halting the Hacker: a Practical Guide to Computer Security* (2nd ed, 2002).

Plague, Grandmaster, *Myths About TCP Spoofing* (2002) <http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=6394&mode=thread&order=0&thold=0> at 21 November 2005.

Poch, Jeremy R., *Cyber-Crime and the Uphill Battle Faced by the Business World* (2005) University of Wisconsin Platteville <http://www.uwplatt.edu/csse/CSSE_411%20Papers%20and%20Presentations/CSSE411Spr2005/PochJ%20-%20%20Final%20Paper.doc> at December 2005.

Pollitt, Mark M, 'Cyberterrorism - Fact or Fancy?' (1998) 1998 (2) *Computer Fraud & Security* 8.

Police Powers, <http://www.lawhandbook.sa.gov.au/ch10s07s05.php> at 13 October 2008.

Price, Simon a, 'Understanding Contemporary Cryptography and its Wider Impact upon the General Law' (1999) 13 (2) *International Review of Law Computers* 95.

Queensland Law Reform Commission, The Role of Justice of the Peace in Queensland, Report No 51 (1998) 50.

Raphael, Winick, 'Searches and seizures of computer and computer data' (1994) 8 *Harvard Journal of Law & Technology.*

RASC: Confidentiality, Integrity and Availability (CIA) (2004) Purdue University <http://www.itap.purdue.edu/security/files/documents/RASCCIAv13.pdf> at 1 May 2006.

Reith, Mark, Clint Carr and Gregg Gunsch, 'An Examination of Digital Forensic Models' (2002) 1 (3) *International Journal of Digital Evidence.*

Regan, Charles et al (eds) ‘Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age’ (Paper presented at The Sedona Conference, September 2004).

Review and recover deleted Internet history. *A Firm of Solicitors v District Court at Auckland* [2004] 3 NZLR 748.

Reyes, Anthony et al, *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors* (2007).

Rheinstein, Max, Common Law and Civil Law: An Elementary Comparison, Rev J UPR (1952-1953) 91.

Rhoden, Carla, 'Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond' (2003) 30 *American of Criminal Law.*

Richard, M.M, ‘ International Assistance in Combating Crime’ in Brice Ruyver, Gert Vermeulen, and Tom Beken (eds), *Strategies of the EU and the US in Combating Transnational Organized Crime* (2002).

Richards, James, *Transnational Criminal Organizations, Cybercrime, and Money Laundering* (1999).

Ritter, Nancy, *Digital Evidence: How Law Enforcement Can Level The Playing Field With Criminals* (2006) National Institute of Justice <http://www.ojp.usdoj.gov/nij/journals/254/digital_evidence.html> at 12 October 2006.

Rittinghouse, John W and William M Hancock, *Cybersecurity Operations Handbook* (1st ed, 2003).

Roebuck, Terrance, *Network Security: DoS vs DDoS Attacks* (2005) Computer Crime Research Center <http://www.crime-research.org/articles/network-security-dos-ddos-attacks/4> at 6 January 2006.

Roger, Brown RFD, 'So You Think Traffic Offences Are Simple? Camera-Detected Offences in NSW' (2006) 30 (5) *Criminal Law Journal* 302.

Ross, Andrew, ‘Hacking Away at the Counter-Culture’ in David Bell, and Barbara M Kennedy (eds), *The Cybercultures Reader* (2000).

Router whatis.com <http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html> at 20 December 2005.

Rowland, Diane, and Elizabeth Macdonald (ed), *Information Technology Law* (3rd, 2005).

Rusnell, Charles, 'Cybercops' (2001) 49 (6) *Law & Order* 52.

Russia Arrests Grandfather of Cybercrime', *BBC News* 26 May 2001.

Russian Hacker Gets 3 Years in Jail, msnbc < http://www.msnbc.msn.com/id/3078748/> at 4 August 2008.

Russell, Ryan ‘et al’ *Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker is to Think Like* One (2001).

Sanderson, Christiane, *The Seduction of Children: Empowering Parents and Teachers to Protect Children from Child Sexual Abuse* (2004).

Sanusian, Silvia S., ‘Argentina’ in ’Dennis Campbell (ed), *The Internet: Laws and Regulatory Regimes* (2006).

Satoh, Akashi and Inoue Tadanobu, 'ASIC-Hardware-Focused Comparison For Hash Functions MD5, RIPEMD-160, and SHS' (2007) 40 *The VLSI Journal* 3.

Schell, Bernadette H and Clemens Martin, *Cybercrime: A Reference Handbook* (2004).

Schneier, Bruce, *Opinion: Cryptanalysis of MD5 and SHA: Time for a New Standard*, (2004)<http://www.landfield.com/isn/mail-archive/2004/Aug/0071.html> at 19 April 2008.

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway* (1st ed, 1994).

Schwartz, Martin A, and John E. Kirklin, *Section 1983 Litigation* (6th ed, 1997)

Scott, Hugh, *Computer and Intellectual Property Crime: Federal and State Law* (2001).

Scott, Hugh, *Computer and Intellectual Property Crime: Federal and State Law, 2006 Cumulative Supplement* (2006).

Sean, Nicholls and Needham Kirsty, *Speedsters Rush For the Fines Exit* (2004) FairfaxDigital <http://www.smh.com.au/articles/2004/11/17/1100574541050.html?from=moreStories> at 6 May 2007.

Serge, Krasavin, *What is Cyber-terrorism*? (2000) Global Information Assurance Certification <http://www.giac.org/certified_professionals/practicals/gsec/1774.php> at 26 April 2006.

Seger, Karl, David Icove, and William Vonstorch, *Computer Crime: A crime fighter's Handbook* (1995).

Serio, Josephd and Alexander Gorkin, 'Changing Lenses: Striving for Sharper Focus on the Nature of the 'Russian Mafia' and its Impact on the Computer Realm' (2003) 17(2) *International Review of Law Computers* 191.

Shafer, Paul, *Freedom, Community and the Third Wave* (1996) Electronic Frontier Foundation <http://www.eff.org/Misc/Publications/E-journals/CyRev/cyrev4.html#freedom> at 26 August 2005.

Shinder, Debra Littlejohn, and Ed Tittel, *Scene of the Cybercrime: Computer Forensics Handbook* (2002).

Shinder, Debra Littlejohn, and Michael Cross, *Scene of the Cybercrime* (2nd ed, 2008).

Shiode, Narushige, *An Outlook For Urban Planning in Cyberspace: Toward The Construction Of Cyber Cities With The Application of Unique Characteristics Of Cyberspace* (1997) UCL Centre for Advanced Spatial Analysis <http://www.casa.ucl.ac.uk/planning/articles2/urban.htm> at 1 May 2006.

Shredder, *Operation Sundevil* (1993) Hack Canada <http://www.hackcanada.com/blackcrawl/general/sundevil.txt> at 30 August 2005.

Sieber, Ulrich, *the International Handbook on Computer Crime* (1986).

Siegel, Jay, *Forensic Science: The Basic* (2007).

Siegel, Larry J and Joseph J Senna, *Introduction to Criminal Justice* (10th 2005).

Sinrod, Eric J and William P Reilly, 'Cyber-Crime: A Practical Approach to the Application of Federal Computer Crime Laws' (2000) 16 *Santa Clara Computer and High Technology Law Journal* 177.

Siris, Vasilios A., and Fotini Papagalou, 'Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks' (2005) *Computer Communication* 1.

Skibell, Reid, Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act, 18 *Berkeley Technology Law Journal* (2003).

Skibell, Reid, 'The Myth of the Computer Hacker' (2002) 5(3) *Information, Communication & Society* 336.

Skorodumova, Olga, 'Hackers as Information Space Phenomenon' (2004) 35 (4) *Social Sciences* 105.

Skoudis, Ed and Lenny Zeltser, *Malware: Fighting Malicious Code* (2004).

Slade Robert M, *Software Forensic: Collecting Evidence from the Scene of a Digital Crime* (2004).

Slobogin, Christopher and Joseph E Schumacher, 'Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Case: An Empirical Look At "Understanding Recognized and Permitted By Society".' (1993) 42 *Duke Law Journal*.

Slosarik, Katherine, 'Identity Theft: An Overview of the Problem ' (2002) 14 (4) *The Justice Professional* 329.

Smith, Johan, *Criminal Law* (9th ed, 1999).

Smith, Russell G, ‘Crime Control in the Digital Age: An Exploration of Human Rights Implications’ (2007) 1 *International Journal of Cyber Criminology* 167.

Smith, Russell G, 'Investigating Cybercrimes: Barriers and Solutions' (Paper presented at the Association of Certified Fraud Examiners, Sydney, 11 September 2003).

Smith, Russell G, Peter Grabosky and Gregor Urbas, *Cyber criminals on trial* (2004).

SMTP whatis.com
<http://searchexchange.techtarget.com/sDefinition/0,,sid43_gci214219,00.html> at 19 December 2005.

Solove, Daniel J, Marc Rotenberg, and Paul M. Schwartz, *Privacy, Information, and Technology* (2006).

Sonne, Warren J, *Criminal Investigation for the Professional Investigator* (2006).

Space <http://www.answers.com/topic/space> at 5 November 2005.

Speer, David L, 'Redefining Borders: The Challenges of Cybercrime' (2000) 34 (3) *Crime, Law and Social Change* 259.

Spindler, Peter, ‘Combating Child Abuse on the Internet: A Law Enforcement Strategy’ in Allyson Macvean and Peter Spindles (eds), *Policing Paedophiles on the Internet* (2003).

Sprague, Robert, ‘Employee Privacy in Virtual Workplaces’ in Pavel Zemliansky, and Kirk St. Amant (eds), Handbook of Research on Virtual Workplaces and The New Nature of Business Practices (2008).

Staff and News services, 'Love Bug Clues Point to Students Computer Virus Leads Suggest the Creator may be in Philippines or Australia. *(*2000) ' *The Atlanta Journal and Constitution.*

Stalking, Nova Network of Victim Assistance < http://www.novabucks.org/info/stalking.htm > at April 2 2006

Stalking Resource Center, Who's watching you--Spyware and Stalkers (2005) Stalking Resource Center <http://www.ncvc.org/src/main.aspx?dbID=DB_WhosWatchingYou--SpywareandStalkers128> at 15 January 2006.

Stallman, Richard, *Can you Trust Your Computer*? (2002) <http://www.gnu.org/philosophy/can-you-trust.html> at 13 September 2005.

Standing Committee on Justice and Community Safety, Legislative Assembly for the Australian Capital Territory, *Incorporating the Duties of a Scrutiny of Bills and Subordinate Legislation Committee* (1999).

Stana, Richard M., 'Identity Theft: Prevalence and Cost Appear to be Growing' in Claudia L. Hayward (ed), *Identity Theft* (2004).

Starkoff's David, *MD5 and the Law* (2005) <http://www.dbs.id.au/blog/law/md5-speed-cameras.html> at 2 May 2007.

State Department, Mutual Legal Assistance (MLA) and Other Agreements <http://travel.state.gov/law/info/judicial/judicial_690.html> at 20 September 2008.

Stephens, Gene, Computer Crimes Will Increasingly Invade People's Privacy' in Paul A. Winters (ed), *Current Controversies: Computers and Society* (1997).

Stephenson, Peter, *Investigating Computer-Related Crimes* (2000).

Stephens, Otis H and Richard A Glenn, *Unreasonable Searches and Seizures: Rights and Liberties under the Law* (2006).

Stering, Robert, *Police Officer's Handbook: An Introductory Guide* (2004).

Stevens, Dennis J, *An Introduction to American Policing* (2008).

Stippich, Matthew J and Christopher J Stippich, 'A Holistic Perspective on the Science of Computer Forensic' (2005) 1 (1) *Journal of Information Privacy & Security* 27.

Surratt, Carla G, *Netaholics: The Creation of a Pathology* (1999).

Swartz, Nikki, 'Canada to Increase Internet Surveillance' (2005) 39 (6) *Information Management Journal* 22.

System administrator Wikipedia <http://en.wikipedia.org/wiki/System_administrator> at 13 September 2007.

Tarte, Robbie, *Understanding Computers: an Overview for the Non-Geek.*

Tavani, Herman T, 'Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace' (2000) *Computers and Society* 3.

Tavani, Herman T, *Ethics and technology: ethical issues in an age of information and communication technology* (2004) .

Tavani, Herman T, 'The Uniqueness Debate in Computer Ethics: What Exactly is at Issue, and Why Does it Matter' (2004) 4 *Ethics and Information Technology.*

Taylor, Greg, *the Council of Europe Cybercrime Convention: A Civil Liberties Perspective* (2001) Computer Crime Research Centre < http://www.crime-research.org/library/CoE_Cybercrime.html> at 7 September 2008.

Taylor, Max, and Ethel Quayle, *Child Pornography: An Internet Crime* (2003).

Taylor Paul, 'Hacktivism: in Search of Lost Ethics' in David S Wall (ed), *Crime and the Internet* (2001).

TCP and UDP Ports, the Free Encyclopaedia <http://en.wikipedia.org/wiki/Computer_port> at 11 May 2006.

TCP/IP, msn <http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?refid=18617 18624> at 22 November 2005.

'Teardrops and Land Bugs Denial of Service Attacks Exploit TCP/IP Vulnerabilities' (1998) *Software Magazine.*

Telecommunications Privacy Laws (2006) Electronic Frontiers Australia <http://www.efa.org.au/Issues/Privacy/privacy-telec.html> at 3 January 2007.

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000) United Nations <http://www.uncjin.org/Documents/congr10/10e.pdf page4> at 20 August 2005.

The cyberspace invaders (2003) The Age Company <http://www.theage.com.au/articles/2003/06/21/1056119529509.html?oneclick=true> at 13 October 2005.

The Law Reform Commission, Criminal Investigation: An Interim Report, Report No 2 (1975).

The New Webster's Encyclopedic Dictionary of The English Language (1997).

The Trojan War: *The Judgment of Paris* (1998) The World of Royalty <http://www.royalty.nu/legends/Troy.html> at 20 January 2006.

Thomas, Douglas, *Hacker Culture* (2002).

Thomas, Douglas, 'New Ways to Break the Law; Cybercrime and the Politics of Hacking' in Yvonne Jewkes, and Gayle Letherby (eds), *Criminology: A Reader* (2002).

Thompson, Eric, 'MD5 Collisions and the Impact on Computer Forensic' (2005) 2 (1) *Digital Investigation* 36.

Thomsen, Dan, 'IP spoofing and session hijacking' (1995) (3) *Network Security.*

Tiller, James S, *The Ethical Hack: A Framework for Business Value Penetration Testing* (2005).

Toren, Peter, *Intellectual Property and Computer Crimes* (2003).

Towle, Holly K, 'Identity Theft: Myths, Methods, and New Law' (2004) 30 *Rutgers Computer & Tech 237.*

Transmission Control Protocol Catalyst Development: Software Applications, Components and Libraries

<http://www.catalyst.com/products/socketwrench/tutorial/tcpdoc02.html> at 22 November 2005.

Trojans: Myths and Facts (2002) <http://www.emsisoft.com/en/kb/articles/tec021007/> at 27 January 2006.

Tronc, Keith, Cliff, Crawford and Doug, Smith, *Search and Seizure in Australia and New Zealand* (1996).

Turkle, Sherry, *Life on the Screen: Identity in the Age of the Internet* (1995).

'UDP port denial-of-service attack' (1996) 1996(2) *Network Security* 2.

UK DDoS Attacks Rise as Zombie Plague Spreads; TeleCity and Prolexic Defend Customers against Cyber-terrorists. (2005) M2 Presswire <http://www.highbeam.com/library/doc3.asp?DOCID=1G1:131169139&num=6&ctrlInfo=Round18%3AProd%3ASR%3AResult&ao=&FreePremium=BOTH> at 23 December 2005.

Urbas, Gregor and Peter Grabosky, 'Cybercrime and Jurisdiction in Australia' in Bert-Jaap Koops and Susan W. Brenner (ed), *Cybercrime and Jurisdiction* (2006).

U.S. Department of State: *Bureau of Consular Affairs, Preparation of Letters Rogatory* (2008) http://www.travel.state.gov/law/info/judicial/judicial_683.html> at 18 September 2008.

User Datagram Protocol Wikipedia <http://en.wikipedia.org/wiki/User_Datagram_Protocol> at 24 December 2005.

Vacca, John R., *Computer Forensics: Computer Crime Scene Investigation* (2nd ed, 2005).

Vahey, Michael "*Understanding Metadata*" CAN Professional Counsel < http://www.pearlinsurance.com/risk-lawyer/metadata.pdf> at 16 April 2008.

Valetk, Harry a, 'Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies' (2004) 2 *Stanford Technology Law Review.*

Vasileva, Mariyana, *Delete Cookies* (2004) <http://www.developer.com/directories/item.php/211041> at 22 November 2006.

Vatis, Michael A., *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment* (June 2002) Institute for Security Technology Studies at Dartmouth College< http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf > at 19 September 2004.

Verton, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism* (2003).

Verton, Dan, *The Hacker Diaries: Confessions of Teenage Hackers* (2002).

Veta, Jean et al, ‘ Cybersecurity: Risk and Liability in the New Information Environment’ in Mark E. Plotkin, Bert Wells, and Kurt A Wimmer (ed), *E-Commerce Law & Business* (2003).

Vincent, Mosco, *The Digital Sublime* (2004).

Volonino, Linda, Reynaldo Anzaldua, and Jana Godwin, *Computer Forensics: Principles and Practices* (2007).

Volonino, Linda and Stephen R Robinson, *Principles and Practice of Information Security* (2004).

Vulnerability (2006) <http://www.answers.com/topic/vulnerability> at 3 April 2006.

Wagstaff, Samuel S, Jr, *Cryptanalysis of Number Theoretic Ciphers* (2003).

Walden, Ian, 'Crime and Security in Cyberspace' (2005) 18(1) *Cambridge Review of International Affairs,* April 2005.

Walker, Darin, 'Faceless-Oriented Policing: Traditional Policing Theories Are Not Adequate in a Cyber World' (2006) 79 (32) *The Police Journal* 169.

Wall, David, *Cybercrime: The Transformation of Crime in the Information Age* (2007).

Wallentine, Ken, *Street Legal: A Guide to Pre-Trial Criminal Procedure for Police, Prosecutors, and Defenders* (2007).

Wang, Haining, Danlu Zhang and Kang G. Shin*, Detecting SYN Flooding Attacks* College of William and Mary <http://www.cs.wm.edu/~hnw/paper/attack.pdf> at 24 December 2005.

Wang, Shiuh-Jeng and Kao Da-Yu, 'Internet Forensics on the Basis of Evidence Gathering With Peep Attacks' (2006) 29 (4) *Computer Standards & Interfaces* 423, 424.

Wang, Xiaoyun and Yu Hongbo, 'How to Break MD5 and Other Hash Functions' in Lecture Notes in Computer Science (2005) vol 3494.

Wang, Xiaoyun and Yu Hongbo "How to Break MD5 and Other Hash Functions" (Paper presented at the 24thAnnual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005).

Wang, Xiaoyun, et al, *Collisions for Hash Functions MD4, MD4 Haval-128 and RIPEMD*" (2004) International Association for Cryptologic Research <http://eprint.iacr.org/2004/199.pdf> at 6 May 2007.

Wagner, Abraham R, 'Terrorism and the Internet: Use and Abuse' in Mark Last and Abraham Kandel (eds), *Fighting Terror in Cyberspace* (2005).

Warren, M, and W. Hutchinson, 'Deception: A Tool and Curse for Security Management' in Michel Dupuy, and Pierre Paradinas (ed), *Trusted Information: The New Decade Challenge* (2001).

Wasik, Martin, *Crime and the Computer* (1991).

Webb, Dan K., Robert W. Tarun, and Steven F Molo, *Corporate Internal Investigation* (1993).

Wegman, Jerry, *Computer Forensics: Admissibility of Evidence in Criminal Cases* (2004) University of Idaho <http://www.cbe.uidaho.edu/wegman/computer%20Forensics%20AA%202004.htm> at 29 May 2007.

Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (2006).

Weimann, Gabriel, 'Cyberterrorism: The Sum of All Fears?' (2005) 28 (2) *Studies in Conflict & Terrorism* 129.

Weismann, Miriam F. Miquelon, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What prospects For Procedural Due Process' (2005) 23 *The John Marshall Journal of Computer & Information Law* 329.

Westby, Jody R, *International Guide to Combating Cybercrime* (2003).

What Is a Computer Virus? (2005) <http://www.microsoft.com/athome/security/viruses/intro_viruses_what.mspx> at 18 January 2006.

What Is a Packet? <http://computer.howstuffworks.com/question525.htm> at 26 November 2005.

What Is Phishing and Pharming? Anti-Phishing Working Group <http://www.antiphishing.org/index.html> at 17 May 2006.

What Is UDP Flood Attack? <http://www.csie.ncu.edu.tw/~cs102085/DDoS/bruteforce/udpflood/description.htm> at 20 December 2005.

Whitworth, Keith H. and Carol Y. Thomspon Ronald G. Burns, 'Assessing law enforcement preparedness to address Internet fraud' (2004) 32 (5) *Journal of Criminal Justice* 477, 5.

William, Gibson, *Neuromancer* (1984).

Williams, Katherine S, *Textbook on Criminology* (2004).

Williams, Phil, *Organized Crime and Cybercrime: Synergies, Trends, and Responses,* Computer Crime Research Centre <http://www.crime-research.org/library/Cybercrime.htm> at 25 April 2006.

Williams, Renee E, Third Party Consent Searches after Georgia V. Randolph: Dueling Approaches to the Dueling Roomates, (2008) 87 *Boston University Law Review.*

Wilson, Clay, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (2005) Federation of American Scientists < http://www.fas.org/sgp/crs/terror/RL32114.pdf> at 9 July 2005.

Wilson, James Q, *The Investigators: Managing FBI and Narcotics Agents* (1978).

Wingfield, Thomas C, *Legal Aspects of Offensive Information Operations in Space* Air University <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/wingfield.doc> at 3 March 2006.

Woody, Robert, *The Law and the Practice of Human Services* (1984).

Working to Halt Online Abuse, Online Harassment/ Cyberstalking Statistics (2006) <http://www.haltabuse.org/resources/stats/index.shtml> at 6 March 2006.

Working to Halt Online Abuse, Online Harassment Statistics Gender of Victims (2006) <http://www.haltabuse.org/resources/stats/genderv.shtml> at 6 March 2006.

Wrobleski, Henry M and Karen M Hess, *Introduction to Law Enforcement and Criminal Justice* (8th ed, 2006).

Yar, Majid, 'Computer hacking :Just another case of juvenile delinquency?' (2005) 44 (4) *Howard Journal of Criminal Justice* 387.

Yar, Majid, *Cybercrime and Society*: *Crime and Punishment in the Information Age* (2006).

Yearwood, Douglas L, and Richard Hayes, *Prosecuting Computer Crime in North Carolina: Assessing the Needs of the State's District Attorneys* (2003) North Carolina Department of Crime Control & Public Safety <http://www.ncgccd.org/PDFs/Pubs/NCCJAC/cybercrime.pdf> 7 May 2006.

Yi Gao, *Efficient Trapdoor-Based Client Puzzle System Against DoS Attacks* (Master, University of Wollongong, 2005).

Young, Susan and Dave Aitel, *The hacker's handbook: The Strategy behind Breaking into and Defending Networks* (2004).

Zanini, Michele and Sean J.A Edwards, ‘ The Networking of Terror in the Information Age’ in John Arquilla et al (eds), *Networks and Netwars: the Future of Terror, Crime, and Militancy* (2001).

2004: Year of the Global Malware Epidemic- Top Ten Lessons (2004) Gale Group. <http://www.highbeam.com/library/doc3.asp?DOCID=1G1:125077476&num=1&ctrlInfo=Round18%3AProd%3ASR%3AResult&ao=&FreePremium=BOTH> at 18 October 2005.

Case Law

Jordan

The Court of Cassation, Court decision قرار محكمة تمييز جزاء رقم 2004/725 2004/6.

The Court of Cassation, Court decision قرار محكمة تمييز جزاء رقم 1999/430 (هيئة عامة تاريخ 1999/8/28).

The Court of Cassation, Court decision قرار محكمة تمييز جزاء رقم 1997/697 (هيئة خماسية تاريخ 1997/12/22).

Australia

Cf *Hart v Commissioner of Australian Federal Police* (2002) 392 FCR 384.

Dpp v Leonard (2001) NSWSC 797.

George v. Rockett (1990) 170 CLR 104.

Kennedy v Baker (2004) FCA 562.

Oke v. Commissioner of the Australian Federal Police (2007) (FCA27).

McKinnon v Secretary, Department of Treasury (2006) 229 ALR 187, 1549.

Mora v. Gaithersburg Police Dept, 519 F. 3D 216 (4th Cir. 2008).

Plenty v. Dillon (1991)171 CLR 635.

The Queen v. Michael Malloy (1999) 118 ACTSC.

Wheare v Police (2008) SASC 13.

USA

Beck V. Ohio 379 US 2d 223 144, 145 (1964).

Carroll v. United States, 267 US 132, 162 (Wash, 1925).

Chimel v California, 395 2d 685 US 753, 763 (Supreme Court of the United State, 1969).

Floria, petitioner v. Luz Piedad Jimeno et al, 114 L. Ed. 2d 297 (1991).

Georgia. v. Randolph, 457 US 103 (2006).

Horton v. California, 495 U.S. 128, 136-37, (1990*).*

In the Matter of Search Warrant for K-Sports Imports Inc 163 F 594 (Cal, 1995).

Illinois v Rodriguez, 497 U.S. 177, 188-189 (1990).

Katz v. United States, 389 U.S. 347 (1967).

Leventhal v. Knapek, 266 F3d 64 (2nd Cir, 2001).

O'Connor v. Ortega 480 U.S 709, 718 (1987).

People v. Blair, 748 N.E.2d 318 (2001).

People v. Camilleri 220 Cal.App.3d 1199, 1206 (1990).

Terry v. Ohio, 392 U.S. 1, 20 (1968).

United States v. Carey 172 F. 3d 1268 (10th Cir, 1999).

United States v. Comprehensive Drug Testing, INC

United States v. Bentley, 825 F.2d 1110 (7th Cir, 1987).

United States v. Brooks, 427 F 3d 1246, 1249 (10th Cir, 2005).

United States v. Carey, 172 F.3d 1268, 1275 (10th Cir, 1999).

United States v. Dennis 100 A.F.T.R.2d (2007).

United States v. Derrick Jackson, 131 F. 3d 1105, 1108 (4th Cir, 1997).

United States v. Finley 477 F. 3d 250, 254 (5th Cir, 2007).

United States v. George Snow, 44 F.3d 133, 135 (2nd Cir.1995).

United States v. Grimmett, 439 F.3d 1236, 1267 (9th Cir, 2006).

United Stares v. Hamvrick, 55 F 2d 504 (1999).

United States v. Hill 459 F 3d 1, 27 (9th Cir, 2006).

United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982).

United States v. Jeffrey Ziegler, 456 F. 3d 1138, 1145 (9th Cir, 2006).

United States v. Johnson 06-4002-17-CR-C-NKL (2007).

United States v. Jonathon Dean, 234 F. 780, 782 (4th Cir, 2007).

United States v. Kennedy, 81 F 2d 1103, 1110 (Kan, 2000).

United States v. Lacy, 119 F.3d 742 (9th Cir, 1997).

United States v. Lamb, 945 F 441, 462 (NY 1996).

United States v. Lemmons, 282 F.3d 920 (7th Cir, 2002).

United States v. Mark L. Simons, 206 F. 3d 392 (4th Cir, 2000).

United States v. Matlock 415 U.S 164 (1974).

United States v. Mattlock, 476 F.2d 1038 (7th Cir, 1973).

United States v. Montgomery Gray, 78 F. Supp. 2d 524, 528 (1999).

United States v. New York Tel.Co, 434 U.S. 159 (1977).

United States v. Olson, 03-CR-51-S (Wis, 2003).

United States v. Patrick Carey, 172 F. 3d 1268, (10th Cir 1999).

United States v. Perez, 247 2d 2, 75 461,481 (NY 2003).

United States v. Perez, 485 F 3d 735, 738 (5th Cir, 2007).

United States v. Rafael Mercado-Nava, 486 F. Supp 2d 1271, 1274 (Kan, 2007).

United States v. Ray Andrus, 483 F.3d 711 (10th Cir, 2007).

United States v. Reed, 935 F.2d 641 (4th Cir, 1991). (Cited from *United States v. Taylor*, 650 F.2d 526 (4th Cir. 1981).

United States v. Schultz 14 F. 3d 1093, 1097 (6th Cir, 1994).

United States v. Simons, 206 F.3d 392, 398 (4th Cir, 2000).

United States v. Slanina, 283 F.3d 670 (5th Cir, 2002).

United States v. Spilotro, 800 F.2d 959, 963 (9th Cir, 1986).

United States v. Tamura, 694 F.2d at 596-97 (9th Cir, 1982).

United States v. Todd Andrews, 442 F. 3d 966 (7th Cir, 2006).

United States v. Young, 909 F.2d 442, 446 (11th Cir, 1990).

Williford v. State of Texas, 127 S.W 3d 310, 313 (Tex, 2004).

Legislation

Jordan

Credit Information Law 2003.

Criminal Law 1960.

Criminal Procedure Law 1961.

Custom Law 1998.

Electronic Transaction Law 2001.

Evidence Law 1952, amended by the *Evidence Law 2005.*

Jordanian Constitution Act 1952.

Telecommunications Law of 1995 s 11 (72) (a) amended by *Telecommunications Law 2002.*

Terrorism Prevention Law 2006.

Australia

Crimes Act 1995 (Cth) Div 473. 1 amended by (*Telecommunications Offences and Other Measures) Act 2004* (Cth).

Crimes Act 1914 (Cth).

Criminal Code Act 1995 (Cth) amended by *Criminal Code Amendment (Theft, Fraud, Bribery & Related Offence Act) 2000* (Cth) div 133 (1).

Criminal Law consolidation Act 1935 (SA).

Cybercrime Act 2001 (Cth) div 476(1).

Evidence Act 1995 (Cth).

Mutual Assistance in Criminal Matters Act 1987.

The Uniform Evidence Act 1995 (2004).

USA

Communications Act 1934 amended by *Violence against Women and Department of Justice Reauthorization Act* §§ 18.U.S.C 223 s (s) (2005).

*Computer Fraud and Abuse Act 1984.*U.S.C 1030.

Crimes and Criminal Procedures 18 USC § 3109.

Domestic Security Enhancement Act USC §§ 404 (2003).

Electronic Communications Privacy Act of 1986.

Identity Theft and Assumption Deterrence Act, 18 USCS § 1028 (a) (1998).

Identity Theft Penalty Enhancement Act, 18 USCS §§ 1028A (2004).

PATRIOT Act, 18 USC §201-16 (2001).

Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act 18 U.S.C §§ 501-4 (A) (2003).

The Fair and Accurate Credit Transaction Act, 18 USCS §§ 1028 (3) (d) (2) (a) (2003).

Treaties

Convention on Cybercrime opened for signature 23 November, 2001 (entered into force 1 July 2004).

The United Nation Convention on Civil and Political Rights art 12.

Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, opined for signature 30 April 1997, No 19, art 15 (1) (entered into force 30 September 1999).

Other Sources:

Ahmad, Kamal, *The Practical Principles of Computer Crime Investigation* (Alaeldin Maghaireh trans, 2002 Unpublished [trans of: الاصول الفنية للتحقيق في جرائم الحاسوب].

ابراهيم حامد طنطاوي, *The Criminal responsibility of forge crimes on formal documents scholarly and Judicially* (Alaeldin Mansour Maghaireh trans, 1995) [trans of: المسؤلية " الجنائية عن جرائم التزوير في المحررات فقهاء وقضاء].

أمل عبدالرحمن عثمان, *Criminal Procedure Law Explanation* (Alaeldin Mansour Maghaireh trans, 1975) [Trans of: شرح قانون الاجراءات الجنائية].

الادلة الرقمية في مسرح الجريمة ,مديرية الامن العام, ادارة المختبرات و الادلة الجرمية , قسم جرائم الحاسوب *Computer & Cyber Crime Digital Evidence*, (Alaeldin Mansour Maghaireh, trans unpublished) [trans of: الادلة الرقمية في مسرح الجريمة].

حسين علم, *the Law of Criminal Procedures* (Alaeldin Maghaireh, trans) [trans of قانون الاجراءات الجنائية].

علاء الدين منصور مغايرة, *The Modern Aspect of Information Crimes: comparative study* (Alaeldin Mansour Maghaireh trans, 2000) [trans of: الاوجه الحديثة للجرائم المعلوماتية " دراسة مقارنة].

عصام الطوالبة, Computer Search and Seizure Procedures (Alaeldin Mansour Maghaireh trans, 2003) [trans of اجراءات البحث و التفيش في الكمبيوتر]

سامي الشوا, *Informatics Fraud as a new phenomenon* (Alaeldin Mansour Maghaireh trans, 1993) [trans of: الغش المعلوماتي كظاهرة اجرامية مستحدثة].

صلاح الدين جمال الدين, *the Validity of Search Procedures* (Alaeldin Maghaireh trans, 2005) [trans of: [الطعن في اجراؤات التفتيش].

كمال احمد, *The Practical Principles of Computer Crime Investigation* (Alaeldin Maghaireh trans, 2002 Unpublished [trans of: الاصول الفنية للتحقيق في جرائم الحاسوب].

كامل السعيد, *Computer and Information Technology Crimes* (Alaeldin Mansour Maghaireh trans, 1993). [trans of: جرائم الكمبيوتر والجرائم الاخري في مجال التكنولوجيا].

كامل السعيد, *Explanation of the Criminal Procedure Law: Analytical Comparative Study* (Alaeldin Maghaireh trans, 2005) [trans of: شرح قانون اصول المحاكمات الجزائية : دراسة تحليلية
تاصيلية مقارنه]

قدري عبدالفتاح الشهاوي, *Search Disciplines in the Egyptian Law: Comparative Study* (Alaeldin Mansour Maghaireh trans, 2005) [trans of: ضوابط التفتيش في التشريع المصري والمقارن].

محمود نجيب حسني, “ *Criminal Code explanation – crimes division* (Alaeldin Mansour Maghaireh trans, 1992) [trans of: شرح قانون العقوبات-القسم الخاص].

مديرية الامن العام الاردني , *Annual Report, Department of Laboratories and Criminal Evidence* (Alaeldin Mansour Maghaireh trans, 2002) [trans of: التقرير السنوي, ادارة المختبرات والادلة الجرمية].

مديرية الامن العام الاردني , *Environmental Police Department* (Alaeldin Mansour Maghaireh trans) [trans of:إدارة الشرطة البيئية].
http://www.psd.gov.jo/arabic/index.php?option=com_content&task=view&id=62&Itemid=139> 7 December 2006.

مديرية الامن العام الاردني , *Public Security Directorate: Overview and Achievements* (Alaeldin Mansour Maghaireh trans) [trans of: الامن العام في سطور تاريخ وانجاز].
<http://www.psd.gov.jo/arabic/index.php?option=com_content&task=view&id=571&Itemid=384> at 7 December 2006.

هلالي عبداللاه احمد, *Searching Computer Systems and Suspect’s Rights: Comparative Study* (Alaeldin Maghaireh, trans 1997) [trans of: تفتيش نظم الحاسب الالي و : دراسة مقارنة
ضمانات المتهم المعلومات].