Hacking in Cyberspace Identity Theft: A Comparative Analysis of Malaysia, United Kingdom, and Iran

Article *in* Baltica · November 2020

CITATIONS
0

READS
460

4 authors, including:

Rizal Rahman
Universiti Kebangsaan Malaysia
41 PUBLICATIONS **20** CITATIONS
SEE PROFILE

Nazura Abdul Manap
Universiti Kebangsaan Malaysia
55 PUBLICATIONS **164** CITATIONS
SEE PROFILE

Sohaib Mukhtar
Bahria University Islamabad Campus
22 PUBLICATIONS **24** CITATIONS
SEE PROFILE

ISSN: 0067-3064

HACKING IN CYBERSPACE IDENTITY THEFT: A COMPARATIVE ANALYSIS OF MALAYSIA, UNITED KINGDOM AND IRAN

Mohamad Rizal[1], Nazura Abdul Manap[1], Sohaib Mukhtar[2], Hossein Taji[3]

[1] Faculty of Law, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia, noryn@ukm.edu.my, nazura@ukm.edu.my

[2] Department of Law, Bahria University, Islamabad, Pakistan, smukhtar.buic@bahria.edu.pk

[3] Faculty of Law, Islamic Azad University, Mashhsad, Iran, b.taji359@gmail.com

ABSTRACT

Hacking is an unauthorized access to computer data to steal personal information of another. Computer Misuse Act 1990 in United Kingdom, Computer Crimes Act 1997 in Malaysia and Islamic Penal Code as well as Computer Crimes Act 2009 in Iran deal with the issue of hacking. Cyberspace identity theft does not occur until unauthorized access occurs. In United Kingdom and Malaysia intention is not required to be directed towards any program or data of any kind while under Computer Crimes Act 2009 it is required to secure data. Notion of unauthorized access is computer protection by security measures, this security element is not applicable in United Kingdom and Malaysia. Perpetrator must have breached security measures to qualify for unauthorized access. Articles 1 and 4 of Computer Crimes Act 2009 require computers to be protected with security measures to meet requirement of unauthorized access in Iran while it applies to cyberspace identity theft. Iran does not recognize concept of exceeding unauthorized access while United Kingdom and Malaysia directly stress on this and treat this as an offence to prevent authorized person from misusing authority. This makes it possible for cyberspace identity theft offences to be easily committed by those who have prior authority to access data. This article adopts qualitative method of research a comparative analysis of hacking in cyberspace identity theft laws of Malaysia, United Kingdom and Iran.

Keywords: *Hacking; Cyberspace Identity Theft; Unauthorized Access.*

ISSN: 0067-3064

INTRODUCTION

Cyberspace identity theft growing due to increased electronic storage of personal information hence its effect is serious. Hackers have strong intent to obtain personal data to secure access to financial accounts and personal data, they acquire account numbers and access financial accounts. Criminal activity of hacking like criminal trespass as hacking is gaining unauthorised access to computer system whereas trespass is gaining access to area belongs to someone else. One can argue that both are same and there is no need to adopt new penal laws to deal with offence of hacking specifically. Though this is technically true but it seems more reasonable to enact penal laws specifically target hacking.

Hacking is an intrusion by hackers in a security network system or a computer system includes electronic tools to obtain personal information. Hacking is also defined as gaining unauthorised access to computer system, programs or data. It is also defined as unauthorised trespass of computer system by an intruder, enables individuals to take control of other's property remotely via Internet or virtual world and use it to spread it to public. It is also defined as unauthorised access to computer systems or networks by violating security regulations and measures

Countries have different approaches to criminalise cyberspace identity theft. Some utilise specific existing legislation while others attempt to introduce new laws. Specific crimes aimed at punishing perpetrators of cyberspace identity theft do exist in small number of jurisdictions especially where cyberspace identity theft is only defined as separate crime when they result in other offences while in others such theft are considered standalone act where other illegal acts are required for punishment.

There has been no legislation introduced in United Kingdom which focuses explicitly on cyberspace identity theft or that defines such crime in specific term. United Kingdom considers that there is no need for further legislation on cyberspace identity theft because it has passed two legislations in 2006, instead require policy emphasis and focus on identity crime reduction. It also attempts to improve awareness of cyberspace identity theft and provide preventative actions against cyberspace identity theft risks among potential victims, private sector and third parties. However, weaknesses occur through lack of resources in investigating cyberspace identity theft crimes and complication involved in investigation of incidents particularly in cross border cases. On the other hand, Malaysia's legal position does not address cyberspace identity theft directly although there is comprehensive legislation on unauthorised access Computer Crimes Act 1997 which covers cyberspace identity theft as an offence by hackers using unauthorised access. In Iran, Computer Crimes Act 2009 stipulates jail terms, fines and combination of both for unauthorised access which covers cyberspace identity theft as an offence by hackers using unauthorised access.

This article aims to define hacking from different worldviews, legal issues of hacking includes unauthorised access, exceeding authorized access, unauthorised acts with intent to impair or cause unauthorised modification in relation to cyberspace identity theft in comparison with United Kingdom, Malaysia and Iran.

Furthermore, this article highlights strengths as well as weaknesses of existing legislation of United Kingdom, Malaysia, and Iran and how it can be improved by providing reforms and new solutions to address proliferation of cyberspace identity theft to identify crimes.

UNAUTHORIZED ACCESS

Hacking connotes unauthorized access which involves act of breaching protected computer system. Computer is a device for storing, processing and retrieving information. Cybercrime Convention defines computer system as a device or group of interconnected or related devices which pursuant to program, performs automatic processing of data. Computer data refers to representation of facts, information or concepts in form suitable for processing in computer system including program suitable to cause computer system perform function.[1]

In United Kingdom, section 1 of Computer Misuse Act 1990 states that any person intentionally causes computer to perform any function with intent to secure an unauthorised access to any program or data of any kind held in computer is guilty of an unauthorised access to computer material. Article 2 of Convention on cybercrime 2001 states that hacking is unauthorized access occurs when hacking is carried out on another person's system without his consent. Unauthorized access is an act specifically committed by cyberspace identity thieves when stealing information and data, countries adopt this element in their legislations.[2]

Computer Misuse Act 1990 came into force on 29th August 1990. Scottish Law Commission produced working paper on computer related crimes in 1987. The House of Lords in a case between *R v Gold and Schifreen*[3] held that computer hacking was not criminal offence under British Forgery and Counterfeiting Act of 1981 hence it looked necessary and required to have a legislative intervention and order to bring criminal law up to date with technology.[4] In 1988, the Law Commission of England and Wales produced working paper in respect of computer misuse[5] followed by another working paper released by the Law Commission in 1989.[6] Later, Computer Misuse Bill introduced and Computer Misuse Act came into effect in August 1990.[7]

Section 1 of Computer Misuse Act 1990 states that a person is guilty of an offence of unauthorised access if he causes a computer to perform any function with an

---

[1] Article 1, Convention on Cybercrime, 2001, Council of Europe.
DPP v McKeown, DPP v Jones [1997] 2 Cr App R, 155.
D. Ormerod, *Smith and Hogan Criminal Law,* 1st Edition, Oxford Publication, 2008, United Kingdom, p 727.
[2] Section 1, Computer Misuse Act 1990, United Kingdom.
[3] [1988] 2 WLR, p 984.
[4] A. Charlesworth, 'Legislation against Computer Misuse*:* The trials and tribulations of the UK ComputerMisuseAct1990' (1993) 4 (1) *Journal of Law and Information Science*, p 218.
[5] M. Wasik, 'Law reform proposals on computer misuse', (1989) *The Criminal Law Review*, p 257.
[6] Law Commission Working Paper No. 186 *Criminal law: Computer misuse*, 1989.
[7] Computer Misuse Act United Kingdom 1990.

intent to secure access to any program or data held in any computer or access he intends to secure. Hackers access computer systems through falsified credentials, [8] they steal data while others sell data for profit to those who exploit stolen data to gain unauthorised access to credit card, banking and brokerage accounts.[9] Hackers commit offence of unauthorised access and then they steal personal information and data. Core element defining cyberspace identity theft is unauthorised access falls into (i) harmful intent (ii) resultant harm. [10] Such requirements need proof of intention to commit serious offence such as cyberspace identity theft. Focus of unauthorised access in United Kingdom position is on an intent of perpetrator and unauthorised access to restricted data. Restricted data is data which is subject to password protection which occurs in cyberspace identity theft offences where personal data is stolen by hackers. Since personal details are protected, this offence is punishable in United Kingdom as it does not create incentive for users to place some form of access restrictions on their data but users must place restrictions to achieve legal protection.[11]

Such requirement discriminates unfairly against those who do not employ security system. Further, some offences such as cyberspace identity theft may encounter difficulty about punishment when data required to be restricted. Such requirement is more discriminatory in the context of cyberspace identity theft where steps taken to protection against threats may be beyond ordinary users and may bring different challenges for users. There is no need for such a requirement to be protected in United Kingdom, although it encourages users to take more rational steps in protecting their personal data from unauthorised access.[12]

Law and contract are means through which authorisation to access computer may be restricted. Regulation by former is technical barrier such as requiring username and password to access an account. Regulation by contract subjects access to terms and conditions whether formal, informal, express or implied. Interestingly physical element (*actus reus)* consists in causing computer to perform any function with intent to secure access and appears not to be limited to actual accessing computer.[13] Section 17 (5) of Computer Misuse Act 1990 states that any kind of access by any person to any program or data held in a computer is unauthorised if he/she is not entitled to control access of kind in question to program and data and he/she does not have consent to access by him/her to program and data and he/she does not have consent to access by him/her.[14]

---

[8] S. Shackelford, 'Computer-Related Crime: An International Problem in Need of an International Solution' (1992) 27 *Texas International law journal*, p 489.

[9] K. Raymond Choo, Organised crime groups in cyberspace: A typology, (2008) 11 (3) *Trend in Organised Crime*, p 280.

[10] *North Texas Preventive Imaging LLC v Harvey Eisenberg MD WL* 1996 1359212 (CD Cal, 1996) 13.

[11] Scottish Law Commission, Report on Computer Crime, Final Report, No. 106 (1987) [4.15].

[12] H. Abelson, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption', (1997) *Colombia university academic common*, http://hdl.handle.net/10022/AC:P:9130 (11 December 2013).

[13] D. Orme rod, *Smith and Hogan Criminal Law*, 1st Edition, Oxford Publication, 2008, United Kingdom, p725.

[14] T. Elbra 'A practical guide to the Computer Misuse Act 1990' (1994) 37 *A T H Smith Property offences*, p 362.

Unauthorized access covers data and programs where they are deemed accessed even if authorised. Access to data and programs may be after an authorized access and not limited to initial access to computer and encompasses all possible acts done on or to a computer. Any input to a computer with unauthorised access, if it is accompanied with relevant intent and causes that computer to function at some level qualifies as unauthorized access.[15]

Required mental element (*mens rea*) is that perpetrator must cause a computer to perform a function with purpose to secure access to any program or data held in any computer, considering that he/she knows that access intends to secure is unauthorised. There is no need that intention be directed at any program or data or a program or data which is held in any computer. [16] Unauthorised access to computer systems create huge opportunity for inflicting damage to computer data and programs. Unauthorized access to computer material would include (i) using another person's identifier and password without proper authority to use data or program, (ii) alter, delete, copy or move program or data to output program or data.[17] Prosecution must prove that defendant has intention to secure access and knowledge that was unauthorised although intention of defendant to access any data, program or data held in any computer need not proven.[18]

Hacking is used as a method to commit other crimes such as theft of identity on cyberspace. Hackers often target places where personal data can be stored and then attempt to gain information from computer to carry out more serious offences. Hackers breach databases to steal data but it is impossible to determine whether hacker stole personal information or other files that do not have personal data. Even if evidence is secured that hackers accessed personal information, it is impossible to determine and prove. An attempt to access is sufficient ground to prove unauthorised access for prosecution. Hacking occurs if someone uses another person's username or identifier (ID) and password without proper authority to access data or a program or alters, deletes, copies or moves program or data or even sends data to screen or printer or impersonates someone using email, online chat, web or other services. Unauthorised use of personal information has various types of negative effects. Where breaches of security result in cyberspace identity theft, losses could include expenses incurred to restore credit ratings and time expended on that as well as loss of opportunities that bad credit entails. [19]

---

[15] J. Clough, *Principles of Cybercrime*, Cambridge University Press, 1st Edition, United Kingdom, 2010, p 62.

[16] D. Ormerod, *Smith and Hogan Criminal Law*, 1st Edition, Oxford Publication, 2008, United Kingdom, p 726.

Section 1(2) of the Computer Misuse Act 1990.

[17] N. Robinson et al, comparative study on legislative and non-legislative measures to combat identity theft and identity related crime: final report, p 93.

Section 1(2) Computer Misuse Act 1990.

R. Battcock 'Prosecutions under the Computer Misuse Act 1990' *(*1996) 6 *Computer and Law*, p 22.

[19] Meant for hackers who key in passwords randomly in the attempt to secure the correct password.

V. R. Johnson, 'Cybersecurity, identity theft, and the limits of tort liability' (2005) 57 *South Carolina Law Review*, p 255.

An Information Technology Contractor was sacked by the Welsh Assembly for producing fake pay and display parking tickets as well as for hacking into Assembly's computer system on 21 occasions to read sensitive emails. The Court sentenced him to imprisonment for 4 months which was upheld by Appellate Court.[20] An unemployed hacker accessed gold bullion firm's website to obtain names, addresses and tracking numbers of customers to enable his associates to intercept deliveries of gold. He pleaded guilty of conspiracy to steal, unauthorised access to computer and to blackmail hence sentenced to 2 months' jail.[21] An accused police officer trawled police computers to contact sex workers, track down former lover and make 195 checks on Gates head gangster whom he had fallen out with following Christmas day brawl hence sentenced to 255 hours' of unpaid work and ordered to pay costs.[22] Senior internal auditor at Morrisons Supermarket accessed and uploaded confidential personal data, including names, addresses, national insurance and bank details of nearly 100,000 employees to newspaper and data sharing websites. He was found guilty of fraud by abusing position of trust, securing unauthorised access to computer material and disclosing personal data.[23] Teenager going by nickname Narko launched series of crippling global distributed denial-of-service (DDoS) attacks against internet exchanges and services including Spamhaus. He was found guilty on two accounts of an unauthorised act with intent to impair computer operation and sentenced to 240 hours of community service.[24] An adult student at University of Birmingham installed 4 keyboard spying devices to steal staff passwords which he used to obtain access to his examination results and improve grades. He was found guilty under Computer Misuse Act 1990 for an unauthorized access to computer material, intent to commit further offences and for impairing operation of computer hence sentenced to 4 months' imprisonment.[25]

Section 2 of Computer Misuse Act 1990 covers more offences that are serious and include hacking attempts with intends to do harm. Cyberspace identity theft offences are committed through hacking usernames and passwords by unauthorised access which sometimes may not occur at same time. Therefore, an offence occurs if another person's username or identifier (ID) and password are used without proper authority to access data or program. It is also an offence if a person acquires authorization of someone who then uses it later. Cyberspace identity theft offence occurs following hacking which is included under

[20] R v Oliver Baker, Cardiff Crown Court, 2011 [2011] EWCA Criminal, 928.
[21] R v Adam Penny, Kingston Crown Court, 12 September 2016.
[22] R v Neil Hemp sell, Teesside Crown Court, 5 September 2016.
D. Ormerod, *Smith and Hogan Criminal Law*, 1st Edition, Oxford Publication, 2008, United Kingdom, p 726.
[23] R v Andrew Skelton, Bradford Crown Court, July 2015, United Kingdom.
M. D. Goodman, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3 UCLA Journal of Law and Technology http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php (30 November 2014).
[24] R v Seth Nolan Mcdonagh, South Wark Crown Court, July 2015, United Kingdom.
[25] R v Imran Uddin, Brimingham Crown Court, April 2015, United Kingdom.

unauthorised access and when sufficient information on identity is obtained to facilitate identity fraud, irrespective of whether victim is alive or dead.[26]

The United Kingdom does not consider initial access as unauthorized access and only inputs to computer that have intent behind them and result in computer functioning at some level is deemed as such. Cyberspace identity theft follows same path. Also, since unauthorized access covers access to data and programs, focus is on them in cyberspace identity theft even if access authorization is present. Access to data and programs under cyberspace identity theft follows authorized access and is not limited to initial access to computer and the moment data and program are accessed, it constitutes cyberspace identity theft. It encompasses all possible acts done on or to computer. As per United Kingdom legislation, unauthorized access by itself is an offence and even a hacker inputting numbers at random to discover gateways to computer system is liable to prosecution. Merely conducting unauthorized access in United Kingdom is sufficient condition to create liability and this approach is adopted in Computer Misuse Act 1990.

To prosecute unauthorized access in United Kingdom, it must be proven that defendant has both intentions to secure access and knowledge and that it was unauthorized. There is no necessity to prove intention to access any data or program or data held in any computer. Basis of unauthorized access in United Kingdom is *actus reus* of offender and mere intention to have unauthorized access exposes person to prosecution. Broad phrase "cause computer to perform any function" encompasses all possible acts of unauthorized access with computer such as inputting by persons not having such access with intent and causing computer to function at some level.

In Malaysia, Computer Crimes Act 1997 covers unauthorised access to computer materials alongside with other offences in Malaysia. Section 3 of Computer Crimes Act 1997 states that a person is guilty of an offence if he causes computer to perform any function with intent to secure access to any program or data held in any computer access he intends to secure is unauthorised, he knows that he is not authorized to access any kind program or data held in any computer. A person guilty of an offence of authorized access in Malaysia would be liable to RM. 50.000 fine or imprisonment up to 5 years. [27]

Actus reus involves use of computer with intent to secure access to any program or data held in any computer and where access is obtained without authorisation. *Actus reus* is criminal act or unlawful omission of an act and mere criminal thinking is not punishable since every crime requires specific guilty act and

---

[26] N. Robinson et al, comparative study on legislative and non-legislative measures to combat identity theft and identity related crime: final report, TR-982-EC, 2011, RAND Centre, United Kingdom, 2011, p 573.

D. L. Beatty, 'Malaysia Computer Crime Act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law & Policy Journal*, p 352.

[27] A. Abdul Rahim, N. Abdul Manap, *Cyber-Crimes: Problem and Solutions Under Malaysian Law*, Jenayah Berkatikan dengan Komputer, Perspektif Undang-Undang Malaysia, Dewan Bahasa dan Pustaka, Kuala Lumpur, 2004.

D. L. Beatty, 'Malaysia Computer Crime Act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law & Policy Journal*, p 352.

differs from another crime. To have *actus reus* in any unauthorised access, it is required function happens in computer. Therefore, mere physical contact of computer such as looking at computer while it is performing or reading data displayed on monitor will not be considered an offence.[28]

To gain unauthorised access, hacker must enter login procedure that includes identity information and disguise as another in first instance, if victim's computer rejects unauthorised login, hacker has caused at least 2 computers to function, his own and victim's computer. Victim's computer has performed function that rejects hacker's computer. Where hacker attempts to login with requisite intention, he possesses guilty mind. Despite failure of his mission, hacker may have committed cyberspace identity theft by using third party information to access information.[29] Merely knowing information by watching screen is not an offence. In a case between *Oxford v Moss*, facts of the case are that student looked at the copy of university examination paper. The Court held that he was not guilty of theft because confidential information obtained was not of property under section 4 of Theft Act 1968. When hacking occurs, offender is aiming to link his computer to chain of interconnected computers hence he must create trial of evidence leading to accused.[30]

There is difficulty for prosecution to prove that attempt was made with victim's computer by hacker. This will be hard unless victim's computer maintains log off all successful logins. It is more complicated technically to prove source of an unsuccessful login. Computer Crimes Act of 1997 covers cyberspace identity theft crime through hacking, specifically initial stage of gaining unauthorised computer access through identity information.[31]

Interpretations found under section 2 of Computer Crimes Act 1997 is wide to encompass any form of data and program including identity information and personal data. Although, due to rapid changes in technological innovation leaving such essential terms undefined may allow judge sufficient discretion for him/her to manoeuvre when making decision, it may also result uncertainty in law as lawyers may not be able to predict how judge is going to decide which may be detrimental to parties concerned as they will be ensured of the outcome until judge has decided.[32]

Computer includes hardware parts such as processing unit, memory and storage devices. Computers can purely store and work with two numbers, zero and one. In

---

[28] D. L. Beatty, 'Malaysia Computer Crime Act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law & Policy Journal*, p 87. Section 2(5) the Computer Crimes Act 1997.

[29] G. Sadowsky et al, Technology Security Handbook, 2nd Edition, Info Dev Publication, 2003, United States of America, pp 185-190.

[30] [1989] 68 Cr. App. Rep, p183.
Z. Hamin, 'The legal response to computer misuse in Malaysia-the Computer Crimes Act 1997', (2004) 2 *UiTM Law Review*, p 214. R. Rahman. The Viability of the Malaysian Computer Crimes Act in Defining 'Computers' in the Modern Malware-infested Environment, (2013) 1 LNS (A) *Current Law Journal*, lx.

[31] A. Abdul Rahim, N. Abdul Manap, 'Theft of information: Possible solutions under Malaysian law', (2003) 3 *Malaysian Law Journal*, p ci.

[32] United Nation study on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, New York, 2013, p 110.

short, a computer has ability to store information in binary form and execute instruction. Central processing unit of a computer can store few of these numbers at once but can process them very quickly. However, certain parts of computer cannot process or work with these numbers, they can only store them. Computer Crimes Act 1997 provides references to data or programs held in any removable storage medium which is in computer for time being. Personal information must be stolen to constitute cyberspace identity theft hence section 3(2) (c) of Computer Crimes Act 1997 covers data held in any kind of storage that is stolen including personal data. In addition, access to information found or stored in such removable storage medium can only be achieved if it is inserted or in any way connected to computer.[33]

To establish *mens rea*, there must be essential elements of unauthorised access of cyberspace identity theft and they should constitute offences under Computer Crimes Act 1997. It is mental aspect of crime and hacking that leads to cyberspace identity theft. It is basic element constituting criminal liability under Computer Crimes Act 1997. First, there must be intent on part of perpetrator to secure access to any program or data held in any computer. It should be reiterated that this intention can be directed at any computer. Intention of hacker in cyberspace identity theft to gain personal information of others can be directed at any computer but intention must exist. Subject to presumption of unauthorised access in section 8 of Computer Crimes Act 1997, both limbs must be proven to secure conviction. It must be proved that accused who gained access to personal data had knowledge that what he was doing was unauthorised and his act can be punished as a crime of cyberspace identity theft. Mere belief or suspicion is not sufficient for accused to found guilty. Although it may be quite easy to prove reasonable suspicion, it is more difficult to prove knowledge.[34]

Question of authority is generally not difficult to prove when an outsider to a system uses computer or internet to attempt securing access to any program or personal data on system. However, there are problems when perpetrator has partial authority to access system. In this case, access is unauthorised if person is neither entitled to control access and have no consent of person who controls access. To be found guilty, offender must be aware that he is unauthorised in this sense. Question of fact whether individual knew limits of his authority will often balance it. Proliferation of internet within organisations creates potential arena for insiders to secure unauthorised access to programs and data. Disgruntled employees, temporary staff and even happily employed staff may all attempt to read personal information, which is out of their authority to view. It should be noted that it is easier for an insider to gain unauthorised access or to hack personal information for use in other offences. Generally, an insider is behind firewall hence already beyond security measures.[35]

---

[33] M. Cheang, *Criminal Law of Malaysia and Singapore: Priniciples of Liability*, Professional Law Books Publishers, Kuala Lumpur, Malaysia, 1999, p 31.

[34] S. Azmil, 'Crimes on the electronic frontier-some thoughts on the Computer Crimes Act 1997', (1997) 3 *Malaysian Law Journal*, p IX.

[35] S. Perumal, 'Digital forensic model based on Malaysian investigation process', (2009) 9 (8) *International Journal of Computer Science and Network Security*, p 43.

Section 3(3) of Computer Crimes Act 1997 deals with punishment and amount imposed which is maximum sum of RM 50,000 as considered to be too little to act as a deterrent to perpetrators who may cost victims losses worth millions of Malaysian Ringgits. Instead of imposing maximum fine which may not reflect actual gravity of victim's loss, it is suggested that fines imposed on cybercrime offender should be based on extent of victim's losses.[36]

Malaysia strongly believes that computer hacking in its broad sense is a serious problem and can jeopardise future of Multimedia Super Corridor (MSC) if appropriate actions are not taken to address problem of unauthorised access. Further, due to problems of hacking, growth of electronic contracting has also been stifled. Parties to contract reluctant to contract on line due to fear that others would be able to obtain confidential information while transaction is on-line.[37]

Section 4 of Computer Crimes Act 1997 states that an offence carried out with intent to commit fraud, dishonesty or cause injury as defined in Penal Code 1935 or to facilitate commission of such offence is liable to fine up to 150,000 ringgit or imprisonment up to 10 years or both. In case of cyberspace identity theft, accused must have intent to steal personal data to facilitate commission of misusing such personal data then he will be convicted under section 4 of Computer Crimes Act 1997 otherwise not.[38]

It is immaterial whether offence is committed at the same time when authorised access occurs or on any future occasion. This occurs mostly in cyberspace identity theft cases. Unauthorised access to information by hackers is first round in cyberspace identity theft and second round is sin after successful hacking through use of credential information. In a case between *R v Thompson*, the Court held that as soon as perpetrator obtained access to data with intent to modifying it, an ulterior intention is implied although repetition of conduct could not be prosecuted based on theft or obtaining property. [39]

A person is guilty of an offence if he communicates number, code or password obtained from computer directly or indirectly which he is not authorized to communicate. Penalty for this offence is maximum fine of 25,000 ringgit or 3 years' imprisonment or both. [40] Malaysian government wants to create strict liability but does not state anything clearly about intent. Intention of a defendant plays a key role. Under this section, unintentional communication does not constitute intention or *mens rea*. In other words, statement of article does not

---

[36] P. Gendreau et al, The Effects of Prison Sentences on Recidivism, Centre for Criminal Justice Studies, University of New Brunswick, and Francis T. Cullen, Department of Criminal Justice, University of Cincinnati, http://www.prisonpolicy.org/scans/e199912.htm (12 November 2014).

[37] Multimedia Superior Corrider, nurelimtiaz.uitm.edu.my/wordpressfolder-elimtiaz /wp./08/MSC.pdf. (25 October 2014).

[38] Section 4, Computer Crimes Act 1997.

D. L. Beatty, 'Malaysia Computer Crimes Act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law and Policy Association*, p 87.

[39]A. Abdul Rahim, N. Abdul Manap, 'Theft of information: Possible solutions under Malaysian law', (2000) 3 *Malaysian Law Journal*, p ci.

[1997] 1 CSR 311, p 1143-1146.

[40] Z. Hamin, 'The legal response to computer misuse in Malaysia-the Computer Crimes Act 1997', (2004) 2 *UiTM Law Review*, p 220.

distinguish between intentional and unintentional access, as such it seems that legislators have created strict liability to provide preventive measures by not making this distinction between two concepts. Imprisoning of defendant by judge may face some difficulties because applicability or non-applicability of *mens rea* is left to discretion of judiciary.[41]

As soon as unauthorized access to computer system is gained, hackers can alter information, modify programs, obtain passwords and monitor information being used or stored. Such access to and securing personal information is sufficient to qualify as cyberspace identity theft and it is not necessary for data to be removed. Data must be modified through identity thief where personal data of victims have been altered without their realization e.g. a nurse can be found guilty of unauthorized access to personal information of patient which can be used to alter drug prescription in a way that is potentially lethal. Modification to prescription via computer constitutes an illegal act. Cyberspace identity theft occurs in virtual world and it is through unauthorised access that its methods and applications are perpetuated hence applying cybercrime laws to convict hackers convicted of cyberspace identity theft is completely appropriate. In Malaysia, intent is not required to be directed towards any program or data of any kind or computer as intentional unauthorized access to computer constitutes criminal act.

In Iran, unauthorized access differs from traditional crime and is considered crime arising out of computer. It is also known as the most prominent cybercrime which has catastrophic impact. Unauthorized access in traditional criminal code is the same as home desecration or forceful entry into another person's property.[42] Chapter 26 of Islamic Penal Code deals with properties and home desecration. Article 694 of Islamic Penal Code states that whoever breaks into another person's house forcefully or through intimidation is liable to 6 to 36 months' imprisonment".[43] If crime is committed by two or more persons and at least one of them is armed with weapon, penalty imposed is 1 to 6 years' imprisonment.[44]

Article 694 of Islamic Penal Code does not consider whether house is sealed or protected. If someone breaks another person's house forcefully or through intimidation, act is considered an offense.[45] Unauthorized access not only belongs to cyberspace and is made possible through computer systems but also necessitates protected target. Article 729 of Islamic Penal Code is *pari materia* with Convention of Cybercrime 2001. The most prominent computer crime is unauthorised access and considered first step of computer crime which will cause other computer crimes. Cyberspace identity theft begins with unauthorised access by perpetrator for stealing information and data. Article 1 of Computer Crimes Act 2009 and Article 729 of Islamic Penal Code state that whoever commits

[41] D. L. Beatty, 'Malaysia computer crime act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law and Policy Association*, p 355. O.S. Kerr 'Cyber-crime's scope: Interpreting 'access' and 'authorization' in computer misuse statutes', (2003) 78 *New York University Law Review*, p 1596.

[42] K. Shirzad, *Computer Crimes Viewpoints Iranian Criminal Law and International Law*, Beheyne Publication, Tehran, 2008, p 52.

[43] http://www.majlis.ir (10 October 2013).

[44] http://www.majlis.ir (10 October 2013).

[45] I. Goldoziyan, Specific Criminal Law, 2nd Edition, Tehran Publication, Tehran, 2007, p 237.

unauthorized access to computer telecommunication systems or data protected by security measures is sentenced to 91 days to one year imprisonment or fine between 5 million to 20 million Rials or both.[46]

Article 1 of Computer Crimes Act 1990 covers all kinds of cyberspace identity theft crimes while Article 4 of Computer Crimes Act 1990 covers only special kind of cyberspace identity theft involved in espionage crimes. Article 4 of Computer Crimes Act 2009 and Article 732 of Islamic Penal Code state that whoever violates security of computer or telecommunication rules seeking access to secret data is liable to imprisonment from 6 months to 2 years or fine 10,000,000 to 40,000,000 Rials or both".[47]

Article 1 of Computer Crimes Act 1990 applies to systems storing secret data and perpetrator not only intends to violate security measures or gain access to system but specifically intends to gain access to secret data as well.[48] Article 4 of Computer Crimes Act 1990 covers cyberspace identity theft by hacking as it violates secured data which is not in public domain. Iran has criminalized unauthorized access to computers which have security measures as outlined in article 4 of Computer Crimes Act 2009 while in other cases mere unauthorized access accompanied by intent and knowledge is punishable. Perpetrators must have special intent to access security data beyond mere unauthorized access. Article 4 of Computer Crimes Act 1990 is divided into three main parts (i) *mens rea* of unauthorized access, (ii) actus reus of access, and (iii) condition protecting system with security measures.

MENS REA OF UNAUTHORIZED ACCESS

There are several viewpoints on *mens rea* and its elements. Since there is no law on *mens rea* of crime, these cannot be treated as intentional or unintentional crimes where intention or aim of offender is evident. M*ens rea* must be measured against crime defined by legislation. However, it should be known that every crime has its own special material dimension physics of crime which necessitates *mens rea* as well.[49]

Therefore, it can be said that *mens rea* of all intentional crimes consists of three elements (i) general or behavioral intention which is same as cause of crime (ii) specific or ultimate intention which is intention of perpetrator to attain goal (iii) knowledge and awareness of other elements predicted by law for crime including its subject. Awareness of punishment is not enough to form subject of crime and although it can be said that it depends on person's awareness of all conditions, this statement does not comply with objectives of criminal codes. Awareness of

[46] http://www.majlis.ir (10 October 2013).
[47] http://www.majlis.ir (10 October 2013).
[48] M. Rohani, 'Computer Law and Punishment' (2008) 15 (72) *Informatics*, p18.
[49] H. Meir Mohammad Sadeghi, *Crimes against Properties and Possession*, Mizan Publication, Tehran, 1980, p 127.

punishment does not suggest that behavior is crime because otherwise everyone should be required to know crime and its punishment.[50]

This gives credence to material knowledge comprising knowledge of subject. For example, in case of embezzlement, besides taking property and owning it, perpetrator must be aware that property belongs to another party or government, he must be aware quality of property and be aware that he is government employee. Same case applies to perjury where offender must have knowledge. Although it is hard to believe that a person is unaware of his position as an employee or location as the Court, if it is reasonably proved that employee committing embezzlement has been unaware that property belongs to another party or was not aware that he was an employee and committed perjury without knowing that he had to tell truth in the Court that person is innocent. Knowledge is important in identity theft offence. Perpetrator must know that information and data are private.

Based on points it can be said that in case of unauthorized access to data or systems as crime, perpetrator must commit it intentionally although article 1 of Computer Crimes Act 2009 and article 729 Islamic Penal Code state that there is no need for ultimate intention. Hence, access caused by curiosity is same as access aimed to steal or delete data and the only thing that differs is punishment. In other words, as soon as unauthorized access committed by perpetrator, offence would be occurred and following unauthorized access, offence of cyberspace identity theft occurs if perpetrator steal data and personal information. On the other hand, according to article 4 of Computer Crimes Act and article 732 of Islamic Penal Code, violation of security measures, access to system must be unauthorized and offender must intent gaining access to secret data.

Considering relationship between crime and awareness of knowledge it can be said that awareness of system or data belonging to another person should exist and person must be aware that entry into system and violation of rules was unauthorized and not permitted. It should be mentioned that unauthorized access and violation of security measures are different.[51]

ACTUS REUS OF ACCESS

Unlike similar regulations in other countries, Computer Crimes Act 2009 refers to access instead of unauthorised access. Access or ability to utilize system or data is more general than hacking. Access refers to any use of computer or data belonging to another person. Computer or data may be protected or not but hacking refers to an act of gaining access to computer or telecommunication system protected by security measures. System or computer must be inaccessible to public and hacker must break into it through techniques.[52]

[50] I. Goldoziyan, Specific Criminal Law, 2nd Edition, Tehran Publication, Tehran, 2007, p 186.
[51] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 154.
[52] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 150.

In cyberspace identity theft crime, perpetrator cannot reach to data without hacking system and breaking security measures with some specific technique. Therefore, system is protected by security measures. Article 1 of Computer Crimes Act 2009 states that accessing refers to special act of hacking. Access to system or computer protected by security measures is same as violation of security measures violation of security measures leads to unauthorised access which is done by cyberspace identity theft perpetrator. Hence, there is no difference between behavior described in article 1 of Computer Crimes Act 2009 and article 729 of Islamic Penal Code and behavior predicted in article 4 of Computer Crimes Act 2009 and article 732 of Islamic Penal Code deal with violation of security measures. Therefore, gaining access and violating rules of system storing secret data is considered material invasion and a crime.

Access means owning and if perpetrator steals another person's computer with its software and hardware, it is not considered criminal act unless person breaks into computer. If stolen computer lacks password or other security measures applied by most personal computers. Article 1 of Computer Crimes Act 2009 does not apply to it even if system is broken.[53] However, if perpetrator demonstrates other behaviour such as data sabotage or distribution of personal information then another crime is committed which is totally different from cyberspace identity theft.

Unauthorized access is prohibited by legislation and thus perpetrator ignores prohibition by conducting action. Hence, it is considered crime when it is committed and not at point when it has not been carried out. In this regard, commission of crime refers to behavioral reaction of perpetrator unless access is provided without intention.[54] An example is when data is stored in another person's unprotected computer or system. In both cases, person has access to data or in system but does access it. There is, as such, difference between having and gaining access since only latter can lead to crime.[55] Having access occurs by placing data into third computer while gaining access to data is achieved by breaching security measures. Authorised persons usually fall under former category. Similarly, access is an immediate action carried out in seconds and it is irrelevant whether it is access to part or all system.

Access is of utmost importance since it leads to all computer crimes through unauthorised access. In other words, if someone hacks into another person's computer and steals information or transfers data into their own data storage devices or if person spreads computer virus to enter bank system and transfers funds into their account, is it relevant that access is a prerequisite to cyberspace identity theft?

Unauthorized access is not prerequisite to cybercrime such as cyberspace identity theft as other cybercrimes can be committed without such access. E.g. cases in which a person uses his computer system for training in computer fraud or when someone steals or destroys data from an unprotected system. However, since home desecration and stealing houses are considered two independent crimes, if

[53] J. Moradi, 'Crime in Cyber Space' (2007) 18 (87) *Informatics*, p 28.
[54] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 152.
[55] M. H. Dezyani, 'Computer Crime' (2007) 18 (87) *Informatics*, p 68.

unauthorised access is followed by other crimes, it is considered an independent crime and multiple offences are considered. Similarly, unauthorised access is a behavioral crime and is thus considered crime regardless of its sign or consequences. [56] Therefore, in Iranian context, if unauthorised access is accompanied by other crimes such as cyberspace identity theft, offender is charged with two crimes and subsequent criminal behavior cannot be considered result of access. In other words, unauthorised access is not considered as a precursor to another offence but is treated as complete crime by itself. Thus, under Iranian regulations, criminal would be convicted of two crimes if theft occurred because it originated through unauthorised access. In short, perpetrator is convicted of two crimes (i) unauthorized access, and (ii) cyberspace identity theft.

CONDITION PROTECTING SYSTEM WITH SECURITY MEASURES

Computer security measures are technical and include using firewalls, passwords, encryption, and even concealing codes. Evidently, these methods do not cover physical and human measures. As such, introducing oneself as head of a bank or office to gain access to bank or office computer systems, obtaining key to another person's room and accessing person's computer or placing a computer in a closet or safe before system is protected by security measures is not considered unauthorized access which is subject of article 1 of Computer Crimes Act 2009 and article 729 of Islamic Penal Code.

Computer systems are not different from an automobile or bag where viewing contents of bag and watching car of another person are not considered crimes. Moreover, if someone picks book of another person and reads it, he has not committed a crime but if system or data owned by another person is protected, it is evident that owner would not be agreeable to intrusion and breaking into such a system or computer is akin to property desecration. Cyberspace identity theft offence would not only be occurred with just watching personal data and information by perpetrator but also data must be used for special purpose.[57]

Unauthorised access to another person's computer system is not only associated with use of technical knowledge as offender must also breach security measures. However, technical knowledge and violation must be applied to data or systems instead of users or owners through actions to qualify for cyberspace identity theft. Hence, if someone breaks into system through non-technical ways e.g. social engineering which is form of verbal deceit of user or owner of another system to use it, that act is not considered unauthorised access.[58] Similarly, if deception is committed through sending of spam or by securing passwords to access system of deceived person, it is not considered crime of unauthorised access. This is because

[56] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 152.
[57] H. Meir Mohammad Sadeghi, 'Viewpoint on Computer Crime', *Andishe*, April 2011, p 12.
[58] K. Shirzad, *Computer Crimes Viewpoints Iranian Criminal Law and International Law*, Beheyne Publication, Tehran, 2008, p 97.

no security measure is violated. However, in cases where finding, stealing or getting password from owner and using it to access a system, question is whether this constitutes unauthorized access. Same situation applies when system owner leaves password where it can be seen and it is used by others to gain access to system.[59]

If unauthorized access is measured by behavior of perpetrator i.e. gaining access by violating security measures, it cannot be said that system password is found by someone who has used it to enter system. As per article 1 of Computer Crimes Act 2009, this is not considered unauthorized access, as "system has to be protected by security measures". Hence, offender uses technical means to access protected system because if password was readily available, there would be no need to violate security measures. If unauthorised access is measured by protection of crime subject support for secrecy or another system, lack of security measures is stressed. In any event, since person uses password to ignore measures, access is considered a crime. Accordingly, even previous example of social engineering is an instance of unauthorised access. In this case, unauthorised access is more general than hacking because latter is carried out with technical methods but having access to system passwords and usernames of a system does not require act of hacking.[60]

Seemingly, measures for supporting subject crime is more in compliance with basics of criminal law. Article 2 of Computer Crimes Act 2009 and article 730 of Islamic Penal Code state that access to any protected system is prohibited. It is obvious for legislation that through unauthorised access any further offence can be committed. Selling, distributing or exposing passwords or any other data that enables unauthorised access to computer or telecommunication data or systems owned by others will attract penalty of 91 days to 1 year's imprisonment or fine 5,000,000 to 20,000,000 million Rials or both. Therefore, even when someone knows another person's password and uses to enter a system, crime of unauthorised access is committed. Then, perpetrator can enter to victim's account and steals his/her personal data. System or data security measures should be adequate and efficient otherwise condition of 'protected by security measures' is not met e.g. if someone saves his password and username in his mailbox and it is possible to read them by entering initial characters or if upon loading web page, mailbox of another person is shown on the screen, condition of security measures is not met. Therefore, it is same as displaying information to the public.[61]

Violation of security measures may be accompanied by commission of crimes e.g. unauthorized access is committed if someone spreads harmful software to break into security and gain access to system.[62] Although spread of virus may lead to elimination of security measures such as passwords and leaves system exposed, access must be by someone who spreads virus to remove security measures or at least agrees to spread a virus so that another person can hack system. Therefore, if someone enters system exposed because of virus, issue of unauthorised access

[59] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 152.
[60] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 153.
[61] A. Khoram Abadi, *Computer Crime*, PhD thesis, University of Tehran, 2008, p 96.
[62] J. Moradi, 'Crime in Cyber Space' (2007) 18 (87) *Informatics*, p 7.

does not arise. It is worth mentioning that removing security measures by spreading virus and accessing system involves three crimes (i) spreading harmful software (ii) data sabotage password (iii) unauthorized access.[63]

Ways of protecting systems and data differ. Latter can be protected using passwords, encryption or concealment. In cases where system is broken through violation of security measures and data security is compromised two identical crimes are committed and magistrate may increase punishment although article 47 of Islamic Penal Code limits charge to one crime only.[64]

Use of proxy to load websites filtered banned by government is not considered violation of security measures or unauthorized access, reason is that unauthorised access to system is considered a crime to maintain system secrecy but filtered websites that are exposed to public are same as spam that are filtered. While security measures are aimed at supporting personal data and systems, filtering seeks to protect users against harmful contents. In other words, filtering is not a security measure to protect information or system. It is a mean to prevent citizens from accessing public information and contents. Hence, penalty for any violation in this regard is not like subject crime under article 1 of Computer Crimes Act 2009 and article 729 of Islamic Penal Code.

Since too much filtering conflicts with freedom of information and since use of proxy anti-filter software is same as using means of crime, it is not considered a crime or a blamable behaviour. Moreover, in Computer Crimes Act 2009 or other laws covering crimes, use of proxy is not addressed as a crime. Therefore, there are no legal rules to deprive citizens of their freedom.

CONCLUSION

Cyberspace identity theft occurs through hacking. It involves stealing personal data through unauthorised access and using information for variety of illegal purposes. Those involved can be charged for deliberately accessing computer data without authorisation. It is easy to prosecute cyberspace identity theft that is conducted through hacking. All three jurisdictions: United Kingdom, Malaysia, and Iran have very broad laws on unauthorised access, hacking and treat them as criminal acts.

Cyberspace identity theft is accompanied by hacking where element of access is present and information so secured is used for illegal purposes that benefits perpetrator of crime. Countries need broad provisions in laws addressing such unauthorised access and hacking to enable effective prosecution to counter these illegal acts. Globally, nations must take necessary steps to address this issue. Malaysia's Computer Crimes Act 1997 is a step in right direction although its general cyberspace identity theft legislation could be strengthened further such as to apply same legal provisions as in United Kingdom to cover all related offences. Iran's Computer Crimes Act 2009 is somewhat narrow as it limits scope of such

[63] H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010, p 153.
[64] http://www.majlis.ir (10 October 2013).

crimes compared to United Kingdom where unauthorised access is so wide as to cover all kinds of crimes. As per Iranian Act, securing unauthorised access using spam messages is not included in illegal activity. Further, Iranian legislation leans more towards strengthening computer security measures and as such does not recognise exceeding unauthorised access. Generally, Iran's legislation on computer crime is limited in scope and does not cover all its various aspects. In addition, it limits enforcement and penalties for unauthorised access by focusing on concept of "protected computer" or "security measures" compared to other jurisdictions like United Kingdom where such offences are more easily prosecuted as they do not involve computer security aspects.

In Iranian legislation, hacking is termed purely as an access whereas in other countries act is identified as an unauthorised access. In United Kingdom and Malaysia, legislators have put in place specific laws that treat unauthorised access as computer crime while in Iran, computer crimes are based on criminal code, although definition of computer crime is not to be found in the code. These deficiencies are required to be corrected to prevent increasing incidents of hacking in cyberspace identity theft in United Kingdom, Malaysia, and Iran.

ACKNOWLEDGEMENT

Associate Professor Dr. Mohamad Rizal from Faculty of Law, National University of Malaysia contributed towards completion and publication of this treatise thus his contribution in this regard is highly appreciated and acknowledged.

REFERENCES

A. Charlesworth, 'Legislation against Computer Misuse: The trials and tribulations of the UK

Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010.

A. Khoram Abadi, *Computer Crime*, PhD thesis, University of Tehran, 2008.

ComputerMisuseAct1990' (1993) 4 (1) *Journal of Law and Information Science*.

Computer Misuse Act 1990, United Kingdom.

A. Abdul Rahim, N. Abdul Manap, *Cyber-Crimes: Problem and Solutions Under Malaysian*

Law, Jenayah Berkatikan dengan Komputer, Perspektif Undang-Undang Malaysia, Dewan Bahasa dan Pustaka, Kuala Lumpur, 2004.

A. Abdul Rahim, N. Abdul Manap, 'Theft of information: Possible solutions under Malaysian law', (2003) 3 *Malaysian Law Journal*.

Convention on Cybercrime, 2001, Council of Europe.

Computer Crimes Act 1997 Malaysia.

D. Ormerod, *Smith and Hogan Criminal Law,* 1st Edition, Oxford Publication, 2008, United Kingdom.

D. L. Beatty, 'Malaysia Computer Crime Act 1997 gets tough on cyber-crime but fails to advance the development of cyber law', (1998) 7(2) *Pacific Rim Law & Policy Journal*.

DPP v McKeown, DPP v Jones [1997] 2 Cr App R, 155.

G. Sadowsky et al, Technology Security Handbook, 2nd Edition, Info Dev Publication, 2003, United States of America.

H. Meir Mohammad Sadeghi, 'Viewpoint on Computer Crime', *Andishe*, April 2011.

H. Alipor, *Information Technology Law*, Khorsandi Publication, Tehran, 2010.

H. Abelson, 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption', (1997) *Colombia university academic common*, http://hdl.handle.net/10022/AC:P:9130 (11 December 2013).

H. Meir Mohammad Sadeghi, *Crimes against Properties and Possession*, Mizan Publication, Tehran, 1980.

I. Goldoziyan, Specific Criminal Law, 2nd Edition, Tehran Publication, Tehran, 2007.K. Shirzad, *Computer Crimes Viewpoints Iranian Criminal Law and International Law*, Beheyne Publication, Tehran, 2008.

J. Clough, *Principles of Cybercrime*, Cambridge University Press, 1st Edition, United Kingdom, 2010.

J. Moradi, 'Crime in Cyber Space' (2007) 18 (87) *Informatics*.

K. Raymond Choo, Organised crime groups in cyberspace: A typology, (2008) 11 (3) *Trend in Organised Crime*.

K. Shirzad, *Computer Crimes Viewpoints Iranian Criminal Law and International Law*, Beheyne Publication, Tehran, 2008.

Law Commission Working Paper No. 186 *Criminal law: Computer misuse*, 1989.

Multimedia Superior Corrider, nurelimtiaz.uitm.edu.my/wordpressfolder-elimtiaz /wp./08/MSC.pdf. (25 October 2014).

M. Rohani, 'Computer Law and Punishment' (2008) 15 (72) *Informatics*.

M. H. Dezyani, 'Computer Crime' (2007) 18 (87) *Informatics*.

M. D. Goodman, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3 UCLA Journal of Law and Technology

M. Cheang, *Criminal Law of Malaysia and Singapore: Priniciples of Liability*, Professional Law Books Publishers, Kuala Lumpur, Malaysia, 1999.

M. Wasik, 'Law reform proposals on computer misuse', (1989) *The Criminal Law Review*.

N. Robinson et al, comparative study on legislative and non-legislative measures to combat identity theft and identity related crime: final report, TR-982-EC, 2011, RAND Centre, United Kingdom, 2011.

North Texas Preventive Imaging LLC v Harvey Eisenberg MD WL 1996 1359212 (CD Cal, 1996) 13.

O.S. Kerr 'Cyber-crime's scope: Interpreting 'access' and 'authorisation' in computer misuse statutes', (2003) 78 *New York University Law Review*.

P. Gendreau et al, The Effects of Prison Sentences on Recidivism, Centre for Criminal Justice Studies, University of New Brunswick, and Francis T.

Cullen, Department of Criminal Justice, University of Cincinnati, http://www.prisonpolicy.org/scans/e199912.htm (12 November 2014).
R v Adam Penny, Kingston Crown Court, 12 September 2016.
R v Neil Hemp sell, Teesside Crown Court, 5 September 2016.
R v Andrew Skelton, Bradford Crown Court, July 2015, United Kingdom.
R v Seth Nolan Mcdonagh, South Wark Crown Court, July 2015, United Kingdom.
R v Imran Uddin, Brimingham Crown Court, April 2015, United Kingdom.
R. Rahman. The Viability of the Malaysian Computer Crimes Act in Defining 'Computers' in the Modern Malware-infested Environment, (2013) 1 LNS (A) *Current Law Journal*.
R v Oliver Baker, Cardiff Crown Court, 2011 [2011] EWCA Criminal, 928.
R. Battcock 'Prosecutions under the Computer Misuse Act 1990' *(*1996) 6 *Computer and Law*.
S. Perumal, 'Digital forensic model based on Malaysian investigation process', (2009) 9 (8) *International Journal of Computer Science and Network Security*.
S. Azmil, 'Crimes on the electronic frontier-some thoughts on the Computer Crimes Act 1997', (1997) 3 *Malaysian Law Journal*.
S. Shackelford, 'Computer-Related Crime: An International Problem in Need of an International Solution' (1992) 27 *Texas International law journal*.
Scottish Law Commission, Report on Computer Crime, Final Report, No. 106 (1987) [4.15].
T. Elbra 'A practical guide to the Computer Misuse Act 1990' (1994) 37 *A T H Smith Property offences*.
United Nation study on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, New York, 2013.
V. R. Johnson, 'Cybersecurity, identity theft, and the limits of tort liability' (2005) 57 *South Carolina Law Review*.
Z. Hamin, 'The legal response to computer misuse in Malaysia-the Computer Crimes Act 1997', (2004) 2 *UiTM Law Review*.
http://www.lawtechjournal.com/articles/2002/03_020625_goo dmanbrenner.php (30 November 2014).
http://www.majlis.ir (10 October 2013).
[1997] 1 CSR 311, p 1143-1146.
[1989] 68 Cr. App. Rep, p183.
[1988] 2 WLR, p 984.