ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (403-409), Month: January - March 2015, Available at: www.researchpublish.com

Hacking Between Security, Law and Religion

Ahmed Mohamed Mahmoud[1], Fatimetou Zahra Mohamed Mahmoud[2]

[1,2] International Islamic University Malaysia, School of Information and Communication Technology, Jalan Gombak, Kuala Lumpur 53100, Malaysia

Abstract: **Sources of Islamic law are the Qur'an and Sunnah and diverging from sources and assets linked to them, which is defined in the books of the assets and the Quran and Sunnah as contained in the text and provisions, came with an inherited great deal of accuracy and precision and general principles and rules prescribed, making all of this a valid law for anytime, anywhere, can accommodate for each evolution and evolve life in the shadow without any interruption or an awkward or tight. In contrast, it kept the balance for the human to build and configure and meet the demands of his life in an integrated form a clear and flexible.**

Keywords: **information technology, Islam, Ethics, Hacking, Criminals, Law.**

1. INTRODUCTION

When we talk about ISLAM we talk about a great thing, a great religion or let we say a great system created by ALLAH s.w.t for the humanity to guide them to the right way. Whereas this religion or system sent to the prophet Mohammad PBUH to inform people about it and apply it. WhileIslam created for anytime and anywhere and everything and that what we can call it **SHOMOLEYET AL'SHARI'A AL'ISLAMIYE**Totalitarian Islamic Way. From that Islam came to fix many things in humanity's life and one of that things and very important thing is **AL'AKHLAQ (ETHICS)** as prophet Mohammad PBUH said:

"I have been sent to perfect good manners" {MALIK}[1]

While one of the features that a Muslim should be characterized by is a prevent damage or malignancy in all its forms and manifestations for the people, and this damage imagined its presence in each section of the transactions and dealings between people, which is a great benefit and a great interest base, it is not permissible for a person to harm himself or for someone else, and may not be offset the damage by doing what can damage others.

We talked about **ETHIC** what about **Security**? IS there anything in AL'SHARI'A AL'ISLAMIYE about it?

Yes, There is. ALLAH s.w.t demonstrate us how to protect ourselves from our enemies as what happened in the story of DHU AL-QARNAYN while he helped that people by building a wall between them and GOG and MAGOG.

﴾**They said، "O Dhul-Qarnayn, indeed Gog and Magog are [great] corrupters in the land. So may we assign for you expenditure that you might make between us and them a barrier?"**﴿ [2]

AL-KAHF 94

Whereas now it is an important kind of security so-called firewall and it is the first thing of security it install in any system.

Furthermore, when we talk about Security we must talk about **Hacking** or **Spying**. While ALLAH s.w.t shows us how he protects information or knowledge from the heavens from spying by Shaytan or Jinn. And it happens by attacking them with light. It explains to us more and more that all what we have here in the new technology or IT all has been explained from ALLAH s.w.t in Quran.

﴾**And We have certainly beautified the nearest heaven with stars and have made [from] them what is thrown at the devils and have prepared for them the punishment of the Blaze.**﴿[3]

Al-mulk 5

Also, Mohammad PBUH talked about SPYING (TAJASUS). Whilethe protection of individual privacy become a controversial issue today. The problem become bigger than a person who spy and break the privacy of another it expanded to be an act of organisation and government also. Many corporations are demanding now to protect the user rights.

Islamic Shar'iah respect the privacy of any person and come with a clear and crucial rules since long years ago about spying and breaking privacy. As Prophet Mohammad PBUH said:

"Beware of suspicion, for suspicion is the greatest falsehood. do not try to find fault with one another, do not spy on one another, do not vie with one another, do not envy one another, do not be angry with one another, do not turn away from one another, and be servants of Allah, brothers to one another"[1]

Bukhari (6064) and Muslim (2563)

And in the Aya below we have a clear prohibition to not spy on each other so the Quran determine the controversial issue.

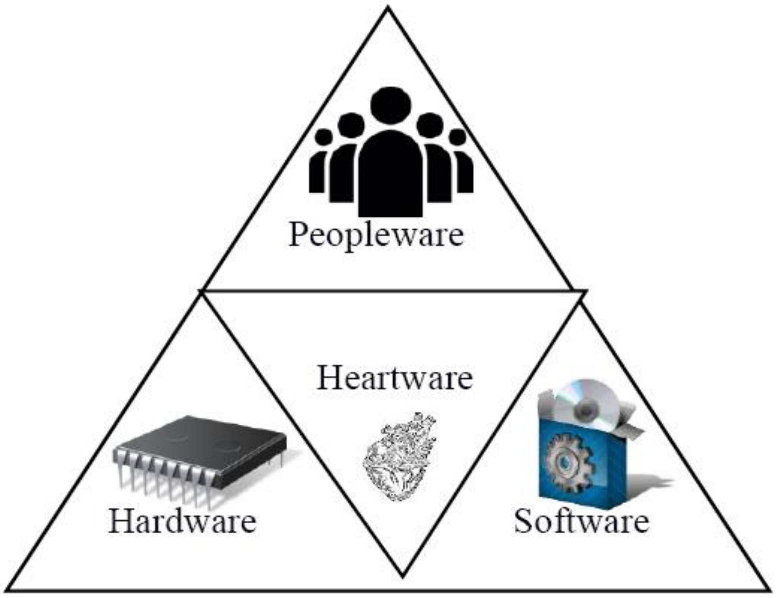
﴾**O ye who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it...But fear Allah: For Allah is Oft-Returning, Most Merciful**﴿ [4]

Al-Hujurat 12

2. ICT AND ISLAM

Let we talk more about ICT in Islam. All of that talking about our normal life, what about our virtual life or so-called virtual world or IT? Are all of that rules applying on it? And if we want to talk about spying in the virtual world. Does it exist? What is so-called?

ICT must not only consist of the Hardware and software, but also the Peopleware and its Heartware[6].



Technology as mentioned before not just Hardware and Software, but also Heartware and Peopleware while when you use Technology there are many things and rules you must understand well. You are not alone in the virtual world you are with other people as same as in the real world and we have to apply what our prophet Mohammad PBUH said about ETHIC and to use this technology with that people to benefit UMMAH and that what we so-called Peopleware. What about Heartware? It is the most important thing while it is the controller between you and others and between you and ALLAH.

Thus, you should be careful with your acts because it can guides you to the right way it is also can guides you to the wrong way.

Hence, it shows that Akhlaq should be highlighted as the most important element in all phases of human life. In making any decision, man must consider whether or not his/her decision is aligned with the Islamic ethical values. The concept is similar to the principles in ICT. Any decision for ICT implementation must not create gaps and injustice or abusive acts [6].

Nowadays people worldwide are too much related to technology such as the computer and internet to accomplish their work or to communicate and it is what created the virtual world. Actually internet and other technologies are like a double edged sword that's why these technologies constitute a real danger against people today which is caused by cybercrimes and especially spying or hacking. Hacking in his different forms is used by governments, organisations and people for many reasons which can be doing with agood intention or bad intention but regardless to the reason behind this act the only certain thing is that those hackers hack and they are hacked back tooand the result is that we are living in an insecure world. Indeed in Islamic world the situation is not too much different from others, all people everywhere are suffering from hacking. But our Islamic religion and shar'iah contains a solution for all issues or problems that can face humans in their life. So in this context this document is to expose what is hacking in its different forms which can harmfully destroy the security and privacy of others and to show how this issue can be resolved by religion (Islamic shar'iah) and hacker can employ his ability curiosity and computer knowledge in an ethical way without breaking laws.

Consequently, we can say that Spying is exist even in the virtual world and with different names such as: HACKING. Furthermore, the Islamic law or Islamic shar'iah is applied on it.

We know now what is hacking. What are its types?

3. TYPES OF HACKERS

Hacking can be considered as the brainchild of curiosity. Hackers are a computer enthusiasts and people who have a goodand deep knowledge in programming languages, computer systems and networks. But like most things especially in technology this skill and knowledge can be used for a good or bad purpose. hackers target can be simply to satisfy their self-arrogance and it represent a challenge for them to break the unauthorized and prohibited systems security, while others can do for amusement not with an intension to harm or to damage to computer or it can be to gain money.

Hackers can be divided into two groups that follow the same steps and use same tools but with an opposite aim and intension. Those groups are the criminal hackers and ethical hackers.

3.1Criminal hackers:

Criminal hackers of cyber world called also malicious hackers, intruder or cracker they represent the dark side of hacking. Those hackers use some techniques and their knowledge in the computer software and programs by the penetration of some software such as malware or spyware to be able to break the security system of an enterprise and steal their important information's to treat them and gain money.

Actually there is many types of criminal hackers which use many methods for many harmful purposes.

3.1.1 Types of criminal hackers:

There are four different types of criminal hackers who have various capabilities and efficiencies: script kiddies, technically astute hackers, sophisticated and malcontent insider attackers.

- **Script kiddies**: it's a type of hackers without skills or any deep experience or knowledge in programming or attacks. They use a ready scripts and programs developed by other people to attack some computer or systems.
- **Technically astute hackers**: they are a group of hackers who possessed a high level of experience and knowledge in programming, security systems, and know who to collect information's and hack their target.
- **Sophisticated**:they represent the most dangerous types of hackers because of their experience on uncountable types of programming and systems and optimize their skills to not left any trace when they do any hack or offence. In fact they represent the real enemy and challenge for the security team in any organisation.

- **The malcontent insider attackers**: He can be an employee in an organisation who is malcontent of his chief in work. So he not necessary have a good knowledge in hacking but he steal information's from the organisation which can allow him to harm the enterprise.

3.2 Ethical hackers:

Ethical hackers or called also red team they can be defined as it technicians or a security consultant for a business project, so the ethical hacker can be considered as a part and contributor in the staff of knowledge of network security. Ethical hackers can be paid by organisation to hack their systems and discover the weaknesses and vulnerabilities in security system and fix them to protect the organisation from any expected hacking from criminal hackers. Indeed ethical hacker use his capability and knowledge in a good way to repulse the malicious hackers by the protection of network, business and system security from their unexpected attacks.

3.2.1 Benefits from ethical hacking assessments and his role in the enterprise security architecture:

Many organisations today are threatened because of hackers so they should adjust their security system and policies according to that. The enterprises face a real challenges because of the complexity of security requirements caused by the developing of the hacking ways. Here come the role and the necessity to have ethical hacking as a part of it and security staff in any organisation. The ethical hacker can do an objective analyse assessment to extract the vulnerabilities hidden in the security system. So this can economize and safe a lot of money that an organisation can lost because of hacking and the most important is the private information that they can lose by a simple attack by a criminal hacker. In some cases some organisation chooses to use an automated testing tools to know their level of security but they forget that this programs are not able to detect all the vulnerabilities and analyse the situation.

We talked about HACKING, SPYING in Islam and IT, but what about them in our social terms???

In social terms we find that hacking affect negatively on our social. In instance, Malaysia is one of countries that suffer from Cybercrimes that continue to rise.

Cybercrimes continue to rise and have become one of the modern problems that threaten public security and economy of the country. These activities will continue to increase if no effort is taken to reduce or to prevent them. Many countries have made efforts to prevent these ‘diseases’ from spreading but total prevention seems to be impossible. Nevertheless, this does not deter Governments and other organisations from continuing their efforts to reduce such crimes from spreading to broader levels of society. One of the efforts taken by the Government of Malaysia has been to introduce cyber legislation and regulation. This paper discusses these efforts followed by an analysis of the application of cyberlaws and how the laws work together with the traditional laws in combating the threats of cybercrimes[7].

Therefore many efforts taken by the Malaysian government to stop this kind of crimes that make people losing their money and worry about their information that can be hacked.

While this kind of crimes increased approximately 90% from 2010 to 2012 where about 6586 reports of such cases were lodged in 2012 with RM34 million incurred in losses compared with 6238 cases involving RM18 million in 2010[8].

What about security let us now talk also about it with more details but in our new world (IT).

4. SECURITY AND PRIVACY

It's the nightmare that pursues everyone whether people, organisation and even governments.

4.1 Different types of attacks:

The hackers have usually 6 types of attacks to pierce their target, so the knowledge and awareness of those methods can help to prevent them.

- **Backdoors**: it's an unauthorized way to gain access to a program, internet services or a computer system but it appear like a normal certification. Backdoor can be a placed program or an adjustment of existing programs or hardware devices rootkit is an example of backdoors.

- **Denial of service attack**: in contrast to other methods, denial of service intended to totally break and paralyse the system by making it unusable. It's a kind of attacks on the networks through drown it by unimportant data and messages in order to prevent them from working. Many of these attacks exploit errors and bugs in TCP/IP protocol to do disruptive things.

- **Direct access attack**: it can be done if somebody acquired access to the computer or system, he can do modifications in the security system, also can implement a listening programs or steal data.
- **Eavesdropping**: it represent the stealthily listening to private conversations between stewards on a network.
- **Exploits**: it's a piece of software, data, or a range of commands that exploit and benefit from a bug or vulnerability in the system with a view to cause unintended or unexpected action to occur on computer software or hardware. Such action comprises things like gaining control of a computer system or a denial of service attack.
- **Indirect attacks**: it's an attack initiate by a third side where someone use a computer of another person to emit an attack. So it becomes so difficult to identify and track down the real attacker.

4.2 Spying and breaking privacy:

The protection of individual privacy becomes a controversial issue today. The problem become bigger than a person who spy and break the privacy of another it expanded to be an act of organisation and government also. Many corporations are demanding now to protect the user rights.

Far of people and government we will talk about a search engine that all people know and it is GOOGLE.

Before we look at the basics of Google hacking, it’s worth considering how this technique turns the usual image of hacking on its head. By and large, hacking consists of a miscreant targeting a specific site, beavering away to discover its weak spots. And Google hacking is indeed useful as a way of foot printing and probing a specific site.

“Go through the code and remove everything that identifies the software, including any HTML comments or meta tags”

But the real danger it poses is bringing your site to a hacker’s attention [9].

All people know and understand the power that Google has. And in same time there are some information and people that are accuse it hacks others. Why?

If it is right, why Google does not try to use its power by helping others to protect themselves by informing them by weakness that they have in their system. And it’s what called ethical hackers that they hack to protect not to destroy.

Furthermore, from Anonymous and LulzSec, through lone individuals to organised cybercrime gangs, hackers are a constant presence in the thoughts of anyone involved in IT security. One way to prevent outsiders from successfully hacking your system is to beat them to the punch – by carrying out penetration testing to find and address vulnerabilities.

On the other hand, what about people that create security system and build security appliances, what their goals? Are they who created hackers? Are they helping hackers?

It is clear that security appliances vendors have been fighting for a share of a rapidly changing market, as evidenced by the flurry of mergers and acquisitions in the appliances sector in 2012 alone. In March 2012, Trustwave bought M86 Security, which itself had previously snapped up Finjan, and in the same month Beyondtrust bought vulnerability management solution provider eEye and Dell acquired SonicWall [10].

So it can help us to understand well that hackers achieve security appliances builders’ goals.

5. HACKING AND LAW

In fact hacking is known as the breaking of laws, but some people opinion is that hackers in some cases should not be punished because yes they break laws but in the same time they are the cause to discover and detect the vulnerabilities in our systems or programs. But others treat hacker as a criminal who deserve to be punished especially when it comes to steal information and threat people or organisation by it and sometimes it threat the reputation of many people. In this order and in this diversity and difference of point of views many countries have placed laws to reduce hacking and breaking privacy in context of social and business ethics, fraud and computer misuse legislation.

5.1 Law in western and non-Muslim countries:

Since 2010 and 2011 many western and non-Muslim countries start to put rules and law to punish hacker's .The United States, Germany and south-Korea are some of the countries who try to insert new laws which are especially concerned in the cybercrimes in order to limit it. For example in India there is no specific identified law against cyber-attacks and the government has failed to protect civil liberties of Indians including privacy rights.

5.2 Law in Islamic countries:

The two countries which take the initiative and starts to emit laws that criminalize the cyber-attacks were Malaysia and Saudi Arabia. In Malaysia there is many cyber laws such as computer crime act 1997, communication and multimedia act 1998, Malaysian communications and multimedia commission act 1998, digital signature act 1998, and electronic transaction act 2006. In Saudi Arabia there is an application of the system of combating cybercrimes which represent a pattern to defining and identify the IT crimes in order to reduce and face it after becoming a real threaten to the security and safety of human societies. This system contain 16 articles which include strict penalties imprisonment of between 1 and 10 years and fines up to five million Saudi riyals.

6. HACKING FROM AN ISLAMIC PERSPECTIVE

Some Islamic studies has done by Muslim expert in religion to relate and show what are the borders that Muslims should respect and put into account when they are using networks.

Ethics is a major thing that Islam take into and give it a huge value and importance because it's the basic and essential thing to build a good society and humans as prophet Mohammad[PBUH] said:

"Nothing will be heavier on the Day of Resurrection in the Scale of the believer than good manners. Allah hates one who utters foul or coarse language.'' [1]

(*At-Tirmidhi*)

"From an Islamic perspective, guiding principles in ICT must be based on Islamic philosophy which is from al-Quran and al Sunnah. Three divisions are derived from the ICT guiding principles, namely: ethics, security and privacy." [6].

6.1 Respectable side of internet world:

6.1.1 The punishment of hacking the respectable side:

This side which is the respectable one it is prohibited to attack it especially if for example a system or network contain a benefit for Islam and Muslims without the opposition of Islamic shar'iah such as educational , economical, governmental , or medical services.

In this case if someone hack a system or account of another one and steal his information or harm him. Actually here this account in the virtual world is considered and has the same rights of property in real world. So the hacker should bring back the account to his owner as Allah s.w.t say:

﴿O you who have believed، do not consume one another's wealth unjustly but only [in lawful] business by mutual consent. And do not kill yourselves [or one another]. Indeed, Allah is to you ever Merciful.﴾

AL-NISA' (29)

In this ayah Allah s.w.t prohibit us to take and to use anything that not own to us without compromise and acceptance of the owner.

6.2 Immoral side of the cyber world:

6.2.1 The judgement of the attack on the immoral side:

This side is the part of cyber world where the network is used in a bad and unethical way, or to gain money illegally. So this part should be banned and blocked but here how to act it depend on the situation and in how much this system is harmful. For example for the sites which are considered as pornographic sites, this kind should be attacked and blocked for the benefit of all people.

Our Prophet Mohammad PBUH said:

"Whoever among you sees a wrongdoing, let him change it with his hand. If he has no enough power to do so, let him (change it) with his tongue. If he has no enough power even to do so, let him (disapprove of it) with his heart; and that is the least degree of faith." [1]**[Muslim]**

In this hadith our prophet Mohammad PBUH demands Muslims to change the bad things in society and to start by their hands which are the more effective way to do changes completely. And here the unethical side of cyber world contain bad things that harm and affect Muslims everywhere and from this context we can start by our hand by the block and closing of those systems.

7. CONCLUSION

Many debates around the world is occur to try to specify what is hacking and hackers, what should be the law towards them and how to deal with them as a heroeswho revealthe vulnerabilities in systems in the way to help us to fix it? Or as a criminals who are trying to steal our security and privacy? We live in an entrusted world where no one today trust to another because of actions of those kinds , governments spy and collaborate all information and data about people and other governments and in the same time they emit a laws to prohibit and punish hackers . So here people become confused and lost the compass leading to the right. But for us as Muslims our religion is the compass that lead us always to the right. Our Islamic religion give us a guidelines to clarify and identify each thing or act in a fair way. The same in the context of hacking where and when we need it and where it should be prohibited and be considered as illegal.

REFERENCES

[1] Al-Hadith

[2] Sahih International. The Holy Quran , 94th verse of chapter 18 (sūrat l-kahf)

[3] Sahih International. The Holy Quran , the fifth verse of chapter 67 (sūrat l-mulk).

[4] Sahih International. The Holy Quran , the twelfth verse of chapter 49 (sūrat l-ḥujurāt).

[5] Sahih International. The Holy Quran ,the 29th verse of chapter 4 (sūrat l-nisāa).

[6] Fauzan, Mohamad. (2013). ICT and ISLAM, 21 - 37. International Islamic University Malaysia (IIUM).

[7] Mohamed, Duryana. (2012). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. 66-74. International Islamic University Malaysia (IIUM).

[8] Bernama, (2012). Cybercriminals scam victims of RM16m in Q1. Bernama. 18 July 2012, http://www.themala ysianinsider.com/ malaysia/article/cyber-criminals-scammed-victims-ofrm16m-in-q1.

[9] Mansfield-Devine, Steve. 2009. Google Hacking 101.

[10] Caldwell, Tracey. 2012. The Perimeter is dead – what next for the appliance?