https://doi.org/10.20943/01201702.3642

Cybercrime in Saudi Arabia: fact or fiction?

Sulaiman Al Amro
Computer Science (CS) Department, Qassim University
Qassim, Saudi Arabia

Abstract

Abstract— Electronic war between states is no less dangerous in its implications and challenges than traditional military war. In fact, it may be even more dangerous, targeting a nation's unity, security, and stability. It may be able to provoke long-lasting discord and division with minimal effort and cost, and thus achieve the goal of multiplying the internal front cohesive spreading lies, and falsifying documents. This would cause confusion for citizens, and lead to a state of weakness and sometimes a decline in freedom of expression, as well as an increase in confrontation and fear, resulting in demands for an excuse or even an explanation of what happened. Cyber-attacks on computers and government agencies' servers may occur through the installation of viruses into computers' operating system. This is a psychological process par excellence; because it has a negative impact in terms of users' lack of awareness of what is happening. This may raise doubts and increase fears, causing a frightening shock if an unexpected result occurs. Attempts could be made to exert pressure and to carry out political blackmail or bargaining in order to obtain further confidential information.

Keywords: *Cybercrime, Saudi Arabia, External attacks, Electronic war, security.*

1. Introduction

Electronic warfare is a threat to everyone; even countries that see themselves as immune to penetration have nevertheless been victims of piracy, and the United States defence ministry has feared a possible electronic attack; there have been some press reports of a breakthrough by US intelligence. Electronic warfare may be used as an alternative to military confrontation to deter adversaries, and to thwart their aspirations and ambitions; this happened with the Stuxnet virus, which damaged Iran's nuclear programme in 2010. A virus that targeted Saudi Aramco was intended to damage the country's economy and the Ministry of Foreign Affairs [6].

Saudi Arabia has faced electronic attacks targeting its unity. Its economy is still facing the worst aspects of this war through-continued repetitive system-sensitive penetration operations, with targets including the National Information Centre, which remains steadfast against multiple penetration attempts. Economic activity has also been targeted, as in the attack on Aramco in August 2012, when virus sabotage delete key files were planted in devices. Phishing emails caused disruption to 30,000 computers, and these attempts lasted for more than a month. Other targets have also been political, with an electronic attack on the Foreign Ministry resulting in the leak of documents that were important for the work of administrative diplomats in many countries, however, the attack on these documents was argued to be a condemnation of the kingdom's foreign policies, which were described in one of the documents. The comments and statements in the documents do not depart from the stated policy of the Foreign Ministry. Some were sent via-mail and fax, and were passed on more than one manager affiliated to the ministry, who did not otherwise carry serious state secrets with them. Many of them originated on social networking sites and were fabrications, or contained content that was out of context. This information has been discovered since these documents first came to light, which suggests that there has been serious fabrication of these documents, which were limited in number and modest in content. Internal opinion was misled more than that on the outside; citizens avoided the publication of any documents that might be rigged, as this could have helped the state's enemies achieve their objectives, as well as being able to access to any site in order to obtain documents. Leaked information may be incorrect and intended to harm homeland security.

It is a responsibility of citizens to avoid the publication of any documents that may be rigged and which could help the country's enemies to achieve their ends. The KSA is one of the most targeted countries in terms of security, unity and independent decision-making. It has fought several wars against terrorism, the protection of borders and national security, or even to correct ideas about violence and militancy. As well as its size and strong economic potential, the country carries religious and political weight, which could make it a target. It is vulnerable to trouble caused by those wishing to influence its stability, which raises several questions. Despite these matters, the Kingdom has successfully led its people out of several crises and there have been many turning points, because loyalty is greater than that obtained one of them, the evidence so many countless.

This all has serious psychological, military and political repercussions, and overcoming electronic warfare requires awareness, confidence, and greater unity. The transfer or transmission of leaked documents must be reduced or blocked. Saudi Arabia is prosperous and people should be partners in the national responsibility for the defence of this country. They should be prepared to make sacrifices and stand behind the government's leadership. Whilst the Politics and Security Council has discussed technical security, a national centre is needed to tackle counter-attacks and to promote the localization of technical positions in government agencies.

However, public awareness also needs government action. The Policy and Security Council, chaired by the Ministry of Interior, has already discussed technical issues relating to security, and continues to disclose and share such advanced steps with wider society. Specifically, financial systems are no less vulnerable to attack than military and security targets. A specialized centre to combat cyber-attacks is preferable to different departments working in isolation. Rather, a national centre should include an elite group of young citizens tasked with exchanging information and experiences as soon as possible. It should act as a reference point for coordination and consultation to serve homeland security, as well as working on the localization of technical positions in government agencies. This should not to be assigned to operating companies. In addition, the further training and qualification of the workforce in advanced research centres around the world should be promoted in order to find out more about the background of electronic warfare, and the methods of advanced penetration. Intelligence is needed to prevent such operations against the Kingdom. Future investigation of everything that might raise the possibility of an attack is needed, specifically at a time when the Kingdom is moving firmly to deal with the issues affecting the region, and has a policy of using multiple opportunities, rather than relying on chance.

Saudi courts have seen a remarkable increase in cases of electronic crime over the past year, dealing with about 776 cases of electronic crimes over the past year. There were 164 cases of electronic crime in Saudi Arabia 2015, a figure that rose to 573 cases last year. The city of Makkah tops the list of areas in Saudi Arabia for the number of court cases of this type, with a total 207 cases of e-crimes in 2015 and 2016. The eastern region had the highest number of e-crimes in 2015 and 2016. In Najran, courts had not dealt with any issues related to electronic crimes over the preceding two years, but have seen 15 over the past year. The court in Tabuk has dealt with e-crime issues for the first time in the past year, presiding over four cases, but had no issues of this type in 2015 [1].

It is worth noting that the Council of Ministers has recently developed a system to combat cybercrime after a study by the Shura Council ordered the emergence of computer crime to be tackled, to identify these offences and to use appropriate penalties to deal with them. The system describes cybercrime as "any act committed, including the use of computers, or the information network in violation of the provisions of this order." The system aims to help achieve information security, preserve the right to the legitimate use of computers and information networks, and to protect the public interest, ethics and morals, and the national economy.

2. Literature Review

Electronic communities have recently suffered from a violation of their right to electronic privacy. The proliferation of cybercrime has occurred alongside developments in computer technology. This has prompted the United States to work carefully to minimize the harm causes by these crimes to individuals through awareness-raising, preventive security and other methods. This should help official and non-official bodies to offer a high degree of protection to their IT systems. Cybercrime is as an act or illegal activity carried out by a group of individuals calling themselves "pirates". This violation is unethical for specific purposes and may cause material or personal loss to victims. The undertaking of this kind of crime over computer networks can penetrate electronic information security, and cause extensive destruction and damage. There are several names for electronic crimes, most notably cybercrime, high-tech crime, and computer and Internet crimes [3]. From the perspective of criminology, information and communication technology and the increasing use of the Internet provide criminals with new opportunities to facilitate the growth of crime [13], as shown in Figure 1.

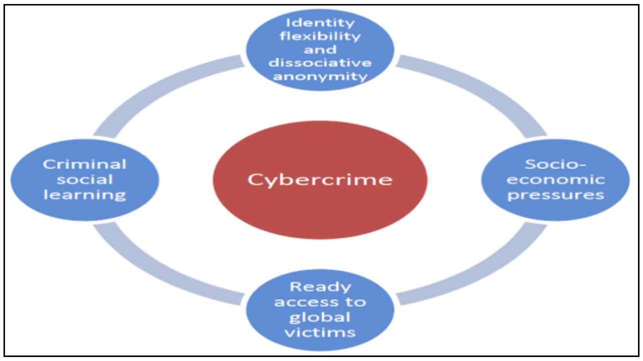
Identity flexibility and dissociative anonymity
Criminal social learning
Cybercrime
Socio-economic pressures
Ready access to global victims

Fig. 1 Possible underlying factors linked to increases in cybercrime [13].

2.1 Types of cybercrimes

Electronic crime targeting individuals, also termed personal Internet crime, may involve illegally obtaining people’s e-mails and passwords, and may extend to identity theft and extracting images and important files from victims' machines to threaten or blackmail them. Crimes against individuals may also occur. In addition, electronic crime targeting property belonging to the government or private individuals focuses on the destruction of critical software files. Malicious software is transferred to the user's computer in several ways, most notably through electronic messages [15].

Electronic crime aimed at governments may involve attacks by pirates on official government sites and systems or networks. It usually focuses on completely destroying the infrastructure of the site or the networking system, and such attacks are often intended to be political. Furthermore, e-political crimes may focus on military targets in some countries to steal information related to state security. The theft of information may be electronically documented and published illegally. Viruses are one of the most prevalent means of e-crime; examples include Trojans, the virus Love 18, and the Sircam virus. Defamation offences have the objective of harming the reputation of individuals. Assaults on finances, extortion e-crimes, preventing access to blocked sites, cyber-terrorism and electronic crimes targeting citizenship also occur.

2.2 The motives for committing cybercrimes

Perpetrators of the cybercrimes seek is a material benefit in order to satisfy their desire to achieve wealth. Personal motives are as follows:

One motive is learning, with the penetration or piracy of a site serving as a practical application of what the criminal learned in beginner piracy. Revenge is considered the most harmful and dangerous motivation for cybercrime. Some criminals may wish to demonstrate their personal and technical capabilities by showing their ability to carry out piracy. Others may be motivated solely by entertainment, and have no particular motives or goals. Some criminals may be politically motivated, and usually target government sites, or those expressing different political opinions [3].

3. Discussion

Specialists in information security estimate that the financial loss experienced by Saudi companies as a result of piracy and electronic sabotage ranges from SR 300,000 to more than SR1 million for each case, with bank losses, estimated at more than a billion US dollars. The head of the Commission for Communication and Information Technology at the Chamber of Commerce in the eastern region and the CEO of "Sahara Net" explain that large companies have been targeted by hackers wishing to leak inside information about their facilities. However, the financial losses caused by the attack on Aramco resulted were not considerable [4]. The Al-Riyadh newspaper reports that anti-hacking experts have been employed by companies to undertake what is termed "good piracy", in which, subject to the approval of the owner of the site, they try to infiltrate mail to the site in order to protect the company and to discover any gaps or weaknesses in the site. These would be closed before any actual attack could occur, thus reducing risks and barring any attempt at piracy, espionage and thefts or breaches of the information systems.

The most prominent economic cyber-attacks faced by the KSA have been carried out externally by hackers from organized groups from Eastern Europe and Russia, in addition to politically motivated pirates from Israel and Iran. Some 70% of breaches experienced by companies and government agencies in the Kingdom are thought to be internal and not linked to outsourcing, with hackers exploiting weaknesses in the sites to penetrate the lack of protection, modernization and continuous supervision [4]. One specialist information security engineer explained that no security software can offer 100% protection to any company or country; all the sites offer opportunities for attacks and thus to varying degrees depend on the strength of protection available and ensuring that any gaps in protection are assessed rapidly and regularly. Cyber-attacks are estimated to have cost the Saudi banks financial losses of more than a billion US dollars, according to a statement from the Committee on Communications and Information Technology of the Shura Council. It noted that four to six out of every 10 people using the Internet have been exposed to electronic attacks. In addition, Saudi banks' losses from cybercrimes amounted to more than a billion US dollars in just two years (2015 and 2016). High-risk groups within Saudi Arabia may be exposed to the risk of cybercrime, according to the Casper Spybot company. Perpetrators penetrating Internet sites in the Kingdom could affect over a million people [2]:

- **What is the actual situation of computer crime in the Kingdom of Saudi Arabia (KSA)?**

Information technology crimes range from eavesdropping on what someone is doing online to the theft of credit card data, and may result in people being threatened or blackmailed. Victims may also experience defamation, and criminals may make an illegal entry in a website to destroy, modify or disable it.

The Casper Spybot company, a specialist in computer protection products, has divided countries into three groups according to their risk of exposure to cybercrime. In the high-risk group, 41% to 60% of Internet users have experienced electronic attacks, compared to 21% to 41% in the medium-risk group, and less than 21% in the low-risk group. According to a report issued in mid-2011, Saudi Arabia falls within the high-risk group, along with several other countries, such as Russia, Iraq, Armenia, Oman, Sudan, Azerbaijan and India.

According to reports from the same company, India accounts for the highest proportion (14.8%) of attacks, while the figure is 1.33% for each of the Gulf Cooperation Council (GCC) states. Saudi Arabia accounts for the highest proportion of Internet crime in the GCC states. However, the GCC countries account for a higher proportion of attacks if the total number of Internet users is considered (141 million users in India and about 17 million in all the GCC countries).

A study of cybercrime in the KSA indicated that 14.2% of Saudi Arabian sites had been infiltrated, compared with 8.9% of non-Saudi sites.

Data show that 15.1% of Internet users in Saudi society have had their e-mail accounts targeted, of whom 11.8% were Saudis and 3.3% foreigners. Bearing in mind that there are about 11 million Internet users in Saudi Arabia, it is alarming that one million people have been affected by cybercrime in the Kingdom.

• Are the existing systems a sufficient deterrent? What are the most prominent disadvantages, and why?

In 2007, the Kingdom issued a Royal Decree No.M/17 to target cybercrime, which defined IT crimes and prescribed punishments for them. Although this is a good system, new Internet crimes occur every day, which requires adjustments to be made to the system to add these new crimes and to prescribe appropriate punishments. For example, impersonation crimes have sprung up recently.

In addition, the Interior Ministry has the role of implementing cybercrime measures, which is extremely difficult due to the difficulty of obtaining digital evidence and linking it to the perpetrators, because of the ease of destroying evidence, or because the perpetrators may live in other countries. Thus, without action to catch the culprits, it remains difficult to implement a suitable system to combat IT crimes.

• Who is responsible for the failure of the system to deal with computer crime?

The system needs periodic adjustments whenever a new type of computer-related crime occurs. Such crimes are experienced by all countries, and in the information age it is essential to enact laws and regulations to tackle them. However, these may be inadequate to deal with such crimes, unless they are accompanied by procedures for obtaining proof of criminality, as mentioned above. The Ministry of the Interior will not be able to trace cybercrime outside its borders without international cooperation, including with other Arab states, to prevent the abuse of e-mail from outside the KSA, and to trace the perpetrators of cybercrimes across international networks.

Regulatory action is also needed to limit, monitor and organize the work of Internet cafés in the Kingdom, as general computing devices in Internet cafés, or intermediary (proxy) devices may be used in cybercrime. Let give the assumption of the Fair Multi-Priority MAC protocol.

3.1 External Attacks

The National Centre for Electronic Security in Saudi Arabia monitors electronic attacks originating from outside the KSA on a number of government agencies and facilities. Some attacks are designed to disable all servers and to target facilities, which has an impact on all the services provided by these facilities. The Saudi Press Agency reports that an electronic attack seeking to capture information about the system planted malicious software to disable the user's data, indicating that the attack targeted several sectors, including the government and the transport sector. On its website, the agency notes that the source of this attack was from outside Saudi Arabia, with several electronic continuous attacks targeting government agencies and vital sectors [5].

The centre sent warnings to government agencies and facilities about for a possible threat to services for the disabled. The warnings included the information necessary to avoid injury or assault. There are several ways to protect users, and technical steps that can be taken to avoid the consequences of the breach. The PCHR recommends following best practices in the protection of electronic systems, particularly with regard to the reduction of remote access via VPN "in the BNP" (VPN) service to access the Remote Desktop "RDB" (RDP). The centre stressed the need to follow best practice used by businesses in various sectors, and the preventive measures that should be followed to maintain and protect the data and systems from potential intrusions using electronic means.

In addition, events in the region affect the security of the Kingdom. In April 2015, during the Saudi-led war against Houthi militants in Yemen, a group of Houthi supporters called the "Yemen Cyber Army" hacked into the website of a Saudi-sponsored daily newspaper, displaying pictures of the Hezbollah chief Hassan Nasrallah and writing in Arabic: "We have a few words to tell you, prepare your shelters" [10]. In May, the same group attacked the mail service of the Ministry of Foreign Affairs, publishing thousands of e-mails that they claimed were "top secret" [11].

3.2 Statistics

Some of the statistics for this type of issue are produced by the Saudi Interpol. E-mail breaches were the most common form of cybercrime, (27%), while child sexual exploitation cases accounted for 14 %, libel and defamation 13%, financial breaches 12%, e-mediated malicious programs 6% and electronic deception and fraud 5%. The proportion of terrorist threats across sites was 4% , while complaints of suspicious contacts did not exceed 1% [14], as shown in Figure 2.

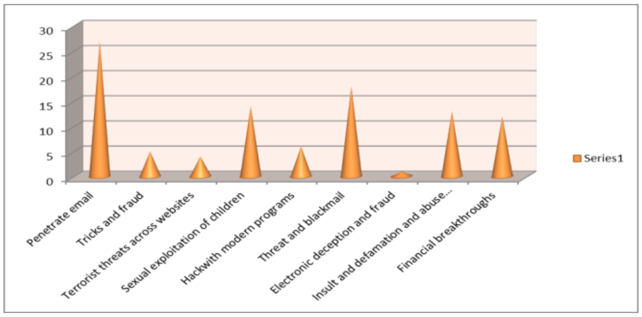

Fig. 2 Cybercrimes addressed by the Saudi Interpol [14].

In total, 776 cases of electronic crimes were dealt with by the KSA courts during ten months in 2016. The number of crimes of this type was higher during 2016 than during the preceding two years. There were about 164 cases throughout the Kingdom in 2015, and about 573 cases in 2016 [7].

The rise in the number of cases is positive, reflecting the community’s awareness, and the effectiveness of the information posted on the Ministry of Justice website, as well as the information on informatics crimes provided by the Interior Ministry. The community awareness of the need to combat IT crimes has helped to increase the number of cases of this type in the Ministry of Justice indicators. In a healthy community, this will form an upward curve that will then decline after a period of time, demanding the continued deployment of special provisions against electronic crime in order to deter criminals and reduce the number of crimes.

The 2016 Internet Security Threat Report released by Norton’s Symantec showed that more than 3.6 million people in the Kingdom of Saudi Arabia had been victims of cybercrime over the preceding 12 months, leading them to each incur direct financial losses amounting to US$195 or $730 SR [8]. The aim of the report, which is one of the world’s largest studies of Internet crimes, was to examine the impact of cybercrime on consumers, and how it affects the development and adoption of new technologies designed to improve the security of individuals. According to the results of surveys of more than 13,000 adult users in 24 countries, the 2012 version of the Norton report stated that the direct costs associated with consumer Internet crimes in the United States amounted to about US$ 110 billion over the previous 12 months.

The report confirmed that an adult becomes the victim of cybercrime every 18 seconds, leading to more than 1.5 million people falling victim to cybercrime every day around the world, with an average loss amounting to the equivalent of US$197 for each victim. The total cost of consumer Internet crime is equivalent to the cost of one week of food for a family of four people in the United States. In the past 12 months, about 556 million adults around the world have experienced Internet crime, a number greater than the entire population of the EU. This figure represents 46 percent of the number of adults who use the Internet, and very similar results were obtained in 2011 (45%). In Saudi Arabia, 40 per cent of users of social networks in the KSA have been victims of Internet crimes on social networking platforms. Among social network users, 20% of adults fell victim to cybercrime on social networks and mobile devices in the past 12 months in the KSA, compared with 21% at the global level.

In 2016, some 6.5 million people in the KSA were affected by Internet crimes, according to US security software provider Symantec, which conducted a survey in the KSA. The Symantec report revealed that 6538262 people were victims of attacks by hackers or affected by crime online. The report also reveals that nearly half (46%) of millennials have been the victims of Internet crimes, compared with 37 percent of the younger generation. Surprisingly, nearly one out of five of millennials admitted to sharing passwords with other people, despite understanding the risks associated with this. On this occasion, Ayas Houari, Regional Director of Symantec Saudi Arabia, said, “Unfortunately, crime online has become commonplace in Saudi Arabia with 58 percent of the population having seen last year.” He added, "This is 10% higher than the global average of 48 percent, and reinforces the need for a shift in consumer mentality in the country.” He argues that consumers need to be more effective at protecting personal data, and be aware that simple precautionary steps can easily help thwart possible attacks [9].

With an increasing number of individuals staying in touch using mobile devices, cyber threats are becoming increasingly prevalent among all age groups. One in four consumers have had their mobile phone stolen, potentially exposing sensitive information in their emails, social media and banking applications to web thieves. According to one report, one in seven users had had their identity stolen, one in six has had someone break into their social media account, and one in four have had their email account hacked by pirates. The software provider also surveyed 1,000 people in the KSA to examine the security implications of consumer electronic crime. Consumers lost nearly a day of in dealing with the fallout from crime on the Internet, the report found, adding that it also costs an average of SR 3,230 per person, with consumers losing over 21 billion SAR in total.

In addition, cybercrimes cost the kingdom SR 2.8 billion annually, indicating that 1.5 million victims a day around the world are exposed to electronic crimes, as shown in Figure 3. Only 20% have sufficient technical awareness. The major problems in Saudi Arabia and the Arab world are the need to educate young people about cybercrime and to lobby the state to tackle it. Currently, more effort is needed to raise awareness, and to show that measures to tackle security breaches and IT crimes are very weak in Saudi society [12].

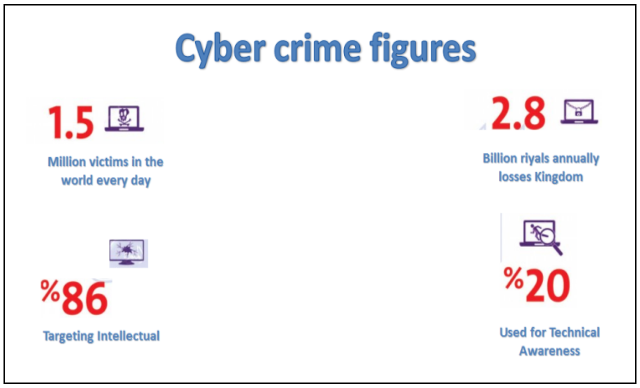

Fig. 3 Cybercrime figures in Saudi Arabia [12].

4. Conclusions and Recommendations

Technology has witnessed many improvements and new developments, and cybercrime has become more complex and hard-hitting than before, which obliges states to develop measures to combat these crimes and to keep track of all developments. Strong lines of defence need to be developed when enacting laws and regulations, and people should be made aware of these crimes and encouraged to report them. Effort should be made by individuals, organizations and the state to limit and reduce the amount of loss as much as possible, which has clear economic implications. This paper has shown that it is apparent that the number of cybercrimes and financial losses incurred by the government has increased annually. The two Norton reports from 2012 and 2016 have shown an increase in the number of people affected by cybercrime, from 3.6 million in 2012 to 5.6 million people in 2016.

The fight against cybercrime requires both states and individuals to take a long-term and strong stance against it. Everyone should take as much responsibility as possible to address the issue. The goal is to try to secure the use of computers and international information networks. The Internet is vulnerable to people aiming to commit financial crimes, terrorism, libel and defamation, and money-laundering offences. Therefore, future research should study the criteria that the Saudi Arabian government should take into account in order to avoid an increase in the number of cybercrimes that affect individuals and cause financial losses. This disturbing topic needs to be addressed as quickly as possible. The crisis can be contained now, but its increasingly widespread use means it may be difficult to control in the future.

References

[1] Sayidaty, 2016. High rate of cybercrimes in Saudi Arabia (2016). Available at: https://goo.gl/ACnzUt [Online; accessed Jan 15, 2017].

[2] Okaz, 2012. Billion Dollars Saudi banks' losses due to cybercrimes (2012). Available at: http://www.okaz.com.sa/article/449185/%D8%A7%D9%84%D8%B1%D8%A3%D9%8A/ [Online; accessed Oct 21, 2016].

[3] Clough, J., 2015. Principles of Cybercrime. Cambridge: Cambridge University Press.

[4] Sahara, 2016. Cyber-attacks cost companies a lot of money in Saudi Arabia. Available at: http://www.sahara.com/ar/news/post/88/cyber-attacks-cost-saudi-firms-heavily [Online; accessed Jan 08, 2017].

[5] Aljazeera.net, 2016. Outside organization electronic attack on Saudi Arabia (2016). Available at: https://goo.gl/cP2IPx [Online; accessed Nov 14, 2016].

[6] Alriyadh, 2015. Cyber-attacks on the KSA… The next is more challenging .Available at: http://www.alriyadh.com/1058934 [Online; accessed Jan 20, 2017].

[7] Alsakinah, 2016. Saudi Arabia: escalating cybercrimes. Available at: http://www.assakina.com/awareness-net/rebounds/90908.html [Online; accessed Dec 21, 2016].

[8] Electrony.net, 2012. Cybercrimes cost the kingdom 2.6 billion Saudi riyals (2012). Available at: https://goo.gl/gnCHe4 [Online; accessed De 21, 2016].

[9] Arab News, 2016. Cybercrime hit 6.5m in Kingdom last year. Available at: http://www.arabnews.com/node/967966/saudi-arabia [Online; accessed Aug 25, 2016].

[10] Al-Arabiya, 2015. Pan-Arab newspaper al-Hayat hacked by Yemen ‘Cyber Army’. Available at: http://bit.ly/1LXtN3H. [Online; accessed Nov 05, 2016].

[11] RT.com, 2015. Yemeni group hacks 3,000 Saudi govt. computers to reveal top secret docs – report. Available at: http://on.rt.com/ncqjk6. [Online; accessed Dec 25, 2016].

[12] Almadinah, 2015. Electronic crimes cost the Saudi 2.8 billion SAR annually. Available at: http://www.al-madina.com/node/641706# [Online; accessed Oct 15, 2016].

[13] United Nations Office on Drugs and Crime (UNODC), 2013. Comprehensive Study on Cybercrime. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Online; accessed Jan 15, 2017].

[14] Al-Eqtisadiah, 2012. The exploitation of children «sexual» represents 14% of cybercrimes.. Available at: http://www.aleqt.com/2012/07/25/article_677367.html [Online; accessed Dec 20, 2016].

[15] Schell, B.H and Martin, C., 2004. Cybercrime: A Reference Handbook. ABC-CLIO.

Dr. Sulaiman Al amro. received his B.Sc degree in Computer Science from Qassim University, Qassim (Saudi Arabia) in 2007, M.Sc. degree in Information Technology from De Montfort University (DMU), Leicester (UK) in 2009, and Ph.D. degree in Computer Science from De Montfort University (DMU), Leicester (UK) in 2013. He is currently a working as an Assistant Professor in computer science department of Qassim University. His research interests are Network and System Security, Formal Methods and Computational Intelligence.