Challenges of Computer Crime Investigation In North Africa's Countries

Mohamed Sarrab
Communication and Information Research Center, Sultan Qaboos University, Sultanate of Oman

Hamza Aldabbas
Prince Abdullah bin Ghazi Faculty of Information & Technology, Al-Balqa Applied University, Jordan

Mahmoud Elbasir
Center for Computing & Social Responsibility, De Montfort University, Leicester, UK

Abstract: Computer crime is the use of information technology in any suspicious criminal activities. Recently, our life becomes increasingly depending on modern information technology; however, it becomes very important to improve the computer crime investigation procedure especially in cases of processing very important and sensitive information such as government and military intelligence, banking information or personal private information. Cybercrime investigation helps detecting unauthorized access to any digital source information with the intent of modifying, destroying or stealing that digital data or information. Such suspicious actions can cause financial damages or important information loss; moreover, it might distribute or destroy high secret and private or confidential information. Therefore, this paper focuses mainly on highlighting the main challenges of the North Africa's countries (Libya, Tunis, Algeria, and Morocco) in computer crime investigation system by taking a look at the recent developments in the continent’s Internet infrastructure and the need of information security laws in these particular countries.

Keywords: Computer Crime; Cybercrime; Computer Crime investigation procedure.

1. Introduction

Due to the revolution of communication and information technology the use of internet has been enlarged which increases the rate of digital crime all over the world. Digital crime can be defined as “crimes directed at digital devices or their application systems.” It is very important to secure sensitive information that are processed over the web (Internet) such as government and military intelligence, banking information or personal private information. Nowadays, our life becomes increasingly depending on modern information technology; however, it becomes very important to improve the computer crime investigation procedure especially in case of processing very important and sensitive information.

Computer crimes may include different suspicious activities such as machine unauthorized access, digital frauds, system interference as well as computer misuse which might not involve any type of machine physical damage. In fact, computer crime is not just unauthorized access to a computer system with intent to delete, modify or damage computer data and information but it's so far more complex. It can be freeing of a computer virus into the wild. It can have the form of simple snooping into a computer system without authorization. It can also be theft of money, data or secret information. These different and complex types of computer crime make the work of computer crime investigator become very hard to trace, detect and prevent any type of computer crimes. The main challenge in this study is that the North Africa's countries are in different stages or level of electronic management implementation such as E-commerce, E-government, E-business and E-services overall.

The motivation of this research is raised from the rapid proliferation of the computer crimes. Some countries have a good progress and spent good steps in the investigation procedures as well as in the law of cybercrime. As well as in some other countries the investigators have a good experience in different kinds of cybercrimes and they modified their law to protect the personal private and government secret information. In all of these countries, the law is enforced to be responsible for criminal penalties for any identified computer crimes. This may lead the other countries to be as a worth field of computer crime and attract criminal to steal, destroy or distribute
any type of information. The purpose of this paper is therefore to highlight the main challenges of the North Africa's countries (Libya, Tunis, Algeria, and Morocco) in computer crime investigation system, by taking a look at the recent developments in the continent’s Internet infrastructure and the need of information security laws in these particular countries [1, 2, 3].

The reminder of the paper is structured as follows. Sections 2 and 3 provide general overview about computer crimes and introduce the computer crime context. Section 4 discusses the state of information security in North Africa's countries. Sections 5 and 6 provide Internet users and population statistics for North Africa's countries and its discussion respectively. Section 7 highlights the challenges of North Africa's countries computer crime investigation system.

2. General Overview
The synergy between telecommunication and information technologies has increased the number of users as well as raising the number of computer crimes. To secure data or information from computer criminals, it is very important to have a database to prevent unauthorized access based on confidentiality [5]. Computer crime investigation is slightly complex than traditional crime investigation. But both have similar investigation procedure including (collecting evidences, inspection and analysing evidences). In addition to that, in both traditional and computer crimes the investigators strive for answering [6].

- What was the type of the crime?
- When did it happen?
- Where did it happen?
- How did it happen?
- Who did it?
- Why did it happen?

Computer crimes are dealing with specific areas such as computer devices, network, and storage devices and might include any other digital communication Medias. In computer crimes investigation it's very important to have huge record of any available devices’ catalogues, manuals or any logging files which can help in tracing or can be used as evidence for detecting the computer crime perpetrator [7, 8]. The strategic plan is the most important step in computer crimes which can be as a long term plan or map that is concerned with national data network infrastructure [9].

The investigation team is another important factor as well to discover any computer crime. In fact it's very difficult to have one investigation team with different skills such as a good experience in information technology, network, computer machines and software tools. Moreover, the guide or team leader should be the most expert in forensic and computer crimes investigation [5]. Digital forensics can be defined as the science of identifying, collecting, documenting, preserving, analysing, examining and presenting evidence from computer devices, networks, and other electronic devices.

In general, digital forensics classifies and deals with the digital evidence in such way that is officially acceptable by courts [10, 11]. The court accepted digital evidence is a necessary part of the computer crime investigation procedure where they might involve computer hardware, software, manuals, or phone numbers [12, 13, 14]. Despite a long history and many work has been done on the computer crime investigation [15, 16, 17]; to the best of our knowledge no work has been done about computer crime investigation in this particular area generally North Africa’s countries.

3. Context of Computer crime
Computer crimes are any suspicious criminal activities those are committed against computer hardware machines or software tools. In computer crime, the computer device is the target of any suspicious criminal activities. In fact, computer crime types are not only associated to the software, data, information or any other program applications or tools. The criminal actions in the context of computer is often refers to the computer functions; such as file transfer facilities, social media applications, audio or visual conferencing tools and electronic mailing etc. However, computer crimes are any suspicious criminal activities committed using computer and network (Internet) to violate the existing legislation laws or forensic roles. Computer crime might also involve the use of digital resources to commit any type of normal crimes such as theft of identifiable card information and other forms of proprietary information or property in both digital and physical form [16, 18].

4. State of information security In North Africa
The state of computer crime in the North Africa is different from other countries all over the world, where the state of information technology security in North Africa and all Africa regions is affected by many factors such as IT infrastructure, growth of IT user and lack of regulation and training of law enforcements.

- Information Technology Infrastructure.

In the past, it was very difficult to has Internet connectivity in Africa [19] but, recently North Africa’s countries are showing signs of becoming a major player in the information and
communication technology (ICT) arena. All united Nation members, including Africa's countries, have agreed to reach some common objectives by year 2015, involving the development of global partnerships [20]. This goal concentrates on the cooperation with the private sector to maintain the benefits of new technologies, especially information and communication technologies [21].

The North African governments have agreed to cooperate with private sector companies to provide information and communication technology (ICT) services to all of their citizens. Different foreign organizations and companies have already started investing in North Africa, helping and supporting the region in developing its infrastructure. In 2007, SEACOM built the Africa’s first undersea fiber-optic cable is built by SEACOM in 2007 to connect Africa's eastern and southern countries with the rest of the world [22]. Africa and specially the North Africa’s countries are now well connected via cable, giving the local Internet Server Provides the ability to offer faster and cheaper Internet access types to the customers [23].

Table 1. World Internet Usage and Population Statistics June 30, 2012

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>1,073,380,925</td>
<td>4,514,400</td>
<td>167,335,676</td>
<td>3,606.7%</td>
</tr>
<tr>
<td>Asia</td>
<td>3,922,066,987</td>
<td>114,304,000</td>
<td>1,076,681,059</td>
<td>841.9%</td>
</tr>
<tr>
<td>Europe</td>
<td>820,918,446</td>
<td>105,096,093</td>
<td>518,512,109</td>
<td>593.4%</td>
</tr>
<tr>
<td>Mid East</td>
<td>223,608,203</td>
<td>3,284,800</td>
<td>90,000,455</td>
<td>2,639.9%</td>
</tr>
<tr>
<td>North America</td>
<td>348,280,154</td>
<td>108,096,800</td>
<td>273,785,413</td>
<td>153.3%</td>
</tr>
<tr>
<td>America / Caribbean</td>
<td>593,688,638</td>
<td>18,068,919</td>
<td>254,915,745</td>
<td>1,310.8%</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>35,903,569</td>
<td>7,620,480</td>
<td>24,287,919</td>
<td>218.7%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>7,017,846,922</td>
<td>360,985,492</td>
<td>2,405,518,376</td>
<td>566.4%</td>
</tr>
</tbody>
</table>

- **Growth of IT user.**

With currently cheap network broadband connections the number of IT users is growing every day. According to Internet World statistics, Africa’s Internet penetration rate as of June 2012 was 5%. Where, this percentage refers to the number of users divided by the population. In 2009, Africa’s population reached 1 billion but on June 2012 was increased to 1,073,380,925 [24, 25] as indicated in Table 1 the world internet usage and population statistics in June 2012. In terms of being connected with the rest of the world, only a few Africa’s countries can be considered as emerging or developed. Many Africa’s countries have yet to garner high-enough penetration rates, due to the fact that most of them are not politically stable or in case of North Africa’s countries have many work to do in terms of infrastructure.

This huge growth of number of users in Africa from 4,514,400 in December 2000 to 167,335,676 in June 2012 has made many new online business opportunities. On the other hand, this penetration growth has increase the potential for IT bad manipulation. Because of IT and information security policy enforcement many Internet and IT users have become victims of computer crime attacks [1].

- **Lack of regulations and training of law enforcements.**

The North Africa’s countries suffer from the lack of IT and information security awareness and different kind of security policy enforcement among IT users. The security awareness and security policy enforcement in the North Africa’s countries are far behind the main players of the dangerous game Europe, Russia, China and USA. Because of that North Africa’s countries spend less effort to raise awareness and security policy enforcement among their IT users. The North Africa’s countries are lack of training and regulations of law enforcements.

These countries need strong security awareness training, targeting native speakers to educate users, employees and law enforcers to understand the dangers and risks of attacks and hackers [26]. Moreover, the computer criminal activities in North Africa are not well reported. Hacktivist attacks and scams are very common in North Africa's countries, following the unknown attacks defacing different sites for political reasons. e.g. an Algerian hacking attack that defaced several Romanian sites, including PayPal and Google [25].

5. **Internet users and population statistics for North Africa**

With nowadays cheaper and faster Internet access, more North Africans will be Internet online or continually connected which increases the number of new users. But the IT and internet security is a concept that it's not known to the vast majority of North African users [2]. Table 2 indicates the Internet users and population in North Africa's countries.
Table 2. Internet users and population in North Africa's countries.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>34,994,937</td>
<td>50,000</td>
<td>4,700,000</td>
<td>13.4 %</td>
</tr>
<tr>
<td>Morocco</td>
<td>31,968,361</td>
<td>100,000</td>
<td>15,656,192</td>
<td>49.0 %</td>
</tr>
<tr>
<td>Tunisia</td>
<td>10,629,186</td>
<td>100,000</td>
<td>3,856,984</td>
<td>36.3 %</td>
</tr>
<tr>
<td>Libya</td>
<td>6,597,960</td>
<td>10,000</td>
<td>391,880</td>
<td>5.9 %</td>
</tr>
<tr>
<td>TOTAL</td>
<td>84,190,444</td>
<td>260,000</td>
<td>24,605,056</td>
<td>104.6%</td>
</tr>
</tbody>
</table>

6. Discussion

As shown in Figure 1 Algeria has the highest population with 34,994,937 but it was the third country in the number of Internet users by December 2000 but it was moved to be the second North Africa's countries as indicated in Figure 2 with 4,700,000 users in December 2011 Figure 3.

As shown in Figure 1 that Morocco is the second biggest North Africa's country with population of 31,968,361 which is 38% of North Africa's countries population in 2011 and its Internet users are moved from 100,000 to be more than 15 million users with the highest penetration population 49.0.

The population of Tunisia is three times less than Morocco but their Internet users in December 2000 were 100,000 users as indicated in Figure 2 and by December 2011 reached nearly 4 Million users being as the second penetration population 36.3 in North Africa's countries Figure 4. Libya is the smallest among the North Africa's countries with population 6,597,960 and 391,880 Internet users in December 2011 as indicated in Figure 3.

Table 1 indicated that Africa had 167,335,676 Internet users in June 2012. Whereas, Algeria, Morocco and Tunisia with the ten Africa's countries with the biggest Internet user bases. The exponential growth of North Africa's user's base will force Internet provider to reduce their service prices, which will benefit both users and attackers.

The estimated number of Internet users in North Africa as of December 2011 was 24,605,056 as shown in Table 2. In December 2000, the Internet users were only 260,000.

Therefore, in these growth continues, there will be millions of future Internet user's potential cybercrime victims in the region. Algeria, Morocco and Tunisia have accepted this risk and started working on a national cyber security policy. The North Africa's countries need to identify and mitigate their unique cyber security vulnerabilities and threats through joint initiatives and sharing of best practices.

There are many challenges need to be defeat in order to improve the computer crime investigation system in North Africa’s countries such as lack of comprehensive study of the main influencing factors of computer crime investigation system in the North Africa's countries. To the best of our knowledge, there has not been any scientific study on the main factors or barriers that influence the work of computer crime investigators in North Africa's countries. One of the important factors is the cultural and social considerations such as user behaviors and the lack of knowledge exchange about computer crime between policy officers of these countries. Moreover, the North Africa’s countries are still in the earlier stages of their E-services implementation. The following are the main challenges of the North Africa's computer crime investigation system.

- Legislation, that involves the criminal offences, requirements to open an investigation, evidences.
- Public and private sector cooperation should assist and exchange of information with each other of any related information to computer crime victim, evidence, legislation, etc.
- North Africa’s should internationally cooperate with other countries to exchange any information related to computer crime victims.
- Dedicated Unit involves the legal framework, field offices, and competence offices, trained and skilled officers.
- Criminal investigative procedures should allow computer and Internet access, data preservation and supports procedure complaint.
- The criminal investigative procedures should support an investigation, surveillance, identifying IP, and phone users and monitoring of phone conversation.

Finally, the most important challenge in the computer crime investigation procedure is to understand the suspicious criminal activity and prove it [27].

8. Conclusion

The North Africa’s countries are still in the earlier stages of their E-services implementation. Therefore, it is very important for these countries’ governments and organizations to maintain and improve their computer crime investigators quality. There is no doubt that the context of computer crime is feasible to the computer crime investigators but our paper discussed many challenges to improve the computer crime investigation system in North Africa's countries and highlighted the most important factors that effects the state of information technology security in North Africa which are the IT infrastructure, growth of IT users and the lack of regulation and training of law enforcements. The paper concentrated on the lack of computer crime investigation experiences exchange between North Africa’s countries and the need of international cooperation with other countries to exchange any information related to computer crime victims. Thus, it is time for these countries’ governments to comprehensively study all related issues in their computer crime investigation system that analyses and discusses all challenges and barriers to improve the computer crime investigators procedure. Whereas, this study should emphasise the need of a single information security law in North Africa's countries.

References


Mohammed Sarrab is currently working as a research associate at CIRC (Communication and Information Research Center), Sultan Qaboos University, Muscat, and Sultanate of Oman. He obtained his Ph.D. degree in computer science from De Montfort University, UK. M.Sc. degree in computer science and information technology from VSB technical university of Ostrava, Czech Republic and B.Sc. degree in computer science from Al Zawia University, Libya. His research interests are in areas of computer security, in particular access control and policy-based system management, Runtime Verification and Information Flow Control. He is also interested in computer forensic, mobile applications, open source software and Java byte code instrumentation for monitoring and security reasons.


Mahmoud Elbasir has M.Sc. in information System from De Montfort University 2007. He received his B.Sc. in computer science from Tripoli University Libya a. His main research interests are in areas of Information System management, E-commerce, E-government and Software Engineering and Free open Source Software. He is also interesting in Human-computer interaction, computer security and computer forensic.