Cybercrime in Iraq

Sattar J. Aboud
Depatment of Computer Science, University of Bedfordshire, UK

Abstract— in some years ago, an Internet has been developed what so-called Web. But, the broad use of an existing Internet services has made individual users the possible target for cybercrimes. In this paper, we study and analysis different cybercrime cases and compare the result with the preceding work. The illustrated results include all cases that described in the cybercrime in Iraqi authority, the Criminal Investigation Bureau.

Index Terms— Cybercrime, cybercrime discovery, cybercrime avoidance, computer-crime, information society, cybecrime cases

1 INTRODUCTION

THE growth of Internet and Web offered society a great variety of selection services, permitting them to communicate and work together. Alternatively, the term cybercrime tends to be utilized by cyber criminals, which are capable to attack the victims beyond any environmental limitations, especially if they are online. Therefore, a broad proliferation of data and connections technology, besides the positive consequences of people and to society, gave the new topic of criminality in cybercrime. The cybercrime incorporates criminal bhavior that is used with the Internet, involving intellectual property crimes, financial frauds, and child pornography. It is worth to indicate that in various cases the use of computer is not altering the basic nature of the crime. For example, a coruption remains a corruption, despite the amount of funds sent electronically on cybercrime and even with the fact of the use of the Internet influence the level of a crime.

The Internet is attractive scientific expertise criminals since it gives them a possibility to find the victims, extends their line of work and then the ability to alter the characteristics. Significantly, they can work from another society, so making their work more complex, because of a different framework and the global procedures that must be followed to understand them. In contrast to conventional crimes, the executor and the victim are not often in the same physical site. Thus, the law enforcment body faces some problems in both inspecting and securing the crime cases. Cybercrime is now characterized as a common domain and in need for organization, collaboration and authorized measures among the countries [1], because the cybercrime tend to increase gradually, leading to high icomes for criminals and luck of trust in an Internet by users. In the latest news, over 80% of online customers indicated that security as a main matter to concern if doing trade across an Internet [2]. In Australia, cybercrime costs the merchants more than $600 million in the year, whereas in the USA one in five online customers has been the victim of cybercrime in 2012 [2]. In 2013, Norton cybercrime in its report indicated that 556 millions of customers being used cybercrime every year, which is more than a whole population of the European Union [3]. An important attempt to fight these sorts of crimes will require colaboration between nations and companies in order to dvel-op the common protection strategy to reach the fame and slight a difficulty in a best possible approach. It is essential to reach the safe and dependable cybercrime setting in a context of the information society to increase the advantages of information and communications technology.

The remainder of this paper is organized as follows. Section 2 considers a related work in both internally and externally. Section 3 presents the cybercrime cases. Section 4 illustrates and analyses the statistical information, whilst Section 5 concludes this paper with some comments concerning the future direction of this study.

2 RELATED WORK

Researches regarding cybercrime are yet in initial phases in Iraq, where community tends to that cybercrime is not one of their main interests. Actually, one research performed by price water house Coopers in UK, gathered some interesting finings regarding Iraq. This firm indicated that the high proportion of Iraqi firms not having been intruded over the last year, wheras the maximum number of attacks noticed by firms was only 3. But, it seems that these firms do not understand the attacks and they are not capable to record it [4]. It must be proposed a so-called Cybex [5]; such system is employed in European nations to ease a problem of cybercrime. Iraq is trying to use a real system to improve cyber security. Cybex is a program that calls upon nations to choose representatives who will work as the public servants. Iraq should subscribe in this program in order to enhance its activites aganist this matter. However, currently more than ten European nations were used this system. The full description on law extent taken anti-cybercrime is illustrated in [6]. It analyzed the cybecrime comitted, with means that cyber criminals use. Also, it shows situation of Iraqi criminals that are connected to cybercrime.

3 CYBERCRIME CASES

Cybercrime has sustained to be more committed between the years of 2011-2014. Currently, cybercrimes have used more powerful attacks to rob information from credit card and other private personal data and intellectual property. Simultaneously, global co-operation is raised and guided to some arrests criminals in coordinated operations around the world. Therefore, we are going to illustrate various cases appeared in cybercrime in a period mentioned above:

Case 1: on December 2011 some documented Nigerian source mails cybercrime appeared. These included passing e-messages to users for apparently pending great amounts of money, mostly deserved by involvement in lotteries. The aim is to gather special information from receivers of these messages, and also posted to mobile phone of users. These letters were posting to the receivers that they had gain for example a million Dollars.

Case 2: on September 2011, three persons were charged for cheating and for abuse the mobile phone firm using marvelous methods. They succeeded in hacking the firm computer and directed to criminally vending internet networks to Cuba. The consequence was a corporation is accused by 690,501 Euros.

Case 3: on October 2011, some were accessing pornographic site, under the running Microsoft Window. Whilst a web is still loading, the letter occurred automatically; notifying user that he has visited site of youth pornography and for this a laptop has been closed by a cybercrime authority. A user should have to pay to stop being charged by a police authority. It was exposed that the information was being kept on Ukrainian server.

Case 4: on May 2012, the travel sale in Thessaloniki was charged for Internet fraud, since posts an advertised by uncommon Facebook. The ticket reservations showed forged whereas in other example cheat of credit cards was seen.

Case 5: on October 2012, cyber hackers attack users of Skype voicemail, Facebook account verification messages, and Windows licenses using Black-holes exploits.

Case 6: on November 2012, the criminal was offered zero-day use for Yahoo Mail become on sale, for $700 millions that will allow the hacker use the cross-site scripting weakness to rob cookies and capture accounts. A hacker, called “The Hell”, generated the video to use the alternative cybercrime market known as Darkode.

Case 7: on June 2013, law enforcement bodies arrested six persons in UK and 12 in USA on FBI-led smart operation that catch the sum of 24 credit card cyber impostors in 13 nations. The arrests followed two years secret FBI search that followed advertising credit card data over the fake online market.

Case 8: on August 2013, the Yahoo user accused a web portal firm of neglect for allows more than 450.000 users and passwords are stolen from one of its web.

Case 9: on Novermber 2013, USA space NASA is to encrypt its laptops after a loss of computer holding data for more than 10,000 workers. This is the latest in series of information violation connecting unencrypted computers in NASA in recent years and comes after a stealing of the computer holding data of 2,300 workers.

Case 10: In September 2013, a cybercrime in USA rose in school with 30% protested of some type of cybercrimes. Also, citizens are yet prone to be cheated on a cause of lottery wins, great-salary jobs and untrue offers.

Case 11: In January 2013, cybercrime rose in vast number in the USA. A cybercrime police station became operational in the year ago selected regarding the cases that it chooses up.

Case 12: In January 2014**,** police in the USA reports that cybercrime grievances rose by 200% compared with 2012.

4 Analysis Of Cybercrime In Iraq

In 2013, the Ministry of Planning in Iraqi reported that, the main part of cybercrime cases in Iraq is using social sites mostly the Facebook. There are some cases using other social sites for example Twitter, Zoo, and Badoo. The cybercrime cases using Facebook for 2013 are illustrated in Figure 1 which is as follows: 78 cases of kidnaps, 55 cases of threats, and 47 cases of hacking personal information such as photos sent and fake profiles, 39 cases of rapes and 17 cases were reported for drugs, and 15 cases possible suicide. As can be observed, the common cases are kidnaps. The following common cases are personal information hacking, whereas young seduction next. It can be remarked that kidnaps are the major problem for social site and good care should be taken, since such site are common between children community.

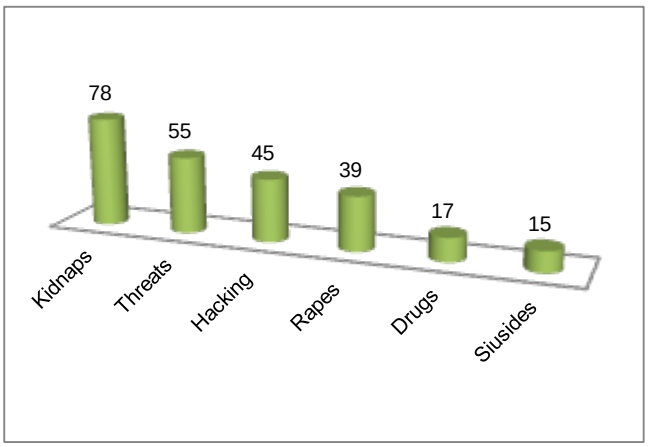

Fig.1. cybercrime cases using social site Facebook

Figure 2 illustrated diverse cybercrime types in Iraq for 2013. The type with the large proportion is the e-commerce and web-typed services protection with 53 cases equal to 12.0%, followed by frauds of social security by 101 cases equal to 22.0%, followed by unauthorized online games with 61 cases equal to 14.0%, then by satellite piracy with 183 cases equal to 41.0%. Then copyright protection with 49 cases equal to 11.0%.

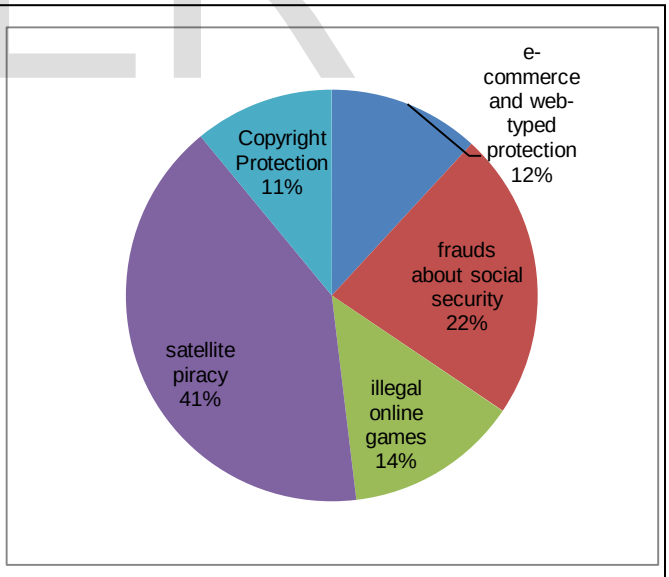

Fig.2. cybercrime types in Iraq

Figure 3 shows the analysis of the number of charged persons for cybercrime in Iraq for 2013. The figure also illustrates six different types of cybercrimes such as satellite piracy with 40 cases, child pornography with 29 cases, internet fraud with 67 cases, computer systems hacking with 13 cases, personal information hacking with 31 cases, and copyright protection with 23 cases. As can be noted, the majority of citizens charged were Internet fraud and satellite piracy.

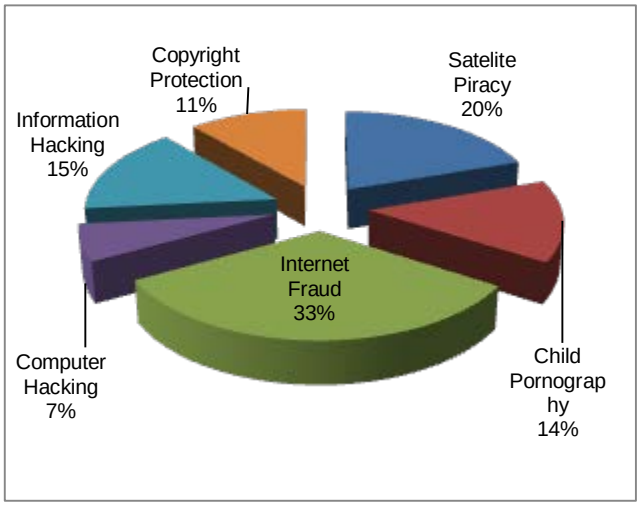

Fig.3. Analysis of charged persons for cybercrime in Iraq

It is expectable for Baghdad to have the lead in number of people arrests about 121 persons and considerably bigger compared to other cities in Iraq. The other two larger cities, Basra and Kirkuk, about equal number of arrests have appeared which about 55 persons. It is also interesting that in certain small cities such as Dellah a noticeably large number of arrests about 51 persons due to their low of population rate. Alternatively, there are the large cities such as Mosul show a much smaller number of arrests about 8 persons. Whileas in Waseet there are 13 persons and in Babylon 11 persons. Figure 4 show the number of people committing a cybercrime in year 2013 is arrested.

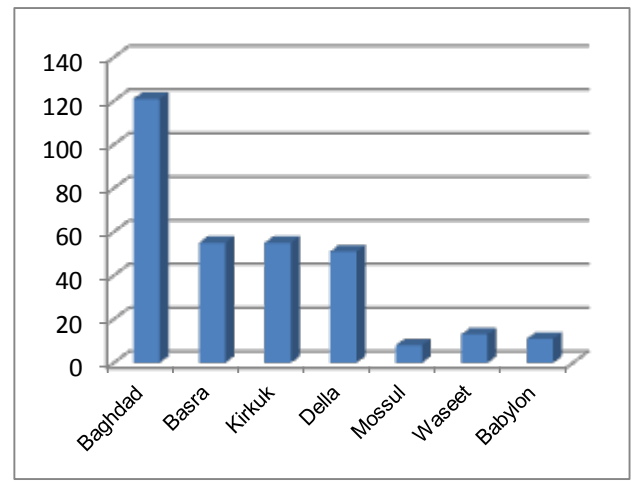

Fig.4. Number of people committing cybercrime arrested

Figure 5 shows that the child abuse has the largest number of arrested about 43 persons, followed by copyright violation with about 38 persons. Then, come in the third Satellite piracy with 31 cases, followed by infringement of computer systems with 21 cases. Then, come after the Internet fraud by 16 cases, followed by privacy legislation breach with 9 cases.

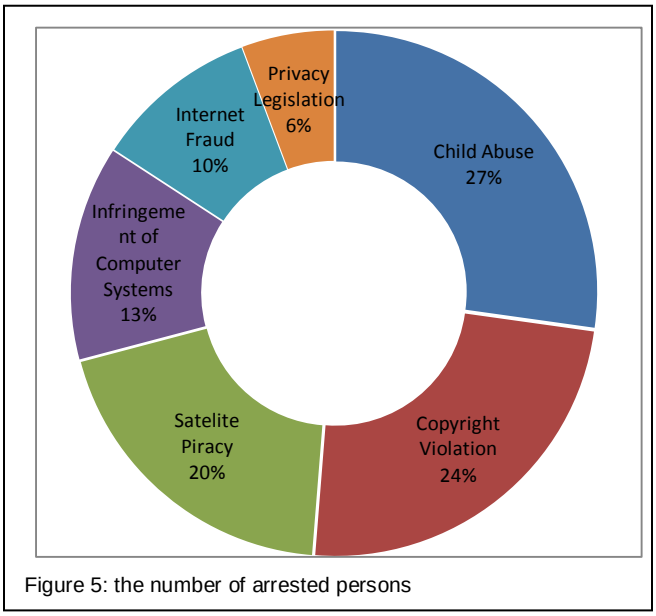

Figure 5: the number of arrested persons

Figure 6 illustrates the cybercrime confiscations for 2013 including hard drives and DVD about 40 cases, routers with 35 cases, USB 53 cases, wireless cameras about 62 cases, printed bags about 79 cases, SIM cards with 187 cases, mobile phone cards about 56 and laptop computers 32 cases. In contrast confiscations about wireless devices such as mobile phones are less. However, such wireless devices have penetrated daily; it is possible that in a near future there is a growing in the confiscations of these devices.

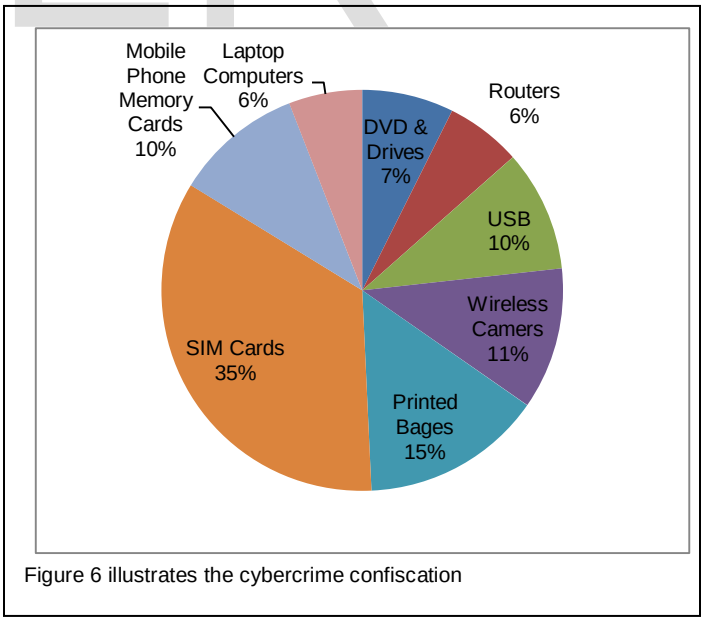

Figure 6 illustrates the cybercrime confiscation

5 Conclusion

Cybercrime denotes the new and rapid growing crime type at Iraq in recent years. In this paper, the report analysis of cybercrimes is provided, studying different aspects. The analysis illustrates that kidnaps challenges over Facebook are the most

often happening cybercrime category, while a common charge and arrests happened for Internet fraud shows the understanding of a law enforcement corpus on this issue, and fine efficiency in managing it. Also, reports illustrate that there were about 40% more cybercrime cases in the 2013 compared with last two years. Finally, most confiscations include laptop computers were fairly anticipatable, as they are the channel for committing cybercrimes. In a future we anticipate that cyber-crime become a dominant crime, as different hi-tech progression have produced societies to steadily become e-society. We deduce that hi-tech revolution of the past 15 years which granted birth of cybercrime, we should discover a method to fight this crime

ACKNOWLEDGMENT

The author would like to kindly acknowledge the Criminal Investigation Bureau in Iraq for giving anonymous statistical data. Also, the author would like to thank the Department of Computer Science at the University of Bedfordshire for its support this project.

REFERENCES

[1] Schjolberg S and Ghernaouti-Helie S, "A Global Treaty on Cyber security and Cybercrime, 2nd edition, AiTOslo, 2011.
[2] Saini H., Rao Y, and Panda T, “Cybercrimes and their impacts: A review”, International Journal of Engineering Research and Applications, Volume 2, pp. 202–209, 2012.
[3] Norton cybercrime report, Symantec, Technical Report, 2013.
[4] Sattar J. Aboud, "An Overview of Cybercrime in Iraq", the Research Bulletin of Jordan ACM, Volume II (II), pp. 31-34, 2012
[5] David Brystowski, "European Certificate on Cybercrime and E-evidence cybercrime Program", United Nations International Crime and Justice Research Institute, 2013
[6] Markopoulou P, “The convention on cybercrime”, Intellectum, 2008.
[7] Papanis E., “Research about the Face book”, http://www.dart.gov.gr/data/2010.
[8] Christdoulaki M and Fragopoulou P, “Reporting illegal internet content”, International Management and Computer Security, volume 18, pp. 54–65, 2010.