Asia Pacific Journal of Advanced Business and Social Studies
ISBN (eBook): 978 0 9943656 7 5 | ISSN : 2205-6033
Year: 2016 , Volume: 2, Issue: 2

SOCIAL MEDIA AS A TOOL FOR COMBATING CYBERCRIMES WITH SPECIAL REFERENCE TO SAUDI ARABIA

Faisal Yousif Alanezi
Prince Mohammad Bin Fahd University (PMU), Saudi Arabia
Email: Falanezi@pmu.edu.sa

Abstract

Social media has undoubtedly been integrated in our everyday live and has therefore become the channel to conduct a lot of business for example marketing, and communication worldwide. However, in the Middle East where social media has gained huge popularity, it has also attracted online criminals in the region to victimize users. Many harmful crimes occur through social media such as blackmailing, terrorists propaganda, online fraud, therefore there is an urgent need to combat them. In the Middle East, and in particularly in Saudi Arabia, social media have been increasing rapidly, and therefore has become a breeding ground for both online criminals and terrorists activities. This becomes a huge concern for both public and private users. Therefore, this paper demonstrates how social media could be an effective instrument in combating cybercrime in Saudi Arabia. It provides an advantageous insight into the essence of online crime, highlighting the motivations for committing online crime and shedding light on the paradoxical nature of social media.

Keywords: Social Media Crime; Online Criminals; Combatting Online Crime; Saudi Arabia.

1. Introduction

Social media has become part of our lives. It has become an indispensable tool in human usage, repeatedly proving their usefulness and effectiveness, and this will no doubt continue to increase in the near future.

Being a part of our lives, social media also poses some dangers, or at least contributes to the dissemination of these dangers. What are the dangers of social media use? Crime is a primary danger, and it is committed on social media so frequently that one may suggest that it has been especially created for this purpose.

The spread of crime on the social media has raised many issues, including questioning over its effectiveness, which, nevertheless, has not diminished its social utility (Kawasaki & Fitzpatrick, 2014). Modern society has become a major consumer of the social media. It has; therefore, become reasonable to fight crime on the social media using the social media. It is not only reasonable, but it has also become a necessity. For this reason, law enforcement agencies, including the police, have developed a variety of techniques and methods designed to prevent online crime.

In the western world, where social media use has reached a peak and online crime has attained the same status as crimes committed in real life, law enforcement agencies, in tandem with various analysts, have gathered invaluable experience in preventing, deterring and fighting online crime (Golbeck & Klavans, 2015).

Asia Pacific Journal of Advanced Business and Social Studies
ISBN (eBook): 978 0 9943656 7 5 | ISSN : 2205-6033
Year: 2016 , Volume: 2, Issue: 2

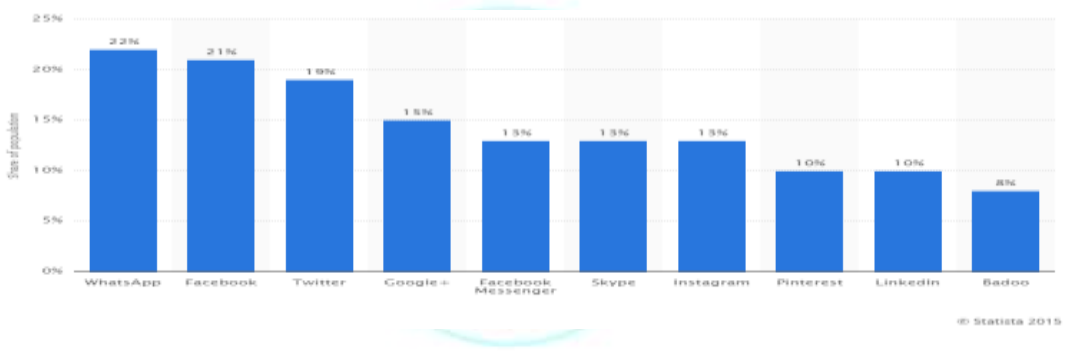
In the Middle East, particularly in Saudi Arabia, the picture is completely different. It is because the social media penetration rate is not as high as in the western world. There are, however, other reasons for such 'backwardness'.

Discussions continue over the feasibility of online crime prevention, and certain parties are of the opinion that the discussion of social media utility for the purpose of the detection and prevention of online crime is somewhat premature. There is a grain of truth in this, particularly with a low internet penetration rate, one cannot argue for effective online crime prevention in Saudi Arabia.

The purpose of this conference paper is to discuss whether online crime can be combated with social media tools with special reference to Saudi Arabia. It is particularly important in the context of the rising significance of social media sites, such as Facebook, Twitter, Instagram and other social media, in Saudi Arabia.

2. The social media in Saudi Arabia

A number of the largest sites (Whatsapp, Facebook, Twitter, Google+, Skype, Instagram, Pininterest, Linkedin and Badoo), represent social media, as illustrated statistically in the bar chart below:



It is not surprising that the three social media giants (Whatsapp, Facebook and Twitter) account for the major proportion of all the social media in Saudi Arabia.

It is reported that, "... as of [the] fourth quarter [of] 2014, 29 percent of the total population [of Saudi Arabia] were active social media users" (Statista, 2014). It implies that social media usage in Saudi Arabia is relatively low in comparison with western countries.

In contrast, the BBC reports that Saudi Arabia has one of the largest social media markets in the Middle East, and its popularity is boosted by a high rate of smart phone ownership (BBC, 2015). It is also reported that the total number of Twitter users comprise 40% of total Twitter users in the Arab region and 10% are Facebook users (BBC, 2015). Moreover, it is said that YouTube users comprise a large number in comparison with any other country in the world.

Interestingly, an authoritative internet source reports that 93% of all internet users in Saudi Arabia spend their time on Facebook, which accounts for 7.6. million of the 8.4. million total internet users in Saudi Arabia (BBC, 2015). Facebook subscribers mostly inhabit cities like Riyadh, Jeddah and Dammam.

Asia Pacific Journal of Advanced Business and Social Studies
ISBN (eBook): 978 0 9943656 7 5 | ISSN : 2205-6033
Year: 2016 , Volume: 2, Issue: 2

Although the above-cited statistics indicate a relatively low percentage of LinkedIn users, it is said that LinkedIn users have grown in number by 50% since last year, which makes this social medium a good prospect for Saudi Arabia (BBC, 2015). Moreover, LinkedIn is the most popular in Saudi Arabia among representatives from the construction, engineering and information technology industries.

The above-cited statistics fail to mention YouTube, but it is one of the most popular social media websites in Saudi Arabia. It is reported that approximately 96 percent of internet users in Saudi Arabia use YouTube to watch video and use it for broadcasting purposes (BBC, 2015).

Twitter is probably the most used website and competes with Facebook and YouTube (about 5.4. million users in Saudi Arabia). Its usage is calculated with reference to the number of tweets sent by users. It is reported that it attains approximately 210 million tweets per month (BBC, 2015). It is also reported that 40% of tweets in the Middle East and North Africa are from Saudi Arabia (BBC, 2015), indicating that this social medium is not only popular but also fast-growing.

As for the impact of the social media in Saudi Arabia, it is a driving force in the country, serving as alternative media and providing users with alternative opinions on events at home and abroad (Bernard, Hegghammer & Lacroix, 2015). Moreover, it has a positive effect on media business, leading to the emergence of a number of Saudi companies. No-one can deny its positive impact on the way people think.

Whereas nearly all television channels in Saudi Arabia are preoccupied with broadcasting about government affairs or religion, the social media provide Saudi citizens with opportunities to look at topics from different points of view. It is not surprising that the social media are very popular with younger users (26 to 34 year olds). It gives them a sense of freedom and liberation. Overall, it is said that the "social media are a force for modernity, albeit at the snail's pace preferred by Saudi Arabia's establishment" (Economist, 2014).

3. The essence of cybercrime

The widespread use of social media means that Saudi Arabia is not free from the danger of online crime. Online crime is a sophisticated social phenomenon and poses a serious danger to society; it is to be studied separately from ordinary crime.

It has specific aspects that distinguish it from other types of crime, in particular as follows: online crime can be latent in character; it can also be transnational, using a distance method for its perpetration, with specific structures and criminal groups.

Online crime closely involves organized criminal groups or online gangs, which preoccupy themselves, not only with innocent "spam sending" activities, but also with crimes that are more serious (Anderson, 2013).

There are several characteristics of online crime that render it more distinctive (Anderson, 2013):

- There is a distance between the perpetrator and the victim that allows the illegal action to be accomplished without any physical contact between them;

- The specific character of the online space increases the secrecy of the crime committed;
- In a large proportion of trans border online crime, the perpetrator and the victim can physically reside in different jurisdictions;
- It requires the serious preparedness of the perpetrators, the intellectual character of their illegal activity needing specific knowledge and skills;
- The locus of the crime has a specific character, e.g. the computer system of the victim, the perpetrator and the provider;
- Taken into account are the complexity, diversity, originality and frequent updates of methods and specific tools;
- The illegal action is multi-episodicin character, potentially with multiple victims (i.e., separate episodes may be regarded as actions that do not pose a danger to society, and, as such, are not crimes);
- There is the possibility of committing crimes in automated mode, the realization of complicated scenarios by one person transforming relatively weak resources of separate computers into the perfect weapon for committing crime;
- The criminal plays on the ignorance of online crime victims about crime;
- Another factor in the non-availability or absence of witnesses, who could have observed crime commission or detect the perpetrator.

Unfortunately, the number of online crimes is on the rise, causing increased damage. It is calculated that damage from online crime, internationally, exceeds billions of US dollars (Anderson, 2013).

Some analysts highlight the importance of the reckless nature of online crime as one of the driving forces behind online crime as a whole (Holt, 2013). There is also a dangerous tendency, observed on the internet recently, concerning the increasing rate of recruitment of persons joining online crime gangs (Holt, 2013).

There are two types of online crime gangs on the internet:

1. Traditional crime gangs, who have realized the usefulness and benefits of online criminal activity;
2. Communities of hackers who are involved only in online crimes.

The uniting factor in both cases is the organized character of these groups. In both cases, perpetrators join forces to achieve their goals.

One of the reasons why online crime gangs have become so powerful on the internet is because of the income they receive. In Europe, for instance, the income from online crime totals about 750 billion US dollars, which exceeds the profits deriving from the drugs business (Holt, 2013).

There are two interrelated constituent parts that play an important role in promoting organized online crime gangs (Casey, 2011):

1. Organized crime comes to cyberspace and attempts to use it for its own purposes;
2. Online crime is sophisticated by nature, leading to online perpetrators coordinating their actions and merging into organized crime groups.

The reasons for the increased interest of organized crime groups in cyberspace are clear. There are opportunities, not only for concealed communication between professional perpetrators and other persons engaged in illegal activities, but also for systematic resolution of specific large-scale criminal tasks, such as:

- Committing criminal activity (e.g. stealing money from bank accounts, the drug trade, child pornography, online fraud, etc.);
- Promoting illegal activity or forming a positive image of organized crime (Casey, 2011).

In Saudi Arabia, cybercriminals realize that the use of global computer networks lead to confrontation with the law enforcement agencies in various countries, and reaches a level where States lose this battle (Bernard, Hegghammer & Lacroix, 2015). They realize that law enforcement bodies are weak, because their employees have low levels of professional training and the non-ability to apply the law appropriately, as well as, an insufficiency of legal tools in the collection of proof and the absence of sufficient sanctions against committing online crime (Bernard, Hegghammer & Lacroix, 2015). In fact, cybercriminals in Saudi Arabia use many opportunities, offered by gaps in online protection. They feel that their acts remain unpunished and continue to commit online crime.

Here, one can speak also about the unpreparedness and the imperfectness of the Saudi legal system, which is based on *Shari'a* law. It has too many flaws, most of them existing because of the backwardness of a law system based on precepts that were developed more than 1,000 years ago. This hindrance does not allow law enforcement bodies to qualify online crimes appropriately, nor does it facilitate their understanding, not only of the seriousness, but also the damaging nature of the crimes.

Another problem with online crime, not only in Saudi Arabia, but also in other countries, is that, because professional and skilled persons commit online crimes, it attracts also the highly intellectual, who do not qualify as criminals in the ordinary sense of the word (Aarts & Roelants, 2015).

This makes the task of detecting and punishing online perpetrators more difficult, and, in most cases, impossible to accomplish. It also contributes to making online crime popular, among those who had no previous criminal intention to act as criminals. This very bad tendency has a negative impact on the way of thinking of citizens in Saudi Arabia (Bernard, Hegghammer & Lacroix, 2015). Such people are also attracted by the latent nature of online crime, hoping that it will disguise their crime. There is also the factor of financial gai nfrom online crime, which may attract underpaid specialists to commit online crime.

For this reason, one can observe the increased activity of online hackers, which, although not united in groups, nevertheless act as if they were. They are difficult to detect, as they may be resident in different countries. A Saudi hacker may commit online crime directed against bank servers in Saudi Arabia from the UK or Europe.

Their organizational form is established in the form of online networks, which can unite or disconnect once danger is pending. Their organizational structure is strictly decentralized, unlike ordinary organized crime groups, and has a steady communication system, providing the stable exchange of resources and results among members of the group (Holt, 2013).

Moreover, one should understand how organized online criminal groups act. They are highly sensitive to change, and there are certain patterns one should bear in mind. First, online criminal structures have flexible management systems. Their management can be affected in various ways, depending on the situation (thus making it situational) (Holt, 2013). There is much space for manoeuvring. On this account, operational capabilities are provided at a very high level.

Secondly, all the members of online criminal networks are equal, and this is a very interesting feature of online crime (Holt, 2013). They can change their status and positions depending on the tasks performed (Holt, 2013). This makes the work of law detection and enforcement agencies almost impossible.

Thirdly is the ability to cope with rapid team changes and the redistribution of roles between members of the group (Holt, 2013). It is difficult to neutralize such groups or heads of groups. After committing a certain criminal act, the group can cease to exist or change its structure (Holt, 2013).

Fourthly, such groups can be easily replenished, on account of the specific nature of the social environment, where the elaborate character of communicative instruments is enhanced to find new associates (Holt, 2013). The online network thus receives opportunities to restore itself at the expense of replacing one associate with another.

Fifthly, online networks are capable of resolving the same task choosing different variants of solutions (Holt, 2013), thus making the task of detecting or preventing their activity difficult for law enforcement agencies.

4. The paradox of the social media in the Middle East

The social media are mostly used as a crime prevention tool, and the history regarding when the social media are used as an effective instrument for crime prevention is full of bright examples (Golbeck & Klavans, 2015). Recent events in the Middle East have, however, revealed paradoxical elements.

A number of revolutionary events have taken place, which, without the social media, would never have taken place, notably the prominent role played by Facebook and Twitter in the Egyptian revolution. The social media played a detrimental role in undermining the Egyptian authorities under Hosni Mobarak (Thompson, 2013). By all standards, they contributed to the people's rebellion by providing a tool for communication and freedom of expression. The same scenario can be discerned in Libya.

At the outset, it was difficult to judge who was right and who was wrong. However, a close examination of these events reveals that the social media played a dual role. They served as an instrument for advancing political interests in various countries in the Middle East and the role of liberation for those aspiring to freedom (U.S. Army Command and General Staff College, 2014).

From this perspective, one can speak of the paradox of the social media, implying that the social media can be a useful and necessary tool for advancing political interests in different countries, even the overthrow of a government, while at the same time serving as a tool for the prevention of commercial crime. These roles will always be taken into account in further discussion of the advantages and disadvantages of cyber crime prevention.

5. The social media against terrorism

The social media are very effective in the hands of terrorists, who tend to use it in order to propagate their ideology. Deploying the social media against cyber terrorism can be very effective, but it should be taken into account that there has to be very strong and sophisticated methods to enable law enforcement bodies to reflect their attacks (Renfer & Henriette, 2008).

Terrorists usually use various forums and discussion boards in order to communicate between them (Renfer & Henriette, 2008). There were cases when they asked permission to initiate offensive action through discussion boards, and received permission to do so from persons holding religious authority (Renfer & Henriette, 2008).

In such cases, it is always useful to be aware of their use of language, their techniques, habits, the frequency and subject of their inquiries (Renfer & Henriette, 2008). These elements will help in preparing for the next inquiry and enable investigators to determine the probable location of the terrorists.

Terrorists, especially members of ISIL, effectively use video broadcasting in the social media as a tool to influence and brainwash people (McCants, 2015). They use videos for dual purposes: either to create a horrendous effect on people, or as a device for recruitment. The videos effectively demonstrate the horrors and bitterness of terrorism. However, there should be a systematic approach; spontaneous video campaigns are unlikely to contribute to the fight against terrorism.

6. Social media as a tool for combating cybercrime in Saudi Arabia

6.1 Overview

Social media is used as a good platform for committing crimes. This is a well-known and undeniable fact. If the social media can be used as an effective tool for detection and prevention in real life, could they also be useful in the detection and prevention of online crime?

Online crime is a more complicated and sophisticated type of criminal activity and it is; therefore, more difficult to find different tools of deterrence than those used to deter ordinary real-life crimes. The reporting system that is quite popular for crime detection and deterrence purposes may not be sufficient for the purposes of online crime detection.

How can the social media be effectively used to detect cybercriminals? The utility of social media is in the fact that it unites not only people to befriend each other, but also people who unite in order to commit crime.

The social media can prove effective in the detection of 'constant' organized crime groups (Golbeck & Klavans, 2015), but hacker groups are not always constant, and therefore, require other methods of detection.
Surprisingly, cybercriminals *can* be discouraged from using social media as they do not give complete anonymity and it is not impossible to trace them. This is because, in most cases, cybercriminals do not know each other personally and their actions are coordinated using online technologies.

A hacker who wants to remain anonymous will resort to fake names or photos, and thus, a representative of a law enforcement agency can categorize these potential perpetrators. However, anonymity can also be used by regular citizens, who do not wish for their identity to be revealed for personal reasons.

It is reasonable to examine the conduct of a person using a fake photo. Terrorists tend to use fake names or nicknames and publish various posts, mostly on Facebook, Twitter or other online forum boards, with incitement to hatred or violence, or use propaganda to disseminate terrorist ideas or group activity.

In such conditions, it is better to group all posts written by this person under one name for comparison and to judge whether they conform to pursue one aim. It is true that, to detect a cyber-terrorist, it is not sufficient to follow where his posts lead to, but also to closely compare grammar and cultural references. Even though one can glean much information about this perpetrator, it is questionable whether one can identify him, because using a fake account possibly allows him to remain in deep secrecy.

On the other hand, the logic of their 'posts' will enable law enforcement agencies to understand when the next terrorist attack may happen. If it is relatively easy to trace terrorists, it is almost impossible to trace cybercriminals who are engaged in commercial crime.

For example, the identity of 'spammers', who are mostly online criminals, is almost impossible to trace. The social media in this case may help to prevent victims from getting into the hands of spammers. Raising awareness is one of the effective methods of preventing spam. There are posts on various social media, including Facebook, LinkedIn and Twitter, containing warnings about the activity of various scammers, not to open emails from unknown sources. These warnings help to make users aware of the dangers of opening 'spam'. Social media are a locus where awareness campaigns can be conducted on a large scale to reach a wider audience. The law enforcement agencies, in cooperation with social media owners and enthusiasts, can conduct massive campaigns and warn a huge number of users about new threats. They can also launch safe modes or antivirus means to help users detect or to understand whether or not a browser is safe.

It is difficult to deter online crime using social media when it is committed on behalf of law enforcement agencies. For instance, there is a well-known virus called FBI, where the perpetrator pretends to be an FBI agent inviting you to open a spam message or follow its content. For the FBI and other law enforcement agencies, it is feasible to conduct campaigns on the social media where emails coming from another agency should not be regarded as coming from the FBI and should not be opened at any price.

In Saudi Arabia, this may a be very effective tool, because the large number of people using WhatsApp on their phones makes the awareness campaign highly effective by reaching nearly all of the citizens in the Kingdom. The difficulty arises when a virus or spam message is sent using a social media site. There was a Trojan virus called SASFIS, which enabled messages coming from Facebook, and induced users to open it. After opening this virus, the whole software was infected.

In Saudi Arabia, many users received the SASFIS file from Facebook and, as a result, this virus infected their software. In this case, if the Saudi law enforcement agency had cooperated with WhatsApp, this threat would have been prevented. Moreover, Facebook and other social media sites could have introduced a set of tools aiming to prevent spam and viruses appearing or penetrating sites visited by local users in Saudi Arabia.

6.2Using Facebook to combat cybercrime

Facebook is the largest and most popular social media website in Saudi Arabia. Since its inception in 2005, it has attracted many users all over the world. It has been used in both social and business networks.

The capabilities of Facebook are vast, and it can be used for the purposes of cybercrime prevention. It has a number of simple but very useful functions, which can be effectively deployed for the purposes of combating cybercrime particularly in Saudi Arabia.

Facebook can be primarily used to find perpetrators using the following functions: (i) by name; (ii) by email address; (iii) by known associations and (iv) by 'likes' (Golbeck & Klavans, 2015).

Looking for a perpetrator on Facebook by his or her name or by email can be questionable at first glance, since perpetrators do not use their original names or emails. However, most perpetrators use the same name, surname or abbreviation combinations; these functions can, therefore, prove to be very effective in many cases.

The same applies for finding perpetrators by known associations. If a perpetrator is a spammer who frequently sends invitations to join a group or 'like' pages, he or she often has the same kind of friends involved in the same kind of activities (Golbeck & Klavans, 2015). For these motives, it is reasonable to allocate the perpetrator by association.

Finding by 'like' is yet another effective way of tracing a perpetrator on Facebook. For instance, the same spammer would like pages related to his or her activity.

The next way of detecting a perpetrator on Facebook would be by obtaining data about him or her activity (Golbeck & Klavans, 2015). Their timelines are good places for obtaining information about them, but in most cases, they would either restrict viewing their timelines or would not post anything there. The same applies to their personal profile, where they would publish false information that would attract someone to befriend him or her.

However, the best way to identify a perpetrator on Facebook is to trace his or her activity. A spammer would continuously join groups with the same themes or topics, or a spammer would continuously 'invite' to the same kind of pages or groups

(Golbeck & Klavans, 2015). The analysis of his or her activities would be of great help in identifying this person.

Facebook has a very valuable and useful function, that of location information (Golbeck & Klavans, 2015). Whenever someone publishes a post, Facebook shows where this person is located. It is easy to find where a perpetrator resides by gleaning this information.

6.3 Using Twitter to combat cybercrime

Twitter is a major competitor of Facebook, being one of the most popular and largest social media websites in Saud Arabia. The major difference between Twitter and Facebook is that it allows the posting of short posts ('tweets'), with or without links.

There are two major methods of finding perpetrators on Twitter, namely by 'search' and by 'follow lists'. Unlike Facebook, Twitter generalizes search options, and if the name of the person or persons is inserted, it will return with many tweets where this person has twitted (Golbeck & Klavans, 2015).

Searching by following lists on Twitter corresponds to finding people on Facebook by association (Golbeck & Klavans, 2015). It is more effective, because it gives, not only information about one person, but a whole range of associated persons.

With regards to Facebook, one can also obtain information about person or persons by using the following patterns: (i) user profiles; (ii) tweets; (iii) tweet time; (iv) tweet location; and (v) following lists (Golbeck & Klavans, 2015).

User profile on Twitter does not contain as valuable information as on Facebook, but it has certain information that can be of particular value for the investigator (Golbeck & Klavans, 2015). Moreover, Twitter has an expanded profile information section, almost resembling the profile information on Facebook.

Tweets may not be as useful as the 'hashtags' in them. Hashtags are a very valuable source of information, and one can trace perpetration through hashtags on Twitter (Golbeck & Klavans, 2015). Moreover, in most cases, perpetrators' tweets tend to be the same,as far as spamming isconcerned.

Tweet time can also be a valuable tool for locating a perpetrator. For instance, a perpetrator may have a tendency to commit crime at a specific time of day. Alternatively, if a perpetrator commits crime at night-time, it signifies that he or she may live on another continent. If a perpetrator commits an act at the same time every day, it may imply that he or she may have access particularly at that time. It may also imply that there may not be proper internet connection where the perpetrator resides.

As in Facebook, location information can be equally useful in Twitter. A Twitter's location may give an idea as to where the criminal perpetrator resides. However, this function can be circumvented by using a proxy server.

6.4Using Pinterest to combat cybercrime

Pinterest is also one of the largest social media websites in Saudi Arabia, but it is not as popular as Facebook or Twitter. Its value as a tool for combating cybercrime is comparatively low in comparison with the above mentioned giants.

There are generally two ways of finding alleged perpetrators on Pinterest, namely via search and via user profile (Golbeck & Klavans, 2015). There are generally two ways for searching people, namely by their actual name and their user name.

One can also obtain information about the supposed arbitrator on Pinterest by going to the main page of the person or browsing through boards, which can offer valuable information (Golbeck & Klavans, 2015). It is rather questionable whether Pinterest can be as useful and effective in combating cybercrime in Saudi Arabia as Facebook and Twitter. There are some reasons for such an assertion. First, Pinterest mostly gathers people together who have the same interests, which in most cases are expressed through pictures. There is no interactive communication between users as in Facebook and Twitter. For this reason, it is unlikely that perpetrators would use this platform.

Secondly, even though it is a very good platform for perpetrator action, it is nonetheless a blank page for investigators. They may go through pages and may be able to identify alleged perpetrators if they already know about their preferences (Golbeck & Klavans, 2015). Otherwise, it would be in vain to go to Pinterest without preliminary information about the alleged perpetrator.

There is, however, a good example of where a perpetrator was found via Pinterest, namely in the case of Shannon Conley, who was arrested on terrorist charges (Golbeck & Klavans, 2015). Even though it was impossible to trace her terrorist activity by browsing her page on Pinterest, her *burka* and violent anti-Christian posts uncovered her identity.

In the case of Saudi Arabia, the picture may be different. That is because the majority of Saudis are religious and all women wear the *hijab*. For this reason, it would have been difficult to determine whether she was a terrorist or not. Even by browsing her posts, which may call for holy war, one cannot say whether she had terrorist intentions, since holy war is an obligation in Islamic law, which is major law in Saudi Arabia. Neither is it a crime to speak about holy war in Saudi Arabia, and it is not a crime to incite hatred in posts against other religions.

6.5Using LinkedIn to combat cybercrime

Even though LinkedIn cannot be compared to Facebook and Twitter, in terms of popularity, it is nevertheless a very effective tool in combating cybercrime. One can find people generally in two ways, namely via search and via known associates. LinkedIn has the very good function of classifying LinkedIn friends into 1st, 2nd and 3rd connections (Golbeck & Klavans, 2015). This allows understanding through whom this person can be found or whether he or she has any already known connections.

One of the advantages of LinkedIn is that it can be effectively used to detect online perpetrators involved in fraud and employment spam. For instance, there was a well-known spam sent on behalf of Exxon mobil, in which the applicant was invited to send his or her CV; when that CV matched all the requirements, the potential victim would be called to interview. An apology was subsequently dispatched with a note, saying that, due to quality issues, the would-be-employee should fill out a questionnaire. After filling out and sending back the questionnaire, the supposed Exxon mobil HR specialist sent out information that the person had been successful, and enclosed a contract stipulating a huge salary, as well as the fact that Exxonmobil

would cover all costs, on condition that the candidate should pay a certain amount of money for a work permit.

This kind of spam is well known and has been discussed on various discussion boards, but how could the perpetrator be identified? First, when one looks at his or her profile, it does not have a picture, or it has a picture of a certain object, but not a person. His or her account has been set up only recently and he or she has few friends, which makes it obvious that it is an online fraudster.

This type of spam can be very relevant in Saudi Arabia, where young people may be interested in getting jobs abroad with high salaries. Without proper knowledge of the business environment and the English language, the majority of youngsters believe that such emails are from a genuine employer, and cough up the fees for the work permit without further hesitation.

It is also worth noting that these fraudsters intentionally use prominent Muslim names in order to attract the attention of victims, making them believe that they would not be deceived or cheated. It makes their task easy and without complication.

Nigerian fraud also has widespread online crime, committed on LinkedIn. Unlike employment spammers, they use pictures and very convincing words to induce victims into making payments. Both Nigerian fraudsters and employment spammers tend to suspend their accounts after committing an illegal action, and then disappear. For this reason, it is difficult to trace their identity. However, their activities can be thwarted by conducting awareness campaigns on LinkedIn, warning every user that messages with specific content should be ignored and reported to LinkedIn.

This is by far the most effective way of preventing this type of online crime. It is quite impossible to detect or punish the perpetrator. However, law enforcement agencies may think about cooperating with LinkedIn in determining the possible location of the perpetrator. It can help both the agency and LinkedIn effectively fight this type of online crime. This is also a matter for careful analysis, but conducting such analysis requiresa certain expertise, which the ordinary Saudi law enforcement officer lacks.

Moreover, LinkedIn contains the profiles of almost all large corporations in the world. This, in turn, makes the task of verification of whether or not a certain person is an employee of the company he or she claims to be from (Golbeck & Klavans, 2015).

6.6Using Instagram to combat cybercrimes

Instagram is another frequently-used social medium in Saudi Arabia. It is distinct from other social media, mainly in that it is photo oriented. It allows users to share recent or not very recent pictures with captions and allows other users to ‘like’ or comment on them (Golbeck & Klavans, 2015).

Unlike Facebook, Twitter, LinkedIn and Pinterest, Instagram offers a variety of opportunities for investigators to locate potential perpetrators, by mobile application, search services, username and social connection.

Since Instagram is photo-oriented, it is most difficult to locate a person involved in online crime. The exception can be cyber terrorists, whose outward appearance can

be a good indicator as to whether they are involved in terrorist activities. Moreover, Instagram can be an excellent tool in detecting and preventing sexual offenders, who are not online criminals.

As with other social media, the function of obtaining information on Instagram through user profiles, hashtags, social connections and location data can also be used (Golbeck & Klavans, 2015). Again, Instagram may not be that effective in fighting cybercrime, particularly in the context of Saudi Arabia, with the exception of some categories like cyber terrorism.

6.7 Using YouTube to combat cybercrime

YouTube is the largest video-sharing social media website in the world. It is very popular in Saudi Arabia and, as has already been indicated, it serves as a substitute for TV in Saudi Arabia. YouTube is nearly always used by both perpetrators and victims. It is very popular among terrorists, who use it as a tool of effective propaganda for their ideology.

Since the videos on YouTube are a main source of information, the identity of a perpetrator cannot be established by examining the profile pages or the associates, but by watching the video (Golbeck & Klavans, 2015). However, YouTube is not as effective as Facebook, Twitter and LinkedIn in combating cybercrimes.

There are several reasons for that. Firstly, online criminals, including fraudsters and spammers, almost never broadcast themselves. Secrecy is one of the main characteristics, and YouTube does not guarantee it when it comes to broadcasting (Golbeck & Klavans, 2015). Again, as with Instagram, YouTube is very effective in locating cyber terrorists and sexual offenders.

6.8 Using forum and discussion boards to combat cybercrime

Forums and discussion boards are probably the most effective instruments in fighting cybercrime, for several reasons. Firstly, forums and discussion boards are loci where many victims of online crimes exchange their bitter experiences. Secondly, the forums and discussion boards are the most appropriate platforms for conducting awareness campaigns against certain types of online crime. Thirdly, online forums and discussion boards provide unique opportunities for investigators to gather valuable information about perpetrators for detection and information about their location. It also enables investigators to devise techniques that may prevent online crime in the future.

As such, forums and discussion boards serve as an exchange and information hub for investigators and ordinary internet users. By visiting online forums and exchange boards, it is possible to ascertain whether or not users were victims of online criminals or not. These forums and exchange boards mostly unite enthusiasts, and, as such, are free platforms for exchange and discussion of ideas.

Conclusion

This paper has attempted to demonstrate the feasibility of social media instruments in combating cybercrime, but it also provides a useful insight into the essence of online crime, explaining the motives for committing online crime and highlighting the paradoxical nature of the social media, particularly in the context of the Middle East.

It has also addressed the issues critical to social media, and demonstrated "what", "when", "why" and "how" cybercrimes can be fought through the social media, with special reference to Saudi Arabia. Saudi Arabia is sometimes seen as a backward country in terms of social media, but this paper demonstrates that it is, in fact, at the forefront of the social media world, being one of the progressive countries in terms of increasing its use within the boundaries of the Kingdom.

It is not an overstatement to refer to the high utility of the social media. Despite the assertions of many that social media is a very effective tool as far as utility for the purposes of combating cybercrime is concerned, it could be argued that their role is relative. It means that the phenomenon of the social media has not been studied particularly well, which indiscriminately puts in doubt to the notion that they cannot be an adequate platform for combating cybercrime.

Only in conjunction with other tools and techniques can the social media be an effective tool for fighting cybercrime, particularly in the context of Saudi Arabia. In addition, Saudi Arabia does not have an elaborate framework for coping with the problem of cybercrime, and even social media cannot fully contribute to this mission.

However, one should not underestimate the value of the social media in fighting cybercrime, and it should be given a chance, since they are becoming increasingly popular, not only in Saudi Arabia, but also in the Middle East.

The discussion over its feasibility shall continue until a sure framework is developed, and until the law enforcement agencies have worked out a clear strategy.

References

i. Aarts, P. & Roelants, C., 2015. *Saudi Arabia: A Kingdom in Peril*, 1st edn, Hurst.

ii. Anderson, N., 2013. *The Internet Police: How Crime Went Online, and the Cops Followed*, 1st edn, W. W. Norton & Company.

iii. Bernard, H., Hegghammer, T. & Lacroix S., 2015. *Saudi Arabia in Transition: Insights on Social, Political, Economic and Religious Change*. Cambridge University Press

iv. Casey, E., 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd edn, Academic Press.

v. Golbeck, J. & Klavans, J. L., 2015. *Introduction to Social Media Investigation: A Hands-on Approach*. Elsevier

vi. Holt, T. J., 2013. *Crime On-Line: Correlates, Causes, and Context*, 2nd edn, Carolina Academic Press.

vii. Kawasaki, G. & Fitzpatrick, P.,2014. *The Art of Social Media: Power Tips for Power Users*. Portfolio.

viii. McCants, W., 2015. *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*. St. Martin's Press.

ix. Renfer, M. A. & Haas, H. S., 2008. Systematic Analysis in Counterterrorism: Messages on an Islamist Internet-Forum. *International Journal of Intelligence and Counter-Intelligence*, 21(2), pp. 314-336.

x. Thompson, D., 2013. *Away with the Gatekeepers: Social Media as a Tool Facilitating Nonviolent Struggle During the 2011 Egyptian Revolution*,1st edn, Create Space Independent Publishing Platform.

xi. U.S. Army Command and General Staff College. 2014. *Social Media and the Arab Spring: How Facebook, Twitter, and Camera Phones Changed the Egyptian Army's Response to Revolution*. Create Space Independent Publishing Platform.

Electronic Resources:

xii. Penetration of leading social networks in Saudi Arabia, As of 4th quarter 2014. Available at: http://www.statista.com/statistics/284451/saudi-arabia-social-network-penetration/

xiii. Saudi Arabia Profile–Media. Available at: http://www.bbc.com/news/world-middle-east-14703480 (Accessed January 23, 2015)