THE IMPLICATIONS OF SOCIAL MEDIA ON UAE NATIONAL SECURITY

A STUDY OF THE POTENTIAL THREATS AND OPPORTUNITIES

ABDULLAH MOHAMMED AL BLOOSHI

JAN 2015

A thesis submitted to Khalifa University of Science, Technology and Research in accordance with the requirements of the degree of MA in International and Civil Security

ABSTRACT

These days, the negative security implications of social media have become the mainstream of the major events in the world as it poses serious threats to state interest and national security. Essentially, the events of the Arab Spring, and the majority of world riots and protests have recorded the depth of this relationship between the social media, security implications and those events. Indeed, social media have become a source for the promotion of a culture of extremism and violence, revealing the ideology of radicals, extremists and terrorists. Today, the negative role of social media is increasing as a result of a number of manipulative factors. The most far-reaching weapons available for their influence on mass consciousness is more being used, by political forces of numerous nations, and global religious organizations in order to artificially widen the gap between societies, and sometimes even to incite extreme forms of hatred. Attempts are being made to encourage the increased energy of aggression in groups on both sides of arguments to cause a political crisis or even a civil war.

This research here addresses the term national security in relation with the public security interconnected with state stability, respectively it study and analyses the potential threats and opportunities introduced by this new form of media. The major sections of this research outline the impacts of social media networks on national security, which relates to the stability of state and public safety. The research will shed light on the best intelligence and global strategies used to mitigate and respond to those threats that violate the laws, encourage violence, chaos, spread of sedition, and corruption in society. The absence of systematic techniques and reliable strategies to tackle these threats has added heavy challenges to national security during the growth and high penetration of social media. Global statistics show there are 1,856,

680, 860 active social networks users with 26% of social media penetration. (Wearesocial, 2014)

The research identified that United Arab Emirates requires a reliable strategy to best serve its nation's security, particularly as UAE has the highest social media penetration rate in the world (equal to 80%), and the highest mobile penetration (252%), while the average time users spend on social media each day is 3 hours and 17 minutes. (Wearesocial, 2014)

The research will essentially review different literature, research, and project publications, to answer the research questions. Based on findings the research will propose an operational strategy to enhance national security use of social media to protect the country and to address the potential threat that destabilizes nation's security and destroys the stability of society.

DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Khalifa University of Science, Technology and Research. The work is entirely my own except where indicated by special reference in the text. Any views expressed in the thesis are those of the author and in no way represent those of Khalifa University of Science, Technology and Research. No part of the thesis has been presented to any other university for any degree.

Signed: _ Abdullah Mohammed Al Blooshi_____

Date: _ FEB 2015_____

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

FIGURES

TABLES

ABBREVIATIONS

UAE: United Arab Emirates

USA: United States of America

UN: United Nations

CIA: Central Intelligence Agency

DHS: Department Of Homeland Security

SNMC: Social Networking/Media Capability

FBI: Federal Bureau of Investigation

SM: Social Media

SOCMINT: Social Media Intelligence

OSINT: Open Source Intelligence

IRC : Internet Relay Chat

ICT: Information and communications technology

WMD: weapon of mass destruction

OSC: Open Source Center

SOIC: Strategic Information and Operations Center

HNSC: Higher Council of National Security

NESA: National Electronic Security Authority

NCEMA: National Crisis and Emergency Management Authority

ECSSR: The Emirates Centre for Strategic Studies and Research

MBR: Mohammed Bin Rashid School of Government

DEFINITIONS

Crowdsourcing: leveraging crowds through social media to provide you with information and help you solve problems. (Gupta, Brooks, 2013)

Social Media: as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. (Boyd, Ellison, 2007)

Malware: refers to software that is purposely designed to damage, disable, or obtain sensitive information and can impact tablets. (Nelson, 2014)

Cyber bulling: the intentional and repeated harm of others through the use of computers, cell phones and other electronic devices. (Li, Cross, Smith, 2012)

Espionage: the act of obtaining secrets from individuals, groups, organization, and governments by exploiting weaknesses in the Internet, software, or computers. (Hastedt, 2011)

Cyber terrorism: a cyber attack using or exploiting computer or communication networks to cause sufficient destruction or destruction to generate fear or to intimidate a society into an ideological goal. (NATO, 2008)

1. INTRODUCTION

Contemporary culture is inextricably linked with social media, and the majority of our information needs are now met through online channels and social networks. This has resulted in "new communication practices, a new type of world perception and a new way of life." However, although popular, the use, prominence and dominance of social media networks has become controversial, particularly within the socio-cultural realm, because it threatens to decentralize culture, identity and nationalism. Not only have social media networks made a significant contribution to the advancement of technology, they have also provoked a number of interesting trends that embody the very basis of contemporary culture. Through offering several different forms of communication, e.g. videos, images and text, within a single platform, the depth of the message become more powerful and vast and can spread much quicker than ever previously imagined. Furthermore, a much wider variety of information is available than was previously possible via traditional forms of media (Cockburn, 12). Through combining various forms of technology with social media networks, traditional special and temporal constraints are diminished, and information spreads freely and without constraint. As the majority of popular social networks are accessible free of charge, there is no inhibitive cost that prevents them from being available to all members of society at all levels (Robbins, Judge, Millett, Boyle, 2011).

Of particular importance in the Arab world is the rise in popularity of mobile social media. Mobile phones and tablet devices provide people with access to social networks from any location, at any time, and people are no longer constrained by the need to be tied to a PC. Rapid growth has been observed in amount of mobile phone users since the 2000s in the, and an especially remarkable performance was shown by the UAE, where since 2002 the number of mobile phones per 100

people increased by a factor of 23. Approximately the same results are observed in the number of Internet users: for example, today in Egypt this figure corresponds to the Arab average and is 26 Internet users per 100 people. (GSM Association, 2013)

It must be borne in mind that the majority of users of mobile phones and the Internet are among young educated, active, English-speaking people. That is not surprising since, in the major cities of Tunisia, Egypt and UAE, the so-called "youth bumps", that is, a sharp increase in the proportion of young people in the population in general, are observed.

The research **shows that in most countries, the most actively used social media, as a resource for protests, is Facebook** with the exception of Bahrain and Syria. In Syria, this is explained by the blocking of many Internet resources, including Facebook. In Bahrain, a similar situation may be associated with the rather precarious situation of the country; in addition, the monarchical nature of the state has a certain effect on the tightening of the controls and restrictions in the media space. (Lynn, 2010)

In the analysis of the most popular websites in the Arab world there are two main trends. On the one hand, a significant number of Internet users choose western resources, such as Facebook, YouTube, Google, etc., which are constantly within the top five most visited sites in each country. On the other hand, as noted above, the volume of Internet content in Arabic is actively growing: relevant applications for mobile phones, as well as Arabic domain names, are becoming increasingly available. At the beginning of 2013, in the Arab world, 51 million Facebook users out of approximately 360 million inhabitants of the Arab countries were registered. These statistics were published by Mohammed Bin Rashid School of Government. 13.5

million Internet users created Internet accounts on Facebook in 2012. The study also **indicates that 25% of Facebook users in the Arab world are people from Egypt, and 80% of users from the Gulf Cooperation Council states live in Saudi Arabia and UAE.** If we take the number of Facebook users in the Arab countries regarding population, the first place for a long time has been occupied by the UAE, followed by Jordan, Lebanon, Qatar and Tunisia. Experts also note that the Arabic language to date reflects the rapid pace of development in the various social networks, which are popular in the region.

Most observers agree that, social media networks with their endless tentacles into different regions are inherently a harmless technology, designed to facilitate banal idle chat, but have acquired features of the WMD threatening the stability and security of individual countries and the international community as a whole.(Carole, 2011). The illicit uses of social media can cause a number of negative impacts on national security and adverse consequences for the **nation's strategic interests** (Montagnese, 2012). Since January 2011, North Africa and the Middle East countries have been swept with an unprecedented wave of social protests that resulted in the resignation of the regimes in some countries, repression interspersed with feverish reforms in others, and even a civil war and the collapse of the actual state. Those events are known as the Arab Spring or the Twitter / Facebook-revolution. The second of these names reflects the feature characteristic of most events of Middle East protests - unprecedented active use of information and communication technologies (ICT), especially social networking services, by protestors. After the riots in 2009 in Iran and Moldova, the Arab Spring has cemented the discourse among the politicians, experts and media "ICT (especially social networks) as a factor of unrest and revolutions". Social media is considered overall an expectable challenge that poses a potential threat to national security.

However, social media can also result in incredible opportunities for nations in order to attain their pertinent strategic goals. The significance of research is not only

in studying the effects of social media on national security and predicted threats and risks, but, based on the findings, it will be easy to formulate strategies in line with the priorities of national security while ensuring personal freedoms through joint cooperation between governments and the public to protect national security, because this means security for all. That relationship must be complementary, combining social media and national security institutions and community partnership on the basis of their mutual awareness. However, creating regulations and strict laws are not sufficient to tackle threats of this phenomenon because this alone does not guarantee to safeguard the nation's security. In fact, surveillance and SOCMINT alone will not achieve any progress without clear strategies to counter and mitigate those threats and potential vulnerabilities. There are however technologies such as Anti which allow determination on whether users, by opening encrypted communications, are breaking existing controls.

1.1 STATEMENT OF THE PROBLEM

The dramatic growth of the social media networks across the globe has altered the concept of information sharing and communicating via the Internet. It has affected e-government, military, business, education, politics and national security. The Internet is transforming society by propelling economic development and giving individuals a new means to connect and collaborate with each other (Montagnese, 2012). Given the declining costs, accessing the Internet has become easier and cheaper, permitting more people around the world to use social media, ‘democratizing' the application of technology, and facilitating the flow of invention and productivity. In fact, it has lead to a quick and easy manipulation of public opinion, and the imposition of ideological attitudes based on distortion of facts. Unfortunately, experts admit that today's society is not able to deal with these

destructive processes and can only take pathetic attempts to limit the power of collective intelligence criminalization through legal and administrative methods. Nevertheless, the negative role of social media is getting worse because of a number of manipulative factors as it being used by political forces of various countries and global religious groups in order to artificially widen the gap between societies, and sometimes even to incite extreme forms of hatred. Attempts are being made to lever the increased energy and aggression in groups on both sides to cause a political crisis or even a civil war.

1.2. RESEARCH AIMS, OBJECTIVE AND QUESTION

The research aim is **to study the implications of social media on the national security, in addition to examine whether those new challenges and opportunities introduced by this new media may allow it to become a primary source of intelligence to serve a nation's security**. By identifying those relevant facts, this study will recommend an effective strategy and propose operational strategies and technical solutions for United Arab Emirates to mitigate social media impacts on national security.

This thesis comprises four sub-questions related to the research study in order to provide a comprehensive analysis of the hypothesis.

1.2.1. Specific objectives include:

a) Determining the challenges of social media networks and the best practice global strategies used to deal with the threats, including countermeasure strategies and Open Source Intelligence (OSINT) applications.

b) Providing a current snapshot of the new threats and opportunities concerning the usage of social media by structured groups and to gauge its presence.

c) Identifing the implications of social media on UAE national security, and providing the strategy.

1.3. RESEARCH QUESTIONS

This study based on the correlation research methodology will mainly review different literatures, a research project, and publications to answer the research questions:

- What are the impacts of social media on UAE security and how can they be mitigated?
- Do the characteristics of social media present a potential threat to national security? If so, how?
- Does the gathering of open source information in social media networks offer a new potential opportunity to national security? If so, how?
- What is the reliable framework to deal with social media network impacts?
- What are examples of current policy or research to mitigate the potential threats of social media networks?

1.3.1 Sub questions:

- How can social media analytics reduce the vulnerability of unrest?
- Can social media monitoring predict threats from groups, individuals and automatically assess hot topics and judge behaviors?
- How can law enforcement benefit from social media monitoring? Can it help in investigating and reducing crimes?
- How reliable are public information sources?

1.4. HYPOTHESIS

The hypothesis claims the exploitation of information from social media networks contributes to decision and policy-making and increases the ability to mitigate potential threats to national security, and thus creates an opportunity for countries.

Hypothesis 1: Social media is a rich source and is considered a potential opportunity for national security.

Hypothesis 2: Social media is considered a potential threat to the national security.

Hypothesis 3: United Arab Emirates require a reliable strategy to mitigate the risks of social media to national security.

1.5. SIGNIFICANCE OF THE RESEARCH

This research will examine how social media is considered a potential threat to the national security in UAE. Respectively, the study will propose an operational strategy upon reviewing best practice methods to enable the national security decision-makers to overcome and mitigate those influences by harnessing the power of social media. The significance of this paper is divided into:

A. The theoretical importance of the study, which is identified as follows:

1. To determine the impacts of social networks on the national security system and to determine on what level those impacts can be vulnerable and cause potential threat to national security.

2. To recognize the ability of social media networks to effect social change among users through what has been published from the viewpoints of political criticism and sarcasm that may lead to the recruitment of users to adopt destructive ideas.

3. To use the information available on social media networks to predict and understand the size of the vulnerability before it is too late, by measuring the pulse of public opinion toward public issues and changes in the region, as well as the new state policies and decisions.

B. The practical importance of the study, which has been identified in the following elements:

1. Assist decision-makers in employing the results of this study to resolve the implications of improper use of social media technology, by adopting strategies and systems to combat the negative elements that may pose a threat to national security, while recognizing the ability of social networks to change attitudes and adoption of ideas.

2. Officials at National Security authorities will benefit from the study, as it will classify the positive and negative effects caused by social networks on public opinion, then work to mitigate those effects by finding appropriate solutions, finally constructing appropriate decision making policies in accordance with the factual evidence available in order to propose a reliable & effective policy for dealing with future threats.

1.6. SCOPE OF THE STUDY

The scope of the study is to offer a current picture of the implication of social media on national security, particularly investigate the potential threats and opportunities exists in social media. Identifying the opportunities in social media can be approached by analyze case studies and discovers the best practices used by several states and other leading national security organizations to counter the riots and fight against the extremist and radicalization ideology in the social media.

1.7. RESEARCH METHODS

This paper will continue from other studies, which have examined the overall implications of social media on national security. The research adapted a descriptive analytical approach focused on retrieving information by surveying literature from books, articles, journals, projects publication, newspapers, guidance and analysis reports to support the hypothesis in the paper. In addition, this paper will conduct semi structure interviews to examine and answer the research questions and validate the three hypotheses.

1.8. STRUCTURE OF THE THESIS

The structures of this thesis are constructed in six chapters; it will begin with an abstract, then followed by chapters and finally close with appendix. Chapter 1 presents with an introduction. Chapter 2 provides a review of the literature, and deals with the implications of social media on national security, as it seeks to uncover and understand the relationship between social media and national security in order to address the threat and potential opportunities.

Chapter 3 provides a description of the approach taken in the search: as well as discuss the data collection methods to search through conducting interviews, and analysis technique used, as will be described and the constraints faced by the researcher. Chapter 4 presents the conclusions drawn from interviews. Chapter 5 will introduce recommended initiatives for social media strategy for UAE national security. Finally, Chapter 6 concludes with conclusion and recommendations for further research.

2. LITERATURE REVIEW

2.1. Emergence of new information and Social Media

The emergence of social media technologies has significantly altered the way people communicate with one another. As individuals who are positioned within a larger communicative network, the way in which we share our attitudes and opinions with a wider group can serve to mediate and conform to the stereotypes of mass consciousness, while also becoming a stereotype in itself. The exchange of information between the people who participate in a social media groups allows modes of communication that were previously unheard of. Participants can pose any question they like and receive answers from multiple sources, interact in unique ways with an interlocutor, a "notional other," and determine a unique position.

While the vast amount of information that is available online in the post-industrial era delivers many tangible benefits, particularly in the areas of learning and communication, it also introduces new risks (Schillinger, 2011). **Virtual sources of knowledge can have a direct impact on the way in which we act and on how information is proliferated to manipulate not only our actions and thought processes, but also the intrapersonal structures that govern us**. Online interlocutors that exist in a virtual world can become a reference group that have a strong impact on an individual (Fourie, 68) and may start to have more influence on someone's actions and motivations than his or her immediate, physical, family and friends. However, while this creates a lot of threats, it also holds significant potential. When engaged in online communications, an individual forms connections with groups, both real and virtual, and enters into dialogue with numerous factions and associations that can result in new meaning and values. **Understanding the role of**

the individual in contemporary society requires developing detailed insights into how individuals and groups interact within and between each other (Schillinger, 2011). As Toivo (2010) stresses, social media has had a profound impact on the way people communicate in eight distinct ways:

a. It has allowed individuals to interact with others on an anonymous basis. Participants in forums and online communities often use nicknames or aliases when they share their opinions, advice and recommendations. This virtual identity gives then **anonymity**, under which they may behave very differently from they would if they were acting under their own identity.

b. It has increased the richness and **diversity** of the knowledge that is available. Users can access several sources of information and can compare stories, news and information quickly and effectively.

c. It creates **omnipresence**. Information can be readily shared and discussed; there are no hiding places. Public figures no longer enjoy privacy, their entire lives, actions and opinions have become public property, whether they agree to it or not.

d. It provides people with **faster access** to information and resources. The Internet allows news and information to be spread at a rapid rate. However, people's demands for quick access to the latest news and gossip often entails that many false and inaccurate reports are shared.

e. It allows people to assume **multiple roles** through their various relationships with each other. This lack of a clear hierarchy is inherent in social media.

f. It has resulted in **a movement from objectivity to subjectivity**. In some areas of the world, for example the United States, the so-called traditional mainstream media has abandoned any pretense to promote equality and pluralism.

g. It provides the option to combine different forms of media in unique ways. Text, video, photographs and images can be combined to create new vehicles through which information can be shared.

h. It lacks regulation. While government agencies may, and do, attempt to restrict the information that is shared online, traditional censorship activities are not effective, and it is difficult to keep abreast of technology updates.

2.2. Social Media network influences: violent extremism and radicalization

According to many experts, **social networks increase radical sentiments and peoples'beliefs and encourage the growth of nationalism and other forms of intolerance in society.**

Since the dawn of its existence, the psychology of mass consciousness, revealed the fact of "the other" behavior of the individual in a group. Subsequently, **sociological experiments showed a distinct relationship between the factor of involvement in the group and the power of conviction of a person**. For example, if you interrogate a few nationalists separately and determine the extent of their hostility to persons of other ethnic groups in a specific coordinate system, you will get the result of everyone, usually, approximating to the average index (Clarke, Knake, 2010).

However, if we gather these same people together in **one group and give them the opportunity to talk on this subject, we will find that their views have undergone significant radicalization and their intolerance towards "the other people" has turned into hatred and even the motive for aggressive actions.** Today this **mechanism of mass psychology is placed as a bomb in social networks, where citizens with antisocial beliefs create their communities of interest and gradually become criminals** - some only mentally, but some turn their hatred into real actions (Carole, 2011).

Unfortunately, the prognosis is unfavorable, since the rate of gain of xenophobia, nationalism, extremism and other dangerous forms of hatred in society is directly proportional to the velocity of propagation and technological development of social media of instant access. **Social networks not only have revolutionized the whole system of human communication, fantastically accelerating information**

exchange, but have erased the borders of nations and continents. These networks have grouped people, **joining them in communities of interests.**

Scientists on all continents constantly study the degree of correlation between the strength of a person's beliefs and the degree of his involvement in interest groups dedicated to the topic of this belief. In one of the most compelling and representative studies conducted in the United States during 2005, a focus group of 63 people was selected in the state of Colorado. In this group the experts provoked the discussion of three contentious issues: gay marriage, a policy aimed at eliminating the effects of discrimination, and global warming (Abdih, 2011).

It turns out that the faster more people share information with their peers, the more extreme their views become. Cass Sunstein, Professor of the University of Chicago, and one of the authors of the Colorado research project, warns in his book of "Infotopia" a **phenomenon that can "lay the foundations of extremism and fanaticism and even terrorism"** (Schillinger, 2011).

It is easy to guess what phenomenon in today's society plays a **catalytic role in the radicalization of the public mood and even the appearance of paramilitary groups directed against any social, ethnic or religious affiliation.** Let us recall that organized attacks of football fans on their opponents initially undergo the stage of crystallization of intentions through "discussions" on the social networks. Here they receive not only the purely organizational possibilities of the Internet community, but also the hardening of positions of each of the members of this community, which at some point reach their climax in the form of a direct aggression. Similarly, it is **in social media that attacks against infidels in Yemen, Syria and other Islamic countries and massive clashes between Shiites and Sunnis began** (Salem, 2012).

2.3. Literature that identifies the threats and influences of Social Media on national security

There is no doubt that social media is one of the manifestations of the new media that has made people become makers of news, not just its recipients, and formal or traditional media institutions are no longer the only source of information for the material after it has been stormed by individuals

On the other hand, the difficulty of verifying the authenticity of what is published, and identifying the source of a ‘news’ item is considered one of the flaws inherent in this form of communication, and in particular, this has become a significant source of broadcast rumors and lies which represent a major challenge. The dissemination of false information about issues and symbols, national broadcast clips or pictorial inaccuracies can cause disruptions to public security, and play on sectarian or ethnic tendencies that could threaten peace as well as the community. The stage has now been reached where threats to national security include broadcasting manuals for manufacturing explosives, spreading extremely damaging ideas about religions, publishing invitations to commit destructive actions, slander, libel, publication of profanity and moral decay, plus calls for civil disobedience. The operators of propaganda campaigns on social networks manipulate facts and figures, exploiting the lethargy common among the average reader on the Internet, thus achieving their aim. Since the dawn of the Internet, there was the opinion that the spread of the World Wide Web will become a factor in the general increase of intelligence. It was supposed that an increase of availability and speed of access to information would contribute to the interpenetration of knowledge and the development of critical thinking among a growing number of people (Robbins, Judge, Millett, Boyle, 2011).

However, these expectations were not met. **In fact, it has had the opposite effect in the form of the intellectual lethargy and the increasing loss of the ability to think critically**. This, in turn, **leads to a quick and easy manipulation of public opinion and the imposition of ideological attitudes based on distortion of facts.** However, if the popularity of social networks diminishes, its negative role may be significantly reduced as is happening with television. Today watching TV is going out of fashion. It is considered that, as a source of information, this media resource is not credible, and the TV audience is shrinking. If the manipulative trend in social networks continues, soon they may share the fate of the television. However, this day will not come tomorrow. People will have to endure numerous explosions in the escalation of violence in various countries, especially in those that are of political interest for certain global users and operators of social networks.

The significance of the role of social networks in organizing of riots in the 21st century is carefully monitored by law enforcement agencies, protesters themselves, many observers, and analysts.

In particular, annually, the Pentagon allocates more than $ 40 million for the study of mechanisms for identification of protest appeals and propaganda on the Internet. In the New York Police Department, a new division, which will monitor social networks and services, has been formed. The Senior Advisor to U.S. Secretary of State, Alec Ross, calls the Internet the "Che Guevara of the 21st century". In other countries, the attitude to this phenomenon is similar, and similar measures are being adopted (Lynn, 2010).

Essentially, most scholars agree that social media poses threats to national security, case studies of the revolution and riots cross the world have proved the significant power of social media tools in accelerating protests, crowd sourcing, and

collective actions. The figure below outlines the greatest potential threats alongside the social media risks and challenges due to its revolutionary characteristics:

FIGURE 1: THREATS AND CHALLENGES

Defining the threats is only one step in the exploration for the ideal solution to mitigate the social media threats; hence to identify the cause and offenders of the threats is extremely critical for the ultimate solution. Table 1 outlines and classifies the threats, who they are caused by, the tools and practices used, and finally the consequences.

TABLE 1: THE POTENTIAL THREATS TO NATIONAL SECURITY

Classification of threats	Caused by	Examples	Tools & practices	Consequences and threats
Individual	• Hackers • Insider official employees	Anonymous	• Hacking • Malware • Propaganda • Robot	• Privacy risks • Malicious content • Regulatory compliance risks • Loss of control over content • Reputation loss • Negative publicity • Identity theft • Impersonation • Violence and extremism • Online abduction • Terrorist Recruitment • Crowd sourcing • Financial crowding • Propaganda • Protests & Riots. • Online harassment or Cyberbullying
Groups	• Terrorism • Organized crime • Activists • Protesters • Underground cyberspace communities	ISIS	• Propaganda • Malware • Malicious code • Social engineering attacks • Hacking • Counter intelligence	
Organization (state and non-states actor)	• Terrorist • Law enforcement • Intelligence • States • Agency of Human rights		• Propaganda • Malware • Hacking Antigovernment • Public opinion campaign • Counter Intelligence	

2.3.1. Social Media: the digital activism potential threats:

The socio-political upheavals of 2011-2012 that entered history as the "Arab Spring", have become a major test of strength for many seemingly "experienced" political regimes, unfortunately many of them have not been able to respond to the challenges, which have confronted them. The Arab countries were in various stages of readiness to meet their "spring of anger." Events have shown that the region was unable to safely negotiate the necessary processes of a peaceful transformation of society. "Arab Spring" has revealed weaknesses in the economic and political systems in the Arab world, which are mainly related to the main problem in the region - providing a decent level of welfare (Lynn, 2010).

To describe the "Arab Spring", many researchers tend to abuse different terms. They refer to the events as revolution, rebellion, revolutionary wave, civil disobedience, and even the "Facebook youth movement". Inconsistency in terminology can be explained by the extremely controversial nature of changes occurring in the Muslim population of the Middle East and North Africa. The

ambiguity about what actually happened, as well as options for resolving the situation, has caused heated discussions among the expert community. Some experts give priority to demographic problems (prevalence of indicators of births over deaths, percentage of the growth of young people in the communities which is running at 30-50%) and socio-economic problems (inability of the economy to "catch up" with population growth, youth unemployment and lack of prospects).

However, it would be naive to believe that the "Arab Spring" in all countries proceeded in exactly the same way and was due to the same reasons.

Propaganda or psychological warfare has always played an important role in internal and external conflicts. However, with the emergence of the "information society", the meaning of this struggle has increased significantly. Newspapers, radio, television, and the Internet, have spawned flows of information that hit people hourly. Incoming messages are immediately analyzed, dissected, annotated and distributed in real-time mode[1]. A striking example of this is the events taking place in Arab countries. These were generated by a whole set of economic, social, political and ideological reasons. However, modern media also made its contribution to them.

2.3.1. Social media as the engine of the "Arab spring protests, Occupy Wall Street, and London riots":

2.3.1.1. Arab Spring Protests

Political uprisings in the Arab world in 2010, have demonstrated the importance of social networks in **synchronization of mass actions, which overturned presidents of Tunisia and Egypt.** The striking effect of these online resources, destabilizing the entire Arab- Muslim world, was caused by the size of their active users. As of **July 2011, Facebook has brought together about 750 million people**, and the audience of Twitter has increased to 200 million during the same period. Alongside this, it is

[1] Arab Unrest: The Role of Propaganda | New Eastern Outlook. (n.d.). Retrieved from http://journal-neo.com/node/118935

important to consider that the social media did not provoke a revolution, but merely **provided tools that allowed revolutionary groups to lower the costs of participation, organization, recruitment and training.** (Papic, and Noona 2011)

Social networks that have turned, in fact, into news agencies can distribute data around the world in seconds, thereby accelerating the progress of the operation. This does not mean that TV and radio are actually losing popularity: there is in fact a kind of symbiosis between the giants of the largest TV networks and social media, which ultimately enhances the effect of information operations, causing hundreds of thousands of protesters to go to the streets. An example of such interaction was the activities of the international television channel Al Jazeera, hosting videos on its portal in YouTube (Clarke, Knake, 2010).

The **revolution in Tunisia, organized through the World Wide Web, is the result of long preparatory work of the Center for Applied Non-Violent Action and Strategies Canvas (CANVAS).** Founded in 2003 in Belgrade, on the basis of "Other" (the NGO that organized the revolution in 2000 in Serbia, in 2003 in Georgia, and in 2004 in Ukraine and so on), "Canvas", headed by S. Popovich, puts into practice the teachings of the Albert Einstein Institution. The organization's members also participate in seminars funded by the OSCE and the UN. Cooperating with the American "Freedom House" (which, in turn, is supported by the Republican National Endowment for Democracy), by 2011 "Canvas" had prepared activists from more than 50 countries, including Zimbabwe, Tunisia, Lebanon, Egypt, Iran, Georgia, Ukraine, Belarus, Kyrgyzstan and North Korea (Carole, 2011).

This training center arose mainly from the fact that access to transnational information provided to people largely through the Internet, displaces national governments from the process of shaping public opinion. It is noteworthy that in 1991 Tunisia, riding the revolutionary wave, became the first Arab and African country to

connect to the network. Despite the subsequent measures of the country's leadership to take control over the World Web, the number of its users among Tunisians (as of 2005) was 9.5 %, in comparison with Egypt at 6.8%. Due to the level of development of mobile telephony, Tunisia took second place with 56.3 % mobile penetration in the Muslim world, surpassed only by Turkey with 59.6% (Badger, 2013).

The events moved rapidly: having organized anti-government propaganda and coordinating revolutionary actions through Facebook and Twitter (the networks most popular among Arab youth) the opposition captured the main communication arteries of the state. Food shortages, growing with each passing day, undermined the resources and the will of the government, which inevitably affected the army that refused to crush the rebellion by force. Speeches made by officials of the European Union and the United States only accelerated the fall of the regime, convincing protesters of the need for perpetual disobedience to authorities that ultimately forced President Z. Ben Ali to leave the country on January 14, 2011 (Abdih, 2011).

The next arena of **similar application of social networks was Egypt. Expandsion of "Canvas" contacts within the Egyptian opposition coincided in time with a series of strikes in 2008** in protest against rising food prices and low wages. These were suppressed by the police. From this period, the union of Egyptians versed in information technology called themselves "April 6 Movement," and in Facebook created a group for nonviolent actions across the country. **Having gathered 70,000 supporters, they decided to develop the success of network actions, sending their activists to Belgrade for training** (Schillinger, 2011).

Soon, this knowledge was used by the Egyptian Movement for Change "Kifayah" (from Arabic “Kifaya” means "enough"). According to experts from the Carnegie Foundation, "Kifayah" was the first political force in Egypt, which managed to draw maximum benefit from social media and digital technology as a primary means of

communication and mobilization of protests. As an **"independent" political tribune, the blogosphere not only generates the necessary contextual environment, but also collects information about the mood in society, allowing building of the necessary tone of antigovernment propaganda. The very emergence of political blogs in Egypt is mainly due to the activities of "Kifayah"** (Abdih, 2011).

Bloggers, posting online audiovisual files and photos of anti-governmental intent, were the main popularizers of revolutionary ideas. Actively involved was e-mail, text messaging, online advertising and the official website of the movement [22]. Ultimately, the indefinitely continuing protesters, fueled by their actions, made it clear that the center of power was unclear and undecided on how to react to this massive information influence, and therefore failed to bring an army to suppress the protest, before surrendering on February 11, 2011 after eighteen days (Badger, 2013).

A few days later, in Libya on February 15, after the proclamation of 213 intellectuals calling for the withdrawal of Gaddafi's government supported by foreign opposition factions, unrest began in the most financially secure country of North Africa countries. However, non-violent resistance was soon suppressed by the government. Anticipating a similar scenario, J. Sharpe urged protesters in his work to observe the strictest discipline, and not to succumb to provocations of security services and police. The unarmed crowd, whose intention was nonviolent, was helpless before the army, which forced the battle to the enemy on the field where it had superiority (Carole, 2011).

Similar actions had taken place in the People's Republic of China (PRC) in June 1989 on Tiananmen Square where the status quo was restored only through the power line supporters who declared a state of emergency. The only difference between1989 and recent events is that in 1989 America's response was limited to ostentatious indignation. Recently the authoritative Henry Kissinger has said that if Gaddafi

remained in power, the influence of the Stars and Stripes in the Muslim world will be questioned. Based on UN Security Council Resolution 1973 of March 17, 2011, a coalition created by Washington began a humanitarian intervention, which, despite the dominant participation of Britain and France, became the next U.S. mission. Moreover, even after the occupation of Tripoli by allies in late August, and the recognition of the Libyan transitional government, the threat of large-scale civil war between tribal groups, previously hampered by the efforts of Gaddafi, was growing rapidly (Clarke, Knake, 2010).

About a month before the start of the nonviolent Syrian struggle, launched in February 2011 on Facebook, a new group "Syrian Revolution 2011" appeared (with initially no more than 15,000 supporters) calling on Syrian President Bashar al-Assad to step down. By March 15, 2011, protests covered Damascus and Daraa (Sunni south-west of the country, hostile to the Alawites). Next, they affected Latakia, Aleppo and the suburbs of the Syrian capital, scattering after numerous military actions of the government, which led to casualties. As a result, it was the principle of force employed by the Syrian authorities that saved them from falling. Considering these developments in the dynamics of the region, the U.S. private intelligence agency Stratfor, explains the strategic advantages of the Syrian leadership in four factors: 1). All political power in the country is concentrated in the hands of the Assad clan; 2). The Alawites, of which the Syrian elite is formed, demonstrate unity; 3).The Syrian leadership control the military intelligence; 4. The "Baas" Party holds a monopoly on power (Himelfarb, 2012).

Meanwhile, Washington, forcing the events, continued to put pressure on Damascus, introducing international sanctions (one of the 198 methods of nonviolent actions) against members of the security services and the president's relatives. Trade relations between the two countries were frozen. The UN Council on Human Rights has also

not remained aloof, adopting a resolution condemning the use of force against demonstrators. J. Sullivan, the Head of Policy Planning at the State Department went further, threatening, if the president of Syria did not abandon violence, that he will also be included in the list of persons who are subject to sanctions. In turn, the European Union, after consultation with its 27 members, confidently followed the example of their powerful ally (Lynn, 2010).

The information pressure on the Syrian leadership is constantly growing. Under the influence of the tense situation in the region, the State Department all the more critically re-estimates the political situation in Iran, accusing the country's ruling circles of trying to "undermine the Arab Spring" in neighboring states. H. Clinton expressed the hope that in Iran there exists a situation where ordinary people can influence the events, urging the opposition to seek international support, as was the case in Libya. For the first time since 1980 (the date of the severance of diplomatic relations with the Islamic Republic of Iran), the U.S. administration is betting on full use of the World Wide Web to broadcast the "soft power" among young Iranians, and is planning to launch a "virtual embassy" informing people about visas and student exchange programs (Robbins, Judge, Millett, Boyle, 2011).

2.3.1.2. Occupy Wall Street

The first "Occupy Wall Street" action was held in mid-September 2011 in New York. Hundreds of its members, coordinating their actions with the help of mobile devices through chat rooms and social networks, blocked traffic in the southern part of Manhattan to protest against the role played, as they thought, by the New York Stock Exchange (NYSE) and other large financial institutions, in the crisis of the American economy (Badger, 2013).

This demonstration was organized by the Canadian non-profit organization Adbusters Media Foundation, as well as organizations and associations such as ‘MoveOn.Org’, ‘Rebuild the Dream’, and the ‘Working Families Party’. However, by the beginning of October, the subsequent protests had spread spontaneously to many other U.S. cities, and were without a single center. Their characteristic feature was the active use of the popular social networks (Facebook and Twitter). The participants also used social networks to attract the attention of the press. In addition to the microblogs in Twitter and groups in Facebook, the movement also had its own website.

The demonstrations spread to other countries around the world: they took place in Australia, Germany, Italy, Canada, New Zealand, France, the Czech Republic, and Japan. In November 2011, the RBC Daily reported that collectively the demonstrations under this "brand" involved over 1.5 million people (Abdih, 2011).

In view of the examples above, we can conclude that social networks have enormous potential and opportunities for the organization of protests of the masses in almost any corner of the world where the Internet is accessible.

2.3.1.3. London Riots

When the law enforcement authorities began, in turn, using social networks to combat riots, they were effective. For example, Scotland Yard Commissioner Tim Godwin reported that through Twitter and BBM messenger they received information that the Olympic facilities, Westfield shopping center, and Oxford Street shops, could become the target of attacks. The police were able to secure all of these places, and they did not suffer any damage (Carole, 2011).

The Guardian newspaper, noting that Sheffield was one of the few major cities in England not affected by the summer riots in 2011, put this fact down to the merit of the local police who used mobile social media. The newspaper especially highlights

Sheffield police inspector Jane Forrest, who, coming to Facebook and Twitter from her Blackberry device, after long, patient and painstaking work, was able to establish contact with protest activists and communities and to mitigate the conflict between protesters and authorities. She believes that "the occupation of the social communities by the police" is fruitful and promising. (Caldwell, 2012)

2.3.3. Social media: Cyber terrorism threats: (The Islamic State in Iraq and Syria)

The evolution of social networks has created a virtual space, awarding extremist and terrorist organizations the privileges that they are using now for propaganda to support their positions, and influence their supporters to crowdsource and terrorize their opponents. Following this trend, social media is being used to influence the political arena. ISIS has employed social media to promote their campaign to announce the setup of the Iraq and Sham Islamic State, a state that has sovereignty, power, money and an army. Social media has been used for publicity and propaganda with the aim of recruiting, lobbying, crowdsourcing, and to terrorize opponents through the distribution of videos, tweet, pictures of the executions, bombings and killings on the social networking networks like Twitter, Facebook, YouTube, Instagram and other available tools. According to CNN ISIS, is “The first terror group to build an Islamic state”. Agreeing with a French news article (2013) “ The Secretary-General of the Council of Arab Interior Ministers, Mohammed Koman, in the Saudi capital Riyadh, blamed " uncontrollable media " and " social media " for the spread of terrorism". Koman added that **" the spread of deviant and hardline Fatawa fuelled by chaos, media boom and mass communication had significant implications for terrorism, and so we have seen a marked increase in terrorist acts".** (Saudi Embassy 2013)

According to a report by United Nations Office on Drugs and Crime (2012) “Propaganda takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers.” In fact, ISIS has used social media as a propaganda tool. When the Islamic State of Iraq and Syria rolled into northern Iraq in June, CBS News reported on the Sunni militant group's sophisticated and brutal use of social media. Since then, even after U.S. airstrikes and the deletion of many of the group's social media accounts, ISIS has continued to leverage social media to promote its cause and threaten its enemies. (CBS News, 2014)

A report by the UN Security Council obtained by the Guardian (2014), finds that 15,000 people have traveled to Syria and Iraq to fight alongside the Islamic State (ISIS) and other extremist. (Guardian, 2014),

In summary, cyber terrorism will remain a challenge and posed a threat to national and international security. The terrorist and extremist has become an expert using social media that allows for easy access to a platform with greater virtual interaction, and a greater sharing and exchanging of information. For example research shows that propaganda videos containing terrorist-promoting material are able to now spread farther, which is thought to be a contributing factor towards the growing support base for these groups in western nations (Weimann 2010). Hezbollah, Hamas, the Tamil Tigers (LTTE) and an assortment of jihadist groups all have propaganda videos on social media site with the majority of the videos being posted in English or with English subtitles (Bakas, 2014). Figure 2 below shows an example of a twitter page of

ISIS. In addition to Table 2 below that indicated the example of the social media “tweets” for recruitment.

FIGURE 2 SCREENSHOT OF THE TWITTER PAGE OF ANSAR AL JIHAD

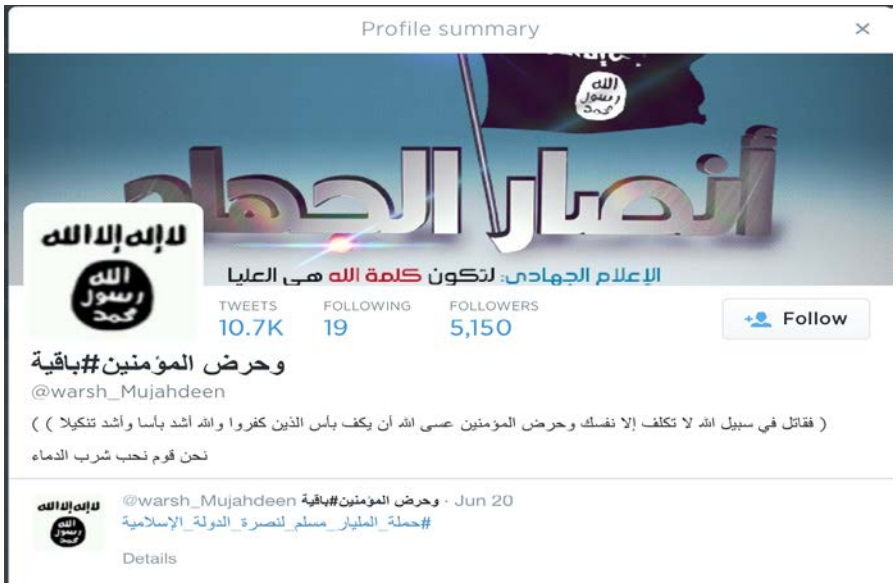


TABLE 2: THE EXAMPLE OF THE SOCIAL MEDIA “TWEETS” RECRUITMENT

# WHEN_THE_JIHAD	# متى _ الجهاد
#IMMIGRATION_TO_HOME_OF_ISLAM _ IS_OBLIGATORY	#الهجرة _ إلى _ دار _ الإسلام _ واجبة
# MARTYRDOM	#الشهادة
# FLAMES_OF_WAR	# لهيب _ الحرب
#HOW_LIKE_INACTION	# كيف _ يحلو _ القعود
#TIPS_TO_THOSE_WHO_WANTED_THE JIHAD	#نصائح _ لمن _ أراد _ الجهاد
# CALIPHATE	#الخلافة
It's a pity ?? The few supporters of the Islamic State of inciting for jihad	Yes, some of them say how the jihad and parental leave. And Allah and God you will leave them " reminder 'does not offer parents an order on the command of Allah,, #How_Like_Inaction

My brother and my darling " do not hesitate to the jihad and Allah that I mentor Where for you from wanting martyrdom for the sake Allah,,, arranged clothes and prepare yourself and trust in God	Most " says how would I go to the jihad and I do not have friend! My brother by Allah is this an excuse in front of god, off course no 'by god is not a excuse for you in front of Allah #How_Like_Inaction
My sister; Imagine if the mujahidin alienate and fighting the enemies of god and you support him..! Support even a little. "After Allah for this place," you and your finances.	

Cyber Terrorist and Extremist groups have taken advantage of social media technologies to serve a variety of purposes, including:[17]

(1) To share best practices.

(2) Recruiting fighters.

(3) Reach the global audience with their propaganda.

(4) Coordinate attacks.

(5) Communicate with supporters globally without borders.

(6) Fund raising.

(7) Crowd sourcing

2.4. Literature that identifies social media provides an opportunity for national security

Besides being a potential threatening instrument, social media can symbolize a useful opportunity. According to Omand, Bartlett and Miller (2012), the surfing of social spaces provides a great opportunity for extra effective, responsive and agile government and broader social and financial gain (Omand, Bartlett & Miller, 2012). In summary, social media intelligence (SOCMINT) could contribute resolutely to

public security: identifying illegal activity; providing timely warning of mayhem and threats to the national security; or creating situational consciousness in rapidly changing environments (HM Government, 2010). Making sure that the intelligence and security effort is legitimate, proportionate and oriented towards public consent relies on measuring and controlling the possible troubles it might generate. The intelligence effort is vindicated in any circumstances, if it is capable of enhancing the value of decision making (Montagnese, 2012).

> ***"Any security organization that is afraid of the new media revolution does not warrant being in movement with modernity and development," said Major-General Khamis Mattar Al Mazeina, Commander-in-Chief of the Dubai Police.*** (***Khaleej Times, 2014)***

In support, Major-General Humaid Mohammed Al Hadidi, Commander-in-Chief of the Sharjah Police, said, "One of the strategies of our MOI is to invest in technology and training that partly explains why we have a substantial number of followers on the social media platform." (Khaleej Times, 2014). Indeed, the top officers contended that several cases are solved with the aid of social media. "For instance, we can easily track a stolen vehicle through sending messages via the social media platform," said Maj-Gen Al Hadidi. "Since the beginning of this year, we have recorded 624 calls related to serious crimes," Maj-Gen Al Mazeina said.

2.4.1. Harnessing the power of social media

Several approaches are being made toward the direction of gathering social media information for intelligence. Most observers and scholars acknowledge that the data from social media provides a wealth of information for a nation's security which in return will provide more understanding, and offers the possibility of empowering analytics (OSINT) to predict issues and risks by studying the nature of society and

build the right strategy to counter any future threat. Indeed, governments have adopted quite a lot of strategies and practices during the global riots and protests e.g. Tunisian revolution 2010, Egyptian revolution 2011, Iran green revolution 2009, Turkey 2013, London riots 2011 and Occupy Wall Street. Added to this problem is the new threat caused by cyber terrorism 'ISIS'. **"Social media has become a primary source of intelligence because it has become the premier first response to key events and the primal alert to possible developing situations."** (BBC, 2012)

According to Cross (2013) these new platforms have provided new approaches to many critical enterprise functions, **including identifying, communicating, and gathering feedback with customers (e.g., Facebook, Ning); locating expertise (e.g., LinkedIn); providing new communication platforms (e.g., Twitter); and collaborating with a community, small or large** (e.g., Wikis). (Cross, 2013)

According to Kerstin Denecke, over the past few years the Internet has become a rich source of personal information. People issue tweets, write blogs and chat online and use various social channels to share their feelings, experiences, news and ideas. For instance, at the first hint of an outbreak of a disease, the death of a celebrity or political changes, millions of people actively participate in online discussions and knowledge sharing.

The way in which information can spread so rapidly through online channels is both a threat and an opportunity. Surveillance or early warning systems are required to identify changes in customer preferences, political ideologies and other data that could have implications for commercial success or public safety. However, creating an effective surveillance system presents a significant challenge. The scale and variety of data that may be used for surveillance purposes is immense and can be derived from a wide range of sources including natural language documents and

sensor-measured values. The primary purpose of Denecke's work was to examine the vast sources of information that can be used in surveillance and to assess its various domains. A large amount of her research concentrates on the use of unstructured data as surveillance information and she reviews many of the existing methods that are in use to translate this data into meaningful information that can guide surveillance strategies. For example, she discusses how Web 2.0 can provide a means of conducting disease surveillance and examines some of the challenges associated with such an approach.

According to an online article entitled *New powers for the Russian surveillance system SORM-*, "The Russian Prime Minister Dmitry Medvedev has signed a decree that will extend the use of SORM-2 to social network surveillance." It is common knowledge that the Russian Government is in the process of conducting extensive surveillance activities on the Internet within Russia, and that the Kremlin is currently using a system code-named "SORM-2," to monitor the online activities of Russian citizens. SORM-2 is a very complex and powerful surveillance system that can track online activity at an individual level through the support of the Russian ISP. (Paganini, 2014)

Controversially, the Global Justice Information and Sharing Initiatives have implemented a policy entitled *Use of Social Media in Intelligence and Investigative Activities*. Within this document, they specify there is a requirement to:

Successfully and lawfully harness the power and value of social media sites, while ensuring that individuals' and groups' privacy, civil rights, and civil liberties are protected, and that agency leadership should support the development of a policy within their agency regarding the use of social media sites in criminal intelligence and investigative activity. (The Global Advisory Committee, 2013)

2.4.1.2. Social media for e-government and public e-participation

According to Montagnese (2011) social media platforms "can be used by governments for content creation, external collaboration, community building, and other applications" (DRAPEAU, WELLS, 2009). The "failure to adopt these tools may reduce an organization's relative capabilities over time" (Montagnese, 2011)

It is worth mentioning that United Arab Emirates has realized the potential of social media in e-government and public participation. In fact on 15th June 2014 the Arab Social Media Award launched been UAE Vice President, Sheikh Mohammed bin Rashid Al Maktoum. The annual award is offered for the most important initiatives of social media in the Arab world that honors individual and institutional innovations in various social media. (Arab Social Media Award, 2014)

The objectives are to:

- Boost interaction and encourage communication through social media channels.
- Encourage creative thinking so as to contribute to the development of various sectors in the community.
- Utilize social media channels to increase awareness on issues of concern to the Arab community.
- Increase awareness on best ways to use social networks and encourage optimal and responsible usage of social media channels.

The Award consists of diverse categories to honor the most distinguished and active persons, private, or government entities as follows:

1. Government Sector: honors government institutions and employees who are engage social media to associate with the public and enhance the quality to achieve customer satisfaction.

2. Blogs: honors bloggers who through their blog posts manage to make

significant achievements in improving the lives of their targeted audience. This category also considers blogs that contribute to spreading awareness about various societal issues.

3. Media: honors media society and journalists who harness social media to engage with the community, spread news, information and studies that contribute to the development of society.

4. Tolerance: Award associations and individuals who promote the values of tolerance, peaceful coexistence in the community, and enhance the unity among Arab societies.

5. Youth: honors institutions and young people who positively use social media and contribute to spreading awareness, community development and the provision of ideas that motivate young people to participate effectively in society.

6. Politics: honors political institutions, politicians and thought leaders, who use social media channels to spread ideas that contribute to positive and constructive development of Arab societies and educate community members about the best practices in this regard.

7. Safety and Security: honors organizations and individuals who have contributed through social media channels to raise the levels of security and community safety, and enhance awareness on the most important issues related to safety and security.

However, based on MBRSG report (2014) “the Arab Social Media Report has indicated that one of the top challenges facing citizen engagement with government entities and public services through social media is a lack of government employee capacity and training. Building government entities’ skills in engaging with citizens

through social media is key to the delivery of more citizen-centric public services, and as such capacity building for government officials in the region, to enable them to better perform in their jobs, is a priority." (Mohammed Bin Rashid School of Government, 2014)

2.4.1.3. Social Media for enforcement

One of the negative aspects of social media sites is that they are being increasingly used for the purposes of criminal activities. As such, it is important that law enforcement (LE) personnel understand how criminals exploit these vehicles to their own advantage and that they themselves use social media technology to investigate, prevent, manage and mitigate criminal activity. (The Global Advisory Committee, 2013)

LE personnel can employ social media platforms to assist their daily functional requirements in a number of ways. These include:

1. Performing pre-employment background investigations
2. Communicating with and engaging the community
3. Issuing emergency alerts and notifications
4. Conducting analytic assessments
5. Producing situational awareness reports
6. Developing intelligence
7. Implementing criminal investigations

J. Rohan (2011) described how many modern-day LE entities use social networking applications to support key activities. These include conducting undercover operations, tracking and identifying criminals and predicting crimes. Through operating undercover, LE agents can communicate with targets, access key

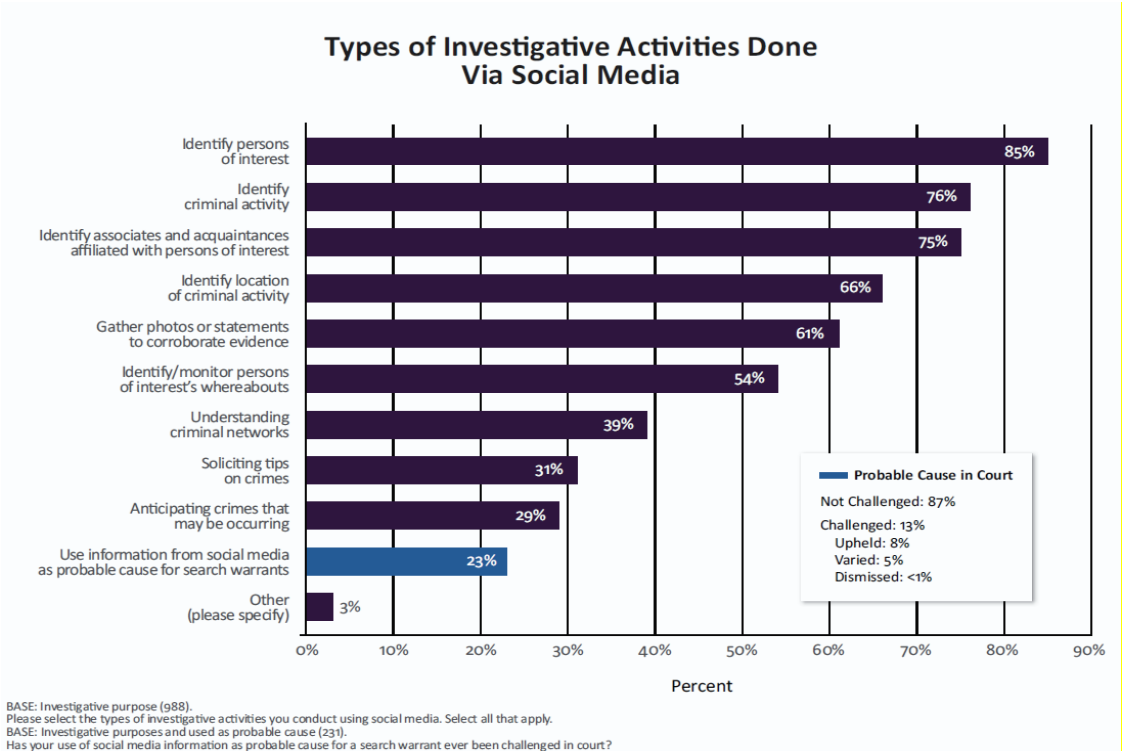
information and identify relevant social relationships (Lynch & Ellickson, n.d., p. 32). Information that is obtained from social networking sites can be used to develop insights into personal communications, establish motives, identify connections and networks between people of interest, provide location information, prove and disprove alibis and establish crime or criminal enterprise (Lynch & Ellickson, n.d., p. 11; Rohan, 2011)

According to a recent report produced by LexisNexis, social media is rapidly changing the way LE professionals both identify crimes and investigate them:

> Social media is a valuable tool because you are able to see the activities of a target in his comfortable environment. Targets brag and post legitimate, valuable information in reference to travel, hobbies, places visited, functions, appointments, circle of friends, family members, relationships, actions, etc. At times, incriminating evidence in the form of statements and pictures can also be obtained. (2013)

According to LexisNexis (2013), the most common ways in which LE professionals use social media is to investigate criminal activities, and they predominantly use information gathered from online platforms to identify people and locations, discover criminal activity and gather evidence. However, social media platforms also provide useful information that can be used to anticipate illegal activities. Communal and personal sites, such as Facebook and YouTube, are more commonly used by LE professionals than sites such as LinkedIn, Twitter and blogs, as users have better control over the content that is published on these platforms.

FIGURE 3: LEXISNEXIS REPORT



(LexisNexis, 2013)

According to the BBC, the FBI's Strategic Information and Operations Center (SOIC) posted its "Social Media Application" market research request on the Web on 19 January, and it was subsequently highlighted by New Scientist magazine. According to this document: "Social media has become a primary source of intelligence because it has become the premier first response to key events and the primal alert to possible developing situations." (BBC, 2012)

The report states that the application should collect "open source" information can:

1. Provide an automated search and filter the capability of social

networks including Facebook and Twitter.

2. Allow users to create new keyword searches.
3. Provide geographical insights into different threats through displaying them as alerts on maps and using color coding to distinguish priorities.
4. Plot a wide range of domestic and global terror data.
5. Immediately translate foreign language tweets into English.

The FBI document says the information would be used to support LE agencies to predict the likely actions of "bad actors," and to identify areas where suspect groups are vulnerable. "Officials can use this type of social media-driven intelligence to gain insight, investigate, construct countermeasures and refocus resources" (Siciliano, 2014).

2.4.1.3. Using Social Media for Intelligence (SOCMINT):

According to Albrechtslund (2008), criminal groups, terrorist organizations, adversary nations and other contestants are increasingly using social media to serve their own agenda. As such, the constant and deep surveillance of information that is published on social media channels can serve as a means of identifying current and future risks to national safety. For this reason, many intelligence agencies throughout the world now engage in the continual examination of media because it provides early warning signals about antagonistic or potentially threatening activities that may place national security at risk (Montagnese, 2012). Analyzing texts and the movements of suspects can help to prevent an uprising or alleviate its negative cost (Andrejevic, 2005; Phillips, 2010; Tokunaga 2011). For example, tracking the people who access online videos that describe/depict the training of armed forces personnel can potentially provide LE agencies with information about would-be terrorists (Callahan, Mary &

Richard, 2012). Furthermore, social media provides strategic warnings and horizon scanning that is aimed at delineating the medium- and long-term tendency of threats through identifying patterns and using this analysis to predict future activities (Andrejevic, 2005). Finally, analyzing information pertaining to global politics and strategic research that is published on online blogs can provide insights into the likely long-term development of foreign strategy and the tactical thinking that underpins a nation's governance (Phillips, 2010). In short, LE personnel can use social media to retrieve, extract and understand key information, gather feedback, assess the impact that the publication of opinions has, bring people together and create loyalty, increase the visibility of LE activities and develop innovative methods of implementing LE initiatives. (Center for Crime Prevention and Safety, 2011)

According to Omand, Bartlett & Miller (2012), social media intelligence holds a lot of potential that governments need to harness and exploit. They argue that in order to ensure the benefits on offer from social intelligence are fully realized, LE professionals must establish an autonomous specialist scientific and industrial panel and a SOCMINT Department of Excellence (Omand, Bartlett & Miller, 2012).

Research by J. Rohan (2011) revealed that the DHS SNMC have used social networking sites to monitor U.S. citizens and internal events; the U.S. Citizenship and Immigration Services have used social networking sites to gather information and conduct surveillance for use in the investigation of citizenship petitions (Lynch, 2010); and other U.S. Government organizations have used social networking sites to conduct investigations or surveillance activities. (Rohan, 2011)

2.5. Identifying security practices and regulations that mitigate the threat of social media

During conflicts, governments have adopted several practices and law enforcement techniques to mitigate riots and protests. Table 3 shows the summary of those methods. However the most frequently practiced is censorship, considered to be one of the most common methods applied to controlling social media sites that occurs to varying degrees in a number of different countries (Cross, 2013).

TABLE 3 - SUMMARY OF SOCIAL MEDIA THREATS, MITIGATION PRACTICES, OR SOLUTIONS

	Social Media Mitigation practices
1	Laws and regulations
2	Social media guidelines
3	Internet and social media blocking
4	Monitoring and surveillance
5	Counter intelligence
6	Propaganda

2.5.1 Electronic criminal laws and regulations for digital crime, information and social media

Recognizing the lack of legislation on electronic crimes committed via the Internet and social media, it was necessary for many countries to develop laws and special regulations, or to work on adjusting its domestic laws in order to ensure the provision of legal protection against these crimes.

United Arab Emirates has identified the potential threats of information technology and impact of social media on the national security and society. Accordingly UAE has taken proactive measures to control and mitigate those potential threats by laws and

regulations. However it is worth considering if can those steps can fully reduce those threats.

1.5.1.1. UAE CYBER CRIMES LAW

In 2006 UAE introduced a new law for the fight against cyber-crimes. The president of the UAE, Sheikh Khalifa bin Zayed Al Nahyan, decreed Federal Law No. (5) for the year 2012, in the fight against the crimes of Information Technology, and included adjustments as stated in Federal Law No. (2) for the year 2006 in the fight against cybercrimes, which was abolished by Decree, which was announced in the Official Newspapers. These decrees ensure to provide legal protection for the privacy of what is published and circulated on the information network including information, data and figures relating to credit card numbers and data bank accounts or any other means of electronic payment, as well as all use of any means of information technology in the rigging or copying of credit cards or civil cards.

The new law has outlined the following offenses and their punishments, set out in articles 24, articles 26, articles 28, articles 29, articles 30, and articles 38 of this Law is considered as an offenses against state security.

Article 24

> **Punishable by imprisonment and a fine of not less than five hundred thousand dirhams but not exceeding million dirhams for the establishment, management or supervision of a website, or dissemination of information on the information network, or another means of information technology, to promote or favor any programs or ideas that encourage sedition or hatred, racial or sectarian, or harming national unity or social peace or disturbing public order or public morals.**

Article 26

Punishable by imprisonment for a term not less than five years and a fine of not less than one million dirhams but not more than two million dirhams for each of the offenses of establishment, management electronically or supervision of a website, or publishing **information on the Internet or any technical information, to assist a terrorist group or any group or association or organization or illegal body with a view to facilitating communication to its leadership or its members, or to attract membership to it, or to promote or favor ideas, or finance activities, or provide actual help, such as to the publishing of incendiary devices or explosive manufacturing methods, or any other tools used in terrorist acts.**

Article 28

Punishable by imprisonment and a fine not exceeding million dirhams for establishment, management electronically or supervision of a website, or publishing information on the information network, or any other means of information technology with a **view to inciting acts, or to publish or broadcast information or news or cartoons or any other images, which would encourage of prejudice or endanger public order or the security of the state and its supreme interests.**

Article 29

Punishable by imprisonment and a fine not exceeding million dirhams for each of the offenses of: dissemination of information or news, data or rumors on a web site or any **information network or any technical information intended to ridicule or harm the reputation, prestige or status of the state or any of its institutions or its president or his deputies, or the rulers of the Emirates, their royal families or guardians, or the state flag or the national anthem or logo or symbols.**

Article 30

Punishable by life imprisonment for each of the following: establishment, management electronically, or supervision of web sites for dissemination of information on the network Informatics, or any other means, of information aimed at or calling for a change in the system of government in the state, or seizing power.

The same punishments will be applied for both promoting or instigating any of the foregoing acts, or facilitating others to do so.

Article 38

Punishable by imprisonment for both offenses of submitting to any organizations or institution or bodies, any data or information which is incorrect , inaccurate, or misleading, that would harm the interests of the state, or offend its reputation, prestige or status, using the Internet or a means of information technology.

In summery, the Law of Electronic Crimes (2012) is the main legal umbrella for dealing with social security issues, and political and economic threats to society. The law covers a wide range of offenses that can be committed in virtual spaces, which include social, security, economic and individual and political spheres. However, there is an urgent need to formulate a comprehensive national strategy for dealing with the social networks because the law alone is just a partial solution to deal with any potential threats posed by the social media. According to Dr. Ayesh, "Laws alone are not sufficient to regulate the social networking sector and there is a need to create discreet awareness of the negative and positive aspects of the networks between individuals" (Dr. Ayesh, 2015).

2.5.2. Censorship

Most researchers agree that social media is no longer just a place for fun to make friends and engage with people. Uprisings in Egypt and Tunisia, Syria and other countries of the world have proven to everyone that it is also crowdsourcing tool where people get together to participate in revolutions. Many states felt that this new weapon threatens the stability of its national security, and so the reaction is online cut and mobile phone services, and in many cases control the use of the Internet. (Ahmed, 2014). Social media a power of knowledge, which offered the average individual in control of the message, is very troublesome for a government's ability to shape public focus.[2] Researchers Cross, M., & Shimonski, R. (2014) outlined in Table 4 different countries that adapted censorship and blocked social media. (Cross & Shimonski, 2014).

TABLE 4: SOCIAL MEDIA BLOCKED BY COUNTRIES

Social media sites	Countries frequency blocking sites	Countries intermittently or partially blocking sites
Facebook	China, Libya, North Korea, Vietnam	Algeria, Bangladesh, Belarus, Burma (Myanmar), Egypt, Indonesia, Iran, Pakistan, Saudi Arabia, Syria, Tunisia, Uzbekistan,
Flicker	North Korea	China, Germany, Iran, Mexico, Pakistan, Saudi Arabia,
Orkut (social networking sites developed by Google	Iran, North Korea, Saudi Arabia	India
Twitter	China, North Korea, Turkey	Algeria, Belarus, Cameroon, Egypt, Iran, Malawi, Pakistan, South Korea
YouTube	China, North Korea, Tunisia, Turkey	Bangladesh, Eretria, Indonesia, Iran, Mexico, Pakistan, Philippines, United Arab Emirates

Cross, M., & Shimonski, R. (2014)

[2] Hacking Censorship: Countries Who Block Social Media http://sumo.ly/2wui via @whoishosting

When law enforcement authorities began in turn using social networks to combat riots, it gave results.

In fact, the true degree of the government's intervention on Facebook, Google and Twitter, comprising listening in to private communication between British people, has been legitimately established for some time (Albrechtslund, 2008). The government's superior security administrator, Charles Farr, gave a comprehensive report on how searches on Google, YouTube, Facebook and Twitter can be surveyed by the security institutions because they are assumed to be exterior communications. The outcome confirms the surveillance, privacy and legality of social media (Omand, Bartlett & Miller, 2012).

The facts of the arrests of instigators of network riots in Europe were reported in March 2007, when during the eviction of the "Youth House" in Copenhagen, the Danish street thugs were joined by several thousand of anti-globalists from Germany, France, Norway and Sweden. Commenting on this case, an expert at the Council on Foreign Relations, Alexander Rahr from Germany, informed that the organization of disorder via telephone or the Internet was common practice among anti-globalists.

During the summer riots in the UK in 2011, arrests and prosecution for activities on social online networks became the typical reaction of authorities. Thus in August 2011, the British police arrested 20 people for organizing mass unrest through smart phones and social networking (Himelfarb, 2012).

In Chester U.K., two men were later sentenced to four years in prison for incitement to pogroms on Facebook. The press emphasized that none of the accused was involved in any real riots and their Facebook appeals have not provoked any real pogroms, so the only crime, which took place, was exclusively in "virtual space".

At the same time in British society discussion of the issue of temporary blocking of Internet services Facebook and Twitter, as well as the BlackBerry

Messenger application, became popular. For example, a member of parliament David Lammy (MP for Tottenham) called for this. At the same time, on the first day of the London riots, the representatives of RIM, BlackBerry phone manufacturer, said they were ready to cooperate with Scotland Yard in providing a variety of data about their users including the time messages were sent with the geographic coordinates of the sender. The only thing they refused to do was "to disclose the content of communications without a warrant issued by a senior police officer". In fact, Scotland Yard Commissioner Tim Godwin was against blocking messages of BlackBerry Twitter, believing that the authorities had no such powers (Clarke, Knake, 2010).

Interestingly, some U.S. government departments have extended their use of social media beyond a vehicle through which they can communicate with citizens to being a means of combating America’s enemies. For example, the State Departments ‘Think Again Turn Away’ Twitter account, has been frequently used to goad and quarrel with pro-jihadi social media users.

According to ABC News (2014), in the same way governments throughout the world operate social media campaigns to communicate with citizens and manage critical messages, terrorist organizations like the Taliban and the Al Qaeda-allied group Al-Shabab in Somalia, have also developed a comprehensive social media presence through which they attempt to proliferate propaganda and recruit followers. (Ferran, 2014)

It is very important that the agency is upfront and honest about the extent and type of information that is collected, assessed and stored. This will prevent members of the public from being suspicious of Government motives and agendas and will provide citizens with the knowledge they need to make informed choices about what information they share online and how they share it. (Walker, 2013)

2.5.3. Cyber Counter-Intelligence methods

Social media can be used both for defense actions such as warning, prevention, crisis management, institutional communication, precision and counter-propaganda and for offensive activities like manipulation, propaganda, or trickery (Montagnese, 2012).

Another approach is, the government can utilize the social media to counter propaganda, according to Dr. Ayesh, social media are also important and effective tools that governments can employ in the dissemination of information that clarify the state point of view and explain its positions to reach millions of individuals around the world, and through the pump information that refutes rumors and clarify official positions, governments take advantage of social media in the creation of the public opinion in them as they work to defeat the hostile views and trends in the virtual space. (Ayesh, 2015)

According to J. Rohan, Counter-intelligence operations or counter operation can be grouped into four categories: (J. Rohan, 2011)

TABLE 5: COUNTERINTELLIGENCE OPERATIONS. SOURCE:

	Counterintelligence operations	**Definition**
1	Passive defense	The classification of information as sensitive or classified and policies stipulating users should not post sensitive or classified information on social networking sites.
2	Active defense	The actions of the DHS's SNMC in conducting surveillance to determine threats against the President during the inauguration or border threats during the 2010 Winter Olympics.
3	Passive offense	When hackers fool users into following links that download and install malware under the guise of viewing something innocent.
4	Active offense	In scenarios where the U.S. military use fake personas or 'sock puppets' to spread propaganda and disinformation.

(J. Rohan, 2011)

2.6. SUMMARY OF THE LITERATURE REVIEW

From these reviews, there are numerous gaps in the various literatures that have been studied. **Particularly, none of the literatures reviews has established a solid base for a social media national security strategy**. In effect, although there are some social media guidelines, cyber crime laws, and good policies for information security, there is no comprehensive strategy for social media implications. Thought, most literature were mostly concerns on defining the threats posed by social media and the existing opportunities that could support the national security. Nevertheless the research also has identified different approach to mitigate the threats of riots, protests, cyber terrorist, extremist ideologies and the risk of cyber security. In conclusion, view of the literature came up with a proactive measures they all deal with consequences of the social media, fewer has paid an attention to Table 6 and Table 7 below summarize the findings in the literatures in terms of the social media threats.

TABLE 6- SUMMARY OF SOCIAL MEDIA THREATS

	SOCIAL MEDIA THREATS		
1	Negative publicity	8	Protests
2	Propaganda	9	Terrorist Recruitment
3	Loss of control over content	10	Crowd sourcing
4	Privacy risks	11	Financial crowding
5	Regulatory compliance risks	12	Impersonation
6	Reputation loss	13	Identity theft
7	Riots		

TABLE 7- SUMMARY OF SOCIAL MEDIA OPPORTUNITIES

	SOCIAL MEDIA OPPORTUNITIES
1	Social media intelligence data
2	Propaganda & Counter Propaganda
3	Public information response and relationship building
4	Crime prevention, monitoring, and tracking
5	Reputation management
6	Counter Riots
7	Operation Influence
8	Mitigation of Terrorist Recruitment
9	Early warning

10	Strategic warning and horizon scanning
11	Communication
12	Deception

3. RESEARCH METHODOLOGY

Research Method

This research aims to examine the extent to which social media contributes to threats and opportunities for national security in the UAE. The study will be primarily based on a literature review of existing research in this specialist area, and will involve a secondary data collection method in which the empirical data collated will be analyzed and examined in depth to form conclusions as to the impact that social media has on security in this region of the world. The validity of the data will be measured by evaluating the extent to which the information collated is representative of the theoretically generated hypotheses pertaining to the area of interest. This quantitative approach will be supplemented with qualitative research in the form of executive interviews with six representatives from relevant United Arab Emirates government organizations who are considered to be experts in the field of social media studies and/or national security.

Data sources

The primary data employed in this research will be obtained through executive interviews with security experts, during which open-ended questions will be employed. The secondary data will be derived from existing research in the area of

social media and security risks. This data will undergo a process of analysis to ascertain the extent to which the findings of existing studies in this area are reliable and legitimate.

The research will commence with a detailed assessment of the secondary data collected through the literature review process. It is envisaged that this data will provide useful insights into the current situation and assist the identification of any full or partial solutions that have been recommended to reduce the risks that social media poses for national security in the UAE. Initial research indicates that data pertaining to this subject is readily available, will provide a useful starting point and will significantly reduce the cost of the research (Carole, 2011).

The majority of the secondary data utilized in this research will be extracted from existing studies that have been published online and/or through an analysis of popular social networks such as Facebook and Twitter. In the event that the initial search for relevant information and data is unsuccessful, a further "manual" search on thematic sites, such as Yellow Pages and a number of other resources, will be performed. The information obtained via the secondary data collection process will be used to develop a high-level overview of the extent to which social media plays a leading role in determining the behavior and interests of protesters (Badger, 2013).

The secondary data employed in this research will be supplemented with primary data that will be collected via an interview and observation process. The information collated at this stage will be used to fill any gaps in the secondary data that were identified during stage one of the research. It is anticipated that the most relevant source of data and information during the primary data analysis will be gained by conducting interviews with professionals who work in the area of national security. Questionnaires will be conducted with relevant individuals including police, academics and researchers. The quality and reliability of the data gathered during this

stage will be determined by reconciling the information gained with existing sources of information, examining the frequency of its use and assessing the competence and credentials of the individuals involved etc. (Abdih, 2011).

Six experts who are believed to have expertise in the area of security intelligence will participate in the primary research process. These individuals have been identified as having professional knowledge of the way in which social media can directly impact security risks and opportunities in the United Arab Emirates. Their first-hand experience and knowledge of the subject area will be employed to identify and investigate the threats that social media poses for national security while also identifying how these risks can be effectively mitigated and managed. The questionnaire conducted with these individuals will incorporate open-ended questions that will be specifically designed to elicit their knowledge and opinions about the extent to which social media is a threat to national security, the implications that social channels can have on this security and the methods by which the opportunities associated with these channels can be managed. It is envisaged that the information gained from these individuals will contribute toward the creation of a comprehensive mitigation strategy that outlines how the threats associated with social media can be effectively managed, mitigated and neutralized to improve national security in the United Arab Emirates.

TABLE **8.** INTERVIEWEES PROFESSIONAL QUALIFICATIONS

Dr. Mohammad Ayish	Professor and Department Head at the University of Sharjah and has worked as a consultant for the UAE National Media Council.
Dr. Khalid Al Khaja	Dean of the Faculty of Information, Media and Humanities at Ajman University
Dr. Jamal Sanad Al-Suwaidi	The Director General of the Emirates Center for Strategic Studies and Research (ECSSR) in Abu Dhabi
Deira Center for Public Opinion and studies.	Watani Al Emarat Foundation

Expert 5	OSINT expert
Expert 6	Law enforcement expert

4. RESULTS AND DISCUSSION

In the search for answers to the research questions and seeking to confirm the three hypotheses, for that reasons the researcher prepared open-ended questions for the interviews. However, the results of the interviews of the respondents have confirmed all three hypotheses and responded to the of the research questions. Most respondents identified the greatest potential threats posed by the social media as being related to **instability of the state, radicalization that leads to riots, reputation loss which hurt individuals and state interests, cyber terrorism and protest movements.** Further more, most respondents also acknowledged that a social media imposes potential threats to the UAE national security. In fact they have agreed on some examples of the threats that occur in UAE, like the presence of Muslim brotherhoods in the UAE, the propaganda against the government of the UAE and the threats of cyber security and Hactivism.

Ultimately, the results of those interviews, acknowledged the lack of national strategy that deal with social media threats, this also leads to confirmed the third hypothesis **"United Arab Emirates require a reliable strategy to mitigate the influences of social media on national security"** the strategy that harness the power of the social media and mitigate most of the threats imposed by social media technologies.

The following section outlines and discusses the results of the interviews that confirmed the three hypotheses, in this regards the researcher arranged the following questions correlated to each hypothesis:

4.1. Hypothesis 1: Social Media is considered a potential threat to the national security.

1. Is Social Media considered a potential threat to national security? If so, how?

All respondents admitted that a social media network imposes potential threats to United Arab Emirates national security. Four of the respondents used the Egyptian revolution as an example of the power of social media to mobilize people into the streets. Three of the respondents noted the vulnerability contained in the propaganda. One respondent commented that social media has been used by extremist and terrorist organizations.

However Dr. Ayish is not totally agree that social media should be considered as the main threat. In his opinion ” Social media itself is considered to be "neutral instruments" for communication between individuals and groups, and what defines the nature of the threat in the first place is the purpose it is used for. He added that to say social media played the role of a political power in the so-called Arab Spring is a kind of exaggeration, which shunned the reality, as it was present in all states and societies, but did not leave the same effects. Social Media does not act independently, but in conjunction with other factors that determine its effectiveness either positively or negatively (Dr.Ayish, 2015).

On the other hand, Dr. Jamal emphasizes that social media fosters the concept of risk to national security. This has become clear with the link between Internet sites,

including social media, and the proliferation of negative security phenomena each extending the security threat to social and political stability, such as terrorism and extremism producing closed groups, which use the social media platform for consultation and dialogue. Some of these closed virtual communities are relatively innocuous, and only use the communication tools for social interaction among its members, while other groups persist in promoting violent premises or extreme hypothetical States. This makes organs of government concerned in the face of difficult security challenges to deal with these default states, which can greatly enhance the power of extremist organizations as communication is an essential element in ensuring unity of any organization and increasing its effectiveness. There is no greater proof than that of the use of "Al Qaeda" web sites and means of social communication in the dissemination of ideas and processes of recruitment, training of extremist elements to carry out criminal operations, the preparation of explosives, and so on. In other words, researchers believe that "virtual" communities States have given birth to their own warrior division, which occupies a wide area of electronic land, if we may call it so.

2. What is the deference between the social media and the traditional media with this respect?

All respondents believe that social media is different than traditional media in that there is no control over the digital sources of information, only mass access with no accountability or filtering. One respondent acknowledged that despite what was raised by researchers about the end of the traditional media era, and the growing role of social media, (turning the media of "Media Foundation" to "inform the individual,") at the current stage, at least, we are witnessing cooperation and mutual support between the traditional and the modern social communication media. For example users of a

site like "YouTube" view a great deal of video footage and videos of talk shows. In contrast, many social media channels are used to view footage, which is also posted in the same locations as video news, while the news content of traditional media depends sometimes on information from social media, such as "Twitter" or "Facebook". Furthermore some famous political figures and leaders are now preferred to communicate quickly, directly and most effectively with the public through social media.

From the above, we find that social media provides a space that was not provided for by traditional means because of tighter government controls and oversight, in addition to the laws regulating this arena. According to Dr. Ayesh, social media is characterized by its availability to individuals who are able to access the Internet, where the user who takes the lead in communicating with others through multimedia messages reaches the global media audiences interactively. This is a critical element in social media compared to traditional media, where the flow of information in the traditional media will be in one direction from the sender to the public. The public in this case is just a recipient who does not have the ability to send information to other members of the public, so the impact is limited compared to what is happening in social media.

One respondent has stated that the difference which exists between the two forms, is that, as the social media allows an individual to participate in media material broadcasts whether to comment or express an opinion, as well as to produce media material itself. These so-called ‘journalist citizens’, are a new type of makers of media material without possession of media skills, or commitment to, or reference to professional ethics. The element of credibility, checking and verifying news sources, can be done through traditional media. Hence one of the most important preserves of

traditional media is its status or reputation. On the other hand authenticity is highly problematic or difficult to ascertain in social media. In social media, as the source of the information is not specified, there is no transparency, nor any gatekeepers to keep the platform safe from threats to national security or community peace. This allows third parties to shake confidence and disseminate sedition and lies between the users.

3. Can social media networks create social change among users through viewpoints that are published, political criticism and sarcasm, which may lead to the recruitment of users to adopt destructive ideas?

All of the respondents reported actual incidents in which information posted on social media was used to negatively impact the nation. They all agreed that social media networks could create social change among users through viewpoints that are published, political criticism, and sarcasm that may lead to the recruitment of users to adopt destructive ideas. Three of the respondents indicated there were examples of negative influences but security measures taken protected the state from social instability, for example the Muslim brotherhood in UAE. Another respondent introduced the case of the Muslim brotherhood in the revolution in Egypt on the 25th of January 2011, where social media was used to miscarry and misalign messages against the regime in order to inspire revolt. This respondent believes that the traditional media also utilized satellite TV channels to escalate propaganda in combination with social media in order to mobilize the protestors.

Another executive respondent also agreed, commenting that, this was particularly true in ‘open’ space where anyone can introduce his or her views to be broadcast, whether this was systematic and intentional, or spontaneous. What concerns us in this regard are the campaigns targeting the so-called "collective conscience" in any society, and the transmitting of ideas that will create a negative

mood. These societies start with cynical, political critique, or inquiries for information regarding the mechanisms and roles of governments. This subsequently leads to the adoption of individual groups of extremist ideas and destructive intent, which then turns to unjustified violence. All of this is due to the growth of the "electronic power" of the individual or the group using social media, and its role in the mobilization of the masses, both in support of public policy, or opposition. One respondent believes that any new media phenomena are always in vogue at the beginning. In his opinion however, the current social media carries so many dangerous implications and creates chaos. These negative aspects include unjustified and non-substantive criticism, at times attacking the reputation of many individuals, showing lack of respect for privacy, irresponsibly inciting sectarian strife, and fuelling ethnic or religious conflicts. Dr. Ayish pointed out that cases of misuse by individuals and groups, may pose a real threat for the stability of states and societies through the publishing of rumors and misinformation which raise confusion, threaten public security, serve to disseminate division in the society, and even incitement to carry out acts of breach of security and stability. This is especially threatening as social media allows individuals and terrorist groups to send messages to ordinary people that encourages and incites them to commit violence in the society" (Dr. Ayish, 2015).

4.2. Hypothesis 2: Social Media is a rich source and provides potential opportunity for national security.

While it is hard to identify the actual opportunities harnessed by UAE national security, on the second hypothesis, "**Social media is a rich source and considered a potential opportunity for national security",** all respondents were in very strong agreement on the potential opportunity for national security for the government and national security.

There is no doubt that the information available on social networking sites can have important implications for security services in helping them to prepare proactive plans, consider scenarios of potential risks and investigate their mechanisms of interaction.

1. ***Does gathering open source information in social media networks offer a new potential opportunity to national security? If so how?***

   All of the respondents agreed that harvesting open source information in social media networks offers a new potential opportunity to national security, however, none of the respondents shared information regarding any specific usage of social media to mitigate threats or technology used for this purpose. One respondent strongly agreed that social media is a rich source that can be considered beneficial to national security. In fact, he believes that social media could be an ideal source of information to enable it to be more effective in:

   1. **Counter threat profiling**
   2. **Counter terrorist intelligence**
   3. **Competitive intelligence.**

A further respondent agreed that gathering open source information in social media networks offers a new potential opportunity to national security. He added that there was certainly the capacity for those responsible for security to benefit greatly from the size of the data, and the type of information available, such as names, directions, accommodations, contact numbers, photographs, even favorite sites visited. In this way, the security services can classify the political or social attitudes of its citizens, or citizens of other countries, through their pattern of participation, or by

people who communicate and interact with them.

What is published through social media can benefit security agencies in the identification of a general situation or trends that must be dealt with. Even though the credibility of the information may be uncertain or unreliable, it should not be ignored, as it can be indexed and cross referenced through multiple security sources, which can determine the specific weight or value of what is being published. Also identifying the source of what is published and accessible to the public on social media is an important part in the fight against national security threats.

2. Does the use of information available on social networks benefit the national security apparatus to predict and understand the dimensions of the threats? How?

All respondents indicated that use of information available on social networks benefits the national security apparatus to predict and understand the dimensions of the social media threats. Many of the respondents gave examples of how could this information commonly can be used to:

1. Network trace
2. Identify meeting points
3. Track plans of actions
4. Geo track individual terrorists
5. Prevent and intercept organized crime

One executive respondent agreed with the national security opportunities in using information available in social networks to predict and understand the dimensions of threats, but this opportunity is conditional on a set of factors. We know that the presence of a large volume of data and information alone is not enough; they are only the "raw materials". We cannot take advantage from this material unless we consider

processing, classification and revision according to a wide set of standards. This requires trained staff who have the ability to handle this data and follow-up its credibility, so that we can later build future scenarios to serve the decision-maker, who must have accurate information to hand. This process of confirming the authenticity and objectivity of information available through cyberspace is a complex problem; messages broadcast vary and have a diversity of sources, there are misleading messages or rumors aimed at defaming the stability of all levels of society: security, economic and social. Additionally, this information cannot be relied upon without being fully ascertained, but at the same time it cannot be ignored. Therefore a strong emphasis on the importance of training personnel dealing with this information is paramount.

3. How can law enforcement benefit from social media information? Can it help in reducing crimes and adding value to investigations? How?

All respondents indicated law enforcement could benefit from social media information, in helping reducing crimes and could add value to investigations. One respondent believed that social media big data could be very beneficial in combination also with GSM interception and virtual border control, with digital forensics, and for law enforcement and digital investigations. He added that there is also an opportunity to track anti-social groups via their handlers to obtain original IDs and track planned disruptive activities.

4. ***Can participation of the state apparatus and the government in social media contribute to reducing potential threats from group and individual users? If so, how?***

Most of the participants stressed that the participation of the state apparatus and the government in social media effectively contributes to reducing the potential threats from the users of either groups or individuals. One of the participants pointed out that, obviously, the presence of the state apparatus and the government in the social media plays an important and vital role in reducing potential threats through broadcasting authentic and reliable information, reducing the path to rumors, which represent a real threat in the light of the growing number of gatherings organized by means of social communication. A recent example of this is how the UAE Ministry of Interior harnessed the power of their social media channel to counteract the case of the "stealth crime" in Abu Dhabi. During the investigation of this incident, the Abu Dhabi Media Security police provided the public with instantaneous detailed information, according to the requirements of the situation, in order to squash the rocket rumors. This led to public reassurance, and increased the confidence in the capabilities of the Emirati police and enforcement agencies.

One respondent believed that the existence of the state media in general is important for creating a state of balance between the functions performed by the private media and functions that must be performed by the media in general; that there are some functions assigned to the traditional media which do not align with the private media, such as guidance, education and counseling, and confronting developing issues. The presence of the state on social media should be maintained for reasons of national security, and in order to avoid an intellectual vacuum, which could be negatively exploited. The leader His Highness Sheikh Mohammed bin Rashid is numbered among the few world leaders to use this new media to communicate with his people as he fully recognizes the importance of this means and its effectiveness.

5. What is the credibility of social media information can you rely on it?

All respondents agreed that, for gathering evidence and investigation, the credibility of unstructured data and information from social media could be suspect, due to its nature which gives people the ability to be anonymous, create propaganda, rumors, and false alarms. Only the national security agencies have the ability to overcome these issues with technologies and research. One respondent, a materials expert in the field of OSINT solutions, advises that by repetitive trending and building RFI databases, the results can show a reliable trend.

4.3. Hypothesis 3: United Arab Emirates require a reliable strategy to mitigate the influences of social media on national security.

1. Does the UAE take steps to mitigate the potential threats?

The UAE was one of the first countries that issued a combat information law associated with a portion of the anticipated threats of social media technology crimes when Sheikh Khalifa bin Zayed Al Nahyan, President of the State issued a decree, Federal Law No. 5 of 2012 Cyber Security. This ensured that adjustments were made to UAE Federal Legal Decree No. 2 of 2006 on cyber crimes, and it contained a decree on many of the materials and technologies that will provide legal protection for the privacy of what is published and circulated on the information network. This includes information, data, and figures relating to credit cards and bank account numbers or any means of electronic payment, as well as all the uses of information technology in the falsification of credit cards or civil cards, replicated or copied. Also punishable under Decree Law is using the information network for unlawful intent, for both forcing or threatening another person to get him to act, or abstain from action. It is an offense against the law to establish, run, or supervise a website for the dissemination of information on the information network, or one of the other means

of information technology, to promote ideas that provoke discord, hatred, racism, damage national union. One respondent stated that there is no doubt that the UAE is one of the first countries to warn of the dangers of using social media on the individual and society. UAE has always sought to evaluate its use to maximize the benefits and protect against the negatives. UAE has issued laws that relate to confronting destructive ideas and protecting the right of individuals, their privacy and reputation and maintaining public peace and security. A community is a state that respects pluralism, but its strategy should be to integrate the legal aspects of the intellectual and educational sectors in a framework founded on cooperation and integration between the cultural and educational institutions plus the security services, so as not to handle events in an isolated manner.

2. Does UAE need a strategy?

Two respondents, commented with regard to the Emirates needing a strategy, that the UAE special anti-cyber crimes law is in itself a strategy; it does not participate in any act or conduct on the Web, but monitors, and immobilizes those who violate the limits of freedom given. However, there is always an urgent need to actively and continuously coordinate between all parties in the government to deal with threats and prevent their occurrence, especially as the United Arab Emirates embraces individuals from more than 200 nationalities from around the world.

3. What are the strategic initiatives required to deal with social media impacts?

One of the respondents agreed that strategic initiatives should start with governance, risk mitigation, and compliance. Dr. Jamal commented on the important research institutes specialized to conduct rigorous studies, and opinion polls to find out how young people are affected. This should include the publication of ideas in the context

of **identifying usage patterns and follow-ups and the nature of what is being published. There should also be a regulatory point of voluntary contact for young people, to make them conscious of how to monitor and deal with subversive ideas disseminated through social networks, and discuss ways to refute, and respond to the same.** State institutions should have a strong presence on social networking pages to clarify facts, and should urge officials and public figures to follow the example of the leaders of the state in communicating with the people, and explaining how to optimize their participation in major societal issues.

The respondents also have proposed some recommendation including initiatives for a comprehensive strategy to deal with social media. Dr. Ayesh recommends the following initiatives:

1. Creation of a Department specialized in social media to coordinate government efforts in this area.
2. Provision of training programs for citizens in how to deal with social networking within the formal frameworks.
3. Creation of a national center for research and studies of social networks.

Dr. Ayesh, concluded his recommendations by stating that "The supervision of this strategy must be shared between several parties: media, political, security, economic, and technological, through a combination of those entities under one umbrella, a joint body." (Dr. Ayesh, 2015).

4. Are laws and regulations alone enough in reducing the negative effects of social media on national security?

All respondents generally agreed that it is not enough just to rely only on laws and regulations in reducing the negative effects of social media on national security. These should be combined with social media awareness plus public safety and national security awareness. One respondent replied that laws and regulations alone

are not sufficient, but it is necessary to initially rely on research centers, as they play a significant role in the research and study of the outcomes, implications and risks that could threaten national security. Then work should be undertaken to develop effective strategies involving all state agencies with the aim of treating the problems, then taking all preventive measures to curb this negative social media trend and relieve the burden of threats to the country's security and safety. One respondent confirmed that the law alone, without awareness of a community is not enough; we have to build individual cultural awareness so that people have the ability to distinguish between what benefits them, and what represents a threat to their country and community. This is where the role of educational institutions, from the family to schools and universities comes in, rather than relying solely on the media. In his opinion, besides the law and security agencies, the conscience of a community is a reliable guarantee of the truth, and conscious community control, which challenges the cultural legitimacy of what is published, sponsors the elimination of all forms of sedition and potential risks.

5. United Arab Emirates National Security Strategy for Social Media

In every nation, especially that with social media and security potential threats, planning an operational strategy is considered a matter of national and public security. Indeed, the negative use of social media has serious consequences for foreign relations, the economy, social development, safety and national security activities. However, most of the UAE governmental organizations including the federal and the local entities have started to harness the social media technologies to engage and communicate with the public. However, according to FAHR (2012) most, if not all of these organizations, **lack guidelines or policy instructions that could help them leverage the benefits of social media and avoid their potential risks and threats**. (FAHR, 2012)

It is worth mentioning that the United Arab Emirates (UAE) government organization and national security have initiated several attempts and have practiced many different approaches to mitigate social media threats and crimes through the enhancement of certain laws and legislation guidelines for government agencies. However, here arises a question. Is there a strategy or initiative to meet those threats before they occur?

In this respect, the thesis has identified a requirement for a national strategy to counter the social media threats, and harness its power and existing opportunities, based on threat assessment and potential opportunities. The UAE National Security

Strategy for Social Media comprises five missions and goals, beside a four major actions and initiatives.

Missions and Goals:

Mission 1: Preventing social media threats, extremism and violent

Mission 2: Enforcing, administering the laws and enhancing security

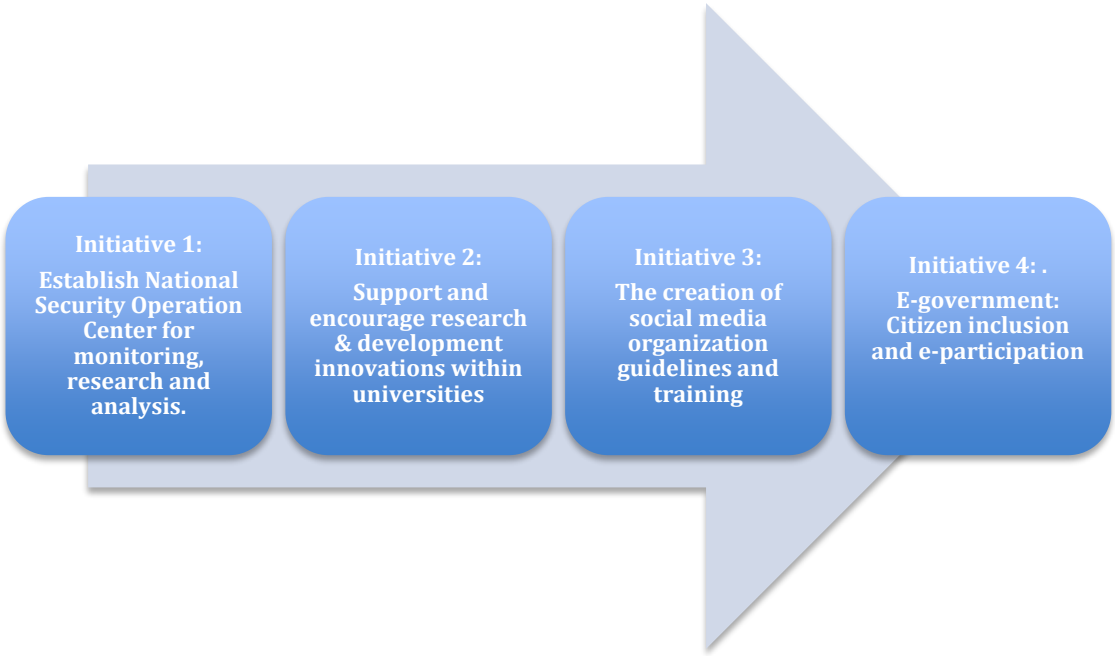
Mission 3: Safeguarding and securing national security

Mission 4: Promoting knowledge, research and innovation

Mission 5: Citizen inclusion, transparency and e-participation

Major Actions and Initiatives:

In this section, the research proposed and recommended the four initiatives and some additions that may contribute to the development of a strategic plan for national security to encounter social media potential threats, as well as the use of such methods in an optimal way in order to respond to these threats, not only by applying the law, but by constantly updating plans to meet the requirements and variables.



Initiative 1: Establish National Security Operation Center for monitoring, research and analysis.

National security community and legislation in UAE has identified social media as a serious challenges for the UAE national security including the government and society. However it is very important to answer the real question; whether the national security in UAE is adequately prepared to counter and mitigate any threat posed by social media and can harness its power to stabilize the national security and protect the state.

In view of that, the paper recommends establishing a National Security Operation Center for UAE federal and local government. This center can be positioned within the **Higher Council of National Security (HNSC) similar to National Electronic Security Authority (NESA) and National Crisis and Emergency Management Authority (NCEMA) or it can be an independent stand-alone entity.**

The main role of a National Security Operation Center is to provide situational awareness and establish a common operating picture for the entire Federal Government, for state, local, and tribal governments as appropriate, and to ensure that

critical disaster-related information reaches government decision makers. (DHS, 2013)

The National Security Operation Center analysts will research, monitor and analyze information using best practices, solutions, and technologies with guidance from a Research & Development Center that serves the national strategy missions and objectives.

The Functions of the National Security Operation Center:

a. Collecting data, monitoring all type of media including traditional media & social media in online platforms and mobile platforms.
b. Analyzing the harvested information. This will need expert analysis skills and think tank methodology.
c. Reporting the situational standing and recommendations to the commanders and decision-makers.
d. Providing National Threat Operations
e. Providing Intelligence and Investigative activities
f. Handling social media related criminal complaints.
g. Information sharing to all national and local government agencies.
h. Reviewing guidelines for social media for government organizations and enforcement**.**
i. Generating risk and threat assessment databases in collaboration with national and local governmental agencies MOI, (NESA, TRA, NCEMA, ECSSR, HEDAYA) and all other policing and intelligence agencies.
j. Establishing yearly conferences to tackle threats, review lessons learned and new findings from case studies; provide situational threat reports, intelligences analysis and research and development.

k. Establishing workshops for all national and local government entities to train, educate and evaluate comprehensive guidelines; additionally raising awareness based on case studies and threat assessment.

The National Security Operation Center can be utilized as a Social Media Intelligence Center for federal and local government entities, to provide a platform that helps manage social media channels.

Initiative 2: Support and encourage research & development innovations within universities.

A Research and Development Center or an academic committee is recommended to be established to develop comprehensive and best scientific methodologies and solutions to tackle and analyze the risks and threats posed by social media. Their major efforts and role should be focused on:

a. Research and development of the analysis and prediction tools and methodology to overcome the challenge of big data (structure and unstructured text) obtained from online open source information.
b. Research and development of the technologies to overcome the languages challenges posed for example by gulf dialects (Emirati, Saudi, Kuwaiti, Saudi, Omani and Bahraini dialects). In fact there is a lack of development in this area. Empowering this field of technology will enhance the threat perdition tools and methodology.
c. Threat assessment methodology and framework should be adapted to direct the path forward for the development and research.

Initiative 3: The creation of social media organization guidelines and training

The reasons for needing the application of a security policy for a country's social media usage are that a society needs guidelines for appropriate usage. In fact, social media tool has lot of advantages, however it has high potential risks. (UAE Guidelines for Social Media Usage, 2011)

With respect to legal risks the guidelines should be followed up with proper training and workshops in coordination with National Security Operation Center to handle all legal risks including: discrimination claims, defamation claims, confidentiality breach, regulatory breach.

The guidelines assist the UAE government entities to develop policies that assure the right way of using social media in a accountable, secure and efficient approach, this will assure the an effective communication with public and engage them in government strategies planning and services (Guidelines for Social Media Usage, 2011).

The scope of these guidelines is defined: they are proper to UAE federal and local government entities (Guidelines for Social Media Usage, 2011).

The guideline stated: "The main driver behind granting access to employees is to ultimately enhance their work performance and contribute to improving their outputs and deliverables." It, therefore, recommends: "Access to social media sites shouldn't be banned. Employees should be held accountable for any improper use of any social media site"(Bahadur, Inasi, Carvalho, 2012).

Summary

The researcher couldn't access to an updated version on the 2011 guidelines in assumption it's the only guidelines so far. However, to improve this policy and guidelines process the government needs to discourse policy for monitoring and reporting. According to Bahadur, Inasi, Carvalho, (2012) they should also add an incident response policy for when things go wrong. In fact the present guidelines does not tackle these key concepts. (Bahadur, Inasi, Carvalho, 2012).

In addition to the social media policy and guidelines, further steps should be considered:

1. The employee code of conduct should cover social media.
2. Update computer-use and information policy
3. Training users on national and local government to be computer security experts, and make them more advanced.
4. Design security program for the organization with coordination with the national security operation center.

Initiative 4: E-government: Citizen inclusion and e-participation

The explosion in the use and availability of communications technology, in the realm of social media in particular, has resulted in a dramatic increase in the means by which members of society can communicate with one another and organize information. Prior to the rise in availability of such technologies, governments and state representatives had the ability to limit the information that was available to, and exchanged between, members of the public. However, the rise in popularity of the Internet and the ready accessibility of cell phones and mobile communications has made this much more difficult. (Hardenberg, 2012)

It has become increasingly obvious that in order to manage the risks that social media pose for the management of security, governments need to embrace and harness the available technology to fulfill their own agenda. Furthermore, they also need to ensure that effective policies and laws govern the use of social media. According to United Nations (2012), social media has the potential to:

> Help policy makers set priorities, encourage more citizens to 'buy in' to programs, increase satisfaction levels and thus augment the chances of successful policy outcomes. For example, social networking sites, such as Facebook, YouTube and Twitter, as well as blogging software and mobile technology, allow governments to tap into the collective knowledge of society quickly and directly. In this way, citizens move from being passive consumers of government services to advisers and innovators contributing ideas that are in better accord with their individual and group needs. (United Nations, 2012)

The UAE government realized, early on, the importance of social media as an effective tool of communication. Therefore, the government's deployment of social media tools to directly interact with the public, understand their challenges, and **ensure the design and delivery of innovative, need- based public services (**MBR School of Government, 2014**).** One survey that was conducted by the MBR School of Government in 2014 concluded: "[Social media will] save time and money for the citizen, and allow for public monitoring of government performance...this will be a transparent and unbiased monitoring" (MBR School of Government, 2014). Specifically, the survey revealed that the government in the UAE has achieved a number of indirect or long-term benefits through the use of social media and the research. These are as follows:

a. Innovative practices: The government has been provided with a means of accessing resources and knowledge from members of the public and have used these to devise and develop innovative practices;
b. Better understanding of customer needs: analyzing the aggregate data that is available from social media sources has allowed the government to better understand the needs of the community;
c. Community building: Social media has provided an ideal vehicle through which online communities can be constructed that meet the needs of members of society;
d. Collaboration: Social Media tools have allowed government agencies to collaborate more effectively with one another and with the community as a whole;
e. Trust in government: Through providing a means through which the government can communicate directly with the community, social media has increased customer trust in government agencies.

The rapid rate at which the United Arab Emirates government has adopted and adapted social communication technology serves as a best-practice case that highlights how effective e-government can help to support the development of a nation. Although the UAE has double the population of Norway, three-quarters of the GDP per capita and around the same level of online services, it has risen to become a global leader, ranking 8th in the United Nations E-Government Survey (2012) of emerging leaders.

Citizen inclusion and e-participation

One of the visions and main goals of the development of the United Arab Emirates e-government is to empower citizens, residents and institutions by providing them with greater access to public service information and ensuring that all government entities operate in a clear and transparent manner. In more recent years, the government has adopted a more consultative approach to the formulation of public policy initiatives that takes the views of members of the public into consideration and

increases transparency. Key government entities are now required to provide the public with information about the policies they are implementing, opportunities to give their feedback on initiatives and inform them of how they can participate in the formulation of public policy schemes.

According to the United Nations, social media holds a significant amount of potential to increase citizen's use of e-services. In many countries, members of the public actively use social media to keep abreast of government initiatives and public policies. One of the biggest advantages of the use of social media is that it bridges the gap and encourages social inclusiveness between different socio-economic groups. One of the biggest challenges that modern-day government entities face is identifying the best methods of leveraging and harnessing the opportunities that social media presents. In fact, the use of social media is now becoming an important public service issue that impacts the delivery of new important public services, provides avenues through which the government can share information with citizens and amplifies the impact of initiatives (United Nations E-Government Survey, 2012).

Leading political figures in the Arab region are well aware of the important role that social media plays in the modern political environment. For example, the Vice President of the UAE, Sheikh Mohammed bin Rashid Al Maktoum, has become one of the most prominent public figures on the social network Facebook over the course of the last year (Himelfarb, 2012).

The Facebook personal page created by Sheikh Mohammed in June 2014 had to be converted into a public page within in its first three weeks, as the number of requests to add the ruler of Dubai to friends has exceeded the Facebook allowed limit of 5,000 people. Today, fans of the public page of Sheikh Mohammed account for nearly 74,000 Facebook users. On his page, the Sheikh not only posts information about himself, photos and notes, but also actively communicates with his fans,

including on government issues. Users of the page often turn to the Sheikh on personal matters. Among users there are also critics, with whom he also communicates in an open conversation. **Today, Sheikh Mohammed is already close to being the most popular public figure in the regional segment Facebook** The least popular person in the same segment is the Arabic-speaking Egyptian President Hosni Mubarak, who is supported by only 54 Facebook users (Clarke, Knake, 2010).

Case study: The National Brainstorming Session

As an example of the citizen e-participations, on the 3rd of December 2013, Sheikh Mohammed bin Rashid Al Maktoum, Vice-President of the UAE, issued a call for everyone in the nation to participate in what was dubbed the 'largest ever national brainstorming session' in the country. The purpose of the event was to elicit the opinions of citizens as to how critical issues in the education and healthcare sectors could be resolved. This brainstorming session was conducted over a range of traditional and online platforms, making it accessible to members of the public on an unprecedented scale.

> The actual outcomes of the brainstorming session surpassed initial expectations: the government actively made use of crowd sourcing to allow the public to produce new solutions to solve problems with health and education services in the country. Additionally, new problems in existing public services were identified; this provided an invaluable insight into the unintended negative impact that certain decisions had had on existing government services. The process also produced a platform for the development of new government services, and a direct means of communication between the government and the public. (MBR School of Government, 2014).

Summary

The Research identified that what happened in the Arab and Western world, including demonstrations and riots, were the result of suppression of freedoms, and the policy of suppression. From this, **we found that freedom of expression is an important prerequisite, which should be taken into account and should be handled with wisdom and caution when seeking to develop a new strategy for the state.** The UAE has recognized the priorities of freedom of expression in ensuring the safety of the community and security in the UAE, and it is always striving to preserve the security of the community by reviewing and updating laws to suit the evolution of society.

In fact, the United Arab Emirates has initiated a pioneering step, done through community involvement of citizens and residents with the government in making decisions that concern the state. This effective communication between the open government and the community was characterized by transparency and clarity that respects the right of participation and expression in order to serve the interests of the society and state.

6.0 CONCLUSION

Social media has become in recent times, a dynamic variable within the political and social mobility mechanisms in several regions of the world, especially in some Arab countries.

The study revealed that social media has become a significant global phenomenon at the present time, both on the national and international level, and turned into a seriously approach that threaten the public safety, the state strategies and national security. This new phenomenon has supported the agendas of extremist groups and organizations with political, cultural and sectarian nature, which seeks to deploy the ideologies of extremism, also enabled persons belonging to these groups to express their affiliations and defend this ideology and participate effectively in the political scene and the international arena.

The study responded to the research questions, by investigating influences of social media and its close ties to the political revolutions and cyber terrorism, to clarify how it has evolved into a new revolutionary instrument threatening the stability and the security of nations. In the other word, supports terrorist groups and extremist to recruit and advocating riots and the act of terrorist. The study showed that characterized the of social media from the new communication features such as ease and created wide spread and speed compared with other traditional and new means, which makes them the most effective tool of communication and widespread and more influential in the digital world.

The study has answered the first question in the search Is the social media is a threat to national security, by identifying its relationship the direct and indirect and its impact in revolutions and riots, and identify a number of features that distinguish them as a way an electronic that can be created and managed at the lowest cost by a individual or group people intellectually compatible. And therefore it is a new way communication easy and free and resistant to a monopoly, whether by governments or large companies compared in traditional media and websites. The possibility to anonymize the owner name, in social media has allowed more freedom to users in compare with the traditional media and websites, it has become a platform for expression for destructive criticism and dissemination of sedition, fabricating lies and propaganda against the national security, as it diminishes the fear of the security and legal liability as a result of writing under aliases or through the use of VPN, tunnels and other techniques.

The Study has answered the second question, that despite the fact that the social media is a source of threat to national security, it provides multiple opportunities for governments and national security to support stability. There is no

doubt that social media is rich stock of a massive information can be harnessed in the political, social and security aspects through scientific analysis through the use of specialized software to analyze the information derived from the social networks on the behaviors of communication for individuals and groups in the virtual space, so that they can derive meaningful conclusions utilized in the political and security analysis to support decision-makers. As well the social media provides an important and effective tools that governments can employ them in the dissemination of information that illustrate its point of view and explain its positions to reach millions of individuals around the world, and through the pumping the information refuting the rumors and describes the official positions are thereby benefit social networks in creating its a supportive public opinion as to be functioning to defeat the hostile views and trends in the virtual space.

The study concluded that social media has become a source of power substantial has been used by both individuals and opposition political groups and terrorist groups both in destabilize and lobbying and recruiting for the riots and combat, as it enabled them to communicate with the masses and to win the sympathy and support of more from the supporters at home and abroad. The study revealed that the terrorist groups, or what is known as extremist currents of the most prominent were the forces that represented its the social media outlet appropriate for publicity and to express itself forcefully.

The study concluded that in answer to the third question relating to the United Arab Emirates requires a reliable strategy in the face of impact of social media on national security. Through the contrast and revision of previous studies in the potential threats and existing opportunities in the social media, and with the consideration to the analysis and results of the personal interviews conducted by the

research, the study concluded that there is an urgent need to formulate a national strategy for dealing with social networks.

In light of the previous answers to the research questions, the study has validated the three hypotheses and confirmed that the social media will continue to be a source of threats in the world in general and in the Arab world in particular, however we must not disregard the opportunities offered by social media, in fact the proper it been used would support the stability of states and maintain the national security.

The research problem addressed the threats and opportunities in this social media and based on that, the research recommendation was to re-examine and study those threats and to develop frameworks accordingly to devise a thoughtful approach that seeks to develop a comprehensive national strategy unifying all these initiatives in one frame to serve the interests of national security and preserve the security of the society and ensures stability of the state. As the study has shown laws alone are not enough without a clear and comprehensive overview approach adopted by all the state entities and society as a whole in order to ensure national security.

6.1 Findings

6.1.1 like the rest of the world to confront the challenges of social media, the United Arab Emirates has taken the following steps and procedures:

6.1.1.1. Introduction of legislation to combat electronic crimes and also the formation of the National Commission for the security of mails in 2012.

6.1.1.2. Raising of awareness by launching awareness campaigns and warning of the consequences of misinformation streams behind

extremism and anti-system demonstrations and calls for the organization of extremist groups.

6.1.1.3. Use of social media to connect efficiently with the public as it has been integrated into the uses of E-government.

6.1.1.4. Censorship and blocking of social media sites, which seek to spread extremism, violence, and ideas that seek to overthrow the system of government and national security plus blocking of suspect personal accounts in social networks.

6.1.2 Increasing political awareness among citizens in an unprecedented way; communication between users of social media provides an opportunity for discussion, and allows a greater understanding of the social and political issues raised, especially in the presence of a wide variety of experiences shared between users including intellectuals, politicians, academics and the general public.

6.1.3 Some researchers believe that social media has become the main driver in encouraging citizens to political interaction, as this provides an opportunity for greater understanding of the rights of citizenship, and deepens awareness of citizens of their causes, while others argue that these social media methods contribute to spreading rumors and political misinformation, and make the young prisoners of the idea of "e-protest" instead of effectively making positive contributions to their society.

6.1.4 Political awareness among Internet users is affected by cross-transmission of experiences of citizens from other countries and the lessons learned from each other. There is strong evidence that the transfer of the expertise of the Tunisians protesters in dealing with their own security forces to their Egyptian counterparts, was done via social media. Also it is noted that the protest

slogans raised in several Arab worlds were similar to a large extent, with only minor adjustments to a different character sometimes or using local dialects. However, these slogans carried the same content and the same message that echoed across other parts of the Arab world.

6.1.5 In the absence of national security awareness, citizens believe that the national-security institutions are trying to reduce liberty and freedom. To overcome the problem state institutions must educate citizens and raise awareness on the culture of national security.

6.1.6 Social media by itself should not be taken as a potential threat to state security but groups who use social media pose a potential risk (Jin et al. 2013).

6.1.7 Evidence supports the claim that social media has had an influence on activities such as civil disturbances; good examples are the Arab Spring uprising and the Iranian Green Movement.

6.1.8 Social media are essential components of big data for assessment as intelligence departments can measure and comprehend millions of people communicating in different ways: laughing, arguing, condemning, talking, applauding, and joking.

6.1.9 There is evidence that social media, Facebook, for instance, has been employed to organize contract murders, boast about severe animal abuse, implement cyber-stalking, post graph sexual infringements, violate court orders and cause distress via anti-social gremlins (Christofides, Muise & Desmarais, 2009).

6.2 Limitations of the study

The study was limited due to difficulties in securing interviews with major entities, due to sensitivity and the level of information clearance that was needed to collect data for this research.

6.3 Recommendations for the UAE national security

In line with the recommended comprehensive strategy for national security in the previous chapter, the following summarizes the overall recommendations that should be considered:

6.3.1 Research and Development Centers within major universities should be established to develop the comprehensive and best scientific methodology and solutions to tackle and analyze the risks and threats posed by social media. Their major efforts and role should focus on the following:

i. Research and develop the analysis and prediction tools and methodology to overcome the challenge of big data (structure and unstructured text) obtained from online open source information.
ii. Research and develop the technologies to overcome the language challenges such as gulf dialects (Emirati, Saudi, Kuwaiti, Saudi, Omani and Bahraini dialects), as there is a lack of development in this area, and empowering this field of technology will enhance the threats perdition tools and methodology.
iii. Threat assessment methodology and framework should be adapted to direct the path forward for the development and research.

6.3.2 A National security operation center should be established to research, monitor and analyze information using best solutions, and technology advice the established R&D Center to meet with the UAE strategic tasks and objectives

6.3.3 Use of Social Media for Enforcement, Intelligence and Military to prevent, respond to, and investigate riots through:

i. Evidence collection in collaboration with Social Media Intelligence Center.
ii. Location of suspects in collaboration with Social Media Intelligence Center.

iii. Criminal, terrorist and extremist network identification in collaboration with Social Media Intelligence Center.

iv. Situational awareness.

v. Crisis and disaster management.

vi. Outreach channel to society.

6.3.4 Establishment of a national information sharing framework.

This would involve collaboration between local and federal government entities and the national security operation center.

6.4 Future research direction

Another direction for further research could be to study the possibility of using the social media for:

a. Disaster and crisis management, situational awareness and crowd control for NCEMA.
b. Communication during investigations and surveillance activity to prevent, respond to, and investigate riots and violence.
c. Classify and monitor crimes, violence, extremism, and smuggling in order to predict such threats imposed by social media.

6.5 Recommendations for future research

In order to conduct a deeper analysis of the implications of social media, to harness its power and mitigate the threat to national security, this research recommends further acquaintance with the available scientific literature on the subject. Additionally access to further information could serve the research to successfully go beyond its original objective.

REFERENCES

Abdih, Y. (2011). *Arab Spring: Closing the Jobs Gap. High youth unemployment contributes to widespread unrest in the Middle East*. Finance & Development, in Finance & Development (International Monetary Fund), Giugno..

Badger, Emily. (2013). How the Internet Reinforces Inequality in the Real World. The Atlantic.

Carole, Hughes. (2011). The Relationship between Internet Use and Loneliness Among College Students. Boston College.

Clarke R., Knake R. Cyber War. (2010). *The Next Threat to National Security and What to Do About It*. N.Y.: HarperCollins.

Comer, Douglas. (2006). The Internet book. Prentice Hall.

Engdahl F. Wikileaks: a Big Dangerous US Government Con Job. http://www.voltairenet.org/Wikileaks-a-Big-Dangerous-US.

Fourie, Pieter J. (2008). *Media Studies: Media History, Media and Society*. Juta and Company.

Hafner, Katie. (1998). Where Wizards Stay Up Late: The Origins Of The Internet. Simon & Schuster.

Himelfarb, Sheldon. (2012). "Social Media in the Middle East". United States Institute of Peace.

Lynn W. *Defending a New Domain: The Pentagon's Cyberstrategy*. Foreign Affairs, Sept/Oct. 2010.

Noveck, Beth Simone. (2007). Wikipedia and the Future of Legal Education. Journal of Legal Education.

Robbins, S., Judge, T., Millett, B., & Boyle, M. (2011). Organisational Behaviour. 6th ed. Pearson, French's Forest, NSW.

Salem, Fadi, Mourtada. "Civil Movements: The Impact of Facebook and Twitter". Dubai School of Government. May 16, 2012.

Schillinger, Raymond. "Social Media and the Arab Spring: What Have We Learned?". *Huffington Post*. 20 September 2011.

Willinger, Walter. (2002). Scaling phenomena in the Internet, in Proceedings of the National Academy of Sciences.

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance.First Monday 13 (3).http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.

Andrejevic, M. (2005). The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. Surveillance & Society 2 (4), 479–497.

Boyd, D. (2010). Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In A Networked Self: Identity, Community, and Culture on Social Network Sites, ed. Zizi Papacharissi. New York: Routledge.

Callahan, M., Mary E. & Richard, C. (2012). DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy. Written statements before the

U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, 112th Cong. (February 16).

Christofides, E., Muise, A. & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?

CyberPsychology & Behavior 12 (3) (June), 341–345.

HM Government (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy. http://www.official-documents.gov.uk

Jin, L., Chen, Y., Wang, T., Hui, P., & Vasilakos,V. A. (2013). Understanding User Behavior in Online Social Networks: A Survey. IEEE Communications Magazine. 0163- 6804/13/$25.00 IEEE London, SE1 2TU, UK. ISBN 978 1 906693 08 3

Litwin, M. S. (1996). How to measure survey reliability and validity. Thousand Oaks, Calif. [u.a: Sage. Loska, T. (2013). Integrated reporting. S.l.: Grin Verlag.

Mann, S., Jason, N. & Barry, W. (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance and Society 1 (3): 331–355.

Montagnese, A. (2012). Impact of social media on national security. Research Paper 2011 STEPI -AE-U-3 . Centro Militare di Studi Strategici

Omand, D., Bartlett, J. & Miller, C. (2012). “A balance between security and privacy online must be struck…” #INTELLIGENCE Magdalen House, 136 Tooley Street, Phillips, D. (2010). Identity and Surveillance Play in Hybrid Space. In Online Territories: Mediated Practice and Social Space, ed. Miyase Christensen, Andre Jansson, and Christian Christensen. New York: Peter Lang.

Tokunaga, R. (2011). Social Networking Site or Social Surveillance Site? Understanding the Use of Interpersonal Electronic Surveillance in Romantic Relationships. Computers in Human Behavior 27 (2) (March), 705–713.

Trottier, D. (2011). A Research Agenda for Social Media Surveillance. Fast Capitalism 8 (1) (October).

AUVINEN, A. M. (2012), SOCIAL MEDIA-THE NEW POWER OF POLITICAL INFLUENCE. Suomen Toivo Think Tank Foundation, Wilfried Martens Centre for European Studies, Brussels, Belgium. Retrieved from http://martenscentre.eu/sites/default/files/publication-files/kansio-digital_democracy_-_final_en.pdf

CIO Council, (2013) Privacy Best Practices for Social Media. Retrieved from http://www.slideshare.net/RobSentseBc/privacy-best-practices-for-social-media.

United Nations. (2010). United Nations e-Government survey 2010, leveraging e-Government at the time of economic and financial crisis. (Tech. Rep. No. ST/ESA/PAD/SER.E/131). New York, United States: United Nations.

Global energy politics - Summer Schools in Europe. (n.d.). Retrieved from http://www.summerschoolsineurope.eu/course/1890/global-energy-politics

MBRSG (2014) UAE Social Media Outlook. Retrieved from http://www.mbrsg.ae/getattachment/3122bce8-b0e3-48e7-872e-2644fceb71ff/2014-UAE-Social-Media-Outlook-Increasing-coneectiv.aspx

Media and Communication - Essay - Mrodicheva. (n.d.). Retrieved from http://www.studymode.com/essays/Media-And-Communication-1715885.html

Stratfor: Social Media as a Tool for Protest - Council on ... (n.d.). Retrieved from http://www.cfr.org/social-media/stratfor-social-media-tool-protest/p23994

http://www.homelandsecuritynewswire.com

Bakas, "#Terrorist": The Use of Social Media By Extremist Groups. Retrieved from https://www.academia.edu/9015149/_Terrorist_The_Use_of_Social_Media_By_Extremist_Groups

GSM Association, (2013). Arab States Mobile Observatory. Retrieved from http://www.gsma.com/publicpolicy/wpcontent/uploads/2012/03/GSMA_MobileObservatory_ArabStates2013.pdf

http://www.khaleejtimes.com/kt-article-display-1.asp?xfile=data/government/2014/November/government_November48.xml&section=government

Minority Report is real: FBI wants to use social networks to ... (n.d.). Retrieved from http://www.digitaltrends.com/social-media/minority-report-is-real-fbi-wants-to-use-social-networks-to-prevent-future-crime/

Social Media Security - ScienceDirect.com | Search through ... (n.d.). Retrieved from http://www.sciencedirect.com/science/book/9781597499866

Global Justice information sharing,

http://it.ojp.gov/docdownloader.aspx?ddid=1826

http://tmsp.umd.edu/TMSPreports_files/6.IEEE-Computer-TMSP-Government-Bertot-100817pdf.pdf

DRAPEAU M, WELLS L., (2009), Social Software and National Security: an Initial Net Assessment, Center for Technology and National Security Policy – National Defense University, Washington, DC.

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities , http://it.ojp.gov/docdownloader.aspx?ddid=1826

INT: FBI plans social network map alert mash-up application.(n.d.). Retrieved from http://www.inlandnewstoday.com/story.php?s=22565

SOCINT: Disseminating Cybercrime Through Social Intelligence.(n.d.). Retrieved from http://www.bloggernews.net/130991

Center for Social Media Web site, http://www.IACPsocialmedia.org/.

Guidelines for Social Media Usage in United Arab Emirates Government Entities http://www.fahr.gov.ae