Visual Analysis of Twitter Data to Support Decision-Making in Law Enforcement: An Analytical Study of COVID-19

Abstract:

The COVID-19 epidemic constituted a crisis for health facilities in 2020. This was due to less medical staff available, degrading employment conditions, and higher death rates. These conditions led to tweets (messages posted on Twitter) launching hashtags titled #In_solidarity_with_the_Egyptian_doctors (#متضامن_مع_أطباء_مصر) to urge medical staff in Egypt to strike for better working conditions. This resulted in less medical care being provided and threats to public security. This study addresses the visual analysis of "Twitter platform" data during the COVID-19 pandemic in Egypt in April 2020 to test documented mechanisms to process mass data and identify accounts that lead the public opinion-gathering processes on Twitter. It analyzes the hierarchical structure and their ideological belonging. The study uses the URL Decoder/Encoder tool to transfer Arabic hashtags into codec symbols. The study deduced that dialogue clusters on Twitter formed Community Cluster Networks in the study sample. Findings proved significant in determining the accounts leading the public opinion-gathering process. They were recognized through the coordination and arrangement function, as well as the hierarchical structure of the group and their intellectual and ideological tendencies. Finally, the study confirmed the increase of decision makers' opportunities in gathering accurate information and producing high-quality inferences when using multiple open-source analytical tools, especially information visual analysis tools.

Keywords: Visual analysis, Twitter platform, Corona epidemic, criminal investigations, law, security, police enforcement, decision support.

Visual Analysis of Twitter Data to Support Decision-Making in Law Enforcement: An Analytical Study of COVID-19 Using the NodeXL Tool

The concern of the use of Social Network Analysis Sciences increased on social media platforms in 2005. These platforms started being used in Business Administration and Commercial Marketing through their content analysis. The findings evidenced the significant benefits of networks content analysis (Adedoyin-Olowe et al., 2013). New tools in social media platform analysis enabled shoppers and business owners to communicate directly, without an intermediary. These tools allowed business owners to recognize opinions toward products, listen to comments, and realize the consumer’s mood and the extent of satisfaction of the product or service. They also enabled them to recognize their future needs and deductions, in particular, their product estimation compared to the other competitive products. Network analysis as a science, especially social media networks, became relevant in determining the nature and form of relationships between people and recognizing intellectual trends, with technological progress and the increase of social media networks usage (Abdelkhalek, 2020).

The transfer of the social network and social media platforms in smartphones has contributed to increased interaction with other people and events, 24 hours a day. Merging the geographical location determination systems with these platforms led to the multiplication of this data size. Therefore, the traditional tools of the social network-structural configuration analysis became inaccurate, as it lacked specifics. Thus, the Law Enforcement Authorities realized the importance of social media network analysis by using new tools to monitor their interactions and simultaneously support the intelligence operations decisions (Abdulrazak, 2020).

Despite the utilization of law enforcement authorities in many countries globally, with specialized programs to analyze social networks as a source of intelligence, analysts need to be able to recognize technical matters during the use of these programs and their outputs. These include the terminology of the main network, classifying spatial importance of people within the network, structural configuration, and the classification of spatial importance of individuals inside the network.

There is a growing need to follow up the documented mechanisms for processing mass data and optimizing the support of analysis and decision-making. This came with the increase of law enforcement authorities' abilities in gathering information from open sources data to support analysis and decision-making, particularly in catastrophes and crises. The importance is in using appropriate technological tools to detect and discover accounts within the platform to efficiently lead the public opinion's direction toward public security breaches, thus reducing its effect. This discovery was due to the outbreak of social media applications, especially Twitter, and attempts of using their functions to affect public opinion during the law enforcement agencies' administration crises. It also enabled the security-decisionmakers to communicate effectively and actively with the public in times of crises, in a manner that maintained public order and national security.

Systematic Background of Study

Study Problem

The study problem focuses on the testing ability of modern programs in dealing with mass data, particularly the open-source NodeXL tool. Exploring the identity of opportunities provided as analytical software programs may produce inferences of the intelligence nature of security events, especially for social media networks. The outbreak of COVID-19 in 2020 constituted a crisis for health facilities globally. Due to the importance of obtaining significant information that enables law enforcement authorities to manage the crisis, the NodeXL tool, available on web network as an open-source intelligence tool, was tested to collect information and inferences within Twitter. This is because the platform could publicize such news globally and rapidly while analyzing the general mood of the public, address the issues raised as subjects of interest, and analyze tweets on Twitter. It also detects the possibility of recognizing the sources by which the public obtains their information. This tool also determines the content circulated in these platforms, the method of detecting public reactions about governmental decisions. Further, it deals with the identity of highly influential persons and entities affecting the social platform within their networks and the entity of the related clusters. These individuals and entities may be used to obstruct the publicization of false news and control correct information consumption as rapidly as possible. Finally, it detects the accounts being transferred to the platform to stir up and gather public opinion in a manner that threatens public order and public security.

Study Motivation

This study has theoretical and practical importance. The theoretical importance demonstrates a detailed report about the ability of mass data analysis tools to produce informational intelligence for law enforcement authorities in security events, such as the outbreak of epidemics like COVID-19. Regarding the practical importance of the study, an intelligence analysis method is displayed, which enables law enforcement authorities to make decisions based on information that is proven to be scientifically true.

Study Questions and Inquiries

The study problem pivots on a major question: How can security decision-making be supported through a visual analysis of Twitter platform data by using modern software to process mass data, particularly with the open-source NODEXL tool? Are these tools able to produce information of intelligence significance?

Many sub-questions fall within the main question, as follows:

- How can we recognize trustworthy information sources for social media platforms users?
- How can we recognize the most influential individuals and entities within social platforms? Who are the influencers?
- In what form are the clusters on social media, discussion topics, and intellectual units circulating between such groups? In other words, how do we analyze the language method, general mood, and informational sources of the public?
- What are the logarithms that may detect the extremist groups and clusters on social media?
- How could we monitor extremist groups' accounts and actions in rallying up the public and exploiting the crisis?

Study Methodology

This study uses the study tools to collect the required samples from social media websites and platforms. A case study methodology is among the scientific methodologies that study the phenomena of diagnosing through collecting information and tracing their sources to grasp factors that cause the case, the object of study. Consequently, accurate conclusions from processing the study objectives may be achieved.

Study Tools

This study used groups of specialized analytical tools, as follows:

NodeXL tool.

The NodeXL tool analyzes social media networks. It is an open-source extension of the Microsoft Excel program that is used to extract network data from sites like Twitter, YouTube, Flickr, and Facebook and shows data visually. It is an abbreviation of the following phrase: Network Overview, Discovery, and Exploration for Excel. This tool can also be used to process and analyze other network data, such as e-mail networks, in addition to installing several standards that are related to charts.

International Business Machine I2 Analyst Notebook tool.

The study also used the IBM I2 Analyst Notebook tool as a program that specializes in analyzing massive networks, especially those that meet the needs of law enforcement authorities. It has unique potential in discovering suspected groups and clusters, which may be difficult to identify through traditional methods.

Coding tool (URL Decoder / Encoder).

It is a tool used to transfer Arabic hashtags to codec symbols. It was used because the NodeXL program could not recognize non-English letters. Consequently, the coding tool enables the program to recognize and extract relevant data from Twitter.

Social Network Analysis

Emerging social media platforms contributed to mass data in social networks, which was valid for testing networks science theories. Social network analyses generally seek to discover basic laws regulating and governing people’s conduct on social networks. This is done by using social networks algorithms, including the study of relationships and the effect of these relationships on users of networks (Gupta & Brooks, 2013). In this framework, social network analysis is considered the most appropriate methodology to comprehend methods of people’s exploitation of social media platforms to form social networks, in addition to the method of their continuance and stability. It also uses the method of influencing people and presents an explanation for the formation of relationships inside and outside the internet. Social network analysis helps to design detailed drawings for networks through the visual representation of social networks that are existent on social media platforms. It also enables the identification of influential persons and the recognition of issues or ideas circulated in discussions among people at relevant times.

Therefore, social network analysis is significant for law enforcement authorities in the framework of their operations concerning criminal analysis and police work, based on artificial intelligence and informational analysis known as Intelligence-Led Policing. Intelligence-led policing is a modern law enforcement technique. It is based upon systemized assessments and the collection of data and information through a defined analytical process, which transfers it into strategic and operating analytical conclusions that work as a basis for the rational security-decision-making process based on scientific evidence (Abdelmottlep, 2019).

Active Elements as Actors in the Social Networks Analysis

There are five basic elements or actors in the analysis process: actors, density network, network structure, network positions, connectedness, and geodetic or the shortest distance between two nodes (Hansen et al., 2010).

The network position is one of the most effective actors during the analysis process. Therefore, we must differentiate between the four positions (individuals or entities) within the network, which is the central position inside the network in relation to the rest of the individuals or entities of the network. This entails measurements of the degree and form for actor centrality, which are betweenness centrality, centrality degree, closeness centrality, and finally, eigenvector centrality. This specification aims to discover the identity and degree of importance of nodes within the network (i.e., the importance of a person) through which we can assert the importance degree of this actor, as with other connectors, more authoritatively and accurately (Abdulrazak, 2019).

Many arithmetic algorithms or standards shall be used to reach the identification location within the network, most importantly, betweenness centrality, closeness centrality, centrality degree, and eigenvector centrality.

Betweenness centrality.

We can say that individuals who can control network loggings and determine the messages that network individuals receive have a significant effect on the network. In other words, the more people depend on these individuals to help them communicate and connect with others, the larger the extent of their effect and the more “betweenness” they enjoy (Hansen et al., 2010).

These persons are known as gatekeepers because they control the flow of information and can cancel any intellectual unit from the network that might cause harm. Therefore, betweenness centrality measures the degree of a person’s betweenness by counting the number of times they were in a position between two people within a network. This algorithm is used only in symbolic data links, in which links are numbered with symbols of 0 and 1 and not by adjectives.

Closeness centrality.

The second type of influential person is one who may have fewer communication links but may consider the link between leadership and other actors within the network. Its absence is considered a major factor of effective performance for network operations. This individual is positioned within the middle of the inspected cluster or general network. This is known as the terminology (closeness centrality) (Hansen et al., 2010).

The “closeness centrality” of a node is calculated by measuring the shortest distance between all elements of the network. If we assume that we want to spread information within a social network rapidly, the node of closeness centrality can be examined to be chosen so that the information reaches and spreads to all network members within the shortest possible time. This saves time and effort. Therefore, many criminal and terrorist entities seek to use this scale pacifically to recognize people within the social network whose closeness centrality may be high.

Centrality degree.

The third type of influential individual or account owns a direct links with others. The more the link is owned by the entity or account, the more its centrality and importance. Phillip Bonacich (Bonacich, Phillip 1987) developed an algorithm of the centrality degree to be able to determine the most influential person in any given scenario. Does a person or account that can communicate with many people have communication that is limited to a small group? The Bonacich approach enables one to choose the most appropriate scenario by choosing both the positive and negative mitigating elements.

Eigenvector centrality.

The fourth and final type of node scales and its centrality within the network is called the eigenvector centrality or eigenvectors of geodetic distances. It is a significant scale in determining the level of importance of a node or entity within a network and may also be called prestige or respect, whereas the node is in contact and adjacent to more than one central node (a centrality degree or closeness centrality shall be deemed important). Consequently, it derives its importance by communicating with other nodes (i.e., that node has a special strategic position within the network) (Gupta & Brooks, 2013) because of its connection with extraordinary nodes. That node may have a significant influence globally. Notably, this scale is used in directed nodes and relationships only (Srivastava et al., 2008). This scale disregards the size and number of relationships that link the node and instead considers the entity and importance of associated nodes. Therefore, we find that many programs and websites are currently able to identify influential individuals or entities within social networks (Srivastava et al., 2008).

Social Media Platform Analysis for Decision Support

Analysis entails the methodological study of data that is relevant to a subject for its deeper comprehension. The analysis process includes using objective methods, methodologies, and programs. Correct and accurate results can be produced if the above programs are implemented appropriately to find solutions for specific and defined problems that support security decision-making significantly (Abdelmottlep, 2019). Although the social media platform analysis contributes informational value in supporting security decisionmakers, it is important to consider that social media platform data do not represent an entire population group. With the variance of invasion rates for social media platforms globally, and legal frameworks regulating the circulation and confidentiality of information, it may be reflected on available groups of data (Marcellino et al., 2017).

An analysis of data generated by posts on social media platforms, compared to descriptive and demographic data concerned with users who are linked to accounts, helps in identifying the influential persons in social media networks. Therefore, information protectors may target groups, or individuals may be influenced. Algorithms classifying images may collect and describe the type of images exchanged on social media platforms. The analysis of these images, along with other data with geographical inference software programs and mapping, may allow the practitioners of information collection to embody the tweets on a level of people’s national preferences as visual embodiments (Marcellino et al., 2017). Social media platform analysis also assists security bodies of information-collecting practitioners to comprehend the efforts that are exerted by their opponents to collect intelligence information and efforts of mobilization against the state in an efficient way, in addition to identifying the important networks and remote gatherings of intelligence information on detailed levels. This can also be applied to the frame of efforts that are exerted upon measurements of mood state, public opinion, adverse effect operations, their detection, and opinion effects.

The forms of social network analysis differ by the influence subject of the issue. Therefore, linguistic content analysis may be used, whereas language and emotional analyses are useful in understanding and determining locations of messages sent by human crises victims. It also helps to recognize their identity and possible location for finding intention-suspected bloggers or determine the pattern concerned with criminal activities, such as violent riots and other events (Gupta & Brooks, 2013). Notably, most applications concerned with language and emotional analysis focus on the English language. Few analyses are concerned with processing Arabic language. There are many tools of language and emotional analyses that cannot recognize or process unstructured data. Such data have many slang words, expressions, and sarcastic comments like those written by teenagers in their tweets (Gupta & Brooks, 2013).

The power of the social network does not lie in determining the identity of people and defining the sender and recipients but in identifying nodes and the relationships that control the behaviors of every node within the social network. It also recognizes the influencing persons on social networks who are displayed on social media networks. This may highlight more areas that are focused on scientific research and an open resource investigation. This is apart from the exploitation of efforts and the dedication of designated persons within social media platforms (Hansen et al., 2010). The influence is meant to change the perspective of a person or a group regarding the surrounding world and their relationship to it. The central influencer in social media platforms is a node that allows the intellectual units to be posted and the behaviors to be adopted, which affect others' behaviors within the network. When an influencer speaks, their network and even those outside their network listen to them carefully and then respond.

Intellectual units that are used to influence are deemed ideas, principles, and beliefs that are presented in the form of messages and content that are transferred from one person to another to support the influencing process. Influencing persons may be celebrities who influence many people on different social media platforms, regardless of the content. Any person may be influential—regardless of a reputation for being a prominent person—through their messages posted and their position occupied within the network (Gupta & Brooks, 2013).

The NodeXL open-source program, set up by Social Media Research Foundation, is one of the most important and advanced tools concerning social network analysis and producing the visual analysis of networks. An important advantage of the program is the great similarity to traditional

Excel programs. It does not require technical or software knowledge (Smith et al., 2014). An additional advantage of the NodeXL program is the extraction of social media platform data and producing it in the form of images representing interaction processes between users. In addition to analysis through the traditional Excel tables, it also brings the possibility of visual analysis, producing drawings and figures that simulate and embody interactions between users on a platform and producing accurate reports in multiple formats. Therefore, the NodeXL program provides a significant chance for seekers to deal with mass data and transfer it into visual plans, which enable them to analyze data and interactions of social media platforms.

Practically Applied Study

Study Sample

- The hashtag #In_solidarity_with_the_Egyptian_Doctors (#متضامن_مع_أطباء_مصر) was extracted from Twitter on the April 12, 2020. Sample tweets of this data exceeded 2100 tweets in total from approximately 1425 accounts on the platform.
- This hashtag was chosen due to its interest lead and interaction within Twitter during April 2020 and the onset of the corona epidemic. At the peak of reports on the rise of death rates globally and stress on health facilities, the hashtag was developed and exploited to mobilize claims of doctor strikes. This constituted a threat to the state health facility.
- The analysis targeted detection of the circumstances of transfer for this hashtag to claims of a general strike among doctors. Is this transfer process directed or coincidental? Who are the people behind it? Which accounts lead to its directed mobilization?

Computer Programs used in the Analysis

- The open-source NodeXL program.
- IBM I2 Analyst's Notebook Tool; a free copy may be downloaded for 30 days for study purposes through the following link: https://www.ibm.com/security/resources/demos/i2-analysts-notebook-demo
- IBM I2 Analyst's Notebook tool was used in synchronization with the NodeXL tool to benefit from the potential provided by the International Business Machines products, especially the visual analysis International Business Machines I2 tool, to recognize the common entities. The International Business Machines I2 Analyst's Notebook tool is specialized for meeting the law enforcement authority's needs.

Program Settings used in Analysis

- The program settings were adjusted to identify the influential accounts on target networks. This included identifying the accounts of betweenness centrality, closeness centrality, centrality degree, and eigenvector centrality.
- This program setting adjustment supported security decision from two sides. The first side is a negative defense to protect the network from the outbreak of false information, rumors, or the tendentious mobilization processes. The second side is positive, aiming to deliver information to stakeholders by ensuring it is not blocked or hidden within the network.

Recognition of Content and Intellectual Units

- The recognition of content and intellectual units contributes to identifying the sample's focus of interest that attracted the interactors, the objective issues they searched for, and the entity of accounts sharing this content and other developing content. It also constitutes a benefit to preventive security media-campaign designers to have a perception of the ideal quality of the most attractive media templates within specified communities at relevant periods. Moreover, a relationship is built with the influencers and their influencing skills and assistance in the generalization of highly sharable content by the active participation of security entities.

- Content includes videos or images. The intellectual units also include tweets of content that amplify the challenges faced by doctors in health facilities. An analysis of intellectual units also aims at recognition of the tweet’s linguistic language and their emotional effect.

Analysis Steps

Division of the study sample into clusters for # In_solidarity_with_the_Egyptian_doctors hashtag (#متضامن_مع_أطباء_مصر) by using the NodeXL tool.

- To begin, the interactions of the network were sorted. Subsequently, they were divided into groups according to the function and purpose of the target information. In our study, the division was made according to geographical location (which recognizes the locations where people/entities send their tweets) according to their relationship with each, to identify groups with the same common intellectual interests. This was represented in Figure 1, with separate squares and different color for different groups.

[Figure 1 here]

- The visual analytical outputs were codified per group (for each cluster of nodes) by using a code to identify and easily-recognize as them (e.g., G1-G2-G4..., etc.).
- The third division of interactions aimed to identify the influential accounts or entities in each group (cluster).

Division Objective

The division objective was to distinguish how each influencer within a cluster could process the most circulated topic within a group. This concerned efforts of mobilizing and interacting with other influencers who were not integrated within the clusters or who did not discuss the targeted issue. In return, the influence becomes higher within a particular cluster. Subsequently, this influence diminishes, even relatively, compared to other clusters.

Results of Analysis

1. Figure 2 shows that node numbers have a high degree in the betweenness scale and a high degree in the prestige scale by using the NodeXL tool, such as with an account named “allahmana202” and “dr_do1428.” Consequently, pursuant to these scales, these accounts have a high-effect significance.

[Figure 2 here]

2. Figure 2 also shows four accounts that achieved high central scales in many clusters’ scales, such as “allahmana202,” “dr_do1428,” “han00n88,” and “21olhurbc5wlcc6.” It has been clearly noted that these accounts were monitored within the top ten list for the entire graph.

3. Hence, it is concluded that these accounts have a direct and instant impact on interactions within the platform. It may be targeted by decisionmakers to reduce its effect.
4. It was possible to recognize the twenty most influential accounts' locations, pursuant to the prestige scale, within the general network. The concerned influential location appears clearly, with a large number of the twenty influencers being within cluster 2 (G2) and less being within other clusters.
5. Subsequently, the discussion topics circulated among each group or cluster (e.g., G1-G2-G4....etc.) were recognized. This entailed collecting the most circulated pair of words within each group (i.e., the pair of words that were frequently compared). Therefore, it indicated the language users used when processing and reacting with hashtag and mentions. Hence, the types of intellectual units within each cluster can be recognized accurately or terminologically (micro targeting).

[Figure 3 here]

6. As seen in Figure 3 and the second cluster, there is a fierce discussion regarding doctors being urged to strike as a form of pressure on the Ministry of Health. Conversely, some accounts opposed these demands because those who support them wanted to exploit the crisis for political purposes and embarrass the state in critical and non-traditional circumstances. This is contrary to the first group, in which topics of discussion appear dispersed, as most of the accounts are not interconnected and tweeting individually, with divergent ideological trends.

7. Table 1 shows the most important intellectual units that were used. It demonstrates language analysis of hashtag content with the mood categorization between negative and positive words.

Table 1 – The most important used intellectual units.

[Table 1 here]

8. The analysis of the language used, both for positive and negative words and content within study samples (for the purpose of inference at the study sample's general mood, from which public opinion about a certain topic or issue was discerned), shows that the percentage of positive words is high, with a frequency of 1609, and negative words are lower, with a frequency of 1071. It seems that the study sample temperament is skewed positively (according to the number of words that the program possesses, considering that the negative and positive word lists must be constantly developed to cope with the development of discussion topics, in addition to the method that users employ for those words in discussions that are circulated on the platform). Table 1 shows the most frequently used single words within the study sample, the extent of its compliance of being positive or negative, and the percentage of emergence words for the total number of words used.

[Figure 4 herer]

9. The interaction between the most frequent pair of words within the hashtag, according to its betweenness centrality, shows that the most betweenness word is "doctors" (الأطباء), followed by "brotherhood" (اخوان). This is an indication that many users on the platform acted on accounts supporting the Muslim Brotherhood Organization that was registered as a terrorist organization in Egypt to mobilize and escalate the doctor situation. This type of

visual analytical output is useful in tracing topics that are raised on the platform. Therefore, one can easily notice that each line derives first from a centrality word in the middle and can be considered a separate discussion topic.

10. The conclusions of merging data concerned with each interaction of hashtags #In_solidarity_with_the_Egyptian_Doctors (#متضامن_مع_أطباء_مصر) and Doctors Strike (إضراب الاطباء) led to a recognition of common accounts between both hashtags, by using the IBM I2 Analyst’s Notebook tool in synchronization with the NodeXl tool. This is in addition to the recognition of leading accounts, the nature of their relations, and their hierarchal structure. This was done by using the conditional coordination function that distinguishes important accounts by color and size to be recognized easily by the decisionmaker. Finally, in this stage, the study used the function of clusters for systems finding or what is known as clusters finding. As shown in Figure 5, the bottom left of the figure shows a group of clusters of linked accounts within the red circle, between relations of a special and close nature. This appears clearly from the colors of conditional coordination output. They also form a cluster between each group. This signifies that the relation between them is distinct from the rest of the network that requires the upcoming stage to be highlighted for inspection more closely.

[Figure 5 here]

11. This represents the conclusion of the analysis for regulating relationships and links between actors (i.e., acting persons) in the accounts clustered within hashtags for #In_solidarity_with_the Egyptian_doctors (متضامن_مع_أطباء_مصر#) and #Doctors’_Strike (# إضراب الأطباء). We analyzed the accounts with the highest prestige centrality values or

eigenvectors, which were approximately 15 accounts, according to the communication patterns between current entities, for cluster structural composition recognition. It became evident that these are the same accounts that appeared in the first stage with the hashtag of #Doctors_strike (إضراب_الأطباء#). These accounts had high values in the centrality scales. They appeared with the same high values in the hashtag of #Doctors_strike (إضراب_الأطباء#). They were observed within the leading accounts, which attempted to mobilize and form public opinions against state regimes, in addition to exploiting the COVID-19 crisis to escalate the doctors' situation and urge them to escalate their claims of a strike as a form of pressure on the government.

[Figure 6 here]

12. Exploration of personal profiles on Twitter pointed to a common link between them, being their extremist political affiliation opposing the state regime. This is evident from their permanent activities and posts on their profiles, confirming the extremist affiliation trend. Some accounts have been banned and deleted by service providers for breaching the Twitter system. This interprets the analytical outputs that emerge at the onset of words, language, and cluster analysis within the relevant programs. Therefore, it indicates that the cluster leads to the organization of the mobilization processes against states exploiting the COVID-19 crisis, which escalates the doctor crisis and exploitation.
13. The conclusion of the special cluster exploration, also known as "clusters," is demonstrated by the new centrality scale (the K-Core scale) to detect relations between groups of distinctive nature entities. This is from the perspective that all group members are known to each other. This is an indication of a special cluster (group). Their existence within any

location of networks has meaning and significance. The study activated this scale to confirm the inferences and significations achieved in the previous stage. Indeed, the results were almost identical to the previous stage. Twelve accounts (in green) had higher degrees of the abovementioned scale. This confirms that the relationships between these entities are not transient but are still close. All individuals and groups know each other.

[Figure 7 here]

14. The final step entails returning to the main network to identify the recognized and suspected account locations. These accounts are suspected to mobilize public opinion and exploit the crisis within the main networks by using the hashtags #In_solidarity_with_the Egyptian_doctors (#متضامن_مع_أطباء_مصر) and #Doctors_Strike (الأطباء_اضراب#) while using the International Business Management I2 program (the accounts are in green). Their clustering and position within the middle of the network appear clearly. They certainly have an impact on the other accounts. In addition, they can particularly control informational actions, the spread of information, and false content. The analysis shows that the extremist constitution was located on more than one hashtag and structural organization, under the leadership of the "mohammed0102019" account. Security intervention can be conducted to disintegrate the cluster and control the crisis and intellectual units' actions within the social media platform (Twitter).

[Figure 8 here]

15. To confirm conclusion validity and reliability, a sample was taken from a hashtag that was moved by the Muslims Brotherhood Organization under the name of #Almae'y****

(***المعي #) to recognize inference accuracy in reaching persons or accounts who were acting to mobilize the network on the social platform. It was presupposed that most of the interacting persons from that group were the Muslim Brotherhood Organization supporters. If the defined clusters fall within this hashtag, it means the study inferences are accurate. As shown in Figure 8, all the identified accounts are active with the hashtag #Almae'y**** (****المعي #).

16. The International Business Machines I2 Program was used to implement correspondence and functional exploration of eigenvector centrality scales that were predominantly controlled by the "mohammed0102019" account, assisted by the accounts of "ibn_masr0," "han00n882_bee22," "ossamasoliman3," "allahmana202," "dr_do1428," "fbra2016," "bala22222," "mohammed0102019," "m111964t," "fadilamo_939705," "mm20030001," "s_herif," and "bl_ue_e & rh_aal." These are all active on the platform to support the ideological trends of the Muslim Brotherhood Organization.
17. A correspondence has been carried out to confirm interactors between samples of the #Doctors_Strike (#إضراب الأطباء) hashtag and the Dakahlia hashtag (هاشتاج الدقهلية). The abovementioned accounts of "mohammed0102019" and "s_herif_" appeared to be clearly active in the agitation against police and the disapproval of security intervention in dispersed clusters. This was due to the people's objection to burying a female doctor's body, who died of COVID-19 during the crisis. This confirms extremist organization actions from one network to another, which aggravated discussions during the COVID-19 pandemic to mobilize the public's opinion against the state.
18. The research discovered that the abovementioned elements supporting extremist organizations on social media platforms and achieving their agendas were acting from one

account to another, especially after their accounts have been blocked by the service provider. For example, the “allahmana202” account owner re-logged onto the platform with the same profile picture and username but changed the number attached thereto (“allahmana 777”). This indicated that he intended to be active, hopping from one account to another. He was aware of the possibility that his account would be banned or blocked.

19. A point of consideration while exploring extremist account activities through the crisis within the study sample network is that these accounts’ subject of suspicion was at the center of a general plan, as abovementioned. The question was as follows: How can such a position within the center of a plan be achieved? By detecting the centrality scale of these accounts, it was found that they scored highly. They also had a high score on the prestige scale. This was surprising and drew attention since the onset of the leading actor’s analysis within the extremist actors. The reason emerged from browsing these actors accounts. These actors identified the influential entities on Twitter as having massive amounts of followers or a high betweenness centrality scale and attempted to link them via re-tweeting their tweets, commenting, or referring. Consequently, their intellectual units could appear in front of large numbers of the targeted public and attempt to mobilize public opinion and hence affect them. As shown in Figure 9, accounts in red are the extremist accounts. They attempt to mention the influential accounts (colored in blue) to raise their closeness centrality and prestige due to their link with latter.

[Figure 9 here]

Study Conclusions

- Extremist organizations attempt to exploit the COVID-19 pandemic to change and disturb the general mood, to affect health facilities, which is one of the most vital facilities during a crisis. This is done by encouraging and mobilizing doctors to strike.
- Dialogue crowd clusters on Twitter within the study sample took the form of community cluster networks that used the #Doctors_strike(#إضراب _الأطباء) and #In_solidarity_with_the_Egyptian_doctors (متضامن مع أطباء مصر) hashtags.
- Open-source intelligence tools provide a tremendous opportunity for security decisionmakers and law enforcement authorities to disclose vital information to take appropriate decisions during a crisis, especially during the COVID-19 pandemic.
- A decisionmaker's opportunities to collect accurate information and produce high-quality inferences are growing, where that decisionmaker can use more than one open-source analytical tool introspectively, especially with information visual analysis tools such as NODEXL and International Business Management I2 Analyst's Notebook.
- Security decisionmakers can accurately identify all the topics concerned with the maintenance of the public regime that is circulated on social media platforms and quickly use open-source informational analysis tools. They can also identify the nature of clusters on networks and the topics discussed by each cluster.
- Open-source visual analysis tools enable security decisionmakers to identify influencing accounts. These accounts control the flow of information and other accounts, leading discussions and forming the general mood and public opinion.
- The open-source informational visual analysis tools enable decisionmakers to identify the sources by which social media platform users derive their information during crises and the most shared content among them.

- The study showed close relationships and mutual interactions between extremist actors on a platform. Those actors were attempting to mobilize the public during the pandemic. This evidence confirms personal relationships within our actual reality (real life) and an arrangement between them for this mobilization processes.
- The function of finding groups/clusters and the K-Core function by using IBM I2 Analyst's Notebook tool have proven to have a high effectiveness in identifying accounts that are acting on hashtags to conduct mobilization and escalation on platforms during the epidemic.
- The function of detecting the hierarchical structure of the arrange organization by using IBM I2 Analyst's Notebook tool proved to be considerably efficient in identifying the leading actors of suspected actions on social platforms. The accounts leading the mobilization to strike are identified within the study sample.
- The extremist accounts are clearly active during a specific period, which is from 2 a.m. to 12 p.m. Its activities are virtually non-existent on the platform after this time. Inference may be important for security analysts to comprehend the analysis of activities of extremist organizations, their method of action, and periods of activity throughout the day and night.
- Visual analysis open-source tools of information enable decisionmakers to recognize the general mood of the public and the time evolution for predicting or worsening the crisis.
- The extremist accounts became acquainted with the influential entities on Twitter (by having large amounts of followers or a high betweenness centrality scale) and attempted to link to them via re-tweeting their tweets, commenting, or referring. Consequently, their intellectual units could appear in front of many members of the public, and they could attempt to mobilize the public's opinion, and accordingly, affect them to raise their closeness centrality and prestige due to their link with the latter.

- Based on previous conclusions and study sample analyses, suspicions may be limited, restricted, and defined in accounts that attempted to mobilize public opinion through identifying entities that scored highly in prestige centrality degrees. This suspicion may be confirmed by finding the common actors that are clustered between two groups.

Fifth: Study Recommendations

- Security analysts and law enforcement decisionmakers must constantly act on preparing and developing lists of positive and negative words. Thus, they can accurately measure the public mood and predict the crisis or its escalation.
- Security personnel who specialize in law enforcement agencies must be prepared and trained to professionally use open-source analytical tools and produce high-quality intelligence and visual plans for monitoring and following up on the public’s mood measurements, as well as to monitor suspicious actions that may affect the public regime during crises.
- Decisionmakers should identify the influential accounts on social platforms during the crisis. These accounts have a high degree on the centrality scales. They may assist in combating outbreaks of rumors and fake news on social platforms.
- By following and monitoring linguistic analyses, it is possible to follow the spread of rumors and the extent of their escalation or decline on social platforms.
- These study conclusions contribute to the support of media content for law enforcement authorities.

References

1. Abdelkhalek, Y. (2017). Opportunities of political decision makers to control political crises via new media: The Sudan crisis as a sample. *Faculty of Mass Communication Magazine*. Cairo University.
2. Abdelmottlep, M. (2019). Intelligence-led policing: The police action based on artificial intelligence and information analysis (3rd ed.) *International Police Sciences Association*. Dar Al Nahda Al Arabiya.
3. Abdulrazak, M. (2019). *Criminal intelligence and information analysis governing rules*. Naïf University Publishing House.
4. Abdulrazak, M. (2020). Social media platforms data-visual analysis as information open source in dealing with refugees crisis: Analytical study by using NodeXL program [Published Research]. *Alfikr Alshurti Periodical Journal*.
5. Adedoyin-Olowe, M., Gaber, M. M., & Stahl, F. (2013). A survey of data mining techniques for social media analysis. *arXiv preprint arXiv:1312.4617*.
6. Agarwal, N., Al-Khateeb, S., Galeano, R., & Goolsby, R. (2017). Examining the use of botnets and their evolution in propaganda dissemination. *Defense Strategic Communications, 2*(2017), 87–112.
7. Ahmed, W., & Lugovic, S. (2019). Social media analytics: Analysis and visualization of news diffusion using NodeXL. *Online Information Review, 43*(1), 149–160.
8. Berzinji, A. (2011) *Detecting key players in terrorist networks*. Retrieved from: http://uu.diva-portal.org/smash/get/diva2:442516/FULLTEXT01.pdf

9. Bodine-Baron, E. (2016). *Examining ISIS support and opposition networks on Twitter* [e-Book]. RAND Research Reports, RR-1328-RC. RAND Corporation.
10. Bodine-Baron, E. A., Helmus, T. C., Radin, A., & Treyger, E. (2018). *Countering Russian social media influence.* RAND Corporation.
11. Butt, W. H., Akram, M. U., Khan, S. A., & Javed, M. Y. (2014). Covert network analysis for key player detection and event prediction using a hybrid classifier. *The Scientific World Journal, 2014*.
12. Carter Olson, C. (2016). # BringBackOurGirls: Digital communities supporting real-world change and influencing mainstream media agendas. *Feminist Media Studies, 16*(5), 772–787.
13. Cota, M. P., Rodríguez, M. D., González-Castro, M. R., & Gonçalves, R. M. M. (2017). *Massive data visualization analysis of current visualization techniques and main challenges for the future.* Proceeding of the 12th Iberian Conference on Information Systems and Technologies (pp. 1–6). The Institute of Electrical and Electronics Engineers.
14. Ganis, M., & Kohirkar, A. (2015). *Social media analytics: Techniques and insights for extracting business value out of social media.* IBM Press.
15. Gupta, R., & Brooks, H. (2013). *Using social media for global security*. John Wiley & Sons.
16. Hansen, D., Shneiderman, B., & Smith, M. A. (2010). *Analyzing social media networks with NodeXL: Insights from a connected world.* Morgan Kaufmann.
17. Ianni, F. A. J., & Reuss-Ianni, E. (1990). Network analysis. In Criminal Intelligence Analysis (1990) P. P. Andrews Jr, M. B Peterson (Eds.), *National Criminal Justice-*

125011, https://www.ojp.gov/ncjrs/virtual-library/abstracts/criminal-intelligence-analysis

18. Kase, S. E., Bowman K. E., Al Amin T., & Abdelzaher T. (2014). *Exploiting social media for army operations: Syrian civil war use case*. Aberdeen Proving Ground, Md.: Army Research Laboratory, July 2014. Retrieved from: https://www.researchgate.net/publication/268520959.
19. Kennedy, D. M., Braga, A. A., Piehl, A. M., Weisburd, D., & McEwen, T. (1997). *Crime mapping and crime prevention.*
20. LeClerc, B., & Savona, E. U. (Eds.). (2016). *Crime prevention in the 21st century: Insightful approaches for crime prevention initiatives.* Springer.
21. Marcellino, W., Smith, M. L., Paul, C., & Skrabala, L. (2017). *Monitoring social media: Lessons for future department of defense social media analysis in support of information operations.* Rand National Defense Research Institute Santa Monica. Retrieved from: https://www.rand.org/pubs/research_reports/RR1742.html
22. Omand, D., Bartlett J., & Miller C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security, 27*(6), 801–823. Retrieved from: https://www.researchgate.net/publication/262869934.
23. Ronoh, L., Karie, N., & Rabah, K. (2017). Using SNA centrality metrics to detect suspicious social media users to aid law enforcement agencies in Kenya. *Mara Research Journal of Computer Science & Security*, *2*(1), 1–19. ISSN 2518-8453.
24. Smith, M. A., Rainie, L., Shneiderman, B., & Himelboim, I. (2014). Mapping Twitter topic networks: From polarized crowds to community clusters. *Pew Research Center, 20*, 1–56.

25. Srivastava, J., Ahmad, M. A., Pathak, N., & Hsu, D. K. W. (2008). *Data mining based social network analysis from online behavior*. In Tutorial at the 8th SIAM International Conference on Data Mining (SDM'08).
26. Weber, I., Garimella, V. R. K., & Batayneh, A. (2013, August). *Secular vs. Islamist polarization in Egypt on Twitter*. In Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (pp. 290–297). ACM
27. Yang, Y. B., Li, N., & Zhang, Y. (2008). Networked data mining based on social network visualizations. *Journal of Software, 19*(8), 1980–1994.

Table 1 – The most important used intellectual units.

Word/phrase	Frequency Number	Emergence of word	Correspondence of word with positive list	Correspondence of word with negative list
Positive words inserted in list	1609	0.049		
Negative words inserted in list	1071	0.033		
Non-categorized words	30161	0.922		
Total words	32723	1.000		
Physicians	214	0.008	FALSE	FALSE
#In_solidarity_with_the_Egyptian_Doctors (#متضامن_مع_أطباء_مصر)	191	0.007	FALSE	FALSE
Brotherhood (إخوان)	166	0.007	FALSE	FALSE
The White (الأبيض)	123	0.006	FALSE	FALSE
Hala_Zayed_ Dismissal (#إقالة_هالة_زايد)	110	0.005	FALSE	FALSE
Corona (كورونا)	105	0.005	FALSE	FALSE
Need (حاجة)	104	0.005	FALSE	FALSE
For the sake of (عشان)	97	0.005	FALSE	FALSE
Hospital (مستشفى)	97	0.005	FALSE	FALSE

Word/phrase	Frequency Number	Emergence of word	Correspondence of word with positive list	Correspondence of word with negative list
Doctor’s strike (#إضراب_الأطباء)	95	0.005	FALSE	FALSE
Army (جيش)	93	0.005	FALSE	FALSE
Brotherhood (إخوان)	88	0.005	FALSE	FALSE

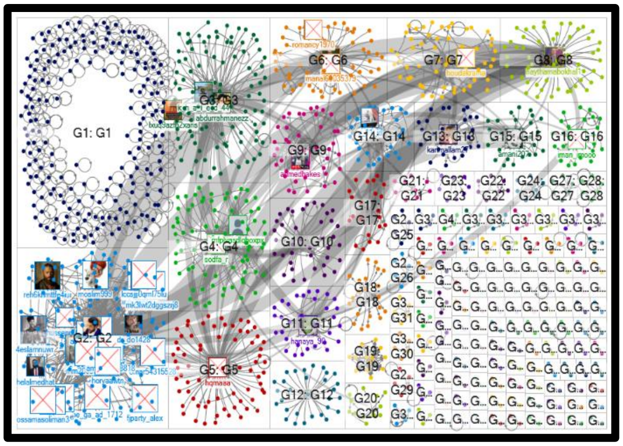

Figure 1 [showing the division of the study sample into clusters, hashtag]

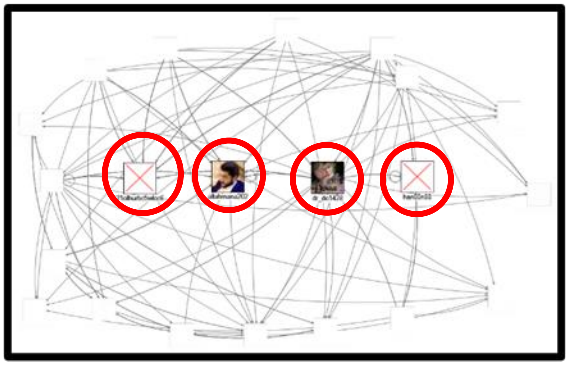

Figure 2 [shows the four accounts that scored high in both the previous two scales] (Betweenness and prestige) using the (NodeXL) tool.

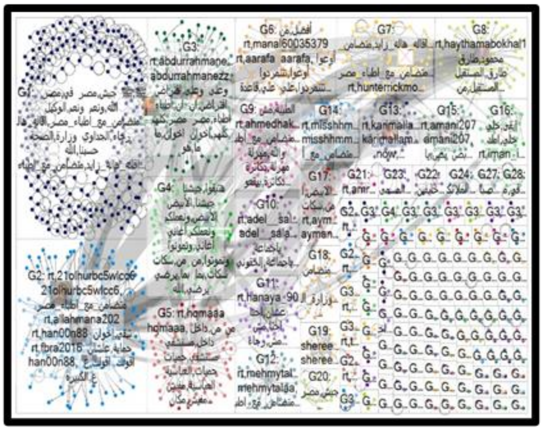

Figure 3 [shows the division of the study sample into clusters and within each cluster the most frequent word pair in] (#by using (NodeXL) (#)

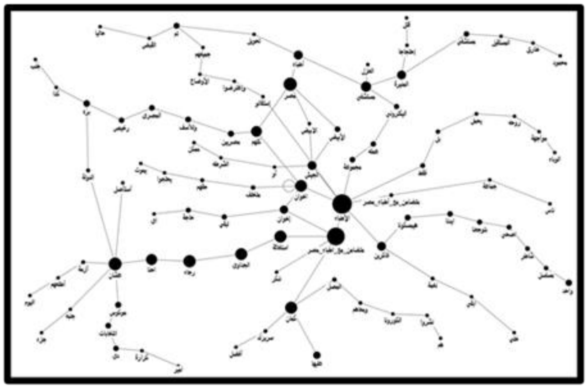

Figure 4 [clarifies the interaction between the most frequent words pair within the hash tag] The words size is adjusted according to Betweenness Centrality scale using the (NodeXL) tool.

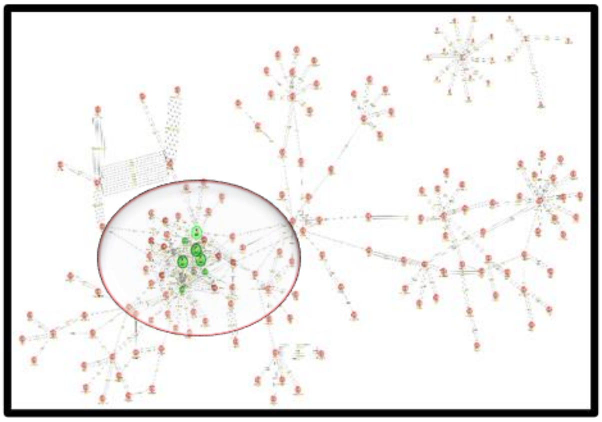

Figure 5 [clarifies that the most important accounts which form cluster in common accounts shared hashtags] (#اضراب_الأطباء) and (#متضامن_مع_أطباء_مصر) in using (IBM i2) program.

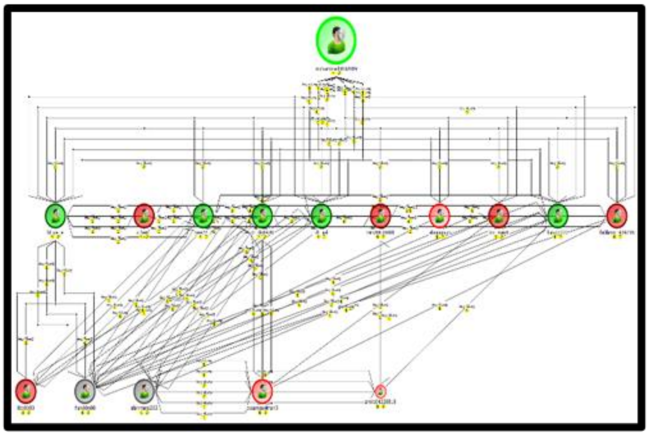

Figure 6 [clarifies that accounts clustered within the hashtags] (#مصر_أطباء_مع_متضامن) and (#الأطباء_اضراب) with identifying its organizational structure using (IBM i2) program.

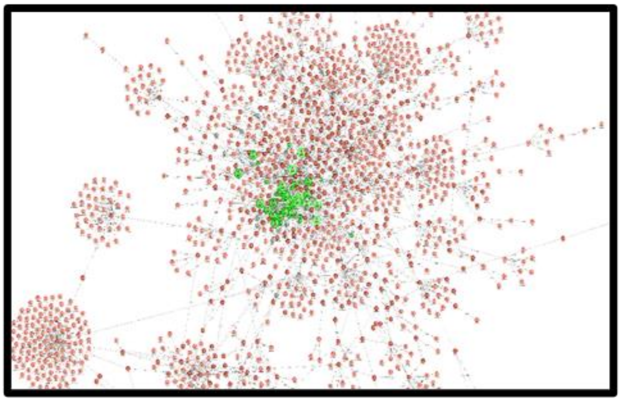

Figure 7 [clarifies the accounts sites with (green color) that are identified and suspected in mobilizing the public opinion].

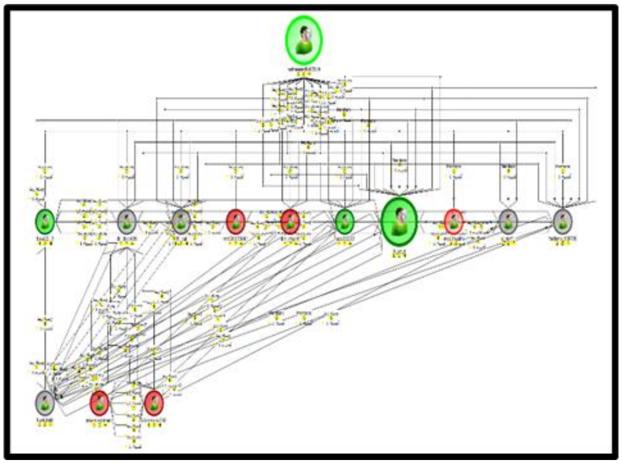

Figure 8 [clarifies that the extremist formation, its sharing more than one hashtag, and its structural organization has been proven that is controlled by the account] (mohammed0102019).

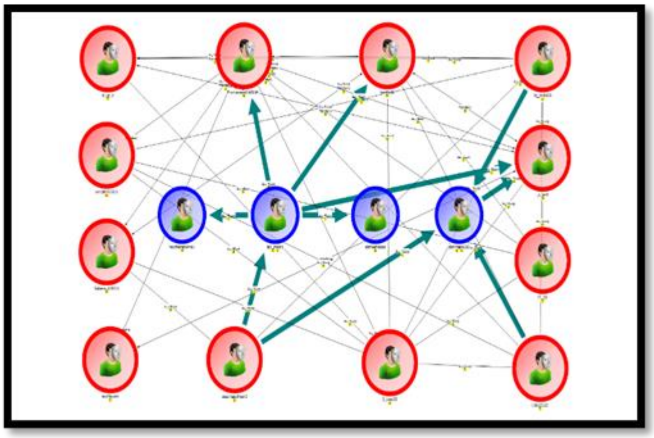

Figure 9