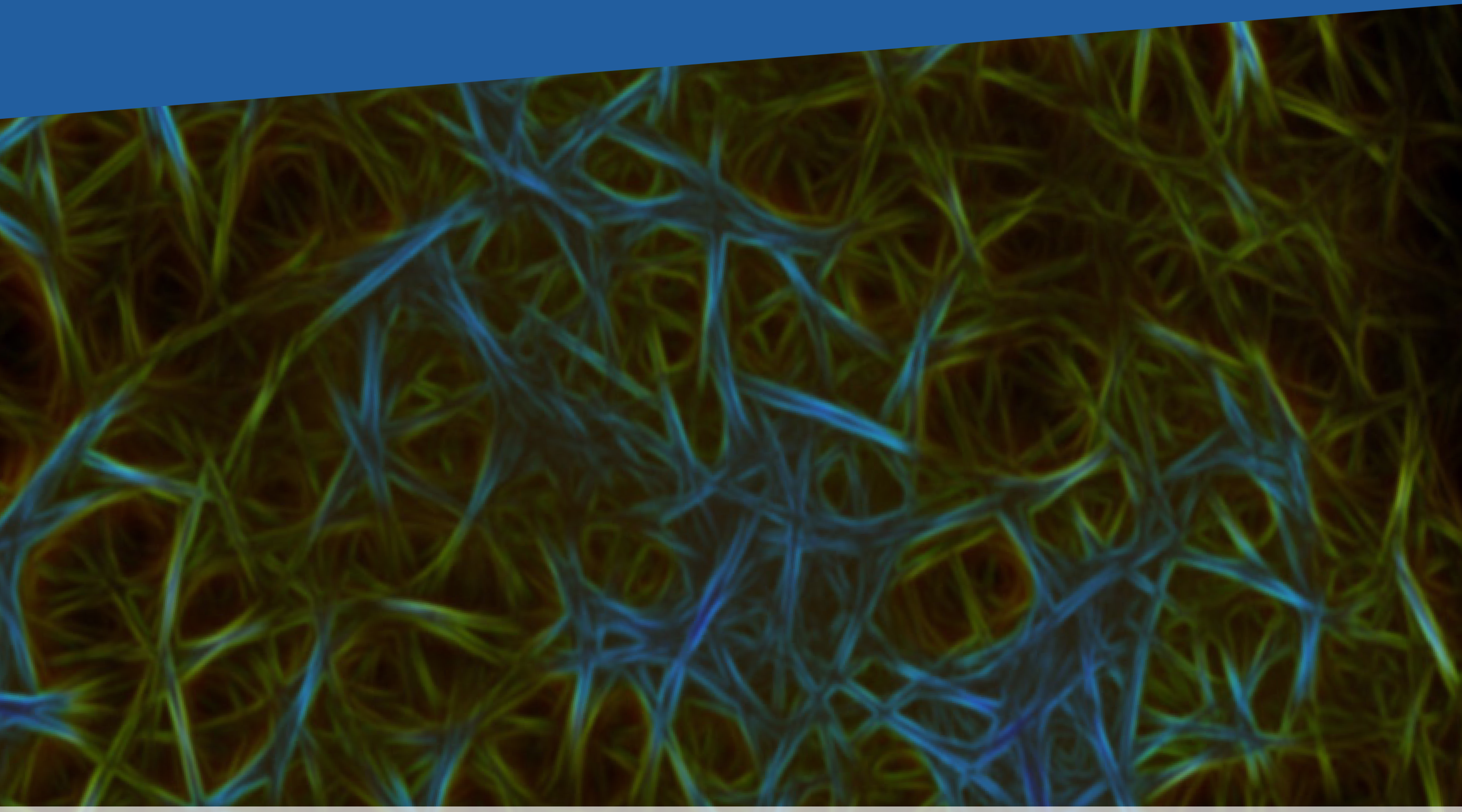


NETWORK OF TERROR: HOW DAESH USES ADAPTIVE SOCIAL NETWORKS TO SPREAD ITS MESSAGE

RESEARCHER: JOSEPH SHAHEEN

RIGA | NOVEMBER 2015

ABOUT THE AUTHOR

Joseph Shaheen is an American researcher, consultant, advisor and academic who has spent more than a decade applying quantitative methods to social science environments, including leading global corporations, and government agencies. His work covers the gamut of People Analytics and the application of data science, social simulations, social network analysis, and statistical analysis to answer some of the world's most critical questions.

Mr. Shaheen holds a Bachelor's degree in Physics, and two Master's degrees. He is also currently pursuing his doctorate in Computational Social Science. He resides in Washington, DC. He can be reached at Joseph.Shaheen@humanalliance.com, or on his website www.josephshaheen.com.

ACKNLOWLEDGEMENTS

I must thank the staff and leadership of NATO StratCom COE for providing an open and positive environment conducive to researching one of the most challenging topics of our times. I must also thank the US Department of State for facilitating the process and providing the funding that made this product possible. Last but not least, thank you to the staff of IIE who have been the underpin of the entire process from start to finish and for facing difficult logistical challenges with professionalism and a solid focus on allowing us to deliver this high quality research.

ABOUT THE NATO STRATCOM COE

The NATO StratCom COE, based in Riga, Latvia, contributes to improved strategic communications capabilities within the Alliance and Allied nations. Strategic communication is an integral part of the efforts to achieve the Alliance's political and military objectives, thus it is increasingly important that the Alliance communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions.

The mission of the NATO StratCom COE is to contribute to the Alliance's communication processes in order to ensure that it communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions. The NATO StratCom COE provides comprehensive analyses, timely advice and practical support to the Alliance, designs programs to advance doctrine development, conducts research and experimentation to find practical solutions to existing challenges, it's strength is built by multinational and cross-sector participants from the civilian and military, private and academic sectors and usage of modern technologies, virtual tools for analyses, research and decision making.

- Support the development of a NATO Military Committee Strategic Communications policy and doctrine,
- Develop Academic Magazine "Defence Strategic Communications",
- Study Russia's Information Campaign against Ukraine,
- Research 10 years of ISAF Strategic Communications efforts to extract best practices and lessons learned,
- Research DAESH information campaign and its influence on NATO countries' societies,
- Develop Strategic Communications online course "Strategic Communications for beginners", courses for senior officials, basic and advanced courses for international staff officers,
- Support NATO StratCom training and education, exercises.

EXECUTIVE SUMMARY

We conducted research aimed at understanding the process by which DAESH disseminates propaganda online.

Our focus was not the content that is distributed but the method by which it is distributed.

We did so using a number of qualitative, statistical, and numerical analysis techniques in hopes of gaining a deeper insight into their operations and making recommendations for NATO and NATO member states on how to combat them effectively.

We discovered a number of important findings the most salient of which is on how individual level decisions made by many of their members have contributed to the survival of their propaganda capabilities, and in some instances an advanced ability to thwart efforts to eliminate their message and their outreach to both locals as well as westerners.

We can summarize our findings as follows:

- Popular social media platforms such as, and especially, Twitter forms the core of DAESH's propaganda and information dissemination efforts. They use these mediums as the core of a web of content that is spread in many parts of the ungoverned internet.
- DAESH (perhaps unknowingly) uses and an adaptive network structure on Twitter to combat outside influences and to react to external operations seeking to curb their operations. This network adapts at high speed and with limited central organization.
- DAESH makes innovative use of platform vulnerabilities that allows them to evade detection, suspension and deletion by state and non-state actors through both automated and manual methods of detection.
- DAESH has amassed a strong following supported by an internal dedicated human infrastructure allowing them to affect a substantial impact on the information environment.
- Through the use of a core-periphery network structure and a high number of network-central actors DAESH created a redundancy factor that can withstand repeated efforts to disrupt their information supply chain.
- Through the use of account inflation, signaling, and closure methods, DAESH has been able to successfully create friend/follow networks that feed into their ability to build sustainable adaptive networks, evade detection, and maintain their level of online activity.
- DAESH has built a network structure that utilizes the flexibility of small communal networks and allows for the large scale interactions commonly associated with large diverse-use networks. This adds to the challenge of combating them in the traditional information warfare environment.
- We create an explanatory process to simplify the reader's understanding of the group's usage of social media. We call it the **DEER process**. The DEER process begins with dissemination and ends with replenishment. We recommend this model as a way to build more effective strategies in combating the group.

Our findings lead us to a more detailed understanding of the DAESH propaganda machine which has gained them notoriety throughout the world and especially on traditional media platforms; and though our conclusions are technical in nature, they have far reaching policy implications.

To begin, these conclusions illustrate the ineffectiveness and inefficiencies of a distributed response to DAESH propaganda. DAESH uses limited centralization from a network perspective in order to evade detection while maintaining some control over method and content of their messages—a hybrid model—where flexibility and potency are both achievable. This means that substantial resources must be dedicated in order to combat their ideology effectively. These resources (human and otherwise) are, at the moment, non-aligned, ineffective, and unsustainable over the long term.

This is not because the resources and methods used are by nature ineffective, but because the

adversary is using strategies and tactics which have never been encountered on this scale ever before.

For example, in this report we show that the targeting of highly visible active accounts on Twitter for deletion or suspension, though can eliminate short terms gains by the group, also provides them with the time and knowledge to build more adaptive, responsive networks. While, if account targeting is based on a community/clustering method, we can increase the transaction costs of our adversary's recovery substantially—gaining invaluable time pinned on lower levels of propaganda diffusion—and simultaneously building more strategic operational tactics.

We propose and recommend that in addition to the adjustments of technical methods used in the targeting of DAESH network infrastructure, that more emphasis should be placed on disrupting the supply chain of propaganda, rather on providing contrasting messages. This implies that permanent investments not only in new technology, but in human resources should be made, and coordinated labor division among NATO members as well as allies in the region should be instituted.

Our discoveries rely on a number of assumptions to produce our recommendations—the most important of which—is that this information battle is based on concepts of adaptive networks and complex systems[1]. This is a direct result of DAESH's approach of relating loose policies to its members and allowing them to make individual level behavioral decisions on how best to conduct an information war.

In turn, this means that traditional methods as have been adopted by various agencies, state, and non-state actors alike simply will and do not suffice, as has been evident from the group's continual ability to conduct a propaganda war while facing insurmountable opposition, both physical and electronic.

We also recommend that more effort must be made to remove the value proposition which DAESH uses to attract recruits to begin with. Though, our research did not engage the socio-economic and geo-political environment under which potential recruits are subjected, we hypothesize that innovative efforts in this space can produce substantial declines in DAESH's ability to disseminate propaganda and ultimately to recruit westerners to their cause.

Finally, we make recommendations for future and ongoing research, some of which is much needed to understand and produce effective strategies to combat the group.

INTRODUCTION

Our mission was to understand the format and methodology which DAESH uses to disseminate information. Our research focus was not the content shared by DAESH, but rather the lines of communication from creation to absorption by its intended target audience. This required deep analysis focused on networks of communication on social media. Our results yielded powerful insights, some common sense recommendations, and a few predictions on future events and actions.

We used a number of techniques to conduct our analysis. These techniques include social network analysis, social simulations, statistical analysis, as well as basic content and categorical analysis.

DAESH has been relatively successful in disseminating its propaganda. In contrast to its competitor and predecessor Al-Qaida, DAESH shows extreme proficiency in understanding their audience, identifying the salient issues facing them, and using those issues to develop high quality recruitment content driven to target those issues.

From an analysis perspective we believe that it is important to not only gain an understanding of the content that DAESH spreads worldwide, but also in how it spreads that content. Our hope is to identify vulnerabilities that can then be used to combat DAESH's propaganda machine.

[1] Complex systems here being used as an academic term positing non-lineardynamics, not to be confused with complicated systems.

Our efforts began with an environmental scan to identify the information supply chain DAESH was using. Once identified, we began the process of building a clear research methodology which we hoped would answer our central question: How is DAESH disseminating its propaganda online?

Method of Analysis

We conducted five modes of analysis.

The first was a scan of current traffic on Twitter which included a semantic and keywords analysis of tweets, an analysis of hyperlinks on the social web and generally mediums used by DAESH, and an activity sweep to help identify levels of online and social media activity.

The second mode of analysis was to conduct sample studies of numerous traffic networks (tweets, replies, and retweets) of Twitter hashtags as we established that this medium serves as the central nervous system of their propaganda effort.

The third mode of analysis was a friend/follow network analysis to understand the friend and follow structure and behavior of the DAESH Twitter network. This meant collecting data on who follows whom on Twitter using high visibility DAESH accounts as seed for the collection of the network[2]. This allowed us to identify community building patterns, methods of account creation, likelihood of cluster formation as well as gaining a general understanding of the network's replenishment methods for suspended, cancelled or deleted accounts.

The fourth mode of analysis consisted of analysis of the leadership of collected friend/follow networks for which we gathered the attributes (number of followers, number of tweets, account creation date etc.) of the most influential accounts and analyzed them qualitatively and categorically to identify behavioral patterns that would not be notable through a structural and quantitative analysis alone. This yielded insight into the process of replacement of leadership accounts, and it also helped us understand the relative mix of account attributes and draw larger insights about the network's ability to churn news and information packages to the public.

The fifth and final mode of analysis consisted of a qualitative content analysis based on individual account actions and behavior. This mode bridged the gap between understanding larger network structure and traffic network activity to the actions of individual members of the group.

Why the Focus on Twitter?

Our analysis focused on DAESH's use of Twitter for several reasons. Primarily, DAESH uses Twitter to disseminate information to those who would not have otherwise sought it. Twitter is a medium that is diverse in its demographics, global in its reach, easy to use, and is much more suited for anonymous and yet open-while-encrypted communications that any subversive entity requires in order to conduct detrimental operations.

Additionally, because Twitter allows for the posting of unrestricted content as long as it is linked to an outside source, it makes for an effective tool of information warfare, and a uniquely supportive tool for hybrid operations.

Therefore, we were not surprised to find that in our analysis DAESH uses Twitter as a connecting medium for all of its distributed content all over the web.

To illustrate further, consider that DAESH utilizes a number of uncontrolled, unsupervised sites[3] to post videos, photos, messages, and press releases all of which reaches supporters who had previous knowledge of the locations of those messages, but for recruitment and media efforts to be successful DAESH had to share these content suppositories in public domains and information stream such as Twitter.

[2] Please see appendix methodology for more details on the seeding algorithm and data collection. Some variations of this report do not include the methodology appendix. If so, please contact the author.

[3] e.g. Justpaste.it or the archive.org

Failing to do so means that they would generate high volumes of high quality content which no one ever sees.

And although they do so through the use of Twitter, Facebook, Snapchat and other mediums, Twitter allows for faster recovery from suspended accounts, possesses stronger encryption for private messaging (point-to-point communication) and a much broader audience.

Additionally, and as you will see in subsequent sections, DAESH engages in replenishment of its deleted and suspended accounts as a matter of due course. Twitter is a platform which allows for recreation of a user's pre-existing network much more effectively than other social media services.

DAESH's choice of Twitter as a medium represents strategic insight into the operational environment for information warfare. It is not by accident.

Through the use of Twitter DAESH is able to amplify both its own perceived size and potency as well as its message across time and geographic space. This is apparent in its ability to recruit much more successfully than their competitors and counterparts who may follow similar ideologies, claim to have as many operatives on the ground, but do not come close to achieving the level of success that DAESH has in recruiting native westerners to their cause.

This is perhaps the most important factor the reader should consider—influence on social media today equals recruits tomorrow. This fact alone is unavoidable, and will change the dynamics of every battle fought this century. DAESH is simply the first to truly capitalize on this dangerous dynamic, and Twitter is simply the world's most open and useful platform for their messages. In fact, given enough and the right kind of data we could infer the total number of future recruits DAESH gathers from platforms such as Twitter, and from that, combined with force projection estimates, we could estimate the total number of fighters on the ground, some of their attributes (age, gender, level of education etc.), and thus provide limited predictions on potential tactics and strategies employed.

Moreover, DAESH's use of Twitter also means that it can conduct recruitment and propaganda operations from any location in the world, and without having to make any investments in infrastructure, technology, or a dedicated workforce. And since Twitter provides more complexity to communication analysis than

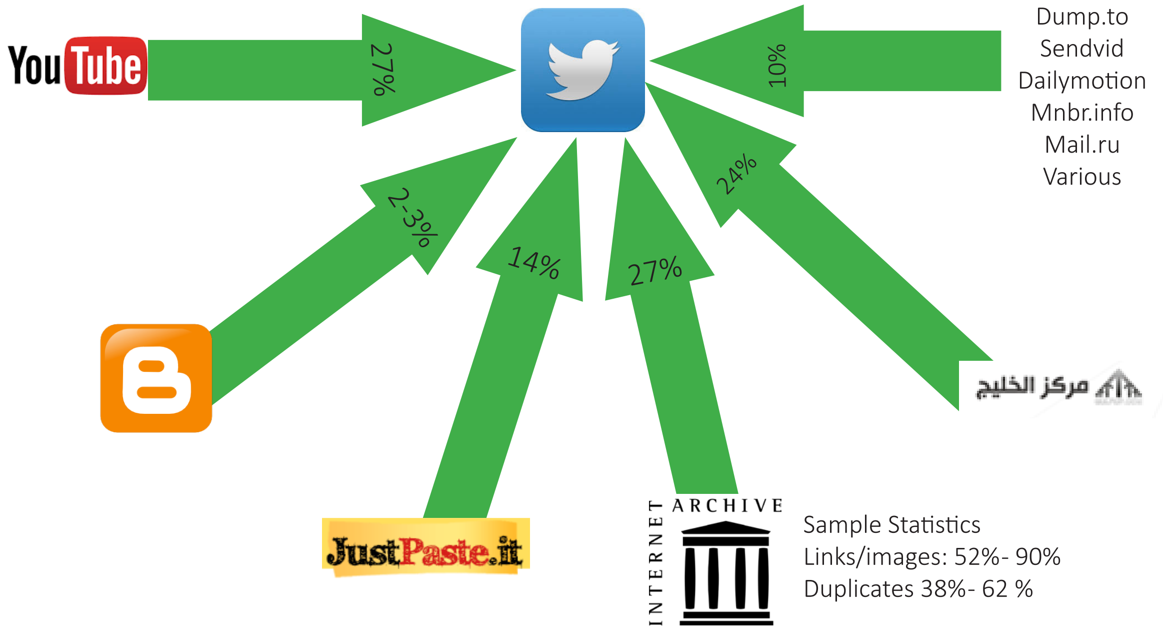


Figure 1: ISIS uses Twitter as a connecting medium for the majority of its content distributed all over the web. This allows for broader propagation of its content, while allowing for faster recovery from opposition actions.

any other medium, discerning grand strategy from their behaviors is a task currently too demanding for any single agency or entity—be it governmental or non-state—to undertake alone.

Finally, the methodology and communication theory required to do discern grand strategy, if any, from this analyst's perspective, is insufficient to provide useful actionable intelligence not already provided by traditional methods. We believe that this group, though unknowingly, realizes this and thus make Twitter their primary choice for information warfare.

MODE I ENVIRONMENTAL SCAN

Structured Media Content[4]

As part of a preliminary evaluation of DAESH propaganda, we evaluated the general structure of DAESH content.

DAESH releases content on a daily basis in several languages including English, Arabic, German, Farsi, Hindi, and French. They use professional press release style imagery and graphics. They also release professionally created and edited videos for which they have become notorious since their inception.

An important feature of the videos to date is the inclusion of ingredients aimed at attracting a young demographic who are more likely be technology savvy and more likely to respond to Hollywood-style imagery and concepts. New recruits can then be brought into ongoing information operations bringing with them lessons learned and suggestions from previous media cycles.[5]

Generally, the structure of the content follows familiar patterns commonly associated with corporate social media marketing programs.

Content is:

- ***Relevant*** to current news and thematic public discourse
- ***Short*** in length (in contrast with Al Qaeda propaganda which typically tends to be long tirades by Al Qaeda leaders)
- Makes strong use of ***Islamic music/ chants*** (where appropriate) and sound effects
- Makes strong use of ***high quality*** and high definition video editing and recording
- Content tends to follow some larger ***narrative*** thus makes for engaging consumption by target audience
- ***Simple*** and easy to digest.
- ***Diverse*** in its content types (action/ battles, normal life, political, and religious).

To some extent, the structure of content is independent of the content supply chain and method of dissemination that it is brought through in the arena of social media.

Most social mediums today offer users the ability to share text, images, video, and sound of varying quality as a core feature, but it is important to note that though DAESH produces high quality well-structured content, if the process of content distribution of that content is ineffective, then quality of content becomes less of a governing dynamic to information operations. In other words, if content is not distributed well then its quality does not matter.

Impact through Volume & General Trends

We began by analyzing the volume of content shared on Twitter expecting to gain a fundamental understanding of the salient trends of DAESH's activity in sharing their propaganda.

[4] Though the focus of our study was in the dissemination (supply chain) of information, we conducted a preliminary analysis of content structure to bridge any content-driven phenomenon with the methods of which that content was widely distributed.

[5] Recruits can also be given tasks in ground operations or civil service depending on a number of factors and needs on the ground.

During the 30 day period[6] studied we identified and subsequently measured keywords (hashtags) used on Twitter which were commonly associated with DAESH members, operatives and supporters, and keywords that were almost always being used by their opponents. All analysis for this mode were conducted in the Arabic language.

We discovered that during this 30-day period there were a total of ***147,412*** tweets using the hashtag *"The Islamic State"*, and ***443,336*** using the hashtag *"The (State of) Caliphate"*[7] for a total of almost ***700,000*** tweets.

Based on other indicators and an ongoing campaign by various governmental and non-state entities to educate the Arabic-speaking public on how to describe DAESH in the middle east, we believe that the largest majority of active Arabic-speaking Twitter users will generally refrain from the use of either hashtags to describe or DAESH, therefore we induce that these tweets represent DAESH members and/or supporters. This conclusion is supported throughout our analysis by other indicators.[8]

On average use of the two DAESH-supporting hashtags ranged from ***5,000*** to ***30,000*** tweets per day.

We also wanted to gain insight into the level of opposition on Twitter to DAESH's message and ideology so we used the keyword "Daesh" which typically represents the acronym for "DAESH" in Arabic but is almost exclusively used as a derogatory description by Arabic-speaking communities and community-aware military and government personnel throughout the world.

We discovered that in that same 30-day period "Daesh" was used in almost ***1.4 Million*** tweets roughly doubling the tweet activity of DAESH supporters and members. A qualitative sampling of the tweets supports our assumptions that generally, DAESH opponents preferred the used of the word "Daesh" rather than describing them as Islamic State or any variation thereof.

Use of this hashtag (Daesh) typically associated with DAESH opposition ranged from ***20,000*** to ***90,000*** tweets per day.

We also found interesting patterns in the levels of activity during this period that allowed us some greater insight about DAESH opposition and supporters on Twitter: Mainly, that though both sides of the issue look at spreading information as a matter of internal policy, activity levels continue to be subservient to cultural and demographic conditions.

For example, we saw a steep decline of tweet activity roughly around the 15th - 17th of July which coincided with the last day of the holy month of Ramadan or the beginning of Eid-al-Fitr, which is a Muslim celebration noting the end of the holy month of Ramadan, and which celebratory activity traditionally takes place. This lower level of activity continued for exactly 3 days (which is the length of festivities) with criticality reached on the 16th of July.

This illustrates an important feature of DAESH's social media activity in that it continues to be a part of local customs and practices and thus predictable to some extent. This predictability is in contrast to the group's ability to evade detection and misinform the public. It could also provide an edge for planning operational counter actions and the timing of those operations for those who oppose the group and its ideology.

Finally, during the period in which our investigation took place there was an active campaign by a number of unknown entities to notify Twitter and ultimately suspend active DAESH accounts. This public campaign took place under the hashtag *"70,000 DAESH accounts have been closed" (in Arabic)."*

It is unclear whether this campaign was

[6] July 6th to August 3rd of 2015 coinciding with 20th of the holy month of Ramadan and ending on 18th of Shawwal (1436 A.H.)

[7] All keywords, and hashtags were in Arabic.

[8] The argument used for promoting the use of Daesh versus Islamic State or DAESH in the Arabic language is that Daesh delegitimizes DAESH claims on the creation of an "Islamic" and "caliphate" state. Don't call them what you won't recognize them as being.

organized by some governmental institution, local or foreign agency, or if it was created by a number of volunteers from different parts of the world.[9] However, our tweet activity measures showed no sign that this campaign was effective.

This was the first major insight into the efficacy of the information operation activity undertaken by the group:

Our expectation after the deletion or the suspension of 70,000 propaganda accounts would be that there should be some sustainable (and measurable) decline in activity during the period in which the campaign was active, or at least in the period immediately following it.

We saw no clear evidence of this taking place.

Keywords as Geo-locator

We found numerous instances of DAESH operative and supporter accounts using a number of hashtags in the content of their messages to designate a geographic location that is either relevant to the content or to the target audience that it was intended for. For example, DAESH would regularly release information relevant to its campaigns in Homs and Raqqa, and would tie that information to Hashtag “State of Homs” and Hashtag “State of Raqqa”.

Mentioned “States”:

- Raqqa
- Sinai
- Tripoli
- Salahuddin
- Furat
- Barqa
- Gaza
- Aljazeera
- Twitter

Operationally, this provides DAESH with an advantage in being able to disseminate target information to specific regions of the world, and for any independent actor to share information within their region using a combination of Islamic State hashtags as well as geographic keyword tagging.

The method itself is likely a reactive mechanism to the dangers of using Twitter’s native geo-tagging function which provides a GPS-produced tag with latitude and longitude coordinates attached to each individual tweet. Twitter’s native method would be dangerous for operatives to use because their location would be pinpointed down to less than a few hundred square meters. In fact, in December 2014 DAESH issued an edict that forbade its fighters from turning on Twitter’s native geo-tagging function.

The systematic use of geo-tagging using keywords also showed the early stages of an organized and planned information operation.

Additionally, structuring content dissemination in this way provides for at least two secondary advantages for DAESH:

1. This method provides for the basic building blocks of an information/knowledge index. Ultimately, the most important feature of this index would be that it is searchable, allowing anyone to search back in time for information about previous operations, political developments, and the state of affairs of other groups all over the world and more importantly, in their own region.
2. It allows for targeted outreach and recruitment campaigns in areas of the world where DAESH may not have any on-the-ground presence, such as western countries and countries in theatres of war where it is possible to sway public opinion and thereby increase resource extraction, human and otherwise.

Fundamentally, using keywords to regionally geotag tweets is not a new idea. However, it is in its use by DAESH consistently and seemingly without prior organization that deems the method worthy of note because it allows us to get insight into DAESH’s method of organizing information campaigns in an unorganized fashion—making it more difficult to pinpoint grand strategies and to develop methods of countering their message.

[9] Publicly, volunteers have claimed it.

As an example, we annotate the ways in which DAESH has expanded their use of the geotag concept: One additional keyword/Hashtag we found in common use was "(the) State of Twitter" which is a hashtag used to widely share Twitter-specific operations and tactical needs and events. We found numerous examples of this Hashtag in use to enlist sharing, tweeting, following, and spamming operations by DAESH members—all designed to increase the reach and potency of their message.

This represents an expansion and an improvement on using the geotagging keyword method which likely came as a natural extension because it allows not just for information sharing within and between regions of operations, but very specifically on and for social media operations. Moreover, it represents a clear signal that DAESH intends to focus on social media operations as a critical part of its long-term strategy and integrate it into tactical and strategic planning.

Semantic Analysis

Semantic (keyword) analysis focuses on a number of linguistic analytical methods to help understand the general theme of a social platform's ongoing or past conversations. For our analysis it was especially useful in finding keyword combinations that would provide insight on how network clusters and cliques were using Twitter as a medium.

We found a number of interesting patterns.

Depending on sample we discovered that somewhere between ***30%-50%*** of tweets included links to outside sources of content. Sources were divided with varying degrees to ***youtube.com, archive.org, justpaste.it, Facebook.com*** and other content sharing sites.[10] We estimate that the majority of those hyperlinks pointed to content on sites that generally do not actively moderate their user's content[11]. Video sharing links were especially susceptible to being shared repeatedly as they were the most likely to be found and deleted by their hosting site. This continues to be a robust conclusion even as the organization adapts and the information environment changes with exceptional speed.

We also found that tweets emanating from DAESH operatives or supporters overwhelmingly used geotagging keywords ***80%-90%*** while almost none used Twitter's built in geotagging feature.

"State of the Caliphate" dominated our samples as the main keyword/Hashtag used in DAESH messaging, followed by ***"Islamic State"*** and other variations of Islamic State.

Two commonly found keywords in our analysis were ***"RT"*** and ***"Urgent"*** (***60%-80%*** and ***20%-30%*** respectively) representing two features of the traffic networks we studied: The majority of participants in the Twitter traffic network simply retweeted what others tweeted, thereby operating as a magnifying force to messages, and a large segment of the tweets shared were news and press release messages. This represents the condition of traffic on the mainly used hashtags, but we did see a large and increasing volume of tweets that contained point-to-point or account-to-account interactions that did not utilize any popular hashtags.

This illustrates a strategic capability to use a number of independent actors for amplification of a central message, usually originating from DAESH central operations while maintain the independent nature and behavior of those individual actors.

We also found keyword pairings with geo-tagged hashtags that identified the type of content shared to be a common occurrence. For example, in regions where DAESH controlled major territory, geo-tagging was often combined with press releases (Keyword: ***"Caliphate Announcements"***) and

[10] Towards the end of our study we began to see more links to independent sites, many of which were used as simple submission portals. Though no other open source public research report has listed these unknown portals, we hypothesize that they are used to send secure communications to some central information operating division. In a follow-up assessment of the DAESH traffic network we estimate that they comprised at least 20% of all links shared of 2 independent samples.

[11] This is especially true for sites like justpaste.it and newer forms constantly being developed and used by DAESH.

news announcements, while in areas with an ongoing battle, the focus was on propaganda dissemination and not as much on press releases (for example: hashtag *"Men of War"* combined with "State of Hamah".)

Finally, for most of our samples collected for major supporter hashtags such as the "state of the caliphate", we found that a high percentage were keyword paired with a geolocation as well as the keyword *"RT"*. As Twitter's convention is to automatically attach RT to any retweeted tweet we believe this to be representative of the overall structure of the network's ability to disseminate information.[12]

Other keywords found to be coupled with geotags were diverse and highly fluid as new, external events occur. They included keywords such as *"one body"*, *"visual" "announcements of the states", "Al Bayan News", "poetry"* and many others.

MODE II
TWITTER TRAFFIC NETWORK

Using core methods of social network analysis we gathered a number of tweet populations during the 30-day study which included data points such as account name, account URL, number of tweets, location (if available), the description provided by the user on the account, time zone, the date the account was created, the number of followers and the number of people followed, with the number of times each account tweeted or designated a favorite tweet.

The most important data point we collected from the populations in questions was whether each tweet was shared/retweeted or replied to and by whom.[13] Our objective was to look at the Twitter traffic network for specific hashtags that, from previous analysis, we strongly associated with extremist and terrorist ideology.

Using the relational structure of replies and retweets we hoped to identify the mechanism in which information propagation takes place, pinpoint accounts of central actors, and gain an understanding of the dynamics of information propagation through any given Twitter network.

Network Structure (Topology)

There are many types of network structures, each of which tells of how a network processes and shares information.

The DAESH Twitter traffic network takes the position of a Core-Periphery structure[14], with some groups forming where 76% of traffic network members belonging to the core group. This means that though message dissemination may become decentralized as it propagates through social media networks, around Hashtag communication hubs, messages are centrally driven by a core group of accounts.

This result contrasts the generally accepted assumption that DAESH social media networks are entirely decentralized but rather supports a hypothesis that there is some decentralization/centralization mix at the account level.

We also take into consideration that over the past few months third party actors, such as intelligence agencies, governmental institutions, and independent parties have begun a systematic approach to counter propaganda through engaging in key Hashtag communities. This could be contributing to the apparent decentralization factor more than expected because in Twitter traffic networks, clustering represents groups that support or agree with one another (and so they share each other's tweets). Therefore, we assume and have anecdotal evidence to support the claim that third party actors provide counter-propaganda which seemingly provides higher levels of decentralization trends.

Moreover, decentralization of message and message propagation are two entirely different concepts.

[12] In some samples RT was found as high as 90% in keyword pairs.

[13] This concept is widely known as meta-data analysis and is used by various intelligence agencies.

[14] As measured by a GINI-based continuous coreness algorithm similar to the E-I Index; GINI coefficient equal to 0.45 (maximum of 1, minimum of-1).

It is true that due to the current structure of DAESH's organization, each regional theater of war (e.g. Libya, Sinai, Syria, Iraq, Somalia etc.) manages their own media efforts, and with it, content and method of broadcasting. This may provide for the argument that DAESH propaganda is decentralized regionally, but in terms of levels of activity on Twitter and general social media, regional media centers pale in comparison with DAESH-core. This means that we can conclude that although decentralization in content and broadcasting methods does exist because of regional differences in goals and capabilities, differences in language or perhaps even regional strategic goals, media messages are essentially almost completely dominated by a small group of DAESH-core accounts. Many of those accounts could very well belong to an even smaller group of DAESH operative if you assume account inflation—a reactionary measure DAESH has continued to engage in to inflate their online presence and counter account suspension activities.[15]

This is also indicative of the difficulty of countering the information supply chain through suspending or removing accounts that appear to be part of the core of the traffic network. If one or more core accounts is removed, there may exist a number of other core accounts (sometimes simply additional accounts created by the same user) which can continue to drive the message to its intended audience. Meanwhile, DAESH operatives incrementally develop countermeasures, as well as widely share lessons learned to improve standard operating procedures for evading detection by governmental and Twitter authorities.

We also considered (explicitly) their use of Bot accounts as a tool for inflating their online presence. In our assessment of leadership accounts (Mode IV), and based on a criteria that assumes that bot accounts typically only retweet other accounts without generating unique content, we estimate (conservatively) that at least 16% of accounts were in fact automated for the majority of their life-cycle.

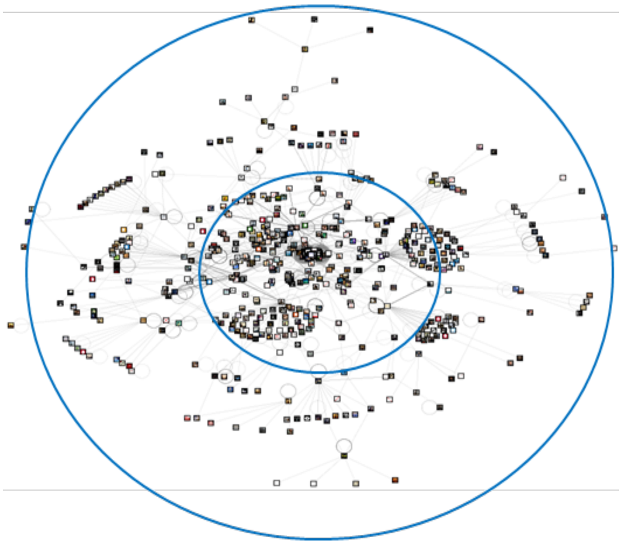


Figure 2: Core-periphery structures are noted for a central group of actors followed by a larger but less dense network. This figure shows an example of one of our collected traffic networks with an added circular visualization to illustrate coreness.

Account Centrality

Centrality measures the extent to which an account is central to the functioning of a network and thus critical to a network's infrastructure and overall performance. In the domain of traffic networks, centrality represents a proxy measure for influence and driving the message to its intended audience.

As part of our study of DAESH's traffic network we discovered, that for each sample, there was a high number of accounts with low centrality measures (peripheral), and only a few accounts with high centrality scores (core group).

Central actors typically had their distributed content retweeted more often than others, and they also retweeted content more frequently and from more diverse sources in the network, thereby becoming more central to information propagation.

Typically, centrality scores[16] provided emphasis on a small group of accounts ranging from 2 to 25 accounts in any daily sample (daily samples typically included 1500-3000 tweets with a

[15] See mode III of our research for a full discussion on account inflation.

[16] We looked at betweenness centrality, closeness centrality, eigenvector centrality, PageRank, and clustering coefficients as the off-the-shelf standard metrics of choice.

few hundred accounts engaged). And, though centrality scores can be seen as arbitrary without proper and universal ranking (which went beyond time and technical resources available for this research,) we found typical network behavior in that a small group of accounts were almost always exponentially[17] more central than the entire traffic network combined.

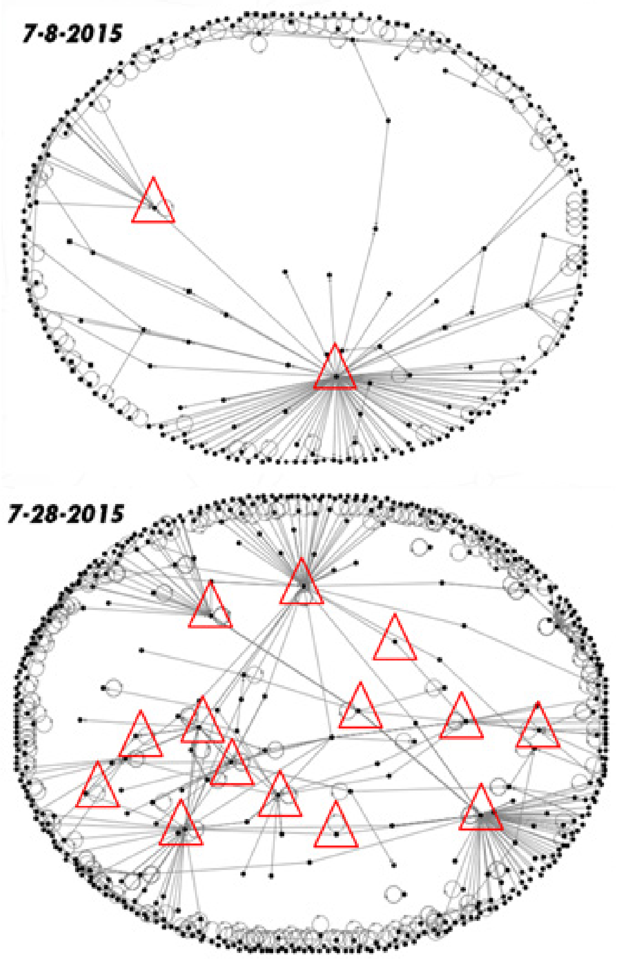


Figure 3: The top network illustrates a sparse traffic network where there are only 2 high ranking central actors (labelled in red triangles). These accounts/users are located in a central position in the network guaranteeing maximum opportunity to see important content, and circulating it to a wider audience, but because there are only a few, it is not a sustainable network. This contrasts the second network visual where the network has built a large number of central actors with redundant access to multiple parts of the network, allowing for continual operation under stress.

We also found that on a regular basis, as accounts became more visible by holding a central position in the network that they were, within a short period of time, suspended by Twitter authorities.

Concurrently, we found that, immediately, other accounts previously inactive or at least unobserved, became more central and with similar intensity and centrality rankings. Thus, we question the effectiveness of simply suspending active accounts as a full counter-strategy to DAESH propaganda. This is due to the complex adaptive nature of traffic networks, and the system in which DAESH uses to rebuild its network infrastructure.

MODE III FRIEND/FOLLOW NETWORKS

In order to gain a better understanding of the full life-cycle of Twitter accounts used for propaganda dissemination, we also conducted a friend/follow network analysis[18]. Friend/follow networks are the networks formed through users of Twitter following other users. This allows followers to receive public and private messages even if the followed account did not use any specific hashtags.

The structure formed by these networks shows patterns very important to understanding influence and public messages sent and received by and to individuals who do not engage in public hashtag discussions.[19]

In our 30-day period of analysis we collected two separate sample networks. The first included ***167,000*** accounts covering ***336,000*** follow relations[20], and the second contains ***159,000*** accounts covering roughly ***half a million*** follow relations.

[17] We use the word "exponentially" loosely here to describe the general nature of the network's centrality, however, centrality scores typically follow a power law distribution.

[18] Also known as Backcloth networks.

[19] This method of analysis, though powerful, is substantially degraded in its power of prediction on Twitter because Twitter Corporation restricts the download of friend/follow relationships to only the top 200 followers of each account. Therefore, researchers engaging in backcloth network analysis need to develop creative techniques to collect the remaining data, which is substantial.

[20] A follow relation is not a unique follow. 1 account can follow hundreds or thousands of accounts.

In order to manage time and resources and avoid scope creep our intended target was to focus only on understanding community, clustering, and clique development/ progression.

We analyzed a number of standard community network measures.[21] We used known DAESH Twitter accounts as seeds and collected their followed and follower accounts and several other iterations of followed and follower accounts yielding the aforementioned networks.[22]

We found friend/follow networks developing in clear and distinct communities, the majority of which we categorized as small communities and the rest of which were categorized as super communities.

On average, there were roughly 10-15 small communities in our network and only one or two super communities. Small communities ranged in size from 500 to 2000 accounts, and super communities were mammoth organizations ranging from ***20,000 to 30,000*** accounts. We studied the collective nature of those communities and though our hypothesis must undergo further studying, we surmise that smaller communities tend to be dominated by small isolated groups of accounts/actors with loyal followers typically engaged around a specific topic and a specific language, and that the majority of these small community accounts belong to DAESH operatives.

Finally, because of subtleties in behavior we concluded that these communities tend to be larger than expected due to account inflation[23].

Super communities tend to contain a larger mix of accounts and actors.

For super community friend/follow networks a larger more complex influence sphere is generated.

Major influencers of these communities tend to be renowned news organizations such as Al Jazeera Arabic, Al Arabiya and others. Additionally, famous (though not always recognized or legitimate) news anchors, political and military figures, activists, notorious propaganda accounts, and some of what may appear as intelligence community accounts are generally found in these communities.

Super communities tend to gather a larger cross section of users coming from different political, social and religious point of views, therefore additional analysis to fully understand them is necessary.

However, it is clear from our analysis that smaller communities tend to develop based on personal communication patterns[24] while larger communities are built when information exchange is more widespread allowing users holding different views to follow other influential users. This culminates in a range of opinions and ideologies.

Because we used highly visible and active accounts to collect both of our large follow networks, our collected network was dominated by DAESH operatives and DAESH agenda but it is worthy of note that some smaller communities developed around active accounts that clearly opposed DAESH propaganda.

This included some near east governmental institutions, official Kurdish military accounts, and accounts belonging to the Free Syrian Army.

We propose that this is the case because of ongoing information operational activity by both sides in which target accounts could possess some intelligence value to the other side.

This means that follow connections do not always indicate agreement with the followed's perspective, but that in some portion of our networks following was simply an act of curiosity or information gathering activity.

The most important take-away of the overall

[21] Average degree (in, out), network diameter, density, modularity, PageRank, clustering coefficient, Eigenvector centrality, average path length, edge betweenness, embeddedness, and connectivity.

[22] This is known as a Snowball sample.

[23] DAESH operatives creating multiple accounts as a countermeasure against deletion or suspension and to deliberately inflate the size of DAESH social presence.

[24] We investigate this further and it forms the basis for the DEER Process outlined later in this report.

network's structure being divided into a number of smaller communities and a much smaller number of larger communities with relatively high density of connections is that DAESH (perhaps unknowingly) has found an efficient solution to combat deletion and suspension of accounts by spreading risk of discovery while attaining activity level on social media.

The solution is dependent upon creating inactive accounts that are immediately reconnected to the network-at-large through following and asking to be followed, and then allowing those accounts to remain inactive for a specified time-period.

Each user typically creates several accounts, and there is specific anecdotal evidence of online operatives being asked to do so as well as evidence that some users do so instinctively.

Once accounts become active and as they're needed, they tend to follow more members of the DAESH network allowing them access to more information and event details as well as engage in actively propagating messages to the larger public.

For authorities seeking to dismember the community structure, they are presented with two challenges: The first is identifying these small communities accurately before being active to begin with. This has to be carried out with precision but it is exceedingly difficult to do so. Typically, inactive accounts rarely identify themselves as DAESH accounts before they become active.

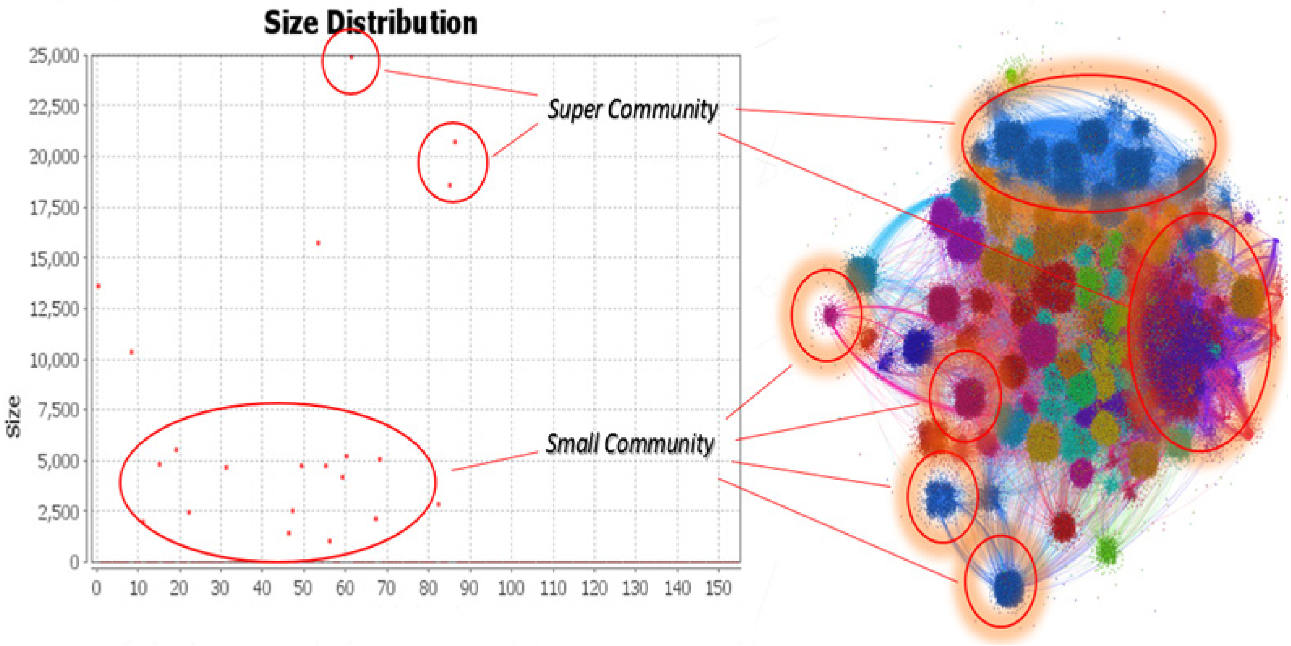


Figure 4: On the right you can see one of two friend follow networks we collected. Each color represents a different community as identified by our clustering algorithm. On the left the size (as counted by number accounts) of those communities. For example, for this network while there were only three super communities, there were 13 small communities ranging in size from 500 to 5200 accounts each. The super communities identified by our clustering algorithm ranged in size from roughly 17,600 to 25,000 accounts.
Clusters on the network diagram (on the right) can be identified by their color. Each mathematical cluster contains a high density of follow relationships (linkages) to others in the same cluster. This is the method by which we mathematically identify clusters. However, as you can see most clusters and communities also have a small number of connections to other clusters—they are not completely isolated.
Note the highly mixed color of the super community on the far right. This is significant because it is unlike the other super community at the top of the network diagram and signals a highly diverse community of accounts not necessarily entirely dominated by DAESH operatives.

The second challenge is that once these accounts are activated they follow a larger number of accounts and receive a larger following as well, blending them into the larger (super) communities and presenting challenges with identification if they maintain a conservative level of activity.

This analysis suggests that traditional methods of discovery and suspension of accounts may not be sufficient, and although our analysis did not include analysis of classified methods and materials at this time, we do not believe that community targeting[25] is utilized in the overall counter-strategy of DAESH propaganda.

We are confident in our assessment that if targeting of community structure and not simply whichever active or highly visible accounts at any given moment is taking place, friend/follow networks are not currently being included in the data inputs for that strategy. We believe this to be a misstep.

MODE IV NETWORK LEADERSHIP

We identified the top leaders of the various friend/follow network by total number of accounts following them, and we isolated them in our sample and conducted a number of quantitative and qualitative analysis to gain a better understanding of the whole network.

We assume that users will follow a leader when this leader features similar opinions, ideology, or some combination thereof. Mainly, we assume that the majority of social media users follow those who they admire, trust, or have something in common with. This assumption holds in theory through numerous peer-reviewed literature as well as anecdotal evidence.

Analyzing the leadership of our networks yielded some powerful insights. We focused on the top one hundred of each network we collected.

We summarize the features of those top 100 leaders of the friend/follow networks as follows:

1. The top 100 accounts had a total follower count of more than **14 Million** accounts.

2. 72% of the top 100 accounts were categorized as “clearly” DAESH accounts with an additional **10%** who we categorized as supporters.

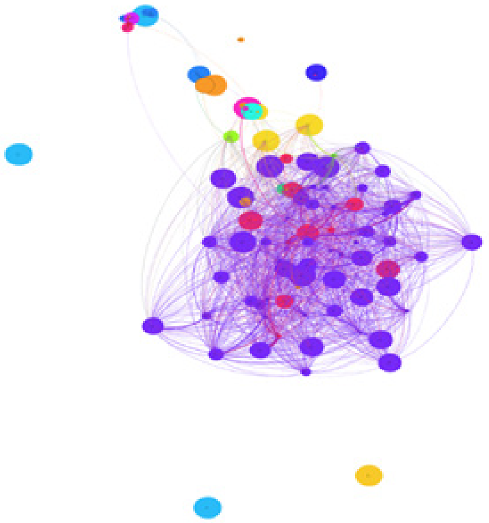
3. 5% of accounts we categorized as “News” accounts but held more than **3 Million** followers of the original **14 Million** accounts.

4. 49% of all network leader accounts were deleted or suspended within 3 weeks of the beginning of our study.

5. We estimate the total number of accounts from the total number of follow relations (**67.5M**) to be roughly **338,000** accounts. This agrees with previous conclusions that accounts and online presence is inflated as most official DAESH counts estimate the organization to be no more than 30,000 members.

6. We estimated that **16%** of leader accounts were “corporate” while **69%** were personal operatives account[26].

7. 95% of accounts used the Arabic language with a minority using other regional languages such as Urdu, Farsi, and Pashto. Though, this trend is very likely due to our method of data collection which uses Arabic language accounts as seed accounts to collect the larger network.



[25] We define community targeting as the targeting of clusters of communities using a clustering/community identification algorithm.

[26] We defined corporate accounts as accounts that were simply retweeting other users’ messages without engaging individual accounts personally or creating new content.

Figure 5. This network graph represents the leader accounts of our previously collected network and their relationships. We used a clustering algorithm to determine common connections between them while removing the connections they possessed to the rest of the network. Note the color of each account—this is not an arbitrary color but represents a community of tightly knit accounts. Our mathematical algorithm reproduces to a large extent our categorical and qualitative analysis of these accounts discussed in Mode III of this report.
Not all leader accounts connect to each other. Note accounts colors in light blue in the bottom left and mid-to-top left. We classify these accounts as isolates (isolated accounts) because they do not connect with any of the main clusters of the leader network.

MODE V
ACCOUNT BEHAVIOR

To tie in network structure to individual user's behaviors, we also conducted a brief investigation of users' micro-behaviors.

We found important patterns that contribute to our understanding of the level of sophistication and planning that DAESH operations undergo, as well as the adaptive nature of their organization even when no previous planning existed.

We categorized those behaviors into distinct themes. We summarize them as follows:

- Continuous building of adaptive cognitive networks
- Signaling to avoid discovery
- Speedy and adaptive closure
- Identifying system vulnerabilities

Continuous Building of Adaptive Cognitive Networks

An adaptive cognitive network is a network that does not rely on the physical formation and building of relations, but one that relies on the natural formation of networks built on memory (cognition). In other words, if one remember the name of a friend then they have a cognitive relation with that friend regardless of actual contact.

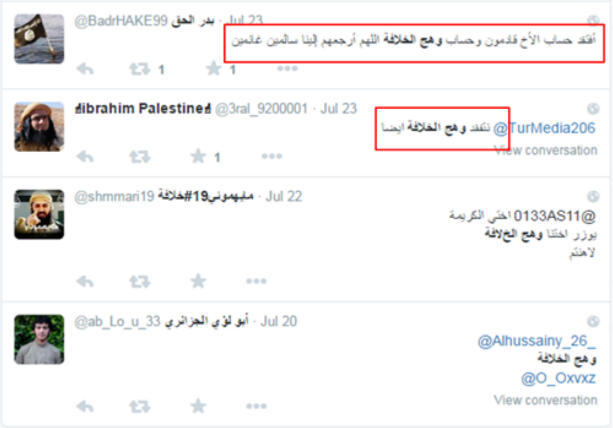
In many ways this is a rather efficient way of building a social network on media platforms because as information networks are disrupted (through suspension and deletion of accounts), if the cognitive networks remain, assailants can rebuild the network without reliance on technology.

The *adaptive* designation we attach to these networks cis derived from a feature that allows them to adapt to outside actions (stimuli) and thus become very responsive.

We saw numerous examples and anecdotal evidence of this process taking place.

In one example, an DAESH operative tweeted that he misses a user by the name of "Wahg Al- Khelafa" or as it is translated *"Blaze of the Caliphate"* who he had not seen on Twitter for some time. He was responded to almost immediately by another who noted that he *"misses him as well"*.

In essence, this small exchange describes a feature such that for this small group of accounts, the network's reliance on the physical/electronic existence of accounts for at least a small number of fellow operatives may not be necessary—as accounts are suspended and deleted, operatives can simply recreate the network by relying on their own memory of whom they've built non-physical relations with.



@BadrHAKE99 بدر الحق · Jul 23
أفتقد حساب الأخ قدمون وحساب وهج الخلافة اللهم أرجعهم إلينا سالمين غانمين

ibrahim Palestine @3ral_9200001 · Jul 23
@TurMedia206 نفتقد وهج الخلافة ايضا
View conversation

@shmmari19 مليهوني19#خلافة · Jul 22
@0133AS11 اختي الكريمة
يوزر اختنا وهج الخلافة
لاهتم

@ab_Lo_u_33 أبو لؤي الجزائري · Jul 20
@Alhussainy_26_
وهج الخلافة
@O_Oxvxz
View conversation

I miss the account of "Wahg Elkhelafa". I pray God returns him safely to us

I miss him too

Figure 6: In this example we see the interactions that produce a cognitive network that does not rely on physical/electronic information networks to facilitate information exchange and propaganda.

This process is important because it facilitates the creation of information exchange even in an environment where messages are difficult to disseminate thereby ensuring that the form of the information network still continues as cognitive networks in the minds of DAESH operatives.

Signaling to Avoid Discovery

As allied efforts increase in scope and magnitude to combat DAESH propaganda while more evasive techniques are adopted to avoid detection, signaling techniques are becoming more common in use by the group.

Signaling can perform many functions. It can aid in avoiding automated detection methods which are in common use by a number of agencies throughout the world, and it can ensure relative anonymity of the user for intelligence gathering operations, while concealing accounts that are not yet ready for active use.

We found numerous methods and ways in which DAESH operatives used signaling to achieve their objectives. We give only a few examples here to illustrate the behavior.

We found a number of accounts using standard-issued DAESH propaganda photos on the profile of their accounts. These images are easily identifiable through automated methods (image search) and thus make for easy detection and thus faster identification of DAESH accounts. However, if these images are slightly modified, such as cropping, reduction in image quality or change in aspect ratio, then most if not all known image detection algorithms fail to recognize them.

Thus, strict reliance on automated algorithms can be counter-productive and through minor changes to images, automated image detection is rendered unsustainable. Human detectors (manually) can still easily identify images that clearly signal that a specific account is an DAESH owned account. Therefore, the transaction cost[27] of identifying accounts is thereby increased and counter-strategy options become more limited.

In other cases, we discovered a number of accounts that had subtle signals to identify them as DAESH accounts by deduction and inference but through no clear signals even to human investigators.

On one account, the location field of the Twitter profile was called "8th account after suspension" and the profile image was simply telling of a Baghdad news agency. The profile had no explicit signals that it belonged to an DAESH media center, but through deduction one can understand that if the previous 7 accounts had been suspended, that this particular account had reasons to be suspended so repeatedly. That, in combination with the content of the tweets that this account was sharing would allow us to deduce that it was an DAESH account. Many human investigators may overlook this fact, especially if they are under time constraints to discover as many accounts as possible. Inference takes time and study—DAESH uses this immutable fact to evade detection.

Speedy and Adaptive Closure

The speed at which the network can be rebuilt after accounts have been suspended or deleted is also important and significant in DAESH's overall strategy.

If speedy connections are readily made after suspension then recovery of the network's structure is more easily achieved and operations can continue in large part without interruptions. We discovered numerous examples of DAESH accounts receiving hundreds of retweets for their main, secondary and even tertiary accounts with information on who they are and usually with a request to follow their new accounts; Thereby giving direct access to their content quickly and attempting to reach previous levels of influence.

In one example, an DAESH account asked for ***1000*** retweets of his new account's username so that fellow operatives would be able to reconnect to him. He received almost ***300*** retweets in less than 24 hours. To put this into perspective, the large majority of Twitter users never receive ***300*** retweets of all their content combined while on Twitter since its inception[28]. Thus, we can

[27] We use transaction cost here as a term to describe the cost in time and resources

assume that speedy closure (reconnecting) is a formal feature of DAESH adaptive strategy. This assumption can be tested in future research under more stringent conditions.

Identifying System Vulnerabilities

As the DAESH network adapts and evolves to external conditions simple yet innovative methods of using system vulnerabilities are adopted.

The most salient instance of this trend is a number of accounts we found that have identified a basic function of Twitter's assignment of account URLs: An account URL is the hyperlink address that one enters into an internet browser in order to reach the intended account's profile page[29]. Account URLs on Twitter are based on an account's user name. If the user name of an account is "DAESH", then the URL for that account would be www.twitter.com/DAESH.

In Twitter (specifically,) if the user changes their account handle/user name then they automatically change the URL that their profile is located at. Twitter allows users to change their account user names within seconds of them deciding to do so and provides no restrictions or monitoring for account-level user name changes.

We found a small number of instances where very active and visible DAESH accounts were using this method to periodically change their usernames and thus their URLs. We consider this a very important trend and are concerned about its potential use in expanding DAESH propaganda reach.

In using automated detection and software algorithms to form the majority of detection efforts of DAESH accounts, it is possible that it would seem as if these accounts were suspended or deleted, but in fact the user simply moved the URL to another location.

We hypothesize that the majority of software used by various intelligence and governmental agencies for detection relies heavily on URLs and user names to systematically identify DAESH propaganda accounts. This means that this method avoids those detection methods altogether.

It is important for the reader to note that we are not suggesting that these accounts and their messages are not being ***collected*** by some intelligence gathering effort—we are suggesting that they are likely not being ***identified*** because of their mobility.

In one case we found an account/user that changed his user name five times during the period of our data collection. When we initially found it the account had ***8,200*** followers and it was eventually suspended at around ***15,500*** followers.

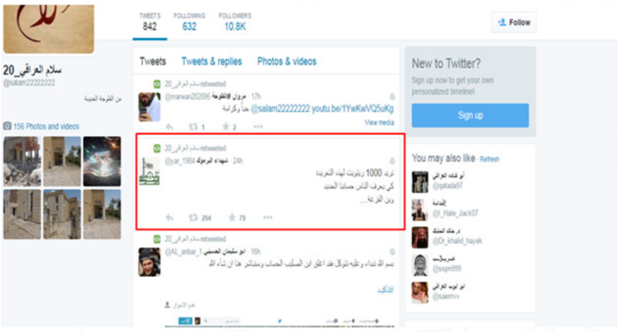
During this time thousands of messages were sent out to tens of thousands of potential recruits on social media. Later (post suspension) we found the same user with two additional accounts in their infancy (***1600*** followers) and we assume that they will repeat the process.

Only a very small sample had identified this vulnerability, perhaps on the order of 1%-5%, but as DAESH continues to find new ways of sharing previously learned lessons as their network continues to become more adaptive there is a reasonable probability that this, and other methods, could be perfected and shared openly amongst the different social media centers.

And, though the outcomes for each account will ultimately be suspension or deletion once accounts become highly active and visible, our discussion should not revolve around the topic of completely shutting DAESH's access to propaganda dissemination mediums, but on reducing the rate, sustainably, in which they do so.

[28] The author of this report has never received that level of retweets since 2008 when he joined Twitter.

[29] For example, the URL for the author's Twitter account is www.Twitter.com/josephshaheen



سلام العراقي_20
@salam22222222
من القوصة الحبيبة
156 Photos and videos
TWEETS 842 FOLLOWING 632 FOLLOWERS 10.8K

سلام العراقي_20 retweeted
مروان الاقلوجة @marwan202095 · 17h
حباً وكرامة @salam22222222 youtu.be/1YwKwVQ5uKg

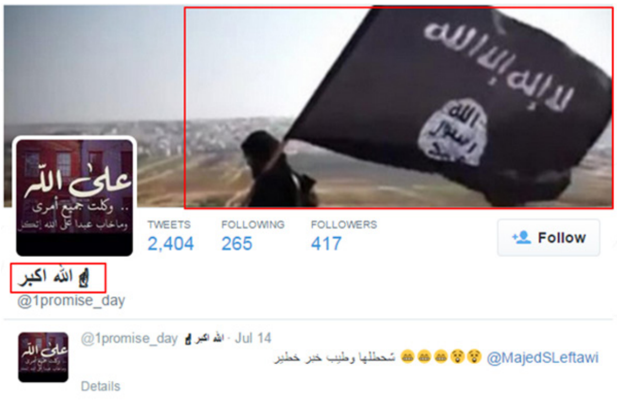
سلام العراقي_20 retweeted
شهداء الرموك @yar_1984 · 24h
نريد 1000 ريتويت لهذه التغريدة
كي يعرف الناس حسابنا الجديد
وين الفزعة ....
294 79

سلام العراقي_20 retweeted
ابو سليمان الحسيني @AL_anbar_1 · 16h

You may also like
@qatada97
@I_Hate_Jack07
@Dr_khalid_hayek
@sspn999
@saemvv

"we (royal) want 1000 retweets of this message so that people will know my new account"

Figure 7: This is an example of speedy closure. In this tweet an DAESH operative asks if he could have his new account URL re-shared across the network so that he could regain his followers. He receives more than 290 retweets in less than 24 hours—a remarkable gain by any measure.



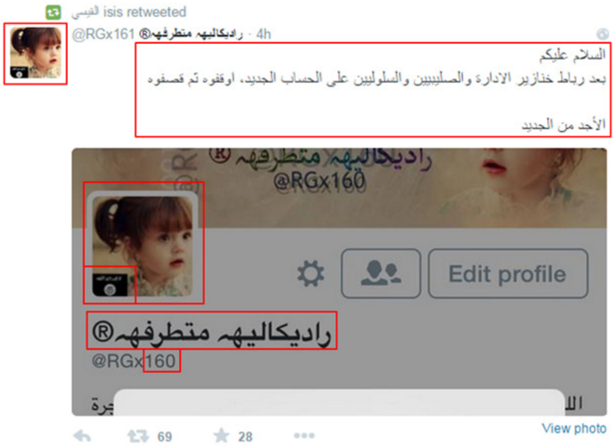
الله اكبر 👆
@1promise_day
TWEETS 2,404 FOLLOWING 265 FOLLOWERS 417

@1promise_day 👆 الله اكبر · Jul 14
@MajedSLeftawi 😲😲😩😩😩 تحطلها وطيب خبر خطير

Figure 8: In this image we find an example of signaling through modified images. The background/profile image shows a standard image used by DAESH propagandists in a number of releases and videos. Through simple modification and cropping this image becomes less detectable through automated algorithms.

Additionally, we find the use of a special characters that are used in the user name field to differentiate this user from other users who may share the same name.

In this case, the name of the account is a simple "God is great". A simple Twitter search reveals hundreds or thousands of account whose user name is God is great, but when combined with the special character (the hand with a finger pointing upwards) one can relocate a specific account/user since that special character is rarely used.



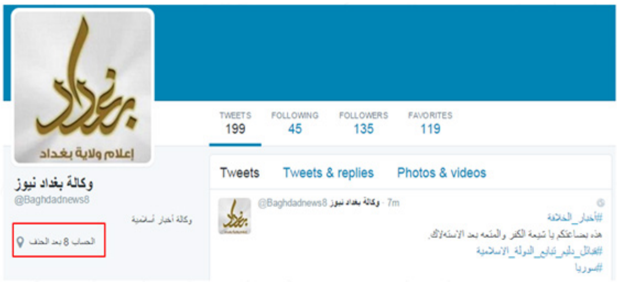
القيسي isis retweeted
@RGx161 راديكاليهه متطرفهه® · 4h
السلام عليكم
بعد رباط خنازير الادارة والصليبيين والسلوليين على الحساب الجديد، اوقفوه ثم قصفوه
الأجد من الجديد

راديكاليهه متطرفهه®
@RGx160
69 28

"After those [expletive] of administrators (twitter) ...suspended then deleted the new account, here's the new new account..."

Figure 9: This is an example of a combination of signaling and speedy closure. The account belongs to a female operative, but her use of a stock photograph of a young female with an DAESH flag in the corner accomplishes detection avoidance (through confusing image detection algorithms) while making clear to human visitors that this account supports DAESH. We also found that this user attaches a number at the end of her user name (160 in this case).

When we investigated further we found that she had created many accounts, each of which had a different 3 digit number attached to her user name. This supports our hypothesis of account inflation as a counter-strategy against suspension or deletion.

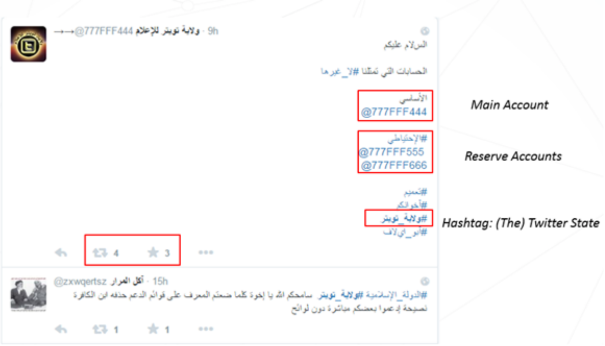


وكالة بغداد نيوز
@Baghdadnews8
وكالة أخبار اسلامية
الحساب 8 بعد الحذف
TWEETS 199 FOLLOWING 45 FOLLOWERS 135 FAVORITES 119

@Baghdadnews8 وكالة بغداد نيوز · 7m
#أخبار_الخلافة
هذه بضاعتكم يا شيعة الكفر والمتعه بعد الانسحاب.
#قتال_دليم_تابع_الدولة_الاسلامية
#سوريا

Translation: "Account number 8 after previous suspensions"

Figure 10. An example of an account that uses subtle signaling. Only the location field is evocative of an DAESH connection, because it lists that this account had had previously been suspended 7 times.



→→@777FFF444 ولاية تويتر للإعلام · 9h

السلام عليكم

الحسابات التي تمثلنا #لا_غيرها

الأساسي
@777FFF444

#الإحتياطي
@777FFF555
@777FFF666

#تعميم
#أخوانكم
#ولاية_تويتر
#أبو_اي‌لاف

4 3

@zxwqertsz أكل المرار · 15h

#الدولة_الإسلامية #ولاية_تويتر سامحكم الله يا إخوة كلما ضعتم المعرف على قوائم الدعم حذفه ابن الكافرة
نصيحة إدعموا بعضكم مباشرة دون لوائح

1 1

Figure 11. This is an example of a user sharing his main and his reserve accounts as a suspension avoidance strategy

CONCLUSIONS

have important policy implications to the overall strategy of combating DAESH propaganda. Therefore, in order to enhance the focus on the policy implications of our technical conclusions, we focus on those implications in this section.

Our recommendations are intended towards reducing the number of western recruits joining their ranks, and the development of sustainable information warfare capabilities to strengthen readiness for the next threat to peace and stability.

Social media and the internet have already become a strategic imperative in any geopolitical conflict today, and in this century battles fought will include the internet and information utilization as an important consideration for active theaters of war.

DAESH represents the first-to-perfect of what we predict will be many state and non-state actors who will use these methods in combination with traditional and asymmetric methods of warfare.

This report does not contain what is traditionally categorized as classified information, though our ability to paint such a detailed picture of the information battle between resourceful state and non-state actors should, on its own merit, represent a shift in how future battles will be fought. These battles will involve many rivals with potentially competing interests and methods of warfare—rivals that when combined under a common platform create a complex web of activities too difficult to discern through traditional analytical methods, and cannot be countered through simple policy-making.

If nothing else, we ask the readers of this report to consider the substantial policy implications of that complex dynamic ***in vacuo.***

To reach our conclusions we observed the battle as it ensued and inferred some behaviors both from DAESH propagandists as well as from state actors. Our inferences, though not always supported by declared statements gained directly and openly from those sources are reasonable.

Our primary conclusion answers our primary question: *How does DAESH use social media to create such an effective media and information propagation machine*. Since DAESH uses Twitter as its connecting medium for all of its diverse content posted all over the web, our question became *how does DAESH disseminate information on Twitter*?

This led us to development of our understanding of the process used by DAESH to broadcast information –all of which is supported and induced from our analysis contained in this report. I call it the **DEER Process**.

The DEER Process

The DEER Process is the method by which DAESH and potentially other organizations use social media to propagate their message in a hostile environment and with applied counter-strategies. It involves:

1. **D**issemination of public propaganda
2. **D**eletion or suspension by adversary
3. **E**volution of (network) structure or methods
4. **E**xpansion of influence or methods
5. **R**eplenishment of accounts and resources.

DEER represents the process by which DAESH has built an infrastructure that can sustain damage on social media.

It begins with the same techniques used by any active social media group—that is—the continuous sharing of agreeable information and propaganda. Over time and as they are engaged, adaptation ensues. As accounts are deleted or suspended in step two of the process, DAESH, through their individual level behaviors, evolve the network structure, much of the time creating a sparser network in terms of number of accounts but a more tightly knit network in terms of density of relationships. This also includes moving accounts from an inactive state to an active state and allowing previously unimportant accounts to become much more central to propaganda dissemination.

The Evolution phase of the process also includes using more sophisticated signaling and closure techniques to avoid detection, and the methods that we have seen evolve include both the techniques used in sharing propaganda and the methods of evasion themselves.

Expansion is a natural probable outcome of evolution. As an enemy gains time and space between adopting a new, evolved process and their adversaries' ability to detect the features of that evolution, they can expand. Since 2013, we believe that on Twitter and other social media platforms, tens if not hundreds of thousands of DAESH accounts have been suspended or deleted. How then have they been able to maintain roughly the same level of activity as they did when there was no battle infrastructure in place to combat them? We believe the answer to that question is *expansion post-evolution*.

The final stage of the DEER Process is replenishment. As DAESH creates new accounts, uses them for propaganda sharing, loses them to suspension or deletion, evolves new network structures and methods of evasion and dissemination, and then expands operations and number of active sources of information, they simply replenish accounts and content sources that were previously suspended or deleted by their adversaries.

By using the DEER Process DAESH has developed a process by which they sustain their presence online in the face of multiple entities attempting to prevent them from doing so, and in turn are able to continually recruit foreign fighters and sustain the battle on the ground.

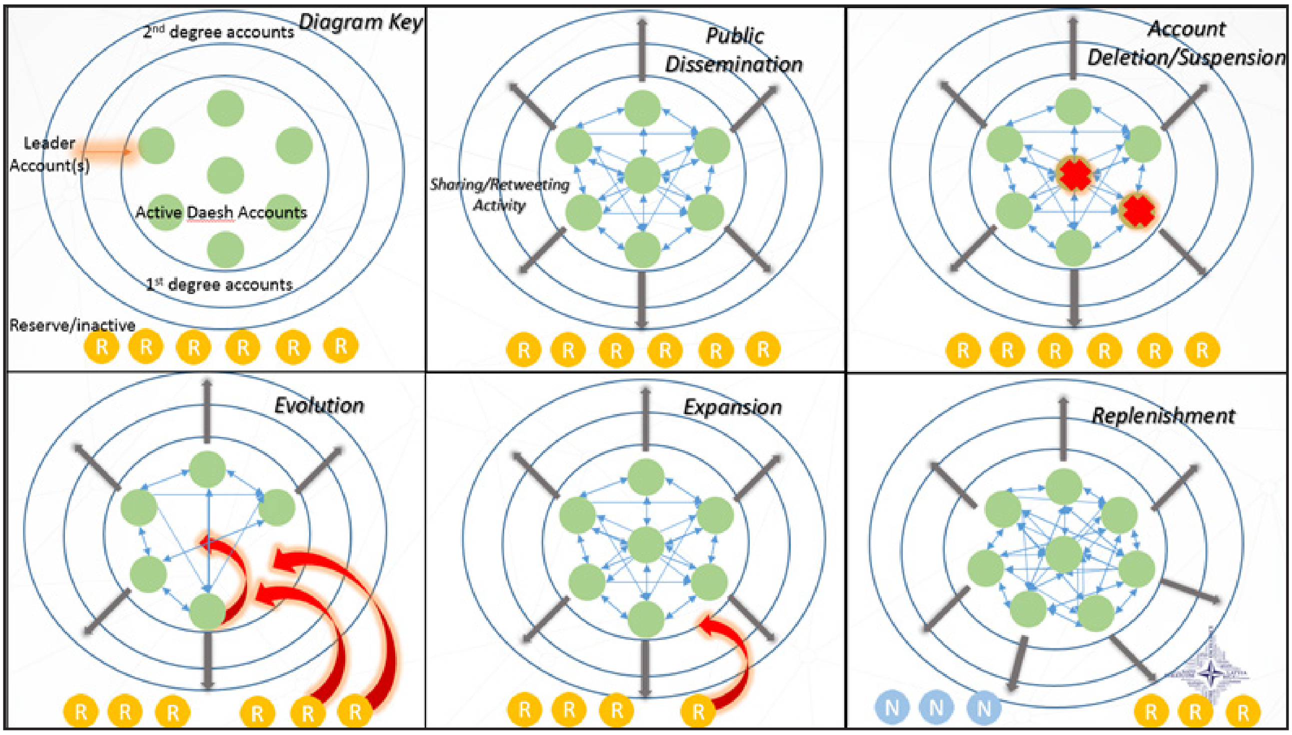


Figure 12. The DEER Process represents the collective core findings of our research into DAESH information and propaganda networks. It is a model intended to simplify our understanding of the process of propaganda battles from an information warfare perspective. The method describes the process by which DAESH has been able to sustainably frustrate strategies aimed at limiting their reach into western countries and to enhance their recruitment operations worldwide.
The explanatory process ties most of our findings together including the DAESH network constantly adapting to ongoing changes, including suspension and deletion of accounts and content online. The process begins with dissemination, thwarted by deletion, moved through evolution, and finally expansion and replenishment. Any fundamental strategy adopted to limit DAESH influence on social media must take this process into account.

Recommendations

The method itself is not impregnable and has many weaknesses—the most salient of which is time and resources.

DAESH must commit a dedicated workforce to sustaining their efforts and to continually create new accounts, reconnect them back into the network and bring them to a functioning capacity. This is a time consuming process. It is my belief that this is precisely where counter-strategies should focus: increasing the incremental transaction cost of every activity that terrorists must undertake in order to spread their message.

Suspending and deleting accounts as well as content throughout the web is a great start for this process, but it is in the details of the method used to do so that innovations must be adopted by any entity which is genuine about preventing DAESH's ideology from spreading.

Primarily, our recommendation hinges on adopting a cluster/community focus in contrast with the current focus of only targeting active accounts.

Simply put, the difference between the two methods is the same as the difference between nullifying your enemy's equipment or their infrastructure. The former allows for short term gains while the later provides for long term strategy and planning with objectives kept in focus.

A community-focused approach is the process of identifying clusters of accounts whether they are active or inactive and targeting them—not just relying on identifying accounts that are currently active in propaganda broadcasting.[30]

This is based specifically on the finding that DAESH creates new accounts then reconnects them to the existing network.

Using this method, combined with a form of online blitzkrieg, NATO and other entities can begin to remove entire clusters of account—many of whom likely belong to the same groups of users (if we assume high level of account inflation), forcing them to continually rebuild their infrastructure from the ground up and forcing them to spend a much longer period of time doing so rather than on spreading their message.

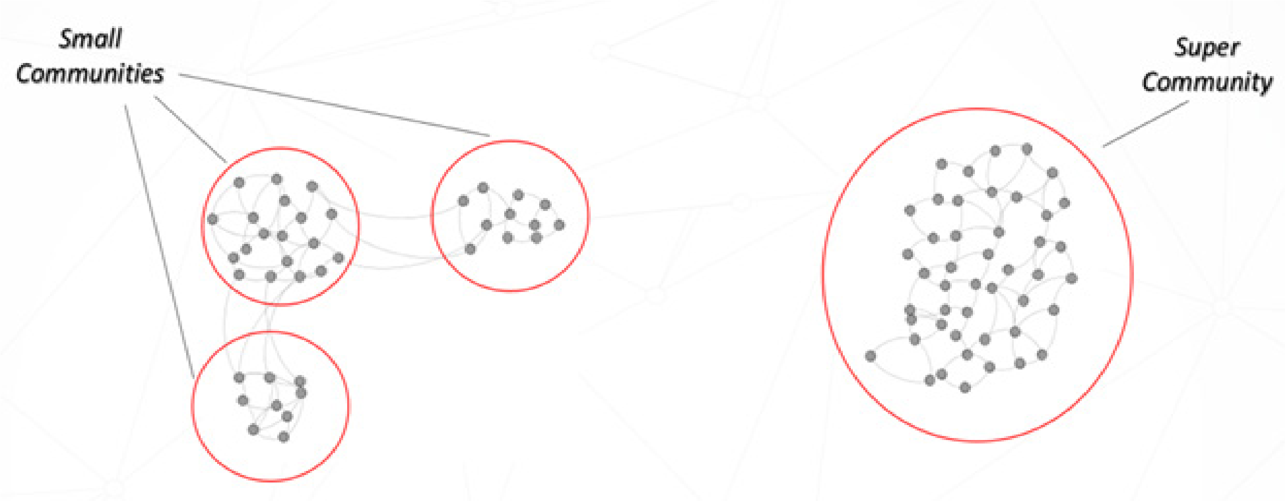


Figure 13-A: As an example, we show the difference in strategy between eliminating super communities and small communities using a community approach. Consider the two fictional networks provided above. If we assume that authorities have limited time and resources then we can assume that for these networks authorities can only suspend the same number of accounts for either network.
On the left we will take a community approach (since we've identified the clusters) and on the right we will target them at random.

[30] This could have legal implications if challenged in a US court.

Additionally, more emphasis must be provided for integrating different approaches from all the different state and non-state actors involved in the information theater of war. At the moment we see numerous parties involved with no real coordination between them, often times having to sidestep each other and in some cases misidentifying each other on social media.

The methods we recommend inherently provide for division of labor and responsibilities as well as the combining of the various agency's efforts into a single entity. This becomes paramount in order to sustainably eliminate DAESH presence from social media and eventually the web entirely.

We believe counter strategies focusing on content are inefficient because opinions do not always work in zero-sum fashion and because the source of the content must have superior credibility in order for their content to be digested and agreed upon. In other words, providing counter messages to DAESH propaganda from sources such as the US Department of State or other entities known to be in opposition to DAESH will be less effective because 1- They come from a source who has publicly declared (USG) that they oppose DAESH and are actively battling them on the ground and 2- Counter messages opposing DAESH do not, cognitively speaking, cancel messages put forth by DAESH. They are simply taken into consideration with the full gamut of messages each individual receives on a daily basis from all sources of media. [31]

The focus of allied effort must be the structure of the network, and it must be done with a community-focused method in line with DEER as a theory of information warfare.

Finally, one of the most important considerations one must make is that this battle is can no longer be fought on the outdated modes of traditional IO and PSYOP[32] doctrines but must fall and be integrated under newly developed paradigms, some of which are likely to be under development by various agencies, but clearly not at full maturity as of the time of this writing.

Future Research

Our analysis is best conducted on a continuing basis with well-developed data and cyber infrastructure.

As the information battle continues and the environment, tactics, and strategies change, almost on a daily basis, policy makers and military personnel cannot rely on snapshots in time to get a sense of current dynamics.

There are many reasons for this, but the most important one is that with complex systems, change is an ongoing and unstoppable paradigm, and by the time analysis is conducted, written, and shared, the situation on the web may have already changed in unexpected ways.

Future research then should be dynamic, ongoing, and adaptive—reflecting the systems and processes under question.

Ideas for future research (executed in an adaptive fashion) should include a deeper level analysis of clustering and community dynamics.

Social media outlets such as Twitter provide for increased limitations on access of their data, and so methods to help understand the bridge between sample data sets and full populations should be considered.

We would also propose a number of research projects to help understand the relationship between propaganda dissemination and language used. We hypothesize that there exists some seldom understood relationship between methods of broadcasting to a native speaking population (in this case, the language is Arabic) and network formation in comparison to media campaigns that are conducted by DAESH in other languages.

This research would also provide for additional tools to combat propaganda spreading in nations outside of the active theaters of war.

Finally, we propose research that focuses on building capabilities to face the next wave of information battles and to understand the minimum required competences to face those future threats.

[31] In wave and light physics, if wave A had the exact same but opposite features as wave B and they both interact, they cancel each other out. In real world psychology that is seldom the case.

[32] IO: Information Operation, PSYOP: Psychological Operations.