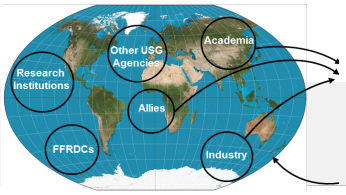

SMA Reach-back

Question Follow-up (QL 3*): The response to QL5 (see Appendix A) noted that ISIL is moving to ZeroNet platform for peer-to-peer messaging, which is extremely robust to distributed denial-of-service (DDOS) attack/other counter measures. What effect could this have on Intel efforts?*

Implications of Da'esh Move to ZeroNet Platform

Spencer Robinson, Eric Perez, Douglas C. Derrick, & Gina Scott Ligon
University of Nebraska Omaha

Through our research into Da'esh cyber messaging (Derrick et al., in press), we have identified an emerging trend in Da'esh forum, propaganda, and fundraising websites: the use of the ZeroNet application. ZeroNet, a peer-to-peer application, uses the same technology as Bitcoin or other cryptocurrencies using shapeshift.io. As Da'esh users begin publishing their websites off servers using this ZeroNet application, visitors are then only able to visit that website (e.g., blogs, chat forums) using that ZeroNet application. This facilitates/mandates that visitors then seed that content to other viewers, as the website is distributed to and from many locations and from multiple small servers. When the website is updated, the update is pushed out to all seeders. Each website visited is also served/seeded by the visitors, thus creating a distributed publishing system that permeates more than just one physical site owner.

Implications. The use of this application is another instance of Da'esh as an early adopter of IT Innovation (Ligon, Derrick, Logan, Fuller, Church, Perez, & Robinson, 2016). ZeroNet is built for hosting all types of dynamic websites, and any type of file can be distributed on it (e.g., VCS repositories, databases, etc). Creating ZeroNet websites is facile and instructions can be located on a variety of open source websites[1] and easily installed. Implications we have identified are 1) DDOS is no longer an option for technical interdiction unless all seed accounts can be hit at one time, 2) taking down a website that violates user terms (e.g., suspicious content, hate speech) is no longer an option, 3) social engineering will play a larger role to gain access to protected sites, and 4) cyber interdiction may need to focus on heavier preventative measures rather than post hoc take-downs/removal. However, one positive implication is that Blue could also use the seeding to find supporters of Da'esh in the following ways. First, by seeding real or other content, analysts can become part of the network that hosts these websites. This can allow them to monitor who seeds the content to identify other potential supporters. However, this technique is limited if the other seeders use an anonymizer, such as an anonymous VPN or tor. The ability to find other seeders will often (not always) be limited to the organizations ability to analyze the tor network. Finally, as with other Da'esh endorsed applications (e.g., Dawn of Glad Tidings), monitoring who downloads the ZeroNet application in months following its

[1] Websites such as https://zeronet.readthedocs.io/en/latest/faq/ walk users through the pros and cons of ZeroNet and are available in at least 22 languages.

endorsement on Da'esh communication channels (circa October 2016 and weeks following), one could track IP addresses for those who do not use TOR to mask their identity (this instruction was not included on the initial post about downloading ZeroNet). Second, because the content is secured in same manner as bitcoin wallet, bitcoin hacking and identification techniques would also be effective on this application. Finally, an innovative way to take down content is to infiltrate creator accounts and make updates with blank content to disrupt files of seed accounts.

Conclusions. Our assessment indicates that site destruction of user content employing ZeroNet will be more difficult due to its crowdsourced, distributed platform. However, collection of data may in fact be easier. Moreover, using the techniques we recommended and others developed to harvest data from bitcoin users, it may in fact be easier to identify other seeders and downloaders than it has been from 2014-present.

Appendix A

Question (QL5): *What are the predominant and secondary means by which both large (macro – globally outside of the CJOA, such as European, North African, and Arabian Peninsula) and more targeted (micro – such as DAESH-held Iraq) audiences receive propaganda?*

SME Input

Da'esh Cyber Domains from August 2015 – August 2016

Gina Scott Ligon, Ph.D., Doug Derrick, Ph.D., Sam Church, and Michael Logan, M.A.
University of Nebraska Omaha

Related Publication: Ideological Rationality: The Cyber Profile of Daesh (available on request and in press at *Dynamics of Asymmetric Conflict Journal*)

Daesh is the most prolific violent extremist group on social media, but their cyber footprint is much more complex than researchers of solely mainstream services such as Twitter imply. Their cyber profile involves pushing content into open infrastructures to disseminate information, such as ideological messages, propaganda, and training instructions. To date, much of the research on Daesh communication has focused on what is publicly available through speeches and videos released by al Hayat Media and Daesh Twitter users (Ingram, 2014; Veilleuz-Lepage, 2014; Zelin, 2015). A notable exception is the important monograph from Saltman and Winter (2014), where the authors identified complex cyber capabilities such as 1) centralized propaganda, 2) global dissemination of threats, 3) custom app development, and 4) decentralized messaging. Given the acknowledgement of Daesh's prolific use of a variety of Internet Communication Technology (ICT), it follows that each aspect they use plays a role in sharing the story Daesh wishes to convey.

An organization's online presence plays a significant role in communicating with a global audience (Ligon, Derrick, & Harms, 2015). In regards to Daesh and its messaging campaigns, popular platforms of more conventional ICT—like Twitter or Facebook—are mere starting points for its multi-faceted, complex cyber profile. Thus, the purpose of this effort is to better understand the nature of the cyber channels and domains most used in the messaging of Daesh, particularly as it manifests through social media connected transient web pages to an English-speaking audience. The organization's end goal vis-à-vis their online marketing campaign is complex and is used to "attract potential recruits, raise money, promote the image of the organization, or just spread fear among its enemies" (Barrett, 2014: 53). While there is some evidence that a centralized authority approves messaging prior to it being disseminated via more conventional channels (e.g., Dabiq, Al-Hayat Media), the cyber footprint of Daesh is more complex. This overall strategic effort is reportedly overseen by a skilled media council (Lister, 2014). However, the deployment and dissemination of Daesh messages is arguably decentralized once content is generated, resulting in a robust cyber presence.

While the Daesh strategic and tactical cyber profiles are unquestionably unprecedented (Zelin, 2015), questions remain as to what we can glean about the organization from its

messaging. The dataset used for assessing Daesh's online presence was unique to this project and comprised of 4.5 million tweets and 16,000 attached transient webpage articles posted by Daesh followers, members, and sympathizers. The research methodology and subsequent data analysis provides insight into the messaging dynamics of Daesh. We conclude the study with a discussion of limitations of our method, implications of our findings, and recommendations for future research.

Method

We collected this data by developing a custom program that follows the method outlined in figure 1 (Derrick et al., 2016). First, our program utilized the Twitter API to follow and log tweets posted by the hacktivist group Anonymous. For the present effort we did not evaluate the "Tweets," but used them as launching points to the open architectures where richer content is housed. During much of this collection, Anonymous posted Daesh members' Twitter handles approximately one every two minutes since August 2014. As stated previously, the goal is to understand the strategic messaging from the deployment of messages by large grassroots followers. Thus, our program compressed a list of Daesh-affiliated accounts identified in the posted content. From that list, our system utilized the Twitter API to download a sample of the latest tweets from each Daesh-affiliated account.

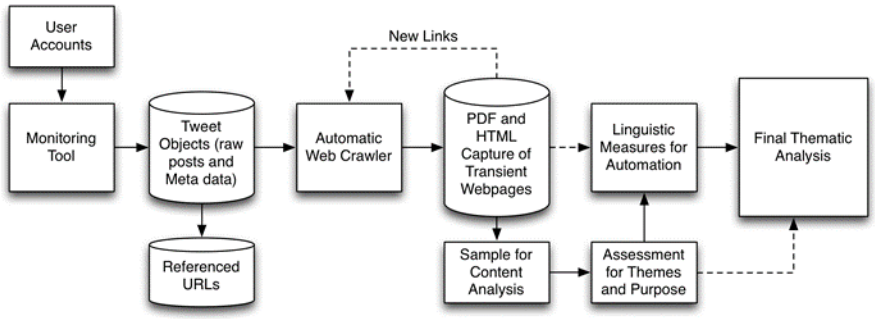

Figure 1. Method for Capturing Transient Webpages

After logged into our database, the tweets were sorted into various components (e.g., web addresses and links, hashtags, mentions) to be analyzed. Our software searched for links within tweets referencing anonymous posting services for open content-publishing transient webpages (e.g., JustPaste.it, dump.to). Next, our software automatically crawled to the referenced webpage and captured both PDF and HTML versions of the actual transient webpages and stored them our database. From these pages, the program identified any links to other transient webpages/open architectures in the online posting. In a recursive manner, the software continued to download and analyze the content until all possible transient links had been found and captured. To date, this process has produced over 4,500,000 tweets, 1,589,623 URLs, and 16,000 transient web pages, and we have labeled this effort the *Social Media for Influence and Radicalization (SMIR) Dataset* (Church, 2016).

Results

For the present QL5, we rank ordered the top domains used by Daesh between the dates of August 2015 to September 2016 in our SMIR dataset. A more detailed analysis of monthly usage could be conducted upon request. Results indicated that Twitter, identified as the "jumping off point" for much of the persuasive content we find on non-indexed, transient webpages, is the most oft used. However, a variety of other types of domains are also used by Daesh to disseminate messaging, as indicated in Tables 1 and 2.

Table 1. Rank Order Daesh Communication Channels 2015-2016

Rank	Domain	*f*	*%*
1	twitter.com	368,652	23.19%
3	youtube.com	213,092	13.41%
2	justpaste.it	105,802	6.66%
4	du3a.org	67,380	4.24%
5	archive.org	67,298	4.23%
6	zad-muslim.com	36,519	2.30%
7	sendvid.com	22,776	1.43%
8	drive.google.com	19,143	1.20%
11	up.top4top.net	18,965	1.19%
9	dump.to	13,394	0.84%
10	web.archive.org	12,904	0.81%
21	wp.me	14,280	0.90%
12	ghared.com	11,496	0.72%
13	qurani.tv	10,811	0.68%
14	quran.to	10,638	0.67%
15	telegram.me	8,726	0.55%
16	7asnat.com	8,624	0.54%
17	dailymotion.com	7,970	0.50%
18	almlf.com	7,958	0.50%
19	d3waapp.org	7,774	0.49%
20	wthker.com	7,067	0.44%
22	my.mail.ru	6,850	0.43%
23	quran.ksu.edu.sa	6,774	0.43%
24	pho2up.net	6,000	0.38%
25	mezani.net	5,712	0.36%
		1,066,605	67.10%

Number of total URLs in SMIR: 1,589,623

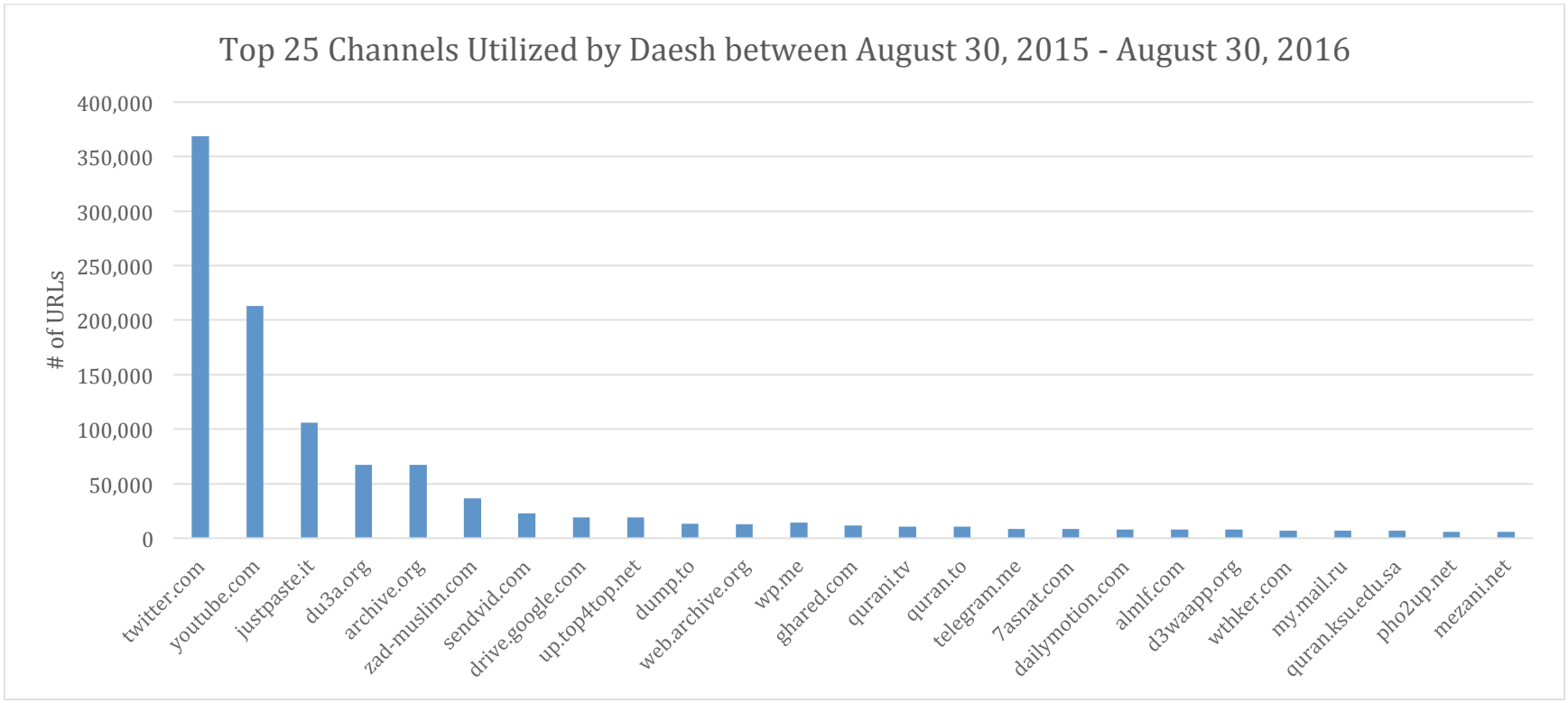

Table 2. Graph of Daesh Domains 2015-2016

Author Biographies

Dr. Gina Ligon is an Associate Professor of Management and Collaboration Science at the University of Nebraska at Omaha. She received her PhD in Industrial and Organizational Psychology with a Minor in Measurement and Statistics from the University of Oklahoma. She is a member of the National Consortium of Studies of Terrorism and Responses to Terrorism (START). Since arriving at UNO, she has been awarded over $2,000,000 in security-related grants and contracts. She currently is the Principal Investigator on a grant from Department of Homeland Security (DHS) examining the leadership and performance of transnational Violent Extremist Organizations (VEOs,) and is the originator of the *Leadership of the Extreme and Dangerous for Innovative Results* (LEADIR) database. Her research interests include violent ideological groups, expertise and leadership development, and collaboration management. Dr. Ligon has worked with DoD agencies on markers of violent ideological groups, leadership assessment, organizational innovation, and succession planning for scientific positions. Prior to joining UNO, she was a faculty member at Villanova University in the Department of Psychology. She also worked in St. Louis as a management consultant with the firm Psychological Associates. She has published over 50 peer-reviewed publications in the areas of leadership, innovation, and violent groups.

Dr. Douglas C. Derrick

Douglas C. Derrick is an Associate Professor of IT Innovation, Director of the Applied Innovations Lab, and Co-Director of the Center for Collaboration Science at the University of Nebraska at Omaha. Doug received his PhD in Management Information Systems from the University of Arizona. He holds a Masters degree in Computer Science from Texas A&M University and a Masters degree in Business of Administration from San Jose State University. He is a Distinguished Graduate of the United States Air Force Academy. His research interests include human-agent interactions, intelligent agents, collaboration technologies, decision support systems, persuasive technology and computer-mediated influence. Prior to joining UNO, Dr. Derrick worked as a Program Manager at MacAulay-Brown, Inc. and also served as an Air Force officer. He has extensive experience working with the Department of Defense. As a contractor and academic, he has been awarded contracts and grants totaling $41.14 Million over the last 12 years (principle investigator awards total $17.47 Million). Doug has published over 40 peer-reviewed journal articles and conference proceedings.

Eric Perez

Eric Perez is an undergraduate student in Computer Science and a research associate in the Center of Collaboration Science at the University of Nebraska, Omaha. His primary research interests include internet based data mining and collaborative computer systems.

Spencer Robinson

Spencer Robinson is an undergraduate student in IT Innovations with a focus in Computer Science and Entrepreneurship and a research associate in the Center of Collaboration Science at the University of Nebraska, Omaha. His primary research interests include web development and holographic technology innovation.