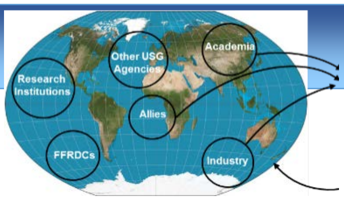

SMA Reach-back

6 January 2017

Question R2 (QL4): *The wide-spread, public access to smartphones has been a game-changer for the distribution and production of propaganda. Is there more data available about the types of apps (e.g., WhatsApp, Facebook, Telegram, Viber) used on smartphones to distribute propaganda, and the methods through which this is accomplished?*

Contributors: *Rebecca Goolsby (Office of Naval Research), Nitin Agarwal (University of Arkansas at Little Rock), Fred Morstatter (Arizona State University), Randy Kluver (Texas A&M University), Willow Brugh, (Center For Civic Media, MIT Media Lab), Todd Huffman & Ryan Paterson (IST Research)*

Executive Summary

Dr. Jen Ziemke, John Carroll University (in collaboration with the rest of the team).

The responses below attempt to summarize a conversation among contributors that began over email.

Twitter & Facebook?

Todd Huffman and Ryan Paterson shared their analysis of the top fifty applications and services used over the last three months to spread VEO propaganda. Top on the list are applications for Twitter, Facebook, and WordPress, among others as shown in the Appendix**.** Our contributors also highlighted others: Fred Morstatter (ASU) flagged Telegram, as well as custom-made apps, while Randy Kluver (TAMU) remarks that alternative platforms tacitly supported by foreign governments (such as Wechat or VKontakte) "re-create the geographical and political divisions that most assumed were ending with the rise of a globalized world." However, many authors argue that the issue is truly platform neutral, and that message circulation is just as effective in any number of other platforms. Rebecca Goolsby (ONR) additionally surmised that the way in which the question was asked explains the "Twitter and Facebook" answer received. Contributors felt that gaining traction on this issue first requires understanding how VEO's leverage social media and vulnerable audiences to attain their goals. We turn to Rebecca Goolsby to elaborate on this issue.

"Anyone that is a true believer in X must also believe Y"

Goolsby asserts that a goal of any VEO is to transform, create, and reframe a conversation by deploying "side-step logic", which amounts to: *If you truly believe X, then you must also believe and support Y.* The crafty use of this logical fallacy is what leads hyper-connected yet vulnerable audiences to leverage social media to recirculate and thus amplify the message. She says a VEO wants "to turn the conversation so that the audience believes if they support Healthy Kittens for America, then they must naturally support <INSERT agitation issue here>. And if you don't support <insert here>, how can you call yourself a Friend of All Kittens?"

Since the narrative is pitched to the target audiences' deep biases, values, and worldview, the audience does not engage in critical thinking about the information. Because the audience emotionally 'knows' that X is true (and right) in its emotional mind, then it accepts the parasite narrative without thorough consideration of its origins, implications, or agenda. And since the audience finds that more and more of its trusted peers are echoing this information, critical evaluation is further suppressed.

At the same time, the VEO insinuates itself into the information networks of the target audience in a way that displays this vulnerability, repeating and amplifying the motifs and sub-narratives that reflect its agenda, until it is hard to find where the host narrative and the parasite narrative are differentiated. The target audience is then repeatedly exposed to the parasite narrative through covert means, using computerized amplification methods (e.g. botnets, fake news).

Audiences as unwitting vectors of amplification

How do the VEO's reframe the conversation that makes this 'logical' side-step possible? By manipulating vulnerable audiences into recirculating this information for them. Messages are amplified by vulnerable audiences and paid intermediaries who recirculate these messages, drowning other views. Goolsby asserts that "the reason phones are a game changer is that it is the easiest and cheapest access to the Internet available to most of the world. Newer users--the newbies--are not especially sophisticated in their understanding of news and fake information, but everyone has cognitive vulnerabilities--hot button issues--that can be exploited." Nitin Agarwal (U. of Arkansas) elaborates on message amplification by noting that messages emerge in one medium but are then massively disseminated across several other platforms: "Strategies such as thread jacking, smoke-screening, hashtag latching, etc. are used to multiply the messages."

Why share?

Youth in particular share or create these messages for a variety of different reasons. As digital natives, they want to be seen sharing insider information as a way to boast about privileged access to content from the frontlines. Youth compete to post information that shows just how enlightened they are about an issue relative to their peers, and to do so faster than anyone else. Jen Ziemke's (John Carroll University) young students remark that when their friends spread information and pictures of weaponry and battlefield activity they do so "to make themselves look good amongst their friends who do not have such access to such exclusive content." Still others share in order to feel like they belong to something, or to "feel cool," or even to feel "morally superior to have shared something that helps craft one's identity around an issue."

Content Consumption & Recirculation

Many who end up sharing content start out by passively looking through media on their phone (their 'feed'), mostly out of boredom, curiosity, or force of habit. For many, it is an obsession born out of an addiction to their phones. Their ritual includes checking several different feeds, nearly all of the time. They often do not start out with the intent to circulate something in particular, rather, they share based on the serendipity of their feed.

Snapchat, Instagram & YouTube

Ziemke's interviewees report that youth generally prefer receiving messages via pictures and video rather than words, which is another reason they increasingly turn to platforms like Instagram, Snapchat, and Youtube. "Pictures make you feel like a part of the battlespace" and powerful imagery "gets stuck in your head" in ways that narratives without visuals do not. Nitin Agarwal likewise finds that millennials are particularly vulnerable to YouTube messaging. Agarwal calls YouTube "*<u>the</u>* platform for crafting the narrative and setting the agenda."

Another reason youth are moving toward other channels seems to be due to differences in the design and user experience across the platforms. Millennials report being *tired of "all of this scrolling"* and thus are likely to continue to move away from the Facebook and Twitter environment and towards Instagram, YouTube & Snapchat. Others remarked that Twitter and Facebook are quickly gaining negative reputations as increasingly full of garbage, spam and propaganda, and that many are drifting away from it, and turning to Snapchat and Instagram as platforms which have less "noise" in their feeds compared with the conventional channels.

It's so easy

However, it is the ease of sharing that sticks with one young student of Ziemke's, who relayed that what actually seems most important is simply how easy all of this is, which is independent of platform. Picking up his phone he noted that he could get access to anything he wanted in a moment through knowing just one contact. What stood out for him was the stupendous simplicity and ease with which the exchange of information can happen, literally in just seconds, and on a phone that is already in your hand. [1]

The heart of the matter

What are the relevant important next steps one might suggest in light of these trends?

Willow Brugh of the Center for Civic Media cautions that simply shutting down the same tools that populations use when infrastructure collapses seems like a terrible idea. After all, these are the same tools that help vulnerable populations self-organize when living under repressive regimes.

Clearly there is an urgent need to solve the *structural problems* that contribute to what makes a VEO's narrative attractive in the first place. Randy Kluver remarks that alternative platforms "re-create the geographical and political divisions that most assumed were ending with the rise of a globalized world. Political, social, and cultural discussions that could happen on globally accessible platforms are moving into different platforms, where there is less ability for US citizens to interact, and thus the technological platforms re-embody the geographical differences."

Brugh elaborates: "Are we yet spending as much (hopefully far more) on youth opportunity and other vectors we know that decrease the likelihood of finding ISIL et al as undesirable? All the tools I know about from online harassment, escalated (aka "weaponized social") which monitor or nudge people's online communications are far more often used to quash meaningful dissent than to actually help anyone."

In conclusion, while we may have taken some limited steps toward answering one question, we know that the question itself is really the core of the matter, and are therefore grateful for this and any future opportunities to engage.

[1] Several of my current students have been working on this problem with me for the past three semesters. Ranging in age from 18-25, one told me a story that illustrates this dynamic. While attending one of the most prestigious international schools in Lebanon, he met the son of an alleged weapons supplier to various Christian militias in Lebanon and Syria. How would this individual have any access to VEO propaganda and/or distribute it to a wide audience? Well, the Christian militias in Syria that his father allegedly supplies are closely allied with Hezbollah. As a result, his contact constantly receives "inside footage" specifically addressed to him, which he then boastingly posts on social media pages such as Instagram and Snapchat, for thousands to see. Furthermore, whenever Hezbollah and the Christian militias triumph in Syria, a victory song plays on his snapchat story for 10 seconds, accompanied by a yellow heart. This means he gets real-time updates, pictures, and videos from the battlefield on his phone.

SME Input

Hosts and Parasites:
the spread of propaganda in the new information environment

Rebecca Goolsby
Office of Naval Research
rebecca.goolsby@navy.mil

The spread of propaganda on the Internet is a dark art. It involved botnets, blogsites, and "grey" social media platforms you may never have heard of (Gab, Zello and others) to coordinate and orchestrate the media campaign. It involves paid actors, botnet operators, advertising companies, and the willing, vulnerable audiences who are easily targeted. As I've argued elsewhere, most human beings (perhaps all human beings) are vulnerable to propaganda when it gets under the defenses of their logical, rational minds and directly impacts their cognitive vulnerabilities--their sacred values, emotional, personal experiences, beliefs and understandings with high emotional appeal. Rand Waltzmann has termed these as "cognitive vulnerabilities," topics and beliefs that are so close to emotional space that analytical thinking is difficult to engage.

Mark Goulston has described the impact of a discourse that hits one of the discussants in their deep emotional spaces as "amygdala hijack." The emotional brain, surrounding the amygdala and its emotions-processing centers, is willing to accept some narratives without engaging higher thinking. Sometimes, such as when a person is afraid or angry, the brain stem's 'fight or flight' mechanisms become engaged--and the cerebral cortex, the analytical, logical mind, becomes disengaged. The person who is in hijack will fight rather than change his stance. Indeed, people in amygdala hijack often pick a fight, putting the other person in discourse into the same, angry, unreasoning frame of mind that perpetuates the argument. This is certainly what we are seeing around us on the Internet today.

Ben Nimmo's description of distort, distract, dismiss and dismay as the four key tactics of Russian disinformation point to this strategy: discover vulnerable narratives, distort those narratives, distract the audience with increasingly outrageous and inflammatory information, and dismiss any suggestion that the West understands the situation. The "distort, distract and dismay" elements have been packaged and injected into vulnerable audiences to inflame and upset them, and to make them see that this distorted truth is legitimate and real information by seeding the information environment and hijiacking their social networks with fake news and thousands, likely millions, of fake users, bots, and cyborg accounts--bot accounts that also have human users.

To create a campaign on any network, platform or app you need four things.

1) a target audience susceptible to messaging whose members are willing to distribute the propaganda far and wide to others. Anyone can be used, but the Russians have used as their ideal target audiences those with narratives consonant with their strategy, including many who are in "chronic" amygdala hijack--those anxious, angry individuals who messages constantly and has many contacts in other networks. UFO believers, paranormal and astrology buffs, conspiracy theorists, white supremecists, and anyone angry, afraid, or latched tightly to some ideal are heavily messaged with propaganda--because it helps if the audience is a bit irrational (to very irrational). Irrational people message heavily and are easily taken in if the message is consonant with their beliefs. But

everyone has their hot button topics--everyone can be a bit irrational when their deeply held beliefs are brought into the narrative.

2) an intermediary network of allies who will insert the propaganda into the message streams that the target audience will eagerly consume, without questioning it very much. Paid troll farms work well. Paid propagandists who can easily and cheaply code "puppet" accounts so that one person looks like he's ten thousand people are quite successful. Size matters, since one must envelope the target population with propaganda coming at them from all sides.

The goal here is to saturate the target audience's message stream and network and gain their trust and buy-in, by associating the propaganda with topics and issues they care about. The goal is gain their trust and buy-in to the source of the messaging, in order to lace the messages that they care about with propaganda and finally turn the conversation so that the audience believes if they support Healthy Kittens for America, then they must naturally support <INSERT agitation issue here>. And if you don't support <insert here>, how can you call yourself a Friend of All Kittens?

3) the classic tactics of distort, dismiss, dismay and distract that can be used to inject new information-- the parasite discussion--into the host narrative.

4) Untrammeled access to the target audience so that will not receive any indication that the propaganda is not real or, if such a message is received, that the target is so emotionally tangled up that they reject any messages that are counter to the propaganda.

You can do this anywhere on any platform. In S. Korea, a youth protest march began with side discussions on a boy-band fan site.

The reason phones are a game changer is that phones are the easiest and cheapest access to the Internet available to most of the world. New users (the “newbies”) are often not especially sophisticated in their understanding of news and fake information or familiar with the social dynamics in cyberspace. They form a great target audience for crowd manipulation and social hysteria propagation. The Russians have been engaged in crowd manipulation and social hysteria propagation on the Internet on a grand scale since at least 2014, with evidence of earlier experiments. The app doesn't matter. If those four conditions are met, any platform CAN be used, but there has to be a sufficiently large target population--or any influential audience that can reach others effectively-- to make it worth the propagandist's while. WhatsApp, Snapchat and the like do not make that as easy as Facebook and Twitter because it is somewhat more difficult to obfuscate identity to the platform and technically more challenging to build the amplifier technology similar to the Twitter botnets. Newer platforms tend to be on the lookout for this kind of technology and try to head it off early, as it creates unacceptable problems for them technically.

If ANY app allows for anonymous accounts (needed by the troll farms to amplify their signal), if it allows messaging to go freely about in groups and through social networks easily and without cost, it is a POSSIBLE vector. It is not a LIKELY vector if the propagandists cannot form an anonymous, automated mob of automated and semi-automated accounts to boost their signal sufficiently to create an echo chamber around the target audience.

Cross-Channel Social Media-Facilitated Disinformation Campaigns

Nitin Agarwal
University of Arkansas at Little Rock
nxagarwal@ualr.edu

Dr. Goolsby's response is spot-on with respect to what we have observed in several studies of disinformation campaigns. These studies shed light on coordination among information actors (including bloggers, trolls, YouTube-rs, botnets) observed during disinformation campaigns, such as the anti-NATO propaganda campaigns conducted by pro-Russian media and ISIS-led propaganda campaigns for radicalization, recruitment, and raising funds. This involves a well-crafted strategy using (1) cross-channel communication, and (2) deploying strategic information maneuvers to amplify the spread. More specifically, propaganda emerges on one medium, say blogs or YouTube, and is then massively disseminated on Twitter and the likes. Strategies such as, thread jacking, smoke-screening, hashtag latching, etc. are used to multiply the messages. YouTube is emerging to be *the* platform for crafting the narrative and setting agenda. The demographics on YouTube is also most vulnerable to these tactics - they are highly impressionable and naturally inclined towards getting information from social media or alternate media (e.g., binge-watching propaganda channels).

Additional channels that warrant exploration vis-a-vis disinformation campaigns include Reddit and Discord (can be considered as "Slack" for gamers). The demographic on these channels primarily consist of millenniums. Both these channels were heavily used during the recent US

Presidential elections to propagate 'fake news': (https://www.theguardian.com/technology/2016/nov/22/moderators-trump-reddit-group-fake-news-crackdown).

Mobile Applications for Disseminating Propaganda

Fred Morstatter
Arizona State University
fred.morstatter@asu.edu

It is important to consider that some propaganda is distributed through custom apps made by the people and organizations whose goal is to distribute the propaganda. For example, ISIS made their own app to distribute propaganda to their followers [1].

Dr. Goolsby and Dr. Agarwal identified the major distribution approaches in their write-ups. Two studies have looked into how ISIS used Telegram to distribute propaganda [2] [3].

Further, it is important to note that many of these organizations, such as ISIS, do not wish to have their true identities known. Thus, they use mobile apps that allow for increased security to prevent leaking their personal information. The Electronic Frontier Foundation has created a survey of mobile applications based on their security [4]. This could be useful for identifying trends in mobile app usage among these groups.

[1]http://www.ibtimes.com/isis-android-app-islamic-state-develops-smartphone-app-propaganda-messaging-2211847

[2]http://www.ibtimes.co.uk/welcome-bizarre-frightening-world-islamic-state-channels-telegram-1561186

[3]http://www.forbes.com/sites/parmyolson/2015/11/19/telegram-isis-propaganda-channels/#50a55ca86f88

[4]https://www.eff.org/node/82654

Platform Gaps: New media platforms and geopolitics

Randy Kluver
Texas A&M University
rkluver@tamu.edu

One of the major problems with analyzing the use of social media platforms (or apps) and in political or social activism (change) is that the technology changes more rapidly than our ability to adequately digest how the apps are being used, the particular affordances of any particular app or platform, and the ways in which users will soon find new ways to use the technology. New apps are being developed all the time, and although at this point there are a few dominant global platforms (such as Facebook and Twitter), soon that dominance is likely to end in favor of new apps. Any app will do, as so many new apps provide opportunities for all kinds of messaging. One of the important assumptions in our discussion needs to be the distinction between apps that are accessible to and used by a broad public (such as Facebook), or those that are used selectively by much more limited groups (such as Snapchat), or those that exist on the dark web.

At Texas A&M, we monitor activity on Twitter, as it is a major platform for tracking political discussions in the Arabic world, but we are also tracking the development and growth of *Weixin* (wechat) in China and *Vkontakte* in Russia as alternative platforms that embody different political and social affordances than Twitter and Facebook. Our goal is to capture broad public sentiment, not private messaging, and Facebook and Twitter remain prominent public apps in the middle east, and are the primary mechanisms to reach broad audiences.

One of the many issues associated with these alternative platforms (or what we call the platform gap) is that they re-create the geographical and political divisions that most assumed were ending with the rise of a globalized world. Political, social, and cultural discussions that could happen on globally accessible platforms are moving into different platforms, where there is less ability for US citizens to interact, and thus the technological platforms re-embody the geographical differences. In addition, these platforms constrain the types of activities that can easily occur. Weixin, for example, limits "public" postings to a small segment of "verified" users, and does not allow for the creation and marketing of public events, such as are chronicled in Wael Ghonem's book Revolution 2.0, which demonstrates the role of Facebook in creating public events that led to the downfall of the Mubarak government in Egypt. Thus, Weixin, which in many ways is a far superior app to Facebook, such as its utility as a mobile commerce platform, embodies far fewer political affordances than Facebook.

A final app that needs to be considered is Firechat, which allows the development of mesh networks using Bluetooth, so that data transfer is possible even when there is no actual phone network available. It has become famous for its role in keeping communication networks alive even when there is an actual network shutdown due to natural disaster or other destabilizing events, and could indeed be a game changer in conditions of political upheaval, when governments decide to shut down data networks in order to prevent political collusion.

Comments on Media Platforms

Willow Brugh
Affiliate at Center for Civic Media, MIT Media Lab
willow.bl00@gmail.com

Are we yet spending as much (hopefully far more) on youth opportunity and other vectors we know that decrease the likelihood of finding ISIL et al as undesirable? All the tools I know about from online harassment, escalated (aka "weaponized social") which monitor or nudge people's online communications are far more often used to quash meaningful dissent than to actually help anyone. Another way to say what I'm trying to get across is: an easy solution to these issues would to be fixing the social and technical vulnerabilities, i.e., making sure *everyone* can use encryption, think critically, etc. Instead, the US is trying to exploit vulnerabilities just like those you're up against are doing, which means you're in an arms race where people are your weapons. And that's appalling and un-winnable.

Goolsby response: I have great respect for Brugh's position. The US response needs to be in the direction of developing a program of responsible global engagement and the promotion of research to develop the new field of cyber-diplomacy. This will involve the study of the crowd manipulation, social hysteria propagation, and disinformation with the aim of improving the resilience of targeted populations against influence and manipulation. The effective programs of this kind will have a "ground game" – such as the activities of public affairs and civil affairs in Phase 0 operations—and a "cyber game" that coordinates with the messaging of the "ground game." Social trust is developed most effectively in people-to-people, face-to-face contexts. Social trust developed from real-world events will be more lasting than pure cyber-campaigns and can mitigate the crowd manipulation that comes from cyberspace.

An appropriate and effective response will be this sort of two-tiered set of activities that seek to bring target audiences back in balance with rational thinking and critical engagement in the world around them. It will involve whole-of-government and also the coordination of activities with non-government organizations and non-profits. We can develop good strategies for this and effective approaches. Much depends on their being effective leadership willing and interested in engaging in this fight.

Top 50 applications and services used over the last 90 days to spread VEO ideology and propaganda

Todd Huffman & Ryan Paterson
huffmantm@gmail.com
ryan.paterson@istresearch.com

Todd and Ryan attached a work product they just completed, 'ISIS Automation and Propaganda Analysis', in which they tracked the top 50 applications and services used over the last 90 days to spread VEO ideology and propaganda. Ryan later articulated, “to be clear, the top 50 we are showing here are the apps that provide bot control for tweets. This was quick analysis this morning looking at what automation platforms are being used to control tweets only.”

What:	*Top 50 applications and services used over the last 90 days to spread VEO ideology and propaganda*
When:	90 day query ending on 7 Dec 16
Source:	Twitter, Telegram, Twitter, Scraped URLs collected by IST Research's Pulse platform
Total documents analyzed:	55,913,780

Count	Client	URL	Description	Multiple accounts or cross-service posts?	Automation?
18,848,412	Twitter for Android	http://twitter.com/download/android	Twitter for Android	N	N
14,951,172	Twitter for iPhone	http://twitter.com/download/iphone	Twitter for iPhone	N	N
9,184,417	Twitter Web Client	http://twitter.com	Twitter Web Client	N	N
3,802,320	TweetDeck	https://about.twitter.com/products/tweetdeck	"The most powerful Twitter tool for real-time tracking, organizing and engagement."	Y	N
1,660,421	Twitter for iPad	http://twitter.com/#!/download/ipad	Twitter for iPad	N	N
1,406,982	IFTTT	http://ifttt.com	IFTTT is a free web-based service that allows users to create chains of simple conditional statements, called "applets", which are triggered based on changes to other web services such as Gmail, Facebook, Instagram, and Pinterest. IFTTT is an abbreviation of "If This Then That".	Y	Y
735,722	Mobile Web (M5)	https://mobile.twitter.com	Twitter Web Client for Mobile Clients	N	N
554,758	twitterfeed	http://twitterfeed.com	Defunct tool for connecting RSS feeds to multiple accounts and services	Y	Y
484,674	dlvr.it	http://dlvr.it	Smart Social Media Automation - The easiest way to find and share great content to Facebook, Twitter, Pinterest and more.	Y	Y
482,228	Facebook	http://www.facebook.com/twitter	Cross-posting from Facebook onto Twitter	Y	N
313,124	GrabInbox	http://www.grabinbox.com	GrabInbox is an easy way to manage multiple twitter, facebook, fan pages and linkedin accounts.	Y	Y
270,969	anode_ghost	http://www.anodeghost.com	Unknown - URL doesn't resolve or is blocked	?	?
259,375	Mobile Web (M2)	https://mobile.twitter.com	Mobile web client for Twitter	N	N
167,329	Hootsuite	http://www.hootsuite.com	Manage all your social media marketing in one place - From finding prospects to serving customers, Hootsuite helps you do more with your social media marketing.	Y	Y
167,270	chernobyl_blow	https://www.chernobylblow.com	Unknown - URL doesn't resolve or is blocked	?	?
159,559	Twitquran	http://twitquran.com/About.aspx	Automates the tweeting of verses of the Koran.	N	Y
151,092	TTYtter	http://www.floodgap.com/software/ttytter/	Perl based Twitter client (no longer supported, but still active) that supports API interfaces	Y	Y
138,036	Postfity.com	http://postfity.com	Manage social networks, schedule messages, engage your audiences, and more - right from one, easy-to-use dashboard.	Y	Y
137,682	Twitter for Windows Phone	http://www.twitter.com	Twitter client for Windows phone	N	N
132,865	twittbot.net	http://twittbot.net/	Bot automation and control tool (free and paid version)	Y	Y
126,595	Twitter for Windows	http://www.twitter.com	Twitter client for Windows	N	N
119,365	Google	http://www.google.com/	Google	N	N
110,188	Put your button on any page!	http://linkis.com	Linkis is a free link customization service for social promotion. It provides the most convenient and easy way to customize links and thus engage more followers.	N	N
103,483	WordPress.com	http://publicize.wp.com/	Blog service	N	N
100,911	Unknown	http://vd1.co/lop	URL redirect to Jihahist video channel on YouTube (custom posting app suspected)	N	N
97,346	Tweet Old Post	http://www.ajaymatharu.com/	Tweet Old Post is a plugin designed to tweet your older posts to get more traffic.	N	Y
92,108	Tweetbot for iOS	http://tapbots.com/tweetbot	Twitter client for iOS	Y	N
88,836	Postcron App	https://postcron.com	Service to automate the scheduling and posting of content across multiple sites and accounts	Y	Y
88,340	twitkato	http://127.0.0.1/website	Unknown - URL resolves to a localhost address (custom posting app suspected)	U	U
86,514	TweetNow112233	http://www.placeholder.com	Unknown - URL doesn't resolve or is blocked (custom posting app suspected)	U	U
74,168	TweetCaster for Android	http://www.tweetcaster.com	Twitter client for Android	Y	N
66,833	Twitter for BlackBerry	http://www.twitter.com	Twitter client for Blackberry	N	N
61,490	Automated Allah Tweets	http://k-632.com	Connects a user's account to automatically Tweet religious posts hourly	N	Y
58,970	Aya FM	http://aya.fm	Automates the posting of verses on a six hour timeframe for a user's account	N	Y
55,165	Khawarizmi.net	http://vps275619.ovh.net/	Automate the management and posting of content from multiple accounts	Y	Y
51,597	zs Beta	https://zs.com/	Unknown - URL redirects to an unrelated website (custom posting app suspected)	U	U
45,164	CtrlSec	https://twitter.com/CtrlSec	CtrlSec advocates for the shutdown of ISIL accounts on multiple services	N	N
44,921	BOTlibre!	http://www.botlibre.com	Service to create bots to connect multiple accounts and services	Y	Y
44,343	RoundTeam	https://roundteam.co	RoundTeam automates the task of searching and sharing Tweets while allowing greater control, including source, type of content, frequency, hashtags of interest, and more.	N	Y
41,765	yumtra	https://www.yumtra.com/	Unknown - URL doesn't resolve or is blocked (custom posting app suspected)	N	N
41,629	wrapix	https://www.wrapix.com/	Unknown - URL doesn't resolve or is blocked (custom posting app suspected)	N	N
38,167	Buffer	http://bufferapp.com	Buffer is a tool for automating the sharing of content across services and accounts	Y	Y
37,437	FeedBlitz	http://www.feedblitz.com/f/f.fbz?help/default#twitter	FeedBlitz allows users to automatically create mailings from any RSS feed, easily manage multiple mailing lists, filter by content preferences, and more.	N	Y
36,571	zsApp Beta	https://zsapp.com/	Unknown - URL doesn't resolve or is blocked (custom posting app suspected)	U	U
35,283	ArmyOfBots	https://twitter.com/	URL resolves to Twitter, but the tag of "ArmyOfBots" implies automation being employed	N	Y
34,515	Dua App	http://du3a.org	Dua automates the sharing of "blessings" on a user account based on a time frequency	N	Y
32,218	schrumbeulappz	http://shrumbeleu.lol	Unknown - URL doesn't resolve or is blocked (custom posting app suspected)	N	N
31,669	SocialOomph	https://www.socialoomph.com	Boost your social media productivity -- it doesn't have to be a manual time-consuming process! Twitter, Facebook, Pinterest, LinkedIn, Tumblr, RSS feeds, blogs, and Plurk! Easily schedule updates, find quality people to follow, and monitor social media activity!	Y	Y
31,268	SocialPilot.co	https://panel.socialpilot.co/	SocialPilot is a social media scheduling and marketing platform developed specifically for agencies and social media professionals. Used by over 40,000 agencies and social media teams, SocialPilot is designed to help users enhance the efficiency of their online marketing strategies and efforts, and save time and money.	Y	Y
28,514	ControllingSection1	https://twitter.com	CtrlSec - automated posts	U	Y

Total documents collected:	55,913,780
Total documents that use an automation service:	4,196,343
Percentage of total documents that are posted using an automation service*	7.51%

*This analysis only explicitly totaled documents posted using automation services. The actual percentage of automation is likely significantly higher as accounts can be linked to the automation services and posts appear to be coming from the accounts without reference to the automation service. The sheer number of services being employed within the subset of Twitter data that is ISIL specific suggests a number of TTPs in place to automate the dissemination of information, 'season' accounts using automated call to prayer apps, and various customized services to mask the source of a posted document. Additionally, it does not take into account the significant number of documents that are Counter-VEO messaging. When these two factors are taken into consideration, the percentage of automation of the ISIL data set could approach double-digit automation numbers.

Author Biographies

Nitin Agarwal

Nitin Agarwal is the Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor of Information Science and director of the Center of Social Media and Online Behavioral Studies (COSMOS) at the University of Arkansas at Little Rock.

Dr. Agarwal obtained Ph.D. in Computer Science from Arizona State University with outstanding dissertation recognition in 2009. He has a Bachelor's of Technology in Information Technology from the Indian Institute of Information Technology, India. In 2012, he was recognized as one of "The New Influentials: 20 In Their 20s" by Arkansas Business for being among creative and talented individuals who have found not only early success in their profession but also show future potential to step up as a leader in business or politics to highlight their accomplishments within their businesses, organizations or community. He was recognized with the University-wide Faculty Excellence Award in Research and Creative Endeavors in 2015. Dr. Agarwal received the Social Media 2015 Educator of the Year Award at the 21st International Education and Technology Conference, Cyberport, Hong Kong SAR, China, 10-12 April 2015. The Educator of the Year award recognizes Springer authors/educators who have made or are making a difference in the ICT Education/Research.

Dr. Agarwal's research interests include social computing, knowledge extraction in social media, (deviant) behavioral modeling, group dynamics, influence, trust, collective action, social-cyber forensics, health informatics, data mining, and privacy. From Saudi Arabian women's right to drive cyber campaigns to Autism awareness campaigns to ISIS' and anti-West/anti-NATO propaganda campaigns, at COSMOS, he is directing several projects with multi-million dollar funding from the U.S. National Science Foundation (NSF), U.S. Office of Naval Research (ONR), U.S. Air Force Research Lab (AFRL), and U.S. Army Research Office (ARO). Dr. Agarwal's research has made foundational contributions to computational social network analysis to study digital/cyber campaign coordination, identify powerful actors and groups, study propaganda dissemination, and monitor cyber threats through social media. The applicational contributions of his research include, but not limited to, digital campaign coordination, propaganda dissemination analysis, event analysis, monitoring cyberthreats through social media, social-cyberforensics, smart health and wellbeing, social media in learning environments, network and communication, and socially aware mobile networks. Dr. Agarwal's research efforts bring together researchers from various disciplines such as information science, social science, economics, political science, communication and organization science, and computer and mobile networks and practitioners including defense analysts from NATO, U.S. Naval Research Lab, Dillards, Acxiom, @WalmartLabs, and other organizations. The research has resulted in 5 books and over 100 peer-reviewed publications at various prestigious forums including journal articles, book chapters/encyclopedia entries, and conference proceeding papers. The research studies have resulted in Best Information System Publication of 2012 Award recognized by the AIS Senior Scholar Consortium, a few Best Paper Awards including two at IARIA's SOTICS 2015 and SOTICS 2016, and several best paper nominees.

U.S. National Science Foundation (NSF) and U.S. Army Research Office (ARO) awarded Dr. Agarwal multiple grants to extend outreach efforts to increase diversity and minority participation in emerging and interdisciplinary areas (such as, social computing) under Science, Technology, Engineering, and Mathematics (STEM) disciplines. Organizing the International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction (SBP), is one effort in this direction. To foster an interdisciplinary collaboration and a synergistic environment, Dr. Agarwal has edited several books and journal special issues for IEEE, Elsevier, Springer, and Oxford. Dr. Agarwal currently serves as program chair and program committee member of several prestigious conferences and journals. He has served on the U.S. National Science Foundation (NSF) review panels and external reviewer for the U.S. Army Research Office (ARO), U.S. National Institutes of Health (NIH), Canadian Natural Sciences and Engineering Research Council (NSERC), Saudi Arabia's King Abdulaziz City for Science and Technology (KACST), and Hong Kong's Research Grants Council (RGC) review panels.

Willow Brugh

Affiliate at Center for Civic Media, MIT Media Lab
willow.bl00@gmail.com

Rebecca Goolsby, PhD

Dr. Goolsby holds a doctorate in anthropology from the University of Washington in Seattle. She is a former Fulbright Scholar, a scholar and writer in the fields of computational social science and cyberanthropology. She currently serves as a program officer at the Office of Naval Research. She leads a NATO Research Technology Group on Information Technology and Crisis and is an advisor to the recently formed NATO Digital Working Group under the NATO Public Diplomacy Division at NATO SHAPE headquarters in Brussels. She resides in Virginia.

Todd Huffman

Istresearch.com

Randy Kluver

Randy Kluver is Professor of Communication at Texas A&M University, where he conducts theoretically driven research on political communication (including rhetorical and new media approaches), and global and new media. His work explores the role of political culture on political communication, and the ways in which cultural expectations, values, and habits condition political messaging practices and reception in a variety of contexts. Recently, Dr. Kluver has been exploring the role of communication and geopolitics, and developing research agenda that articulates ‘media-centric’ views of geopolitics. Currently, he is leading a research group focused on media and geopolitics, utilizing the Media Monitoring System, a real time international broadcast transcription and translation system, and is developing research protocols and agendas using this pioneering technology. Dr. Kluver was the founder and Executive Director of the Singapore Internet Research Centre, and one of the principal investigators of the international “Internet and Elections” project, a groundbreaking international analysis of the use of the Internet in the elections. Prior to coming to Texas A&M, Dr. Kluver taught at Oklahoma City University, Jiangxi Normal University, the National University of Singapore, and Nanyang Technological University in Singapore. He serves on the editorial boards of the Journal of Communication, the Journal of Computer-mediated Communication, the Asian Journal of Communication, New Media and Society, China Media Research, and the Western Journal of Communication.

Fred Morstatter

Fred Morstatter is a PhD student in computer science at Arizona State University in Tempe, Arizona. Fred won the Dean's Fellowship for outstanding leadership and scholarship during his time at ASU. He is a 2016 Faculty Emeriti Fellow, and has won the 2016 University Graduate Fellowship. Fred's research focuses on finding and removing biases that impinge social media research. Among his publications is an ICWSM paper that investigates the representativeness of Twitter's Streaming API, a WWW Web Science paper that seek to find periods of bias automatically in streaming Twitter data, 2 KDD demo papers, an article in IEEE Intelligent Systems, and a book: Twitter Data Analytics. He won the World Wide Web conference's Best Poster Award in 2016. He has served as a PC member of ICWSM 2014, 2016, and 2017, the IEEE/CIC ICCC 2014 Symposium on Social Networks and Big Data, and has been a co-chair of the Social Computing, Behavioral-Cultural Modeling and Prediction Conference's Grand Challenge organizing committee in 2014, 2015, and 2016. He has been a Visiting Scholar at Carnegie Mellon University as well as a Research Intern at Microsoft Research. He is the Principal Architect for TweetXplorer, an advanced visual analytic system for Twitter data. A full list of publications can be found at http://www.public.asu.edu/~fmorstat.

Ryan Paterson

Istresearch.com

Dr. Jen Ziemke

Jen Ziemke, (Ph.D., Political Science, University of Wisconsin-Madison), engages national and international institutions on ideation for a diverse set of hard problems, such as how citizen reporting from live conflict events shapes the nature of the battle space in real time. She is currently exploring how multimodal data perceptualization (visual & audio) can be leveraged to help understand and peripherally monitor temporal datastreams.

Jen served as Co-Founder & Co-Director of the International Network of Crisis Mappers, an international community of experts, practitioners, policymakers, technologists, researchers, journalists, scholars, hackers and skilled volunteers engaged at the intersection between humanitarian crises, technology and rapid mapping**.** Reuters AlertNet named Crisis Mapping one of its Top 20 Big Ideas in 2011. She also managed an international conference event, the ICCM, held in Manila (2016), New York (2014), Nairobi (2013), the World Bank (2012), Geneva (2011), Harvard (2010), and Cleveland (2009).

Jen has consulted with, briefed, or engaged programs within the DoD, ONR, DARPA, DIA/MINERVA, National Intelligence Council, NDU, the United Nations Office of the Secretary General, UN-OCHA, UN-SPIDER, the World Bank, US Department of State, Rockefeller Foundation, Woodrow Wilson Center, Yale, Carnegie Mellon, Rochester Institute of Technology, Notre Dame, & TED. Her projects have been covered in several national and international outlets, including the Voice of America, Reuters, NPR, CNN, Huffington Post, Wired, The Chronicle of Higher Education, among others.

In her role as Associate Professor of International Relations at John Carroll University she teaches courses at the intersection of research methodology, international security, international relations, and conflict processes. She serves on the Board of Directors for the Open Geospatial Consortium(OGC) & the MapStory Foundation, & is principal consultant at Endogeneity, LLC.

Jen received her Ph.D. from the University of Wisconsin-Madison (Political Science) and undergraduate degree from the University of Michigan-Ann Arbor. She also served as a Crisis Mapping and Early Warning Fellow at the Harvard Humanitarian Initiative (HHI) and was named a 2013 recipient of the University of Michigan's LSA Humanitarian Service Award, presented annually by the Dean to 3 living alumni in recognition of their work. Jen was a Peace Corps volunteer on the Namibian side of the Angolan border from 1997-1999. She has hitchhiked 20,000 miles in over a dozen African countries and has a set of very cursory experiences drawn from short stints in several different warzones around the world.