All the World is Staged: An Analysis of Social Media Influence Operations against US Counterproliferation Efforts in Syria

Jack O. Nassetta and Ethan P. Fecht
The James Martin Center for Nonproliferation Studies (CNS) strives to combat the spread of weapons of mass destruction by training the next generation of nonproliferation specialists and disseminating timely information and analysis. CNS at the Middlebury Institute of International Studies at Monterey is the largest nongovernmental organization in the United States devoted exclusively to research and training on nonproliferation issues.

The Middlebury Institute for International Studies at Monterey provides international professional education in areas of critical importance to a rapidly changing global community, including international policy and management, translation and interpretation, language teaching, sustainable development, and nonproliferation. We prepare students from all over the world to make a meaningful impact in their chosen fields through degree programs characterized by immersive and collaborative learning, and opportunities to acquire and apply practical professional skills. Our students are emerging leaders capable of bridging cultural, organizational, and language divides to produce sustainable, equitable solutions to a variety of global challenges.

Disclaimer

The James Martin Center for Nonproliferation Studies (CNS) has relied exclusively upon open-source intelligence for the research underpinning this report. Classification of specific social media users as likely synthetic actors is not necessarily conclusive. While unlikely, it is possible that some users mentioned in this report are in reality genuine users whose profiles coincidentally met the subjective criteria to be classified as a likely synthetic actor. The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or agreement, in the United States or elsewhere. The views, judgments, and conclusions in this report are the sole representations of the authors and do not necessarily represent either the official position or policy or bear the endorsement CNS or the Middlebury Institute of International Studies at Monterey.

© The President and Trustees of Middlebury College, 2018
All the World is Staged:

An Analysis of Social Media Influence Operations against US Counterproliferation Efforts in Syria

James Martin Center for Nonproliferation Studies

Jack O. Nassetta and Ethan P. Fecht
# Contents

**Executive Summary**
- Context  
- Aims  
- Definitions  
- Findings  
- Recommendations  

**Methodology**
- Factors Indicating Synthetic Actor Activity  
- Collection Methods  
- Analytical Methods  
- Limitations  

**Trends and Statistics**
- Breakdown of Collected Accounts  
- Creation Dates for Users Tweeting “@realDonaldTrump”  
- Breakdown of Accounts Created Following the Attack in Douma  
- User Descriptions Word Frequency  

**Tactics**
- Content Themes  
- Procedural Tactics  
- Target Audiences  

**Profiles**

**Results**  

**Concluding Remarks**

**About the Authors**  

**Acknowledgements**
Executive Summary

Though much of the scrutiny into foreign interference in US political debates focuses on long-term election operations, foreign actors have now turned to social media to conduct short-term tactical operations. These operations aim to affect American attitudes toward specific US foreign and military policy, and ultimately affect the policy itself. In recent years, state actors and loosely affiliated patriotic operators have inorganically inserted themselves into the political discussion surrounding US intervention in Syria following the use of chemical weapons. Through continually evolving techniques, these “synthetic actors” are likely the main driving force behind shaping the character of the counternarrative discussion surrounding the use of chemical weapons in Syria.

Aims

This paper seeks to analyze the tradecraft, trends, themes, and possible effects of disinformation produced by suspected synthetic actors (i.e., bots, trolls, and cyborgs) on Twitter concerning chemical weapons use in Syria.1 Although it is highly likely these synthetic actors exist on other social media platforms as well, this analysis focuses exclusively on Twitter, since the open nature of the platform allows for study without special access. Furthermore, we aim to improve public and academic awareness of foreign, inorganic disinformation efforts against our domestic decision-making processes. We hope that this text contributes to the efforts to prevent the erosion of the integrity of the political conversations that matter most.

Definitions

For the purposes of this paper, the following terms2 are defined as:

- **Troll** – A Twitter user that operates as an undeclared state actor, usually masquerading as an average westerner expressing personal political opinions, while participating in some level of coordination to circulate state-sponsored narratives.
- **Bot** – A fully automated Twitter account, engaging in content creation or perpetuation solely based on a software script.
- **Cyborg** – A Twitter account that mostly operates based on automated script behavior, but that is taken over and operated by a human user occasionally.
- **Synthetic actor** – A Twitter account fitting into any of the above categories; an actor masquerading under false pretenses in order to accomplish a political end.
- **Commercial bot account** – A Twitter account that is engaging in automated posting in order to generate profit for its owner. This can be through posting links to items for sale or by posting links to fake news in order to drive web traffic. Crucially, the posting of fake news by commercial bots is

---

2 Ibid.
not for political purposes, but rather to drive traffic. Synthetic actors who are bots often operate as commercial accounts when there is no salient political event for which they are needed.

Findings

- A significant minority (16–20%) of Twitter counternarrative messaging in the immediate aftermath of and regarding Syrian chemical weapons attacks is disseminated by a well-coordinated, narrowly focused state actor, almost certainly the Russian Federation. We did not, however, find evidence that the Syrian government maintains its own independent apparatus for extensive counternarrative messaging on Twitter.

- A network of highly message-disciplined synthetic actors was activated in the days following the April 7, 2018, chemical attack in Douma, Syria. Nearly half of the counternarrative accounts created in the week between the Douma chemical attack and the Western strike against the Syrian regime were observed to be synthetic actors. After the messaging attempt “failed,” many counternarrative accounts became immediately inactive, bolstering our assessment that they were synthetic actors.

- The single most common procedural tactic employed by our observed synthetic actor accounts was threatening not to vote for President Donald Trump again. We assess that this tactic is especially effective because the president’s political base is less likely to immediately discount the interlocutor as an unconditional “Trump critic.”

- The synthetic actors primarily utilize several thematic tactics. Most notably, they:
  1. attempt to defame Western institutions in order to discredit their claims about Syrian use of chemical weapons;
  2. suggest jihadist responsibility for the attacks;
  3. hint that a destructive (often nuclear) escalation would result from a Western retaliatory strike;
  4. prey on Western religious and cultural sympathies for supposedly besieged Syrian Christians and the secular Bashar al-Assad regime.

- While the majority of the synthetic actors seemed to target the American political discourse, we also observed counternarrative messaging to Western European audiences. This may suggest that Russia correctly expected that any strike against Syria would be a coalition effort.

- The vast majority of all users (synthetic and genuine) propagating Syrian chemical weapons counternarratives masqueraded as members of the American ideological right.

- Russia probably views bot and cyborg accounts as long-term resources which can be commercialized when necessary, while troll accounts are often disposable, short-term, and created ad hoc.
Recommendations

The goal of preventing information manipulation on social networks is one that policy makers will be forced to grapple with for years to come. Based on our study, we have compiled a set of recommendations for both policy makers and social network companies, focusing on how they can prevent synthetic actors from abusing their platforms for influence operations.

- Our research showed that a plurality of accounts that were created following the April 2018 Douma attack and used counternarrative keywords were synthetic. Social networks should take care to scrutinize accounts that were created immediately after controversial events if the accounts only engage in discussion about that event.

- The simplest step social networks can take to prevent manipulation by synthetic actors is to find and ban scripted bot accounts. These accounts are the easiest to distinguish from organic accounts in that their fully automated content typically consists of large, abnormal degrees of repetition. This repetitive nature creates easily recognizable patterns which are likely detectable via metadata analysis.
  - Twitter has already started this process, claiming to have banned 70 million accounts in the first half of 2018, however our dataset includes bots that are still active, indicating there is still work to be done.3

- High influence individuals (HIIs), such as the US president, should avoid making contentious statements on social networks. Salient statements, such as the announcement of an upcoming missile strike, provide a breeding ground for synthetic actors.
  - The synthetic accounts we examined typically have a very low number of followers, making it difficult for their content to spread under normal circumstances. However, when HIIs tweet, it becomes possible for synthetic actors to reply to them and potentially be seen by the millions of users who view the HII’s tweet. Contentious statements, such as military plans, should be reserved for more formal channels.

- Twitter currently “verifies” many HIIs by placing a blue check mark next to their name. We recommend the addition of an intermediate level of verification for normal users. This type of verification could be as simple as verification by phone number to as stringent as uploading a photo ID. This type of intermediate verification could allow typical users to spot those in the conversation who may be synthetic.

---

Methodology

Our analysis was conducted from a targeted dataset extracted from Twitter, one of the largest social media platforms on the internet and a cornerstone of public online political discourse. Through this lens, we principally focused on tweets posted in the wake of and discussing the April 7, 2018, chemical weapons attack in Douma, Syria.

Factors Indicating Synthetic Actor Activity

When analyzing a Twitter user for possible synthetic actor activity, many factors can indicate inorganic control of the account. If the account exhibits the below characteristics, it may suggest that the user is actually controlled by a state actor or a loosely associated organization with a specific propagandistic agenda. Nevertheless, care should be taken not to conclude such a connection based on just one or two factors; rather, the account should fulfill several of these characteristics before being classified as a synthetic actor.

The following list is organized in descending order, with the most definitive features of synthetic Twitter accounts near the beginning and the least conclusive traits toward the end.

1. **Synthetic actors often have bizarre, seemingly random alphanumeric usernames.** Trolls can employ this unusual naming convention, but it is most frequently observed with bot accounts. Examples include entirely random usernames such as “@12wevwT5dWLwtyK” (a likely bot) and partially random usernames such as “@Christo04083985” (a likely troll).

2. **Synthetic actors often use spurious images as their own profile pictures.** A common tactic among bots, trolls, and cyborgs alike is their use of stock images, photos of little-known foreign public figures, or images appropriated from private individuals’ social media accounts. An analyst can fairly reliably expose the use of this tactic by conducting a reverse image search of a suspected image.

3. **Synthetic actors may be active only sporadically.** Oftentimes, such accounts will leave weeks or months between periods of high-tempo posting. For example, one discovered troll account was active in February 2017 before falling silent until April 2017. Then, its inactivity returned until posting continued in November 2017.

4. **Synthetic actors often post extremely frequently when active.** Typical Twitter users tend to tweet several to a dozen times per day, but inorganic accounts may generate dozens or hundreds of posts in a single day.

5. **Synthetic actors often only generate one narrow category of post.** Bots, for example, will generally only “retweet” other users or will post only links (e.g., to “fake news” articles). We assess that the software behind these bot accounts may attempt to mask this tactic by recycling the article’s headline and using it as the tweet’s caption. Meanwhile, trolls often only tweet messages replying to other prominent Twitter users and may rarely generate non-targeted, more general posts (e.g., discussing their day or activities).

6. **Synthetic actors often generate out-of-place or unexpected political commentary.** For example, a bot account masquerading as an American conservative may post a link challenging the credibility of a Russian domestic opposition leader.
7. Synthetic actors sometimes post similar content in multiple languages, generally with poor translations. For example, in April 2018, a troll generated content in three languages — English, French, and Italian; its English and French content was likely not written by native speakers of the respective languages and may have been created by translation software.

8. Synthetic actors often post only about one or two specific political or societal topics. For example, if most or all of a user’s activity is dedicated to refuting the “official Western narrative” of the Russian annexation of Crimea, it may be a synthetic actor.

9. Synthetic actors often use awkward phrases or sayings that are not present in common English. Because such accounts are often controlled by non-native English speakers, their posts may include poorly translated idioms from their managers’ native languages. For example, a Russian-controlled account may write that someone is “making an elephant out of a fly” — the literal translation of a Russian idiom meaning “to exaggerate.”

10. Synthetic actors frequently make grammatical mistakes which are not typically made by native English speakers. For example, a suspected Russian-controlled cyborg account wrote “I thought you were against the wars” instead of the more natural “I thought you were against wars/war.” This mistake was likely due to the absence of indefinite (or definite) articles in the Russian language.

11. Synthetic actors often have little to no interaction with genuine users. Humans have friends, whereas trolls and bots do not. Genuine Twitter users will occasionally mention real-life friends or colleagues in posts, typically by linking to their profiles (i.e., “tagging” them). Synthetic actor accounts do not represent real people and thus lack the social connections which are indicative of legitimate profiles.

12. Synthetic actors often do not have a profile picture at all. Genuine users typically upload profile photos to their accounts. Synthetic users, probably in an attempt to save time and effort, regularly lack such a photo entirely.

13. Synthetic actors are almost always extremely partisan. There is no room for moderation in the world of bots and trolls—their job is to convince the target audience that their opinion is the only valid one. It is, however, worth noting that this factor is the least indicative of synthetic actor behavior, since tens of millions of genuine users are also zealously politically one-sided on social media.

Collection Methods

Collection was undertaken using DiscoverText, which conducted a raw pull from the Twitter API. The raw pull of the Twitter API includes 31 categories of data; our research focused primarily on the Tweet text, the date the Tweet was posted, the user who posted the Tweet, and that user’s creation date. From a collection of over 850,000 tweets, we closely analyzed 3,740 from 3,081 unique users, between the dates of March 28 and May 5, 2018. Tweets analyzed met two filters—they were in reply to “@realDonaldTrump” and they contained one or more of the following terms: “chemical attack fake,” “chemical attack false flag,” “chemical attack staged,” “chlorine,” “douma fake,” “douma false flag,” “douma staged,” “soros false flag,” “soros syria,” “soros white helmets,” “syria false flag,” “syria staged,” “trump false flag,” or “white helmets.”

Data from before the April 7, 2018, attack date is the result of DiscoverText’s broad collection. Only six tweets in the dataset were posted before April 7.
Analytical Methods

After exporting the data, we conducted several quantitative queries looking for any significant trends or outliers that would point to inorganic activity. The most conspicuous of these was a timeline of account creation dates, which was generated by importing all unique users and their creation dates into the data visualization software Tableau.

We then created a 10% randomized sample of all unique Twitter users from our dataset and coded them into the following typology:\(^5\)

1. **Troll** – A Twitter user that operates as an undeclared state actor, usually masquerading as an average westerner expressing personal political opinions, while participating in some level of coordination to circulate state-sponsored narratives.
2. **Bot** – A fully automated Twitter account, engaging in content creation or perpetuation solely based on a software script.
3. **Cyborg** – A Twitter account that mostly operates based on automated script behavior, but that is taken over and operated by a human user occasionally.
4. **Suspended** – An account permanently suspended based on Twitter terms of use violations.
5. **Uncertain** – An account that has either been deleted, made private, or has a tweet history which is too ambiguous to confidently classify.
6. **Typical User** – An account that engages in organic behavior on Twitter. Typical users participate in the conversation by their own will and express their personal political opinions.

Limitations

- In May and June 2018, Twitter purged an estimated 70 million accounts that it suspected to be bots or to be generating spam.\(^6\) By the time of our analysis in June and July 2018, many accounts that we classified as “Suspended” probably would have otherwise been classified as synthetic actors. Therefore, we believe that our synthetic actors figures may be slightly conservative.
- Classifying our sample dataset into the synthetic actor typology is an intrinsically subjective task. Because of the ambiguous nature of coding these accounts, we assess that our synthetic actor figures have a non-negligible margin of error.

\(^5\) Bradshaw and Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.*

\(^6\) Craig and Dwoskin, “Twitter Is Sweeping out Fake Accounts like Never Before, Putting User Growth at Risk.”
Trends and Statistics

Figure 1. Ratio of synthetic actors present in the general Syrian chemical weapons counternarrative conversation.
Figure 2. Graph mapping the creation dates for unique users who were collected as part of our filter. Several important dates annotated with correlated peaks. Timeframe of interest indicates the 10 days following the chemical attack in Douma.
Figure 3. Ratio of synthetic actors in accounts created during time frame of interest, the period directly following the chemical attack in Douma. Note the large ratio of suspended accounts only three months post-creation.
User Descriptions Word Frequency

The below tables and word cloud represent the most frequently used words in the Twitter user descriptions of users promoting a counternarrative to Syrian chemical weapons nonproliferation issues during the relevant collection timeframe.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Text</th>
<th>Word Count</th>
<th>Rank</th>
<th>Text</th>
<th>Word Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MAGA</td>
<td>170</td>
<td>26</td>
<td>Retired</td>
<td>53</td>
</tr>
<tr>
<td>2</td>
<td>Love</td>
<td>163</td>
<td>27</td>
<td>Time</td>
<td>53</td>
</tr>
<tr>
<td>3</td>
<td>Trump</td>
<td>145</td>
<td>28</td>
<td>Lover</td>
<td>51</td>
</tr>
<tr>
<td>4</td>
<td>Politics</td>
<td>123</td>
<td>29</td>
<td>People</td>
<td>51</td>
</tr>
<tr>
<td>5</td>
<td>Truth</td>
<td>107</td>
<td>30</td>
<td>Father</td>
<td>50</td>
</tr>
<tr>
<td>6</td>
<td>Life</td>
<td>94</td>
<td>31</td>
<td>Liber</td>
<td>49</td>
</tr>
<tr>
<td>7</td>
<td>God</td>
<td>91</td>
<td>32</td>
<td>Human</td>
<td>47</td>
</tr>
<tr>
<td>8</td>
<td>Anti</td>
<td>85</td>
<td>33</td>
<td>Veteran</td>
<td>46</td>
</tr>
<tr>
<td>9</td>
<td>Patriot</td>
<td>83</td>
<td>34</td>
<td>Twitter</td>
<td>45</td>
</tr>
<tr>
<td>10</td>
<td>American</td>
<td>79</td>
<td>35</td>
<td>Anime</td>
<td>45</td>
</tr>
<tr>
<td>11</td>
<td>Conservative</td>
<td>79</td>
<td>36</td>
<td>Fan</td>
<td>43</td>
</tr>
<tr>
<td>12</td>
<td>New</td>
<td>78</td>
<td>37</td>
<td>America</td>
<td>41</td>
</tr>
<tr>
<td>13</td>
<td>World</td>
<td>76</td>
<td>38</td>
<td>Resist</td>
<td>40</td>
</tr>
<tr>
<td>14</td>
<td>Christian</td>
<td>76</td>
<td>39</td>
<td>Up</td>
<td>39</td>
</tr>
<tr>
<td>15</td>
<td>Live</td>
<td>75</td>
<td>40</td>
<td>President</td>
<td>39</td>
</tr>
<tr>
<td>16</td>
<td>Proud</td>
<td>73</td>
<td>41</td>
<td>Make</td>
<td>38</td>
</tr>
<tr>
<td>17</td>
<td>Pro</td>
<td>73</td>
<td>42</td>
<td>Man</td>
<td>38</td>
</tr>
<tr>
<td>18</td>
<td>Right</td>
<td>71</td>
<td>43</td>
<td>Work</td>
<td>38</td>
</tr>
<tr>
<td>19</td>
<td>Country</td>
<td>70</td>
<td>44</td>
<td>Freedom</td>
<td>38</td>
</tr>
<tr>
<td>20</td>
<td>Support</td>
<td>69</td>
<td>45</td>
<td>Free</td>
<td>37</td>
</tr>
<tr>
<td>21</td>
<td>Follow</td>
<td>66</td>
<td>46</td>
<td>Constitution</td>
<td>37</td>
</tr>
<tr>
<td>22</td>
<td>Family</td>
<td>56</td>
<td>47</td>
<td>Thing</td>
<td>37</td>
</tr>
<tr>
<td>23</td>
<td>Believe</td>
<td>55</td>
<td>48</td>
<td>Writer</td>
<td>37</td>
</tr>
<tr>
<td>24</td>
<td>Music</td>
<td>54</td>
<td>49</td>
<td>Stand</td>
<td>37</td>
</tr>
<tr>
<td>25</td>
<td>One</td>
<td>53</td>
<td>50</td>
<td>Against</td>
<td>36</td>
</tr>
</tbody>
</table>

*Table 1. Most frequently used words.*

7 We assess that this phrase was improperly parsed by the word count analysis software. It was most likely part of “liberty,” “libertarian,” and/or “liberal.”
The vast majority of words and phrases found in the description sections of counternarrative Twitter users’ profiles are typically associated with ideologically right-leaning Americans. It is worth noting that we encountered very few left-leaning users (genuine or synthetic) who engaged in counternarrative discourse in the Syrian chemical attack context.
Tactics

We identify several tactics as relates to tweet content, procedure, and audience that synthetic actors use in their efforts to undermine the prevailing narrative.

Content Themes\(^8\)

<table>
<thead>
<tr>
<th>Distort</th>
<th>Selectively including pieces of evidence to enhance your narrative over a competing one. Alternatively, creating evidence that gives a false representation of reality.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>‧ The Assad regime has always been transparent in calling for chemical weapons inspections at the alleged attack sites.</td>
<td></td>
</tr>
</tbody>
</table>

---

Distract - Using conspiracy theories about an incident to cast doubt on the prevailing narrative. Also, introducing doubt about the credibility of a source.

Examples:

- The West has previously lied about their justifications for wars, therefore they are likely lying about these chemical attacks.
- If there was a chemical attack, it was committed by the rebels or jihadist organizations (e.g., Islamic State or Al-Qaeda).
- The attack was committed by the CIA in order to provide a pretext to launch another war in the Middle East.

---

Charles M
@CharlesMorgn

Replying to @MaxBlumenthal @RT_com

"Trust me, we got proof" worked in the Iraq war.
Turned out to be a lie.
"Trust me" wont work again, so unless they SHOW proof, I will assume they have NONE. They are a bunch of warmongers blind to the fact that a full scale WW3, which they are pushing for, will KILL US ALL!

11:08 AM - 15 Apr 2018

---

Dismay - Trying to intimidate an opponent by warning of the dire consequences of action.

Examples:

- US intervention in Syria would lead to the outbreak of World War III with Russia.
- If the United States bombs Russia’s ally Syria, Russia will sink a US aircraft carrier in response.
- The United States would be acting against its interests by bombing Syria because doing so would assist Islamic State.
Blake Minger
@MingerBlake

Replying to @realDonaldTrump @Cabinet @WhiteHouse

What the hell are you doing? This was another false flag attack by our rebels not Assad. Wake up people they are trying to start WW3. This war would be an extinction level event. No more ISIS False Flags. Take us out of Syria!! #Vets4PeaceInSyria #FakeWars #TrumpIsANeoCon #EndWar

3:13 PM - 9 Apr 2018
Dismiss - Rejecting the allegations by attacking the critic as opposed to the substance of their argument.

Examples:

- The White Helmets staged the attack in order to bait an attack against the Syrian regime.
- The Organization for the Prohibition of Chemical Weapons is a Western-dominated organization that will be biased against the Syrian regime in its inspections.
- The West is not interested in verifying these allegations as it was waiting for a reason to launch a war.

Clearly, a single piece of disinformation may be classified into several of these categories; an effective synthetic actor will employ two, three, or four of them. In the context of the Syrian chemical weapons attack disinformation campaign, the synthetic actors have integrated these themes into a broad strategy to ensure that their messaging takes root and proliferates.
Procedural Tactics

Synthetic accounts employ a number of methods to best convey their messages. These strategies that seek to exploit the platform most effectively are referred to here as “procedural tactics.”

- **Synthetic actors primarily attempt to enter the conversation by responding to high-influence individuals,** such as Donald Trump, Emmanuel Macron, or popular political commentators. In doing this, their content is seen by those who are most interested in these figures’ posts and thus they are able to most effectively influence specific political bases.
  - Moreover, **synthetic actors are useful in swaying the perception of public opinion** as observed by outside analysts seeking to understand political discourse on a given topic. For example, a news agency, political consultant, or pollster may be misled by synthetic actors after reading the comments under the president’s tweets in order to gauge his base’s views on a matter.
- **Synthetic actors often attempt to create influential content by participating in popular internet culture,** such as by creating “memes” that contain their messages. This tactic makes it more likely that their content will “go viral” and be seen by a significantly larger audience than would see it otherwise.
- **Synthetic actor bot accounts often engage in commercial activity until a salient political event occurs** for which they can be utilized. In this context, these bot/cyborg accounts can be understood as long-term resources which can be activated at a convenient time.
- **Synthetic actors frequently purport to be US military active duty troops or veterans,** almost certainly in order to elicit sympathy and build credibility among a broad swath of the American public. We assess that the managers of these accounts have correctly determined that the US military has very high favorability ratings across the country and that many Americans believe that those with a past or current military affiliation are an authoritative voice on issues of foreign conflict.
  - Synthetic actors that can be classified as **troll accounts are often short-term resources deployed for breaking political situations.** They may only tweet less than a dozen times and then go dormant with no further activity.
  - When discussing political events, **synthetic actors generally masquerade as reluctantly disillusioned supporters of President Trump** who disagree with his stance on launching strikes.
    - We assess that they do this in order to overcome the initial mental barrier that political supporters have when reading critical content. They believe that the synthetic actor is “one of them” and not “liberal,” who only seeks opportunities to criticize the President.
- **Synthetic actors can engage in a mix of domestic and foreign propaganda on their accounts.** We observed that they promote pro-Vladimir Putin domestic Russian news stories while claiming to be genuine Western Twitter users.
- **Bots demonstrate a symbiotic relationship with each other.** In order to generate the impression of engagement, they will retweet and “like” each other’s posts.

---

Target Audiences

- The synthetic actors’ target audience was most often supporters of the president in an attempt to undermine the domestic political support for a strike against the Syrian regime.

- We occasionally identified synthetic actors targeting Western European political audiences, such as in attempts to dissuade a coalition strike.

- In our sample of Syria-related tweets responding to President Trump, we found no significant attempt to engage with left-leaning political audiences.
  - This is consistent with our assessment that the synthetic actors’ goal in this context was to discourage a strike by agitating the president’s base.

- The synthetic actor accounts had significant engagement and narrative cross-over with accounts promoting Infowars.com content. The content was specifically from Alex Jones, the main personality of Infowars, and Paul Joseph Watson, the Infowars editor-in-chief.
  - Infowars has previously been shown to repackaging and distribute Kremlin narratives that originated on explicitly state-controlled sites.\(^\text{10}\)

- Synthetic accounts can also be seen responding to actors in the media or policy circles who promote the mainstream Western narrative of Assad’s culpability for the attack. Synthetic actors introduce a counternarrative in an attempt to sow doubt.

---

Profiles

The below profiles are examples of accounts that have, based on our analysis, an extremely high likelihood of being synthetic actors.

@12wewvT5dWLwtyK
-likely Cyborg

The random alphanumeric username of this account is the primary indicator of its synthetic nature. A reverse image search of its profile image reveals that it was taken from a photo of a UK fashion model, another strong indicator that this account warrants further examination.
A cursory examination of the user’s tweets reveals that the user almost solely engages in posting links and retweeting domestic Russian political content. These links lead to a number of questionable commercial sites and fake news articles. The vast majority of the content has no relation to foreign influence operations and the account appears to primarily be a commercial bot account.
Альбина Султанова @12wewvT5dWLwtyK - Feb 7
Польза зеленого чая zen.yandex.ru/media/oldlekar...

Альбина Султанова @12wewvT5dWLwtyK - Feb 7
Польза ананаса zen.yandex.ru/media/oldlekar...

Альбина Султанова @12wewvT5dWLwtyK - Jan 19
maihov-plus.com/user/mitsmafre...
massage.ru/forum/memberli ...
krasotulya.ru/love/user/3566...
Upon examination of the user’s account during the time frame surrounding the chemical attack in Douma, it can be seen that the user’s operating behavior shifts entirely. The account engages in commercial activity up to February 7, 2018, at which point the account “goes dark” and posts no content until April 11, 2018, immediately following President Trump’s tweet announcing his intention to launch a missile strike against Syria. The account begins to post numerous tweets responding to the president and introducing a counternarrative.

The rapid switch from evidently automated link posting to tailored political responses in English indicates that this account is a synthetic actor of the cyborg type. The account operates as a bot for the majority of its
lifespan, but switches to tailored content following a salient event. This suggests that the owner of the account likely took over control from the automated script in an attempt to influence US political discourse. It is possible that whoever is controlling these accounts keeps a large number of bots ready for deployment when needed. In the interim, the owner makes use of them by exploiting them for commercial purposes.
To better understand the operation of this cyborg account, we created a network map of the user’s interactions. It revealed that the account frequently mentioned the Russian opposition leader Alexei Navalny. Further examination showed these mentions to be antagonistic. The map also revealed that the account was in a symbiotic relationship with another bot/cyborg account. These accounts frequently engaged with each other’s content in order to cross-promote. A map of the second user revealed that it was tied to the hashtag “FreeMariaButina,” a campaign currently being promoted by official Russian sources.¹¹

¹¹ Maria Butina, a Russian national residing in the United States, was arrested in July 2018 on charges of acting as unregistered foreign agent. Accounts officially attached to the Russian government have launched an online campaign, including the hashtag, alleging her innocence and calling for her release.
Both the random character user name and the fake profile image indicate a high likelihood of the user being synthetic.

This user engages in generic commercial activity posting addresses through which funds can be routed.
The account reposts popular music videos with requests for money in the description of the videos.
Following the chemical attack in Syria, the user transitioned to posting counternarrative content. However, unlike the previously examined cyborg account, the content posted is not a tailored message. It reposts a link to counternarrative YouTube videos multiple times.
The user continues posting links to the same video, responding to different users—President Trump and the US State Department for example—in order to maximize exposure. This type of counternarrative behavior is indicative of full automation. The change to Syria-related content was likely done when the account’s owner wrote a new script for this video to be posted in response to certain HII’s tweets.
A continuation of automated, Syrian themed posting activity.
The user would later go on to engage in counternarrative activity following the Russian Novichok incident in Salisbury, England.
Here we see a transition to a new strategy in which the bot reposts links that are aimed as framing Russia and Putin in a favorable light. Throughout the middle of 2018, the user posted high volumes of content that purport to demonstrate the strength and prestige of the Russian Federation.

Building on the above strategy, the user promoted content that showed Putin’s successful preparation and execution of the 2018 FIFA World Cup.
In many ways, this user exemplifies a large subset of foreign troll profiles on Twitter. Its description, as well as its header and profile photos, suggest that the owner lives in the American South and demonstrates extreme patriotism, including themes of gun rights activism and religiosity. The account’s final non-reply tweet, posted three months before our July 2018 analysis, is a simple pro-Putin message. It is worth noting that the account was created in March 2018 and became inactive in April 2018, indicating that the manager disposed of the account after it was no longer politically useful.

An examination of this account’s history led us to discover that the user had changed its profile photo multiple times over the course of the account’s short history, each time posting a tweet with the caption “#NewProfilePic.” One of these changes stood out to us: a picture of man’s legs facing outward from a camping tent.
The user was clearly attempting to convey that he was the one behind the camera in the camping image, lending legitimacy to his account. A reverse image search of the profile picture revealed it first appeared on the Instagram account “igorcibulsky.” The account appears to belong to a Russian nature photographer with a substantial, primarily Russian, following.
The fact that the deceptive profile picture was taken from a Russian account strongly indicates that @RDJ641 is a synthetic actor.
The top tweet in this combined example interweaves several counternarrative themes mentioned earlier in this text. The lower tweet in this example demonstrates another common theme: the use of US armed forces or veteran identity to lend credibility to counternarratives in the context of military action.
This tweet falls under the “Dismay” tactic. The tweet’s recipient—the Bulletin of the Atomic Scientists—releases updates of its “Doomsday Clock,” a symbolic measure of how close civilization is to destruction. This troll is thus alluding to an apocalyptic nuclear war which would result from US intervention in Syria.
This tweet exemplifies a tactic which we occasionally observed in our analysis. The likely troll exploits President Trump's 2013 tweet advocating Congressional approval for a would-be Syria strike to frame the president as a hypocrite. Moreover, it touches on another common theme—that the Trump administration is controlled by “globalists” who actually determine White House decision making. A final consideration is that this tweet is in reply to Fox News, a popular right-leaning American news network. This tactic of addressing right-leaning audiences is in line with our finding that in the Syrian chemical weapons context, managers of troll accounts prefer to address conservative Americans to increase the chance that their messages affect change.
This April 11, 2018, tweet again falls into the “Dismay” category, as well as suggesting that the Assad regime acts as a bulwark against jihadism in Syria. Moreover, it invokes the consequences of past US military policy failures to deter similar regime change efforts in Syria.
Finally, this tweet demonstrates the connection between Russian troll networks and Infowars, which we frequently observed, as mentioned previously.

**Figure 6. Tweets over time and by type. Generated by Socialbearing.com**

It is important to note that this account began tweeting at exceptionally high volumes in the wake of President Trump’s announcement of a planned missile strike in Syria. Moreover, the account almost
exclusively tweets replies rather than standard tweets, suggesting that the user is attempting to engage with HIIs to have its counternarrative messages gain traction.

The user’s tweets also led us to identify another likely troll that we determined to be within the user’s same network. On April 12, the user quoted a tweet by user @Migxp1. This user claimed to be from Michigan and frequently posted zealously religious, Christian content. However, the user’s full history made us question his purported location and legitimacy. During the week following the chemical attack in Douma, the user posted over 100 pro-Assad tweets. Including:

These tweets, combined with other factors in his account, led us to conclude the user was a likely synthetic actor. The fact that the @RJD641 was promoting him, indicated they were likely in one troll network.
This user who was captured in our collection met some characteristics for a troll: his name is more random than one would expect from a genuine user, and he lacks a profile image. The user’s first tweets immediately followed the chemical attack in Khan Sheikhoun, Syria, in April 2017.
In these tweets, the user masquerades as a disillusioned supporter of President Trump and lays the foundation for continued introduction of counternarratives.

After the above tweet, the user fell dormant for four months before re-emerging to join the counternarrative conversation about potential strikes on Syria. As of our analysis in August 2018, the April 15, 2018, tweet was the user’s last.
This user provides another strong candidate for a synthetic actor. The user engages in the strategy of distraction by attempting to divert attention to another matter. His name also lines up with our indicative factors in that it includes a high degree of randomness. Furthermore (but least conclusively), the user lacks a profile image.

In this tweet, the user repeats the last message but in French, this time directed towards French President Emmanuel Macron. A native French speaker on our team concluded that the French in this tweet is “unnatural,” and almost certainly written in another language and then translated into French.
The user also engaged in reposting counternarratives in Italian, suggesting that he was attempting to engage in influence operations across Western Europe.
Results

Counternarratives surface on official US platforms

Richard N. Haass @RichardHaass · Mar 23
@realDonaldTrump is now set for war on 3 fronts: political vs Bob Mueller, economic vs China/others on trade, and actual vs. Iran and/or North Korea. This is the most perilous moment in modern American history—and it has been largely brought about by ourselves, not by events.

Jackson County GOP @JacomogOP

Replies to @RichardHaass @realDonaldTrump

Where's the "Wow" button! The past 70 years of bullying everyone around world under the auspices of the new world order has brought us to this place. In fact @RichardHaass and the CFR are responsible for pushing propaganda that has created unrest. Destroy the Deep State! #Trump2020

8:42 PM · 11 Apr 2018
In our collection, we discovered two tweets from an account claiming to represent the Republican Committee of Jackson County, Missouri. The tweets contained counternarratives similar to those spread by our synthetic actors of interest. We reached out to the Committee to confirm authenticity of the account and a senior official verified that it was the official account of the Committee. While it is impossible to trace how the counternarratives entered official discourse, it cannot be discounted that synthetic actors, who, during this timeframe, composed a significant portion of counternarrative discussion, may have been the origin.
Concluding Remarks

Social media has transformed the modern political information environment. While previously, citizens were two to three steps away on the information cascade from influencing the administration’s narrative, now a linear plane exists. The administration can bypass the media to transmit its narrative directly to citizens, and citizens can reply directly with their own. Consequently, this has created opportunities for information and media manipulation that were unimaginable a decade ago. It is now possible to infiltrate domestic political discourse through the mass creation of disposable, synthetic accounts. This study has illuminated one example of this new strategy in operation. It is evident that, following the suspected use of chemical weapons by the Syrian regime, their ally, the Russian Federation, acted in an attempt to deter the use of military force by the United States. Although ultimately unsuccessful, their operational narratives abounded in the discourse among the American political right.

Synthetic actors, potentially making up to 16% of all Syrian chemical attack counternarrative users, were fairly prolific in the counternarrative conversation on Twitter in the wake of the April 2018 chemical attack in Douma, Syria. However, nearly half of Twitter accounts created in the immediate aftermath of this attack propagated counternarratives about it, and thus were likely synthetic actors. Without further research, it is not possible to know the extent these synthetic actors incited a wider Syrian chemical attack counternarrative conversation among genuine Twitter users and citizens more broadly. However, it seems reasonable to assume that at least some sectors of the domestic Western populace were affected by the discourse.

The analyzed synthetic actors employed a number of tactics to disseminate their messages, which typically followed a seemingly standardized set of themes. Tweets were addressed to prominent public figures and politicians to garner a wide audience and used popular internet culture and a purported military affiliation to increase share potential and credibility. Moreover, when disapproving of President Trump’s actions, these synthetic actors posed as supporters who disagreed on an individual policy decision, likely in an attempt to seem like “one of us” to members of the president’s political base. On several occasions, we observed synthetic actors joined in reciprocal relationships in which accounts would retweet and/or “like” other synthetic actor accounts’ posts, suggesting the existence a network of coordinated activity.

Synthetic actors’ counternarrative tweets surrounding the Douma attack fell into a relatively narrow set of themes. Many posts focused on domestic concerns through discrediting Western (especially US) government institutions by alluding to past intelligence failures and suggesting the existence of a “Deep State” that manipulates the president. Other tweets sought to deter a US strike on Syria by raising fears that jihadists (especially Islamic State and Al-Qaeda) would benefit or that such jihadists were the true culprits of the chemical attack. More still attempted to intimidate by suggesting that “World War III” would erupt after continued escalation between Russia and the United States over a strike on Syria.

---

Social media has become a weapon of political conflict. In recent years, news and research about influence operations aimed at sowing discord and division in populations has become ubiquitous. However, government social media manipulation is not restricted to such strategic operations. Our research has revealed an example of a more narrow, short-term, and tactical online influence campaign; since they were no longer useful, many discovered synthetic actors’ accounts fell dormant nearly immediately after the joint US–UK–French strike against Syrian chemical weapons facilities. Due to its relatively modest cost and potentially massive payoff, we assess that states and even non-state actors will be highly incentivized to employ such platforms and techniques. Therefore, we can expect more of such short-term, ad hoc influence campaigns as new political events transpire.
Author Bios

**Jack O. Nassetta** is a student of political communication and history at The George Washington University. He focuses on the transformation and manipulation of communication on the internet. During 2018, he was a visiting fellow at the James Martin Center for Nonproliferation Studies in their Summer Undergraduate Nonproliferation Program.

**Ethan P. Fecht** is a former military intelligence analyst and current student of international relations at Brown University. He specializes in the intersection of new technologies and traditional security issues. During 2018, he was a visiting fellow at the James Martin Center for Nonproliferation Studies in their Summer Undergraduate Nonproliferation Program.

Acknowledgements

The authors would like to thank Tom and Sarah Pattison for their generous funding of young researchers; Professor Steven Livingston at The George Washington University, for providing the inspiration that became this project; Dr. William Potter, for his guidance; Masako Toki, for her commitment to the CNS Summer Undergraduate program; Stu Shulman at DiscoverText, for his generosity; Ariel Du Temple, for her assistance with translations; Rhianna Tyson Kreger, for guiding us from paper to publication; and Kirk Nassetta and Theresa Ferryman for their unwavering support.
#37 • All the World is Staged: An Analysis of Social Media Influence Operations against US Counterproliferation Efforts in Syria

#36 • North Korea’s Information Technology Networks

#35 • Countering North Korean Procurement Networks Through Financial Measures: The Role of Southeast Asia

#34 • Open-Source Monitoring of Uranium Mining and Milling for Nuclear Nonproliferation Applications

#33 • WMD Proliferation Risks at the Nexus of 3D Printing and DIY Communities

#32 • Taiwan’s Export Control System: Overview and Recommendations

#31 • Revisiting Compliance in the Biological Weapons Convention

#30 • Crowdsourcing Systems and Potential Applications in Nonproliferation

#29 • The Verification Clearinghouse: Debunking Websites and the Potential for Public Nonproliferation Monitoring

#28 • Geo4nonpro.org: A Geospatial Crowdsourcing Platform for WMD Verification

#27 • Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach

#26 • 2016 Symposium Findings on Export Control of Emerging Biotechnologies

#25 • Outlawing State-Sponsored Nuclear Procurement Programs & Recovery of Misappropriated Nuclear Goods

#24 • Strengthening the ROK-US Nuclear Partnership

#23 • Replacing High-Risk Radiological Materials

#22 • A Blueprint to a Middle East WMD Free Zone

#21 • Biotechnology E-commerce: A Disruptive Challenge to Biological Arms Control

#20 • Countering Nuclear Commodity Smuggling: A System of Systems

#19 • Alternatives to High-Risk Radiological Sources

#18 • Stories of the Soviet Anti-Plague System

#17 • Ugly Truths: Saddam Hussein and Other Insiders on Iraq’s Covert Bioweapons

#16 • Rethinking Spent Fuel Management in South Korea

#15 • Engaging China and Russia on Nuclear Disarmament

#14 • Nuclear Challenges and Policy Options for the Next US Administration

#13 • Trafficking Networks for Chemical Weapons Precursors: Lessons from the 1980s Iran-Iraq War

#12 • New Challenges in Missile Proliferation, Missile Defense, and Space Security

#11 • Commercial Radioactive Sources: Surveying the Security Risks

#10 • Future Security in Space: Commercial, Military, and Arms Control Trade-Offs

#09 • The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program

#08 • After 9/11: Preventing Mass-Destruction Terrorism and Weapons Proliferation

#07 • Missile Proliferation and Defences: Problems and Prospects

#06 • WMD Threats 2001: Critical Choices for the Bush Administration

#05 • International Perspectives on Ballistic Missile Proliferation & Defenses

#04 • Proliferation Challenges and Nonproliferation Opportunities for New Administrations

#03 • Nonproliferation Regimes at Risk

#02 • A History of Ballistic Missile Development in the DPRK

#01 • Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future