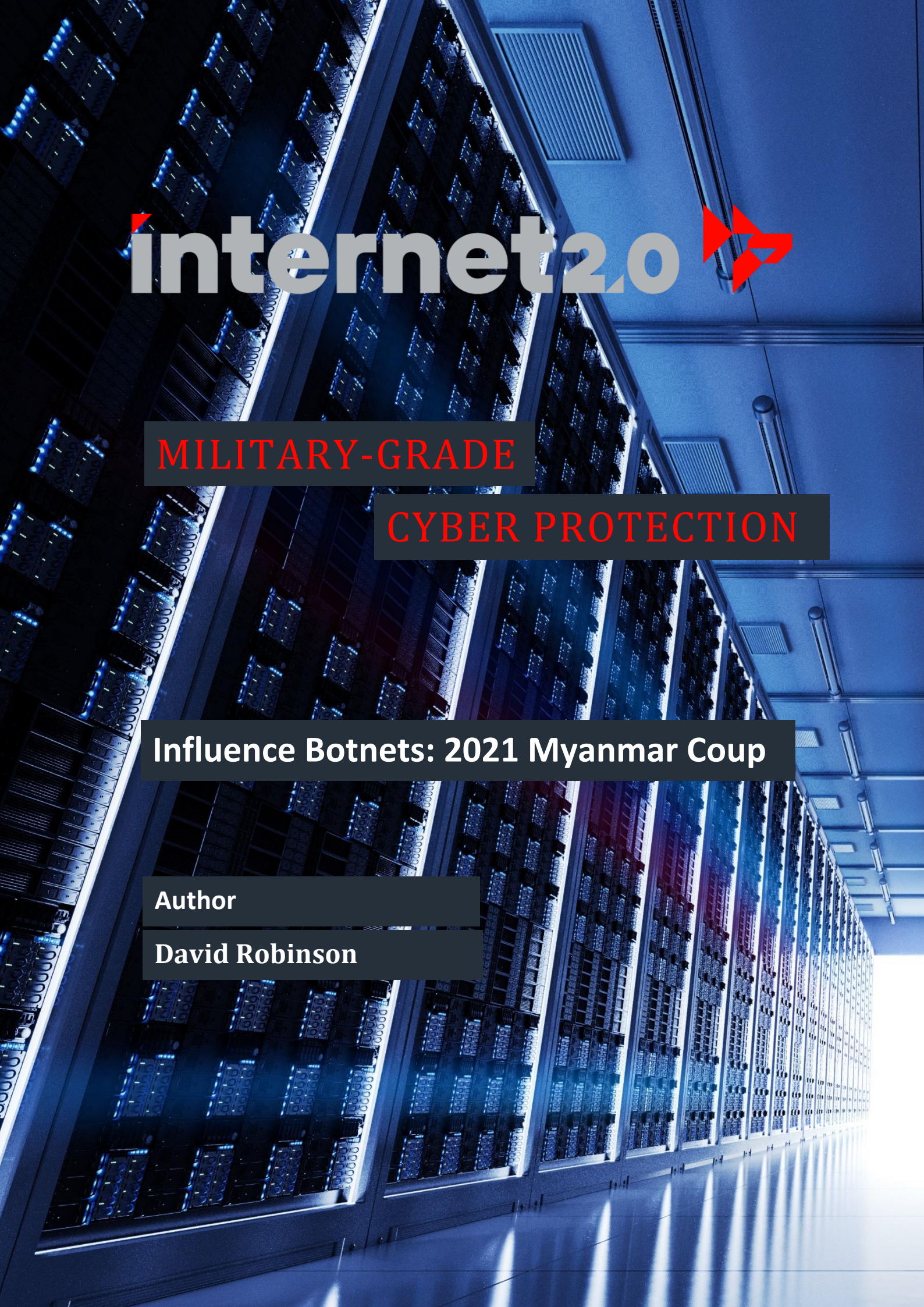

Influence Botnets: 2021 Myanmar Coup

Author

David Robinson

Table of Contents

Executive Summary

US Army's Facebook page comment section was the target of a sophisticated Influence Botnet attack from 16 to 17 February 2021, with over 3000 comments per minute (exponential algorithmic growth), calling for US military intervention into Myanmar in support of "President Aung San Suu Kyi" and "Pro-Democracy Forces", who were imprisoned by the Myanmar military after a recent landslide election victory. The Influence Botnet used 337,463 Sender User Ids and 203,032 Sender Screen Names to post images/videos (436,247; 57%), and text (327,845; 43%), overwhelming the US Army's Facebook page comment section. All 764,092 comments were classified as authentic behavior (not bots) by Facebook and the top ten USER IDs are still active today on Facebook (some accounts are private to the public). Only a handful of entities and individuals in the world maintain and operate Influence Botnets. In this paper we have chosen to make no attribution assessment due to the limited forensic evidence available at this time. Research and experts believe this capability will soon be indistinguishable from authentic behavior online and will be used as a tool of massive influence. Further research and training in this field is needed.

Data Collection and Intent

This study used data collected from commercially available social media data of the US Army's Facebook Page comment section (https://www.facebook.com/USarmy) from 0500 13 February 2021 to 0400 18 February 2021. Variables of Interest: Created Time (time of post), Message (message content), Sender User Id (unique social media message sender user id), Sender Screen Name (social media message sender screen name), and Bot (message detected as spam or not spam). The dataset is composed of 764,092 observations with 15 variables. The opinions and facts in this report are those of the authors only and nothing in this report is the official position of the US Military. It is the target in this public example of an attempted influence operation. We believe this is a good example to learn about such capabilities and to generate discussion on effective countermeasures.

Introduction

On 01 February 2021, the Myanmar military seized power and detained recently elected Aung San Suu Kyi, President Win Myint and other senior officials – declaring a "one-year state of emergency". Protests erupted across Myanmar leading to civil unrest, with the junta ordering

Twitter, Instagram and eventually the internet shutdown. On 11 February the United States imposed sanctions on Myanmar's acting president and several other military officials as nationwide pro-democracy demonstrations continued across Myanmar. On 13 February the military ordered the arrest of key leaders in the pro-democracy protests. The civil disobedience movement spread, and police continued to escalate crackdowns on the protestors. On 15 February the US Army's Facebook page experienced the first spike in their comments section related to the Myanmar Coup. 24 hours later, on 16 February the US Army's Facebook page comment section was targeted by hundreds of thousands of comments, posted by hundreds of thousands of users. This report is an exploratory analysis into the tactics, techniques, and procedures of the social media activity on the US Army's Facebook page from 15 February to 17 February.

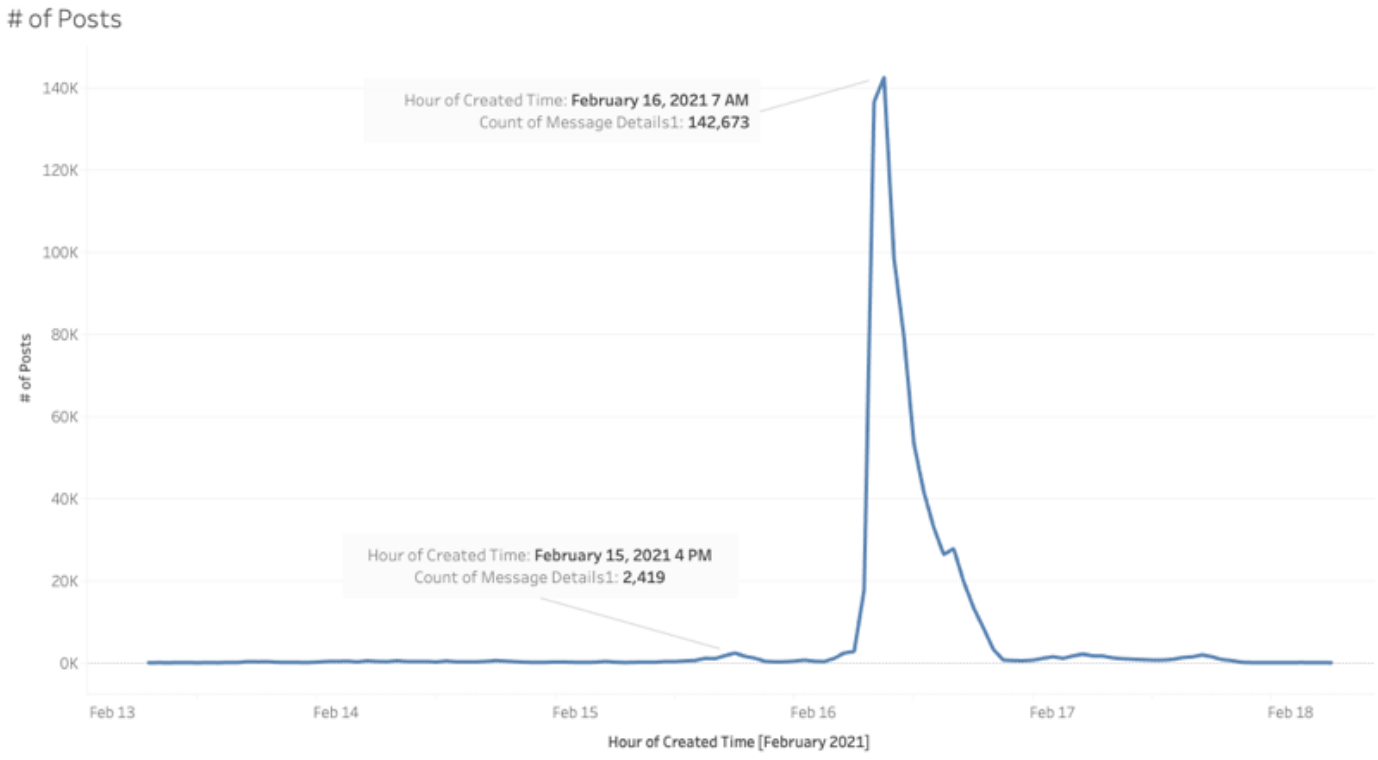

Figure 1. US Army's Facebook page comment section activity.

Figure 1 depicts the comment section activity on the US Army's Facebook page. The comment section activity initially started around 1600 on February 15 with comments peaking at 2,419 (per hour) only to subside and return on February 16 the following day, where the comments peaked at 142,673 (per hour) at 0700. Below are screen captures depicting the comment section activity on the US Army's Facebook page.

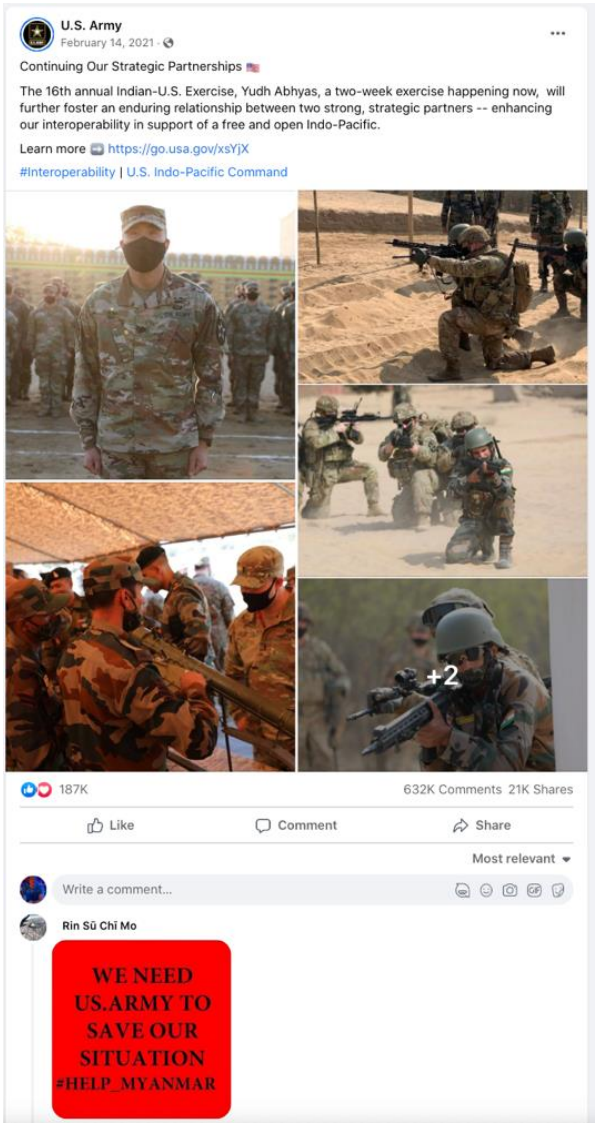

Figure 2. US Army's Facebook page comment section activity.

Figure 3. US Army's Facebook page comment section activity.

Images, videos, and text messages in the comment section stated: “WE NEED US.ARMY TO SAVE OUR SITUATION #HELP_MYANMAR”, “WE NEED US.ARMY To Save Our Situation”, “We, Myanmar People, fully support every action that UN and US take on Terrorist Dictatorship”, and “We need US Army. Please save Myanmar? Please save our country from militarycoup. Welcome for your support #RejectMilitaryCoup”. Below is a depiction of the Message variable overlayed by number of posts across time. Notably, the “NULL” message significantly dominates all other Message types. This is because the “NULL” input represents an image or video file that was posted without a text comment.

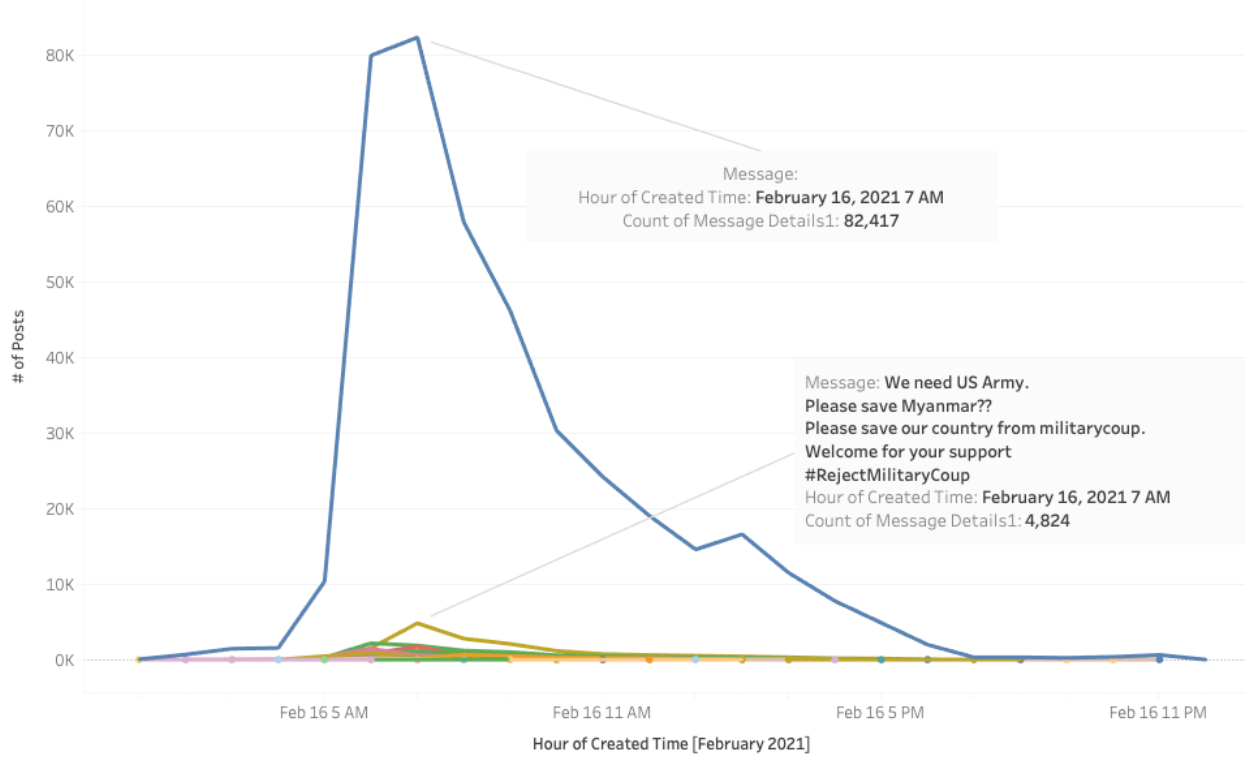

Figure 4. US Army’s Facebook page comment section activity by # of Messages across Time.

In the graphic above, at the peak of the spike, on 0700 February 16, 2021, the count was 82,417 comments (per hour) and the Message was blank (NULL). Under the blue spike the count of the next most posted comment (4,824 comments per hour) was, “We need US Army. Please save Myanmar?? Please save our country from militarycoup. Welcome for your support #RejectMilitaryCoup.” The comment section activity is unique and possibly the activity of an Influence Botnet. In the next section, we will identify and describe Influence Botnet Indicators. This is not the first time Myanmar has been associated with “inauthentic behavior” on Facebook. Reuters reported on the issue on 6 November 2020: “Facebook said it had taken down a network of 36 accounts and six pages run by a Myanmar public relations agency, Openmind,

because it said they were using fictitious people to promote the military-backed Union Solidarity and Development Party (USDP)."[1]

Influence Botnet Indicators

User Names, User IDs, and Comment Generation

Bot detection is not based on just one indicator, rather it's the combination of indicators that provides a degree of confidence to make the assessment on botnet identification. In the visualizations below, we overlayed the variables, Sender User ID, Sender Screen Names and Message to better understand the comment section activity. In Figure 5, the blue color represents "NULL", and all other colors represent various types of other text messages.

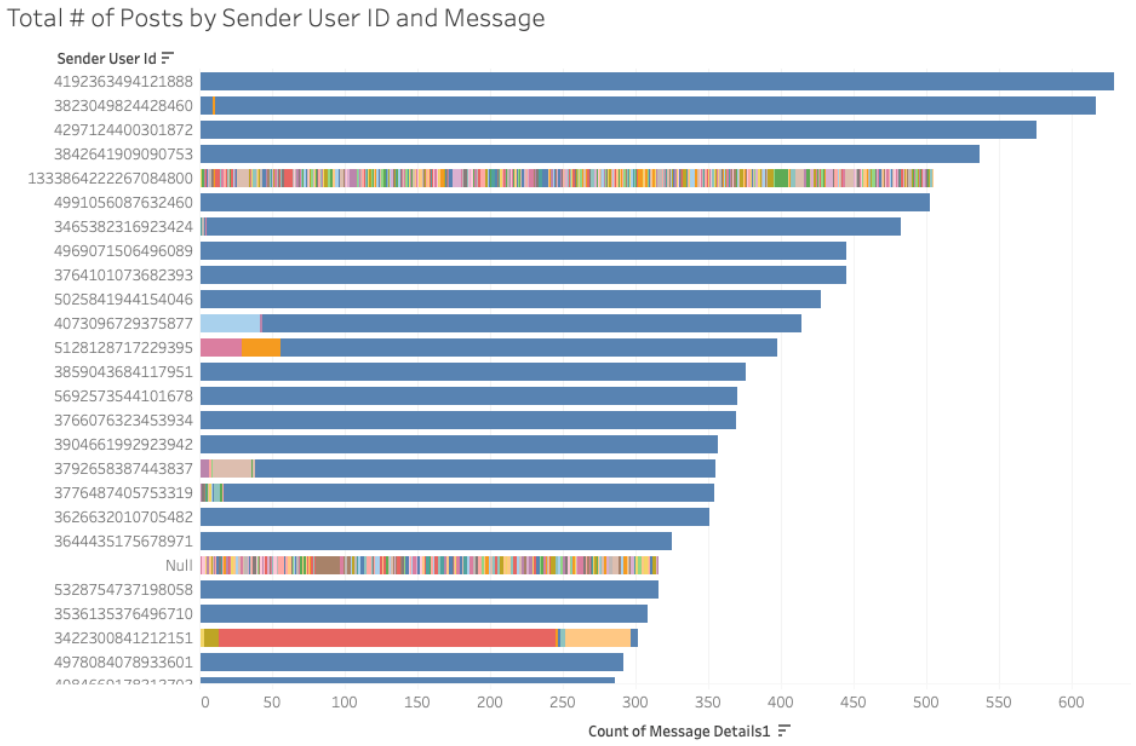

Figure 5. Total number of Posts by Sender User Id and Message.

The top Sender User Ids are as follows: 4192363494121888, 3823049824428460, 4297124400301872, 3842641909090753, 1333864222267084800, and 4991056087632460.

[1] https://www.reuters.com/article/us-facebook-myanmar/facebook-shuts-dozens-of-myanmar-pages-over-inauthentic-behaviour-idUSKBN27M1EH

The top Sender User Names are as follows: Wai Yan, Aung Aung, Ko Ko, Htet Htet, Kyaw Kyaw, Min Min, Min Khant, Kaung Kaung, Zaw Zaw, Nilar Soe Aung, and Jolly Jolly.

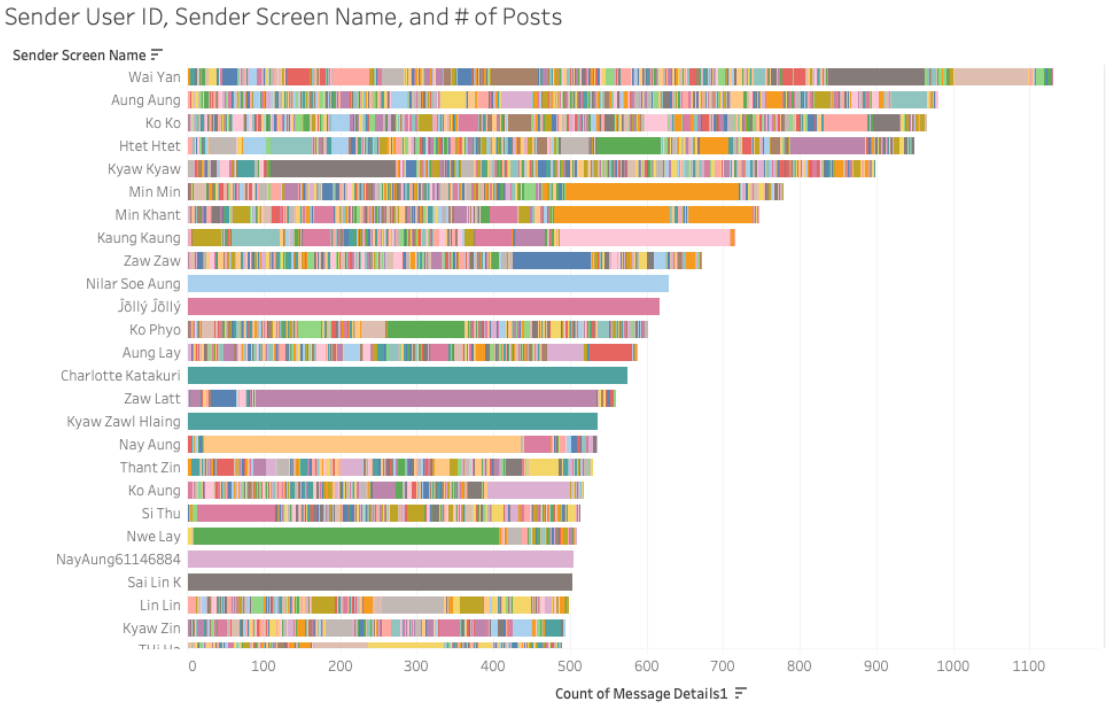

Figure 6. Total number of posts by Sender User Id, and Sender Screen Name.

Figure 6 on the previous page, clearly shows Sender User IDs were using the same exact Sender Screen Name to possibly appear as the same Facebook User. It is logical that as Facebook blocked these User IDs for spamming the US Army comment section, the Botnet created new accounts with the same Sender Screen Names to appear as the same user. Because Bot accounts are often suspended by Facebook, these accounts are often newly created, low in followers, and lacking a complete profile: all common bot indicators.

The social media activity appears to be a combination of actual user accounts and influence bot accounts, acting in coordination to manipulate Facebook's engagement algorithm and bypass its spam countermeasures. For example, in Figure 6, 395 unique Sender User Ids posted 1,311 comments under the Sender Screen Name, 'Wai Yan'; 508 unique Sender User Ids posted 981 comments under the Sender Screen Name, 'Aung Aung'; and 447 unique Sender User Ids posted 966 comments under the Sender Screen Name, 'Ko Ko'. However, Sender Screen Names 'Nilar Soe Aung', 'Jolly Jolly', 'Kyaw Zawl Hlaing', 'NayAung61146884', and 'Sai Lin K' posted all of their comments under their own unique Sender User Id. Of the top ten Sender User Id accounts by number of comments posted, all are still live and active on Facebook and Twitter.

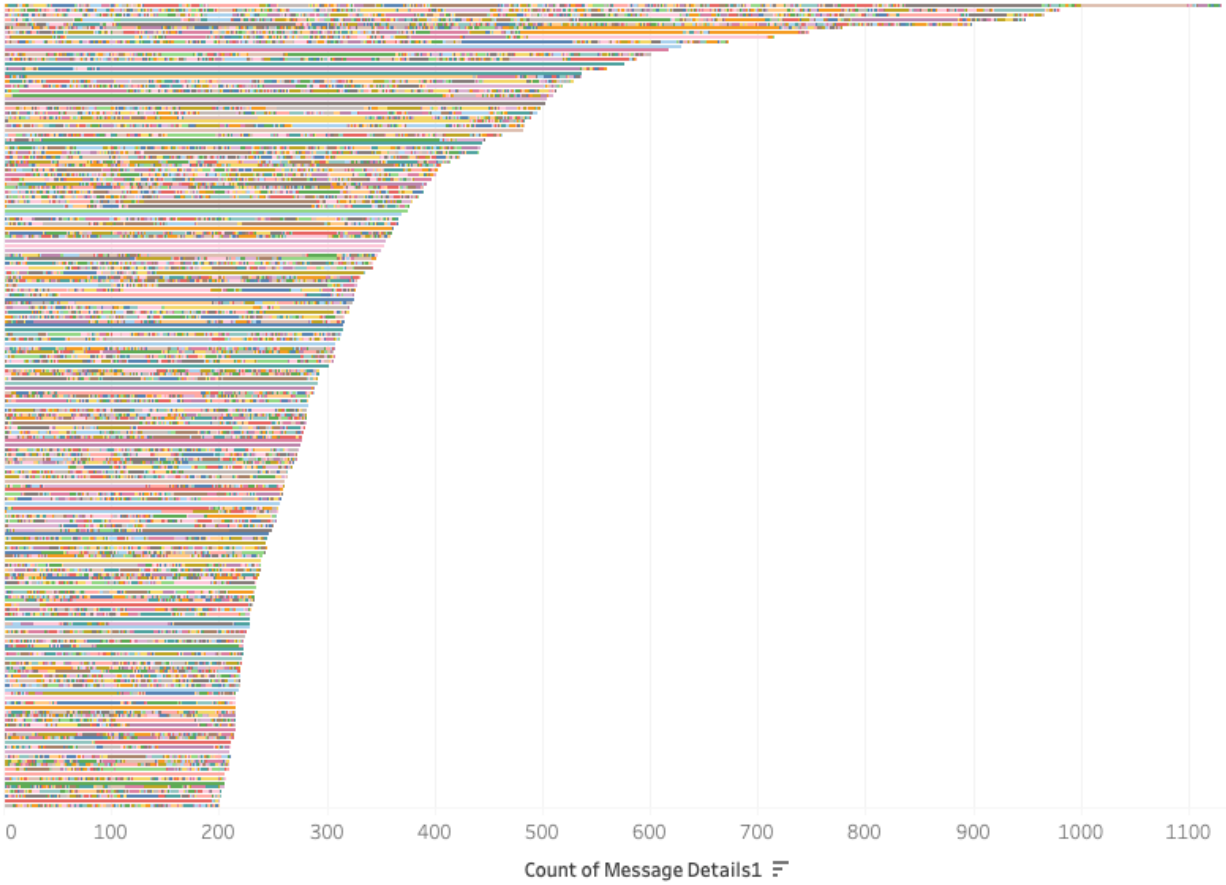

Figure 7. Number of posts by Sender Screen Name and Sender User Id.

Above, Figure 7 colorfully demonstrates the software generating User IDs against a scripted number of Sender Names, with a scripted number of unique Messages, that was possibly generated using something similar to OpenAI's GPT-3. GPT-3 (Generative Pre-trained Transformer 3) is an autoregressive language model that uses deep learning to produce human-like text.[2] GPT-3 is an example of the type of capability required to create an influence botnet. In this report we have not made any attribution assessment due to the limited digital forensics information available.

[2] https://openai.com/

Algorithmic Nature

The Influence Botnet built engagement that is in our assessment inauthentic behavior. The method in which it was built is one of the indicators that contribute to our assessment that this is inauthentic. Firstly, the number of posts per user was algorithmic. Figure 8 is a side-by-side comparison of the total comments made by Sender Screen Names and Sender User IDs. The highest message count by user is 629 and the highest message count by username is 1130. Both numbers are outside of the standard range for authentic human behavior. 629 unique comments are a lot of comments to copy and paste into a single post manually. Of the largest user count the account at some points was creating a comment every 3 seconds.

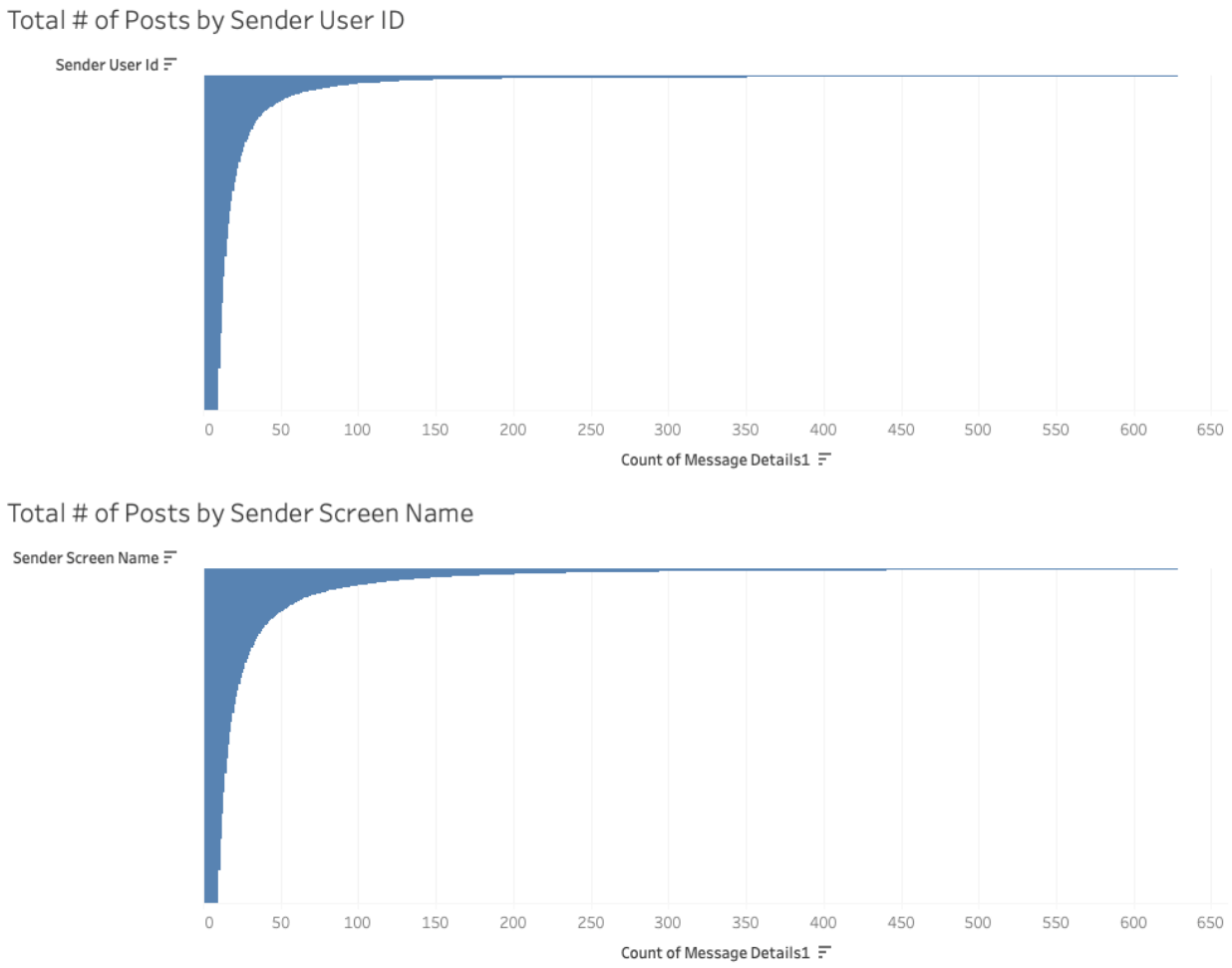

Figure 8. Distribution of Sender Screen Name and Sender User Id by Message count.

Another feature is that every single account we marked as inauthentic at the time of the content release on 16 February 2021 had zero followers while they were commenting on the Myanmar Coup. This showed that the accounts were probably made for this specific campaign. A

sophisticated feature of this capability, which gives us insight into the source code, is the foundational software characteristic of a mathematical algorithm that takes an exponential curve in its deployment of content. Genuine authentic behavior has a limiting factor defined by human limitations. For this reason, authentic behavior would be limited to the number of posts a user could create manually. Authentic behavior is generally seen as an organic growth curve or a logarithmic curve in a dataset. This is because these curves have a ceiling determined by human characteristics in this case. When we analyze the dataset we see an algorithm that deploys content in an exponential way. This is true for how it created usernames; how it manipulated usernames amongst multiple user identities to defeat Facebook's defences; and how it generated character similar content. The software is trying to mimic an authentic viral event but is immature. Figure 9 is an example of the concept of exponential curves compared to logarithmic curves. In this case the exponential curve is seen in Figures 1 when deploying content over time; in figure 7 when generating names across multiple account identities and in figure 8 when deploying similar character content.

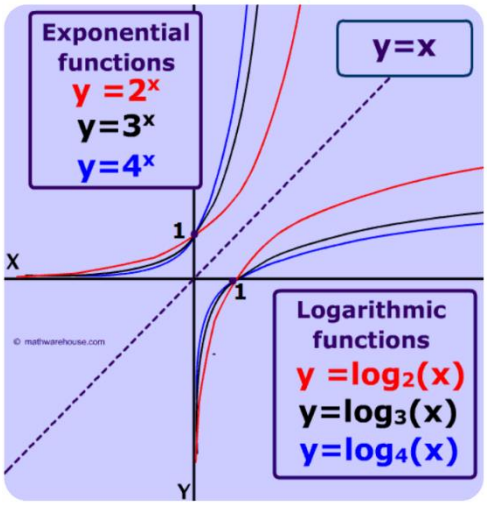

Figure 9. Theoretical curves

Character Perfect Messaging

The Messages in the comment section, along with the rate of posting strongly indicate bot activity. Figure 10 illustrates that 57% of the posts (436,247) were image or video posts without an accompanying text message. The top text post in the comment section was, "We need US Army. Please save Myanmar?? Please save our country from militarycoup. Welcome for your support #Reject Military Coup" This comment was posted 15,621 times as seen in Figure 11. Of note many of the messages had grammar and spacing errors and all were replicated thousands of times. Interesting to note the 5th, 7th and 8th highest message by count was nearly identical except for variations of the number and placement of the "??" character. This limitation of variety of content the software could produce is what we based part our assessment on in that it is what we believe to be inauthentic behavior. The replication of messages that are all character perfect (even the grammatical and spacing errors were exactly the same) and posted at an exponential rate until the attack ceased strongly indicates bot activity. As opposed to a viral growth explanation this feature indicates an influence botnet.

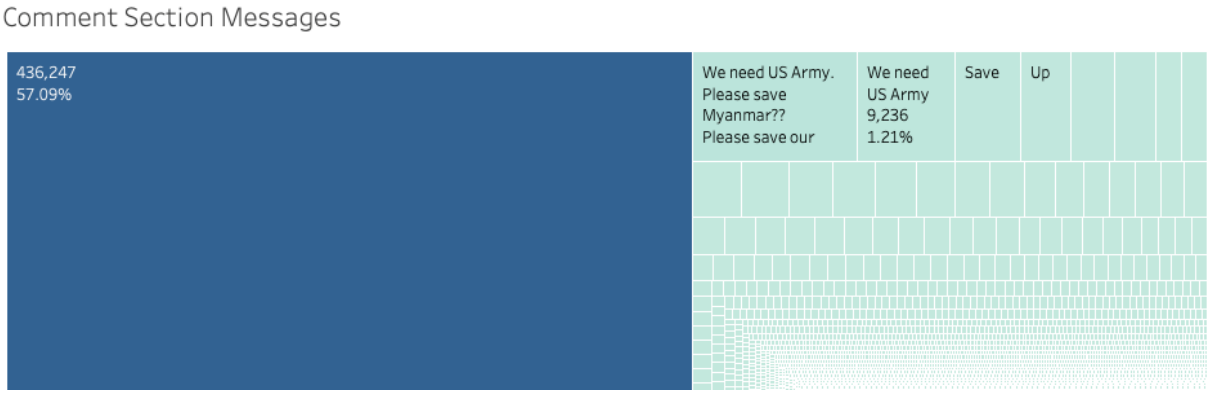

Figure 10. US Army Facebook page comment section activity, number of comments by Message.

In a recent article Harvard Professor Joseph Nye Jr. recognized the use of OpenAI's GPT-3 for Influence Botnets stating, "Generative neural networks can also create new images or texts. In 2019, the company developed a language model that trains itself by consuming freely available texts from the internet."[3] In this case, the programmers could have easily provided a working script for the AI to generate message content. He continued, "Given a few words, it (GPT-3) can extrapolate new sentences and paragraphs by detecting patterns in sequential elements…displaying intelligent behavior indistinguishable from that of a human being."[4]

[3] https://www.project-syndicate.org/onpoint/age-of-ai-and-our-human-future-review-kissinger-schmidt-by-joseph-s-nye-2021-11?barrier=accesspaylog
[4] https://www.project-syndicate.org/onpoint/age-of-ai-and-our-human-future-review-kissinger-schmidt-by-joseph-s-nye-2021-11?barrier=accesspaylog

Count of Unique Messages

Message	
We need US Army. Please save Myanmar?? Please save our country from militarycoup. Welcome for your support #RejectMilitaryCoup	15,576
Please, Save our leader Daw Aung San Su Kyi and Our President U Win Myint We Want justice We want Democracy the leaders of China &Russia support the military dictorship and are evil neighbors who are destroying Democracy we want UN and US Action urgent Help US Army #savemyanamar	4,059
Up	3,972
We need US Army	3,949
We need US Army. Please save Myanmar???? Please save our country from militarycoup. ?? Welcome for your support #RejectMilitaryCoup	3,930
Save Myanmar	2,983
Nobel prize winner, our national leader AungSanSuKyi was detained and put under house arrest by the Military. We are against the military dictatorship which ignore human rights. We citizens, who are uncertain whether the internet will be cut off again but we are still fighting for Democracy even if we disappear on social media. #CivilDisobedienceMovement ..	2,328
We need US Army. Please save Myanmar???? Please save our country from militarycoup. Welcome for your support #RejectMilitaryCoup	2,228
We need US Army. Please save Myanmar Please save our country from militarycoup. Welcome for your support #RejectMilitaryCoup	1,927
Where is our Democracy? Where is our Freedom? Where is justice for Us? #WhatsHappeningInMyanmar #JusticeForMyanmar #WhereisHumanity #Feb16Coup	1,809
We need help please helps us #Savemyabmar	1,627
We need US army	1,543
We need you, US Army! We all citizens support for every action you will take! Please help us!	1,429

Figure 11. Count of Unique Messages

Research Limitations and Implications

This influence botnet is impossible for us to attribute due to the lack of forensic information available. We have chosen not to make any hypothesis on attribution in this paper. It is hard to assess intent on the actor behind this inauthentic event without attribution. The influence botnet also used many emoji, gif and other visual media in the comments and messages. We were unable to provide specific detailed big data analysis on the trends to these visual social media messages due to the restrictions in the dataset and the data ingest process. The standard assessments on who is behind these types of capabilities focus on either influence operations or advertising fraud. For this reason, this topic should be of significant interest to both the military in the fact they were the target as part of the US Government but also the Department of Justice. As these capabilities increase in sophistication the ease for actors to perpetrate advertising fraud is likely to increase. This is a governance and compliance risk for any social media platform.

This cyber weapon was built to sway discourse and influence the information environment. It was a huge number of bots pulled together to push this message in comments across the US Military's social pages. It is backed by software which we believe is in its infancy and when matured will become a serious threat to democratic speech online. This threat will have capability to drown out genuine political speech and make most forms of media redundant. It is a threat to both democratically established institutions and politicians as it could sway the public discourse by amplifying a voice in the majority. This type of capability can be wielded by an individual or an autocracy with the intent to harm democracy.

It is important to be aware of such capabilities because in our opinion the strategic advantage that controlling the dominant narrative has in military operations has only been demonstrated yet again in the conflict between Russia and Ukraine. Often cyber weapons have been pigeonholed in terms of intelligence collection or their technical characteristic as a "Zero Day". As we have experienced during disinformation campaigns over the Covid-19 pandemic and now the Russian invasion of Ukraine is that in our assessment a capable influence botnet is in fact strategically equal to the most dangerous categorized cyber weapons reserved for malware designed to wreck a catastrophic disruption on a critical infrastructure target. This is because high morale is a prerequisite for any victory in conflict and the influence botnet is designed to target morale. In conclusion in our opinion it is important to track and identify such capabilities. Collectively we must strive to share identifying features of such capabilities as they become more prevalent in use.


internet2.0
MILITARY-GRADE
CYBER PROTECTION
Australia
Level 1
18 National Circuit
Barton ACT 2600
ABN: 17 632 726
United States
Suite 100
211 N Union St
Alexandria 22314
EIN: 86-1567068
contact@internet2-0.com