INDIANA UNIVERSITY

OBSERVATORY ON SOCIAL MEDIA

Suspicious Twitter Activity around the Russian Invasion of Ukraine

OSoMe White Paper, 10 March 2022

Introduction

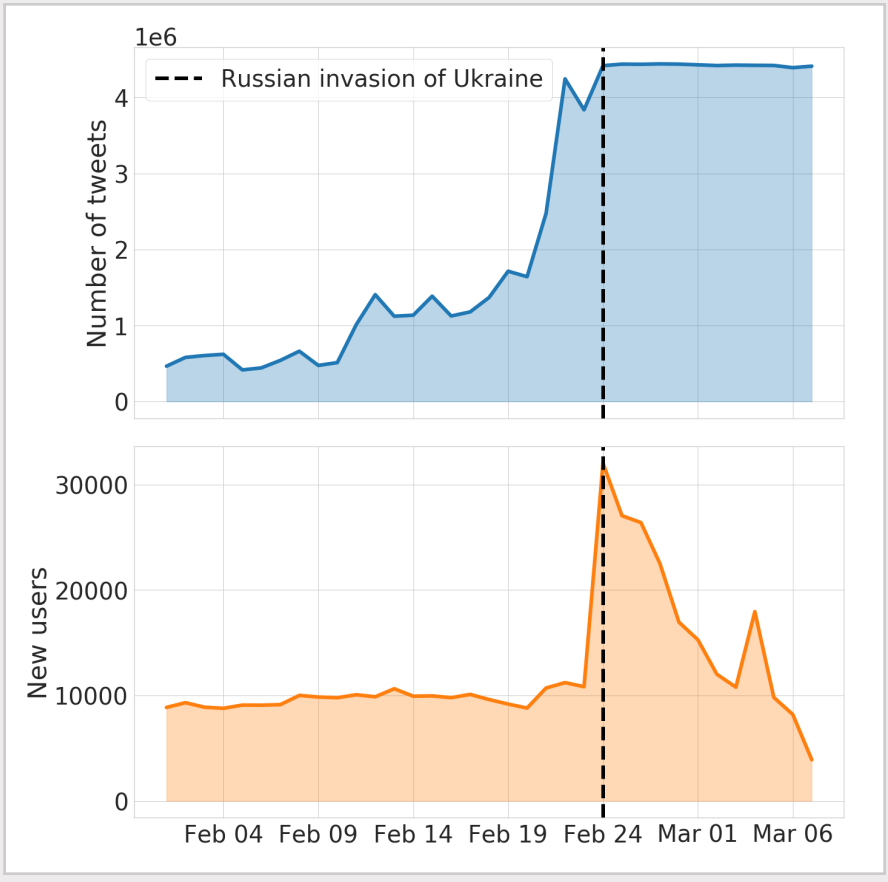
On February 24, 2022, Russia began a full-scale military invasion of Ukraine. The global scale of national interests related to the invasion means that public opinion in many countries is likely to play a significant role in the conflict. In turn, social media can play a key role in shaping public opinion in geopolitical events. Consequently, the potential to exploit social vulnerabilities through social media is of great concern. Detecting and monitoring these kinds of abuse is part of our mission at the Indiana University Observatory on Social Media (OSoMe). We have been monitoring activity about the Ukraine invasion on Twitter, YouTube, and Facebook since early February 2022, in collaboration with Politecnico di Milano.

The forms of abuse studied at OSoMe include the manipulation of social media platforms, such as the use of inauthentic accounts to promote agendas and narratives in deceptive ways. For instance, inauthentic accounts can coordinate to amplify messages that contain links to misinformation websites. Alternatively, we look for evidence of so-called astroturfing (fake grassroots) campaigns in which posts, reshares, likes, and replies create a false or overstated appearance of popular support for an individual or a point of view. Bad actors can also hijack public attention toward some topic or event for private benefit. We have developed machine-learning methods to detect these behaviors. Here we present some preliminary evidence of suspicious activity obtained from analysis of Twitter data about the early stages of the war in Ukraine. We report on a dramatic spike in the creation of new accounts around the date of the invasion, and on several networks of accounts sharing suspiciously similar content.

Preliminary Findings

We compiled a list of almost 40 English, German, Russian, and Ukrainian keywords relevant to the invasion and used them to collect over 60 million tweets posted since February 1. Figure 1 illustrates the rapid growth in content. As a result of the high volume, Twitter caps our collection capabilities, as reflected in the flattening trend starting February 24. The five most linked low-credibility sources include four Russian sources (rt.com, sputniknews.com, ria.ru, and kremlin.ru) and zerohedge.com, a disinformation source amplifying Russian propaganda, according to U.S. intelligence sources.[1] On the date of the full-scale invasion, we observed a significant increase in the creation of new accounts. To identify likely coordinated inauthentic behavior, we applied a framework developed by OSoMe that uncovers clusters of accounts with suspiciously similar sharing patterns.[2]

Figure 1

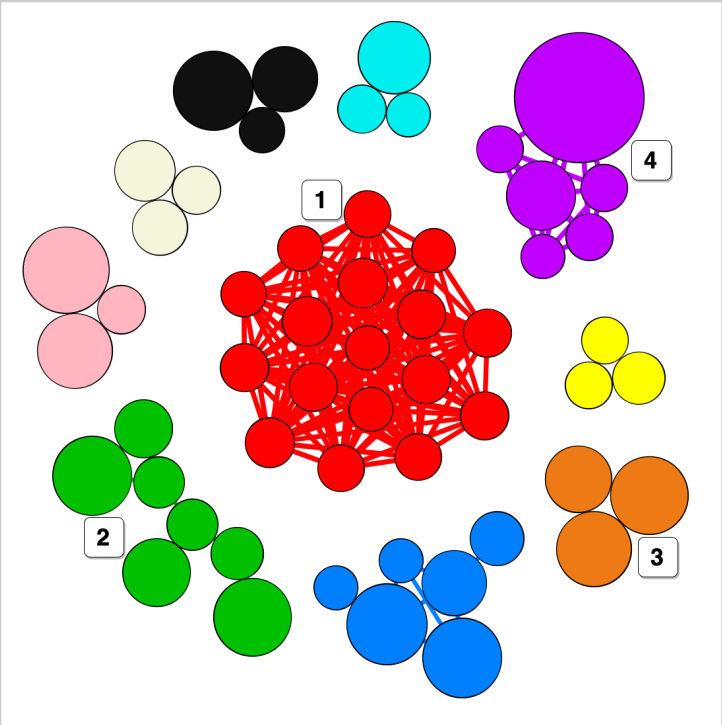


[1] https://www.bloomberg.com/news/articles/2022-02-15/us-accuses-financial-website-of-spreading-russian-propaganda

[2] Pacheco et al (2021): Uncovering Coordinated Networks on Social Media: Methods and Case Studies. Proc. ICWSM. https://ojs.aaai.org/index.php/ICWSM/article/view/18075

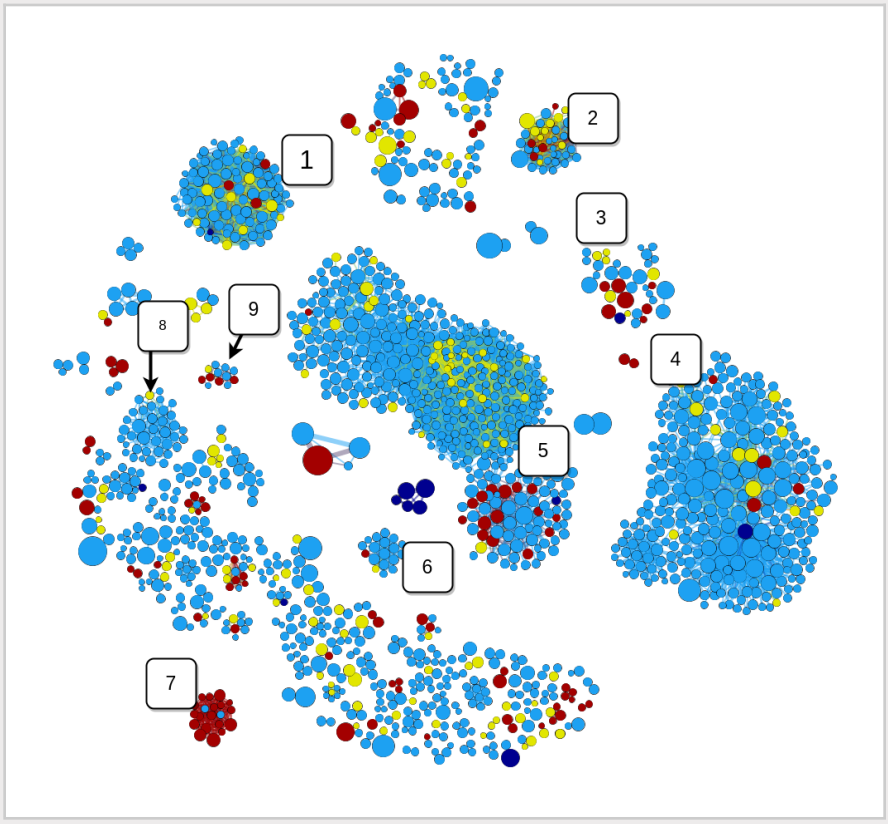
Figure 2 illustrates a network of accounts (nodes) that on February 24 shared common links to external websites. Two accounts are connected if they have a high overlap of shared links. Node size is proportional to the number of tweets containing external links (at least 10). As often happens with trending hashtags, Ukraine keywords are exploited to spread spam and/or content that is not necessarily about Ukraine. Accounts in cluster 1, for example, contain Arabic-language spam. Clusters 2 and 3 shared links to news aggregation blogs that contain many ads and malware. Cluster 4 promoted a Ukraine-themed cryptocurrency pump-and-dump scam.

Figure 2



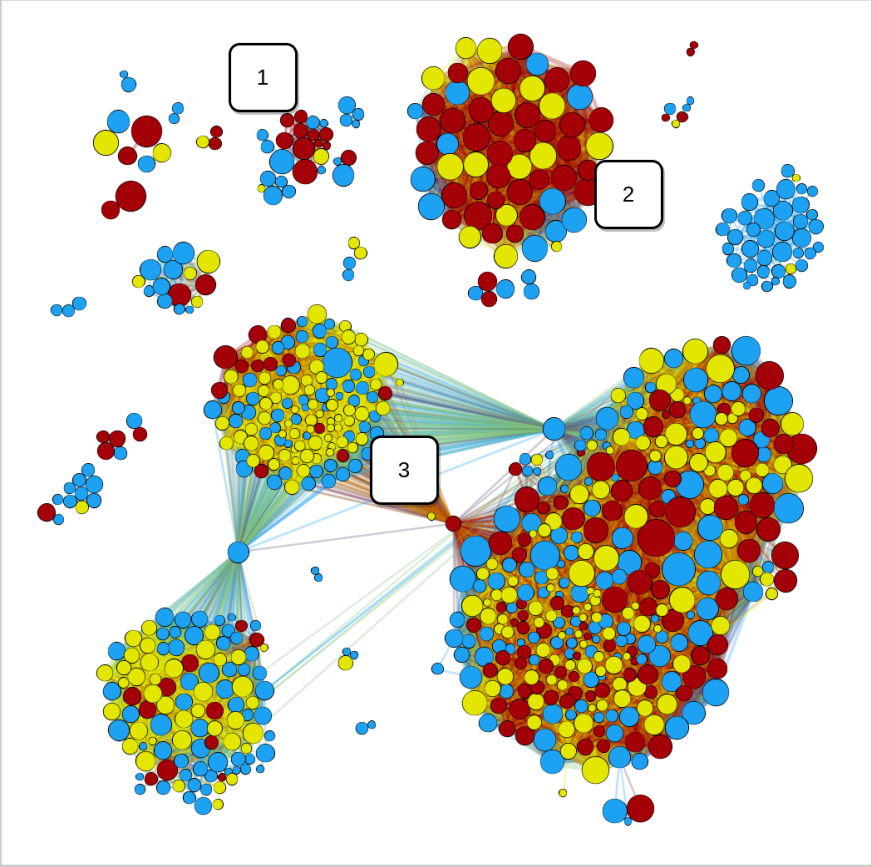
A different type of suspicious network emerges when observing multiple accounts that post many tweets with nearly-identical text. Figure 3 illustrates such a network based on tweets posted throughout February 2022. For an account to be included, it must have posted at least five tweets that are almost identical to those posted by another account. We excluded retweets and tweets linking to websites, as these often create similar content in a grassroots fashion. The size of a node is proportional to the number of nearly-identical tweets by the corresponding account, and the width of an edge is proportional to the number of similar tweets. Yellow nodes represent accounts created in 2022, red accounts are suspended as of March 8, dark blue accounts have been deleted, and light blue accounts are still active. We inspected the accounts to label the clusters: (1) quotes of French far-right politician Eric Zemmour; (2) a pro-Ukraine campaign; (3) spam; (4) a mixture of fake accounts, spammers, and fake news websites; (5) quotes of Turkish President Recep Erdoğan; (6) quotes of exiled Chinese anti-vaxxer and conspiracy theorist Guo Wengui; (7) a cryptocurrency scam pretending to support the Ukrainian resistance; (8) accounts promoting an evangelist's apocalyptic conspiracy content; and (9) pro-Russian propaganda by inauthentic accounts.

Figure 3



During February 2022, we found that on average around 3% of the tweets in our collection were copies or close copies of other tweets. This rose to around 7% on March 3. Figure 4 shows a network that we constructed using the same method as in Figure 3, but based on tweets posted on March 3. We observe a few suspicious clusters amplifying a cryptocurrency donation scam (cluster 1), criticizing the Indian government for supporting Russia (2), and posting pro-Ukraine messages asking the West to set up a no-fly zone and supporting other military escalations (3). These clusters are suspicious because they are very dense, indicating many near-identical messages shared by many accounts, several of which were suspended or created recently.

Figure 4



This brief report focuses on roughly the first week following the Russian invasion of Ukraine. With public attention focused on the tragic war, some see an opportunity to exploit social media to spread propaganda, spam, and scams. The Observatory on Social Media will continue to monitor this information battleground.