Trident Joust 2017, After Action Report

Kathleen M. Carley and David M. Beskow

November 15, 2017
CMU-ISR-17-116

Institute for Software Research
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

This work was supported in part by the Office of Naval Research (ONR) Multidisciplinary University Research Initiative N000140811186 and the North Atlantic Treaty Organization (NATO). Additional support was provided by the center for Computational Analysis of Social and Organizational Systems (CASOS) and the Institute for Software Research (ISR) at Carnegie Mellon University. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the North Atlantic Treaty Organization, the Office of Naval Research, or the U.S. government.

Center for the Computational Analysis of Social and Organizational Systems
CASOS technical report.

Keywords: Trident Joust 2017, social media analytics

Abstract

Trident Joust took place at the Joint Force Training Centre (JFTC) in Bydgoszcz, Poland from Sep 11, 2017 to Sept 21, 2017. It was a joint NATO exercised aimed at maintaining mission skills. Led by Dr. Rebecca Goolsby, the science team participated in this activity both on-site and off. The on-site team consisted of Dr. Rebecca Goolsby of the Office of Naval Research, NATO S&T; Dr. Lucia Flason from Australia DSTA; and Dr. Kathleen M. Carley from Carnegie Mellon University. The off-site team included PhD students and staff from the CASOS Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University and scientific observers at Arizona State University led by Dr. Huan Liu and the University of Arkansas Little Rock led by Dr. Nitin Agarwal.

The science team had three main goals, demonstrate the value of social media assessment to support NATO missions related to PSYOPS; understand how social media would be used in Trident Juncture 2018 and prepare to support that effort and to provide training in December for NATO; and identify gaps and barriers to social media training as operationalized in Trident Joust 2017. To meet these goals, the science team engaged in several parallel lines of activity, they operated as PSYOPS analysts to analyze social media data coming through the Crown Media system; they operated as remote analysts, collecting and analyzing social media messaging in the real world that was concerned with NATO and/or Trident Joust; they provided guidance on how to collect and assess social media data, and provided information on how social media is, has been and can be used for a variety of missions including, but not limited to PAO, PSYOPS, and planning; and engaged in planning sessions for social media analytics in Trident Juncture 2018.

Table of Contents

1 Study 1 – Crown Media World

The on-site team collected on-line media from the Crown-Media (CM) system – exploring the CM equivalents of news, twitter (aka critter) and youtube (videos). Most of the effort was focused on identifying relations between the actors in critter with particular attention to gangs and potential terrorists. The News feeds were used primarily to set context and get proper name spelling. The videos and images were used to identify skills/expertise/resources of key actors.

1.1 Data

The majority of the data collected was from "critter" – a CM twitter like system. Using this system a set of "creets" – the messages, were captured along with information on who sent the message, whether it was replied to and if so by whom, and timestamps on the creets. In addition details on actors were captured including their screen name, who they followed, who followed them, who did the mention in a creets, whose creets did they reply to, and sometimes characteristics such as purported position (e.g., MFA of Romania), age and gender. In some cases position could be confirmed via news. This data was then entered by hand into ORA for network analysis and visualization. A high dimensional meta-network was created with a following network, a mentions/replies network, and a bi-partite people x skills/expertise network. The collection strategy began with observation and then general surfing. Then after a set of actors of interest were identified a snowball strategy was used with the snowball following out the following/follower links and then the mentions/replies link.

The resultant network was analyzed and known informants, NATO actors, and news-site for large national mainstream news sites such as "CNN" were removed. A visualization of the resulting network, with areas of operation highlighted is shown in Figure 1. Areas of operation are identified by looking at content of creets, and information in the news. Of this group 18 were identified as adversaries, 20 as suspect, 102 general accounts, 17 official government accounts and 5 news. Note at least one suspicious account was also a news account. Most actors sent between 1 and 5 messages; however, the most active sent 48 messages.

1.2 Results

In addition, the on-site team captured a number of lessons learned about how to create a more realistic social media experience for training. See Appendix 1.

In less than 24 hours a network comprised of 161 users of critter was identified. Many of the actors had male personas with the average age of those listing age as 47. Many actors were clearly "unvetted" fake personas – such as ones with a male name and age of 50 and an image of an 18 year old female.

Figure 1 shows the identified "suspicious" network and the surrounding network using all ties (following, mentions and replies. Blue lines are mentions or replies and red are follows. The suspected role of parts of the network are highlighted with blue circles.

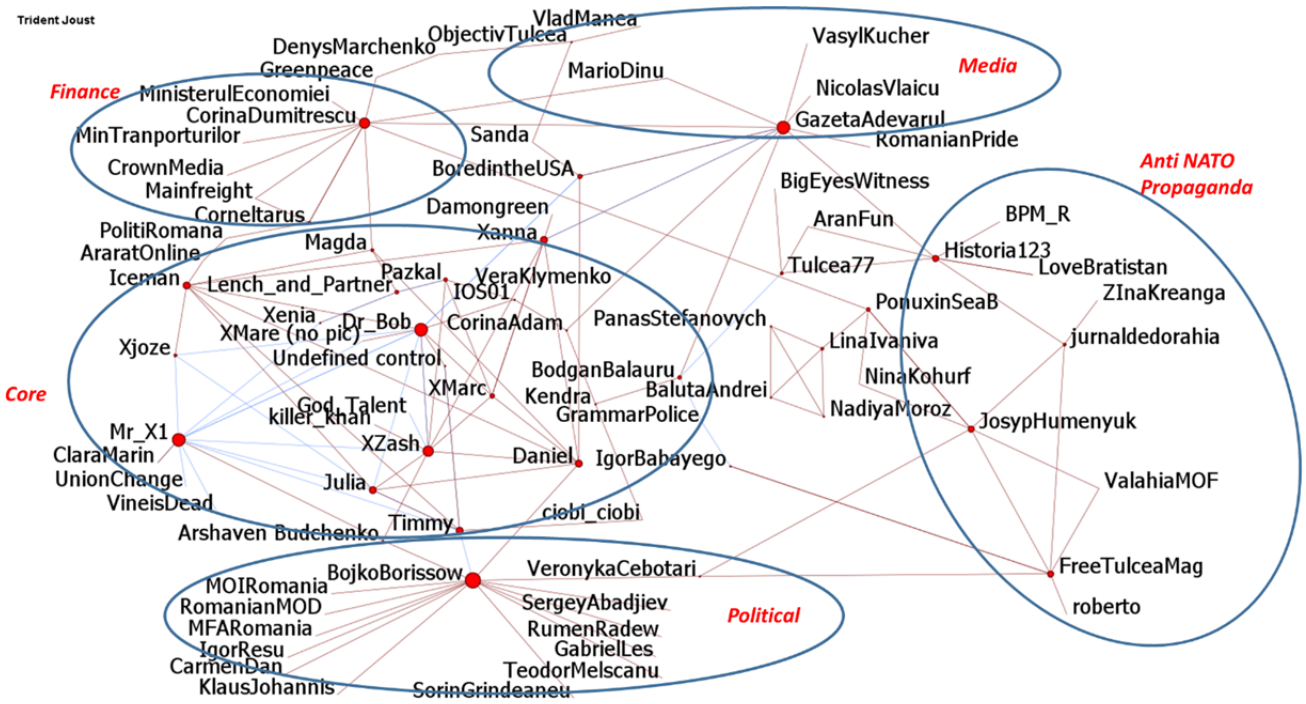


Figure 1

A deeper dive into the core network is shown in Figure 2. In this diagram the resources of agents are shown with green line. The larger the node the more others they are connected to. This network is highly similar to that from the J2.

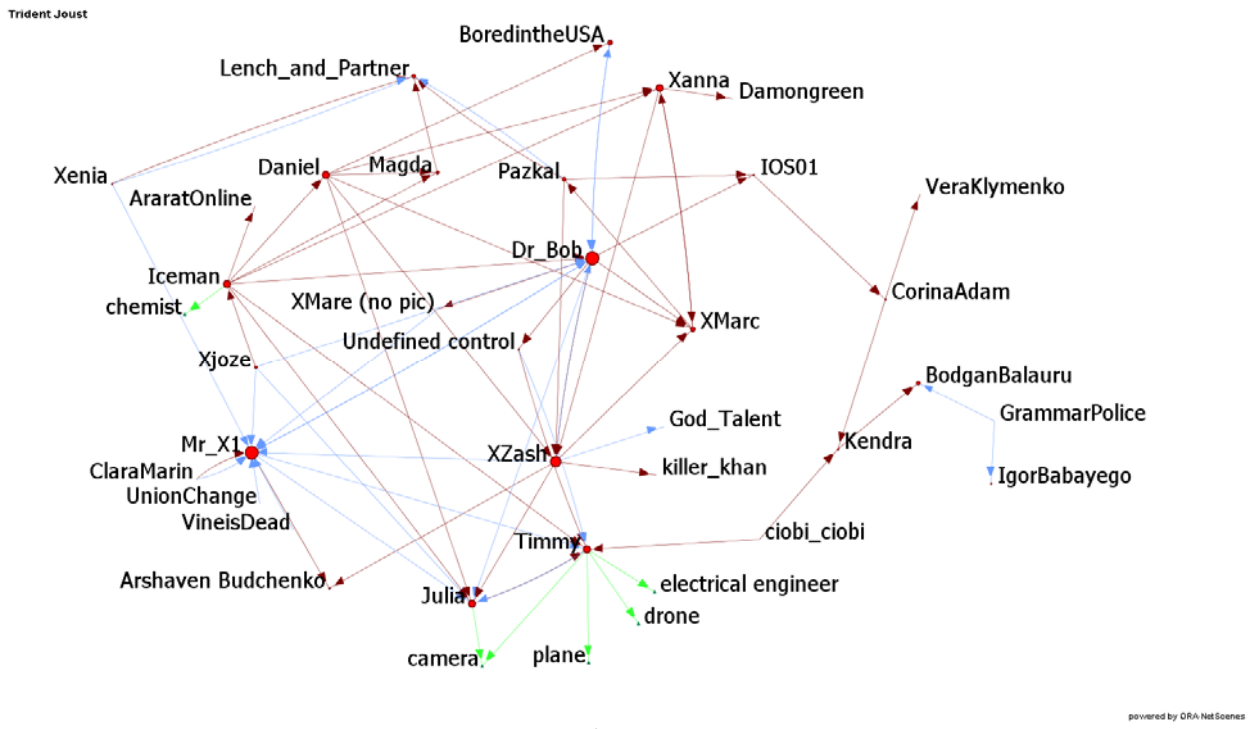


Figure 2

1.3 Conclusions

The science team was able to "discover" the covert terror/gang cell in social media through a combination of types of links. The discovered network bore a striking resemblance to that found by the J2. This process was completed in less than 24 hours (approx 15 working hours) including time to create powerpoints of results for briefings.

The "game" environment used for training was radically different than a real social media environment. Hence extant social media capture tools could not be used and approaches for countering information operations in social media could not be tested. This meant that data collection and upload to the analysis tools was a manual process and so susceptible to human error. Most of the 15 working hours was spent manually collecting and re-entering data. Lessons learned about how to make the gaming environment more realistic are in Appendix 1.

The same tools were used in this game environment as in real environments for analyzing and visualizing the social media data. Specifically, ORA was used for analysis and visualization of the network. Netmapper was used for extracting semantic networks from messages.

Given the collected data a series of secondary analyses could be conducted such as empirical matching of j2 and social media networks, comparison of mention and reply networks, temporal analysis of how the network changed, and additional analyses of the semantic networks.

2 Study 2 – Real World

During the Trident Joust Exercise (and the concurrent Russian Zapad 2017 Exercise) the CMU CASOS team, led by Dr. Kathleen M. Carley, supported the larger efforts related to Social Media Analysis, Open Source Intelligence (OSINT), and the general use of Publicly Available Information (PAI) for operational purposes. As preparation for Trident Juncture 2018, CMU CASOS also collected data in the real world using Twitter about Zapad and Trident Joust.

In general, operational forces use Publicly Available Information (PAI) to support the following requirements during an operation like Trident Joust:

- Identify threat information operations (actors, actions, messaging and narratives)
- Identify friendly/neutral elements that can amplify friendly messaging and narratives
- Identify automated actors (i.e. bots and cyborgs) that are acting on the information battlefield
- Support force protection by identifying risk
- Provide Indicators and Warnings (I&W)
- Measure local public sentiment for ongoing friendly and threat operations
- Provide general situational awareness for leaders and commanders

Considering these general requirements, the rest of this report outlines a description of our current support and proposed future support.

3 Description of Current Support:

Current support consisted of ongoing monitoring of social media streams as well as "deep dives" on areas of interest. The current workflow started with collection from various social

media sources (primarily Twitter for this effort), data cleansing, modeling, and then visualization and communication.

The data was primarily collected from the Twitter Streaming and REST API in accordance with their terms of service. A table of the data that was collected is provided below:

Description	Source	Size – Format	Purpose
Hashtag text collection ("#NATO","#tridentjoust", "#Zapad2017","#zapadwatch", "#Zapad17", "#запад", "#запад2017", "aurora17")	Twitter REST API	78K – Raw JSON	Support temporal, topic, and geo models and analysis
City level location	Twitter REST API	92K – CSV	Track local conversations
Country level location	Twitter Streaming API	130K – Raw JSON	Track national conversations

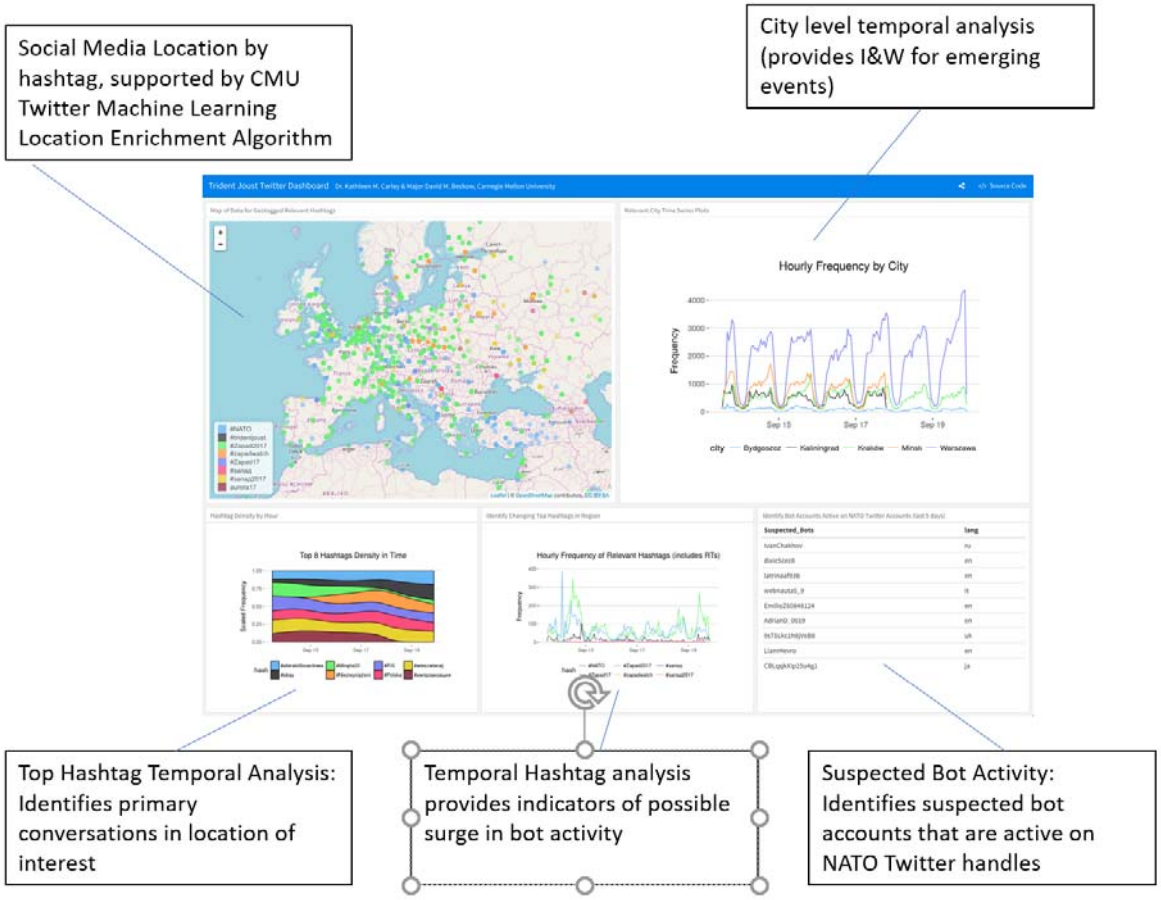
In addition some data was collected on specific users, using the actor API and from generic surfing – just watching twitter live.

3.1 Models and tools:

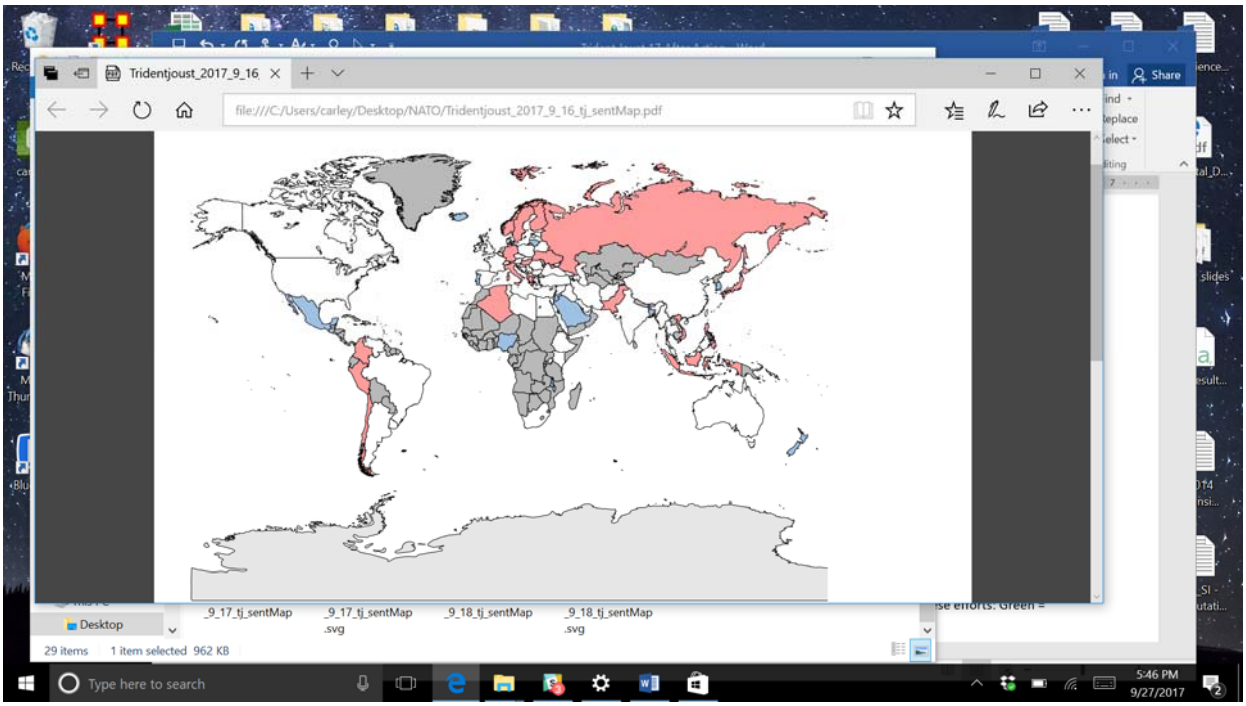
Various models and tools were used in the effort. These models/tools were designed to meet some of the PAI requirements noted above.

3.1.1 Social Network Analytics Tools/Models:

ORA-PRO and NETMAPPER are the primary tools used for social network analysis. ORA-PRO provides robust Extract, Transform, and Load capability for quickly loading social media data, as well as an intuitive GUI to allow a user to interact with the network aspects of the data. This includes easy network creation, manipulation, pruning, and visualization. NetMapper provides an even more robust ETL capability for extracting all possible text entities using specialized models and natural language processing. The CASOS team used both tools to conduct a deep dive on the data in analyzing the network structure, key actors, super-friends/super-spreaders, informal group structure, etc. The CMU CASOS team also demonstrated rapid analytic dashboard development using the R, RStudio, RMarkdown, and FlexDashboard family of open source tools. This dashboard was meant to provide monitoring of important metrics throughout the operation. It provided geo-spatial, temporal, topical analysis as well as some basic automated bot detection and identification. A screenshot of this dashboard is provided below.



A second workflow was developed for additional analytics. This workflow: a) runs a spatial location algorithm to assess what country a tweet is coming from if it is not marked; b) takes all hashtags containing terms of interest and assesses the sentiment associated with those terms; c) place the geo-tagged tweets and sentiments on maps. One of the outputs is a sensor map showing how NATO is doing by country – with red as negative and blue as positive.



Sept 16, 2016

3.2 Outcome:

The workflow, tools, and models described above helped meet the following requirements listed in part 1 above (colored green-amber-red by the degree to which our tools supported these efforts: Green = Strong support, Red = Weak Support).

- Identify threat information operations (actors, actions, messaging and narratives)
- Identify friendly/neutral elements that can amplify friendly messaging and narratives
- Identify automated actors (i.e. bots and cyborgs) that are acting on the information battlefield
- Support force protection by identifying risk (task primarily supported by other tools)
- Provide Indicators and Warnings (I&W)
- Measure local public sentiment for ongoing friendly and threat operations (CMU CASOS has significant sentiment analysis research that should be leveraged for future work)
- Provide general situational awareness for leaders and commanders

4 Proposed Future Work and Improvements:

In future support efforts, we propose the following:

1. All data collection efforts feed a central repository accessible by all members of the team. This requires a uniform agreement on data standards (most likely raw JSON output). This includes building in the tweet streams from partners at ASU.

2. Begin data collection and analytic support efforts 2-3 weeks before event for exercise and 4-5 weeks before training/experiment. It would be best if the training/experiment data could serve as a baseline for the exercise.
3. Routinely run and measure bot detection algorithms (both Machine Learning and Network based algorithms).
4. Routinely run and measure discussions by on-line media providers and official accounts.
5. Leverage existing CMU sentiment algorithms
6. Go beyond Twitter (leverage other SM: Facebook, VK, Tumblr, etc)
7. Develop automated methods to identify threat messaging and narratives
8. Employ context based sentiment tracker that is focused onky on NATO
9. Deploy a live and interactive dashboard with RStudio Shiny on AWS. This would demonstrate agile and tailored analytics to support operations and allow participants to interact with model output.
10. Possibly deploy a tailored honeypot to assist in identifying bot activity.
11. Deploy live updates of the discovered networks of interest
12. Either generate new dashboard for second workflow of integrate it into first dashboard
13. Add meters rather than just country coloring.

5 Overarching Comments

- Social media can be used to support a number of missions.
- Training should be done with more realistic data and using real tools for analysis.

6 Appendix

6.1 Making a synthetic twitter feed more realistic for training exercises

Lessons learned from Trident Joust.
Rebecca Goolsby, Kathleen M. Carley

6.1.1 Key features of the synthetic tweets.

These features are the minimum set needed to make a realistic scenario for training on social media with virtual twitter.

- Volume – need vast quantities of messages multi-topic, multi-messenger. At least 100 per hour.
- Some fraction with images
- Some fraction with videos
- Some fraction with links to urls
- Some historical messages and then an ongoing new stream

Predefined messengers such as news services and official accounts. With tweeting pattern and message content typical of those actors. This includes following and follower patterns, use of hashtags, mentions frequency of being retweeted and of retweeting others being representation. For example news should be more frequently retweeted than most other actors. News actors should always put out messages pointing to new stories they release. Public chatter from random people should appear commenting on news stories.

Messages and actors should be diverse and not all on topic. Background chatter, related messages to topics of interest and messages that are obfuscating to messages of interest due to use of some common key words.

In general, all news government official actors, politicians, key celebrities in the scenario who are part of background – should exist in have some messages in the historic data stream.

6.2 Key technical capabilities needed.

- Ability to retweet
- Ability to reply
- Ability to view
- Ability to search
- API to download a sample of data – ideally the format is close to if not identical to twitter api but with some fields left blank. This lets trainees with social media tools directly employ them.

6.3 Advanced features for realism.

These are items that might be needed in some settings but not others.

- Even more volume

- Messages in multiple languages and messages in which multiple languages are used.
- If spatial analysis is critical - 5% with geo-tagging, also all messages need a time stamp and time zone
- Overlaying an adversarial network.
- Bots with different activity patterns. Three classes to consider – bots that retweet messages, bots mention super spreaders a lot, bots that try to change topics by tweeting out messages on an alternative topic. More sophisticated would be social influence bots.

Institute for Software Research • Carnegie Mellon University • 5000 Forbes Avenue • Pittsburgh, PA 15213-3890