AMITT Techniques Guide

“Need a 1-2 pager for each AMITT tactic: here’s how you investigate each tactic e.g. “they developed pump priming, what are the things you look for”

We have a page for each tactic and technique in the AMITT repo https://github.com/cogsec-collaborative/amitt_framework - using this to build these notes

- T0025 Leak altered documents
- T0026 Create fake research
- T0027 Adapt existing narratives
- T0028 Create competing narratives

TA07 Channel Selection Techniques
- T0029 Manipulate online polls
- T0030 Backstop personas
- T0031 YouTube
- T0032 Reddit
- T0033 Instagram
- T0034 LinkedIn
- T0035 Pinterest
- T0036 WhatsApp
- T0037 Facebook
- T0038 Twitter

TA08 Pump Priming Techniques
- T0039 Bait legitimate influencers
- T0040 Demand unsurmountable proof
- T0041 Deny involvement
- T0042 Kernel of Truth
- T0043 Use SMS/ WhatsApp/ Chat apps
- T0044 Seed distortions
- T0045 Use fake experts
- T0046 Search Engine Optimization

TA09 Exposure Techniques
- T0047 Muzzle social media as a political force
- T0048 Cow online opinion leaders
- T0049 Flooding
- T0050 Cheerleading domestic social media ops
- T0051 Fabricate social media comment
- T0052 Tertiary sites amplify news
- T0053 Twitter trolls amplify and manipulate
- T0054 Twitter bots amplify
- T0055 Use hashtag
- T0056 Dedicated channels disseminate information pollution

TA10 Go Physical Techniques
- T0057 Organise remote rallies and events
- T0061 Sell merchandising

TA11 Persistence Techniques

TA01 Strategic Planning Techniques

T0001 5Ds (dismiss, distort, distract, dismay, divide)

Part of TA01, Strategic planning.

Summary: Nimmo's "4Ds of propaganda": dismiss, distort, distract, dismay (MisinfosecWG added divide in 2019). Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

The four Ds (dismiss, distort, distract, dismay) were designed by Ben Nimmo to describe the techniques used by Russia to create alternative narratives to the facts around an event.

- Dismiss: push back against criticism by dismissing your critics. This might be arguing that the critics use a different standard for you than with other actors or themselves; or arguing that their criticism is biased.
- Distort: twist the narrative. Take information, or artefacts like images, and change the framing around them.
- Distract: shift attention to a different narrative or actor, for instance by accusing critics of the same activity that they've accused you of (e.g. police brutality).
- Dismay: threaten the critic or narrator of events. For instance, threaten journalists or news outlets reporting on a story.

MisinfosecWG added a fifth D, Divide, to the list:

- Divide: create conflict between subgroups, to widen divisions in a community

Narratives are the stories that we tell ourselves about who we are, who we belong to, and what's happening in the world. Narratives can be personal, or group narratives, or the basis of who we believe ourselves to be as nations. The 5 Ds are usually used to affect narratives at the nationstate level.

Things to look for:

- Explicit attacks on the storytellers - attacks on the integrity of journalists and reports, ad-hominem attacks and direct threats.
- Twists in narrative framing that go beyond differences in viewpoint. Look for omissions of key information, and use of already-debunked narratives key to the actor.
- Misdirection

Potential counters

- Media: moving from the 24-hour news cycle, so storytelling becomes less of a tactical back-and forth.

References

- Ben Nimmo, Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It, Stop Fake, May 19 2015 - original description of the 4Ds
- Digital Sherlocks: PROPAGANDA: Dismiss, Distort, Distract, & Dismay (30 minute presentation)
- Lukas Andriukaitis, Disinfo bingo: The 4 Ds of disinformation in the Moscow protests, Sept 24, 2019
- Andrew Wilson, Four Types of Russian Propaganda, Aspen Review, 2015. Nudge propaganda and alternative realities: mentions 4D as an older Soviet tradition.
- Rhetorical fallacies: Propaganda in 4 D's - interesting additions to the Ds

T0002 Facilitate State Propaganda

Part of TA01

Summary: Organize citizens around pro-state messaging. Paid or volunteer groups coordinated to push state propaganda (examples include 2016 Diba Facebook Expedition, coordinated to overcome China's Great Firewall to flood the Facebook pages of Taiwanese politicians and news agencies with a pro-PRC message).

Strategic move: generates positive will of the people.

Things to look out for:

- Nationalist messaging from private social media accounts
- Amplification of government messaging from private social media accounts

Examples:

- Russian-speaking coordinated messaging in Ukraine
- China coordinated messaging on Uyghurs
- 50-Cent army
- Diba facebook expedition

Potential counters:

-

References

T0003 Leverage Existing Narratives

Part of TA01

Summary: Use or adapt existing narrative themes, where narratives are the baseline stories of a target audience. Narratives form the bedrock of our worldviews. New information is understood through a process firmly grounded in this bedrock. If new information is not consistent with the prevailing narratives of an audience, it will be ignored. Effective campaigns will frame their misinformation in the context of these narratives. Highly effective campaigns will make extensive use of audience-appropriate archetypes and meta-narratives throughout their content creation and amplification practices. Examples include: midwesterners are generous, Russia is under attack from outside.

Using narratives that already exist in the targeted communities, and adapting them. Can be seen as a Distort technique for a community's baseline narratives.

Things to look for:

- Second amplification peak in news traffic (from weaponised news)
-

Potential counters

- C00031 - dilute the core narratives

References:

T0004 Competing Narratives

Part of TA01

Summary: Advance competing narratives connected to same issue ie: on one hand deny incident while at same time expresses dismiss. MH17 (example) "Russian Foreign Ministry again claimed that “absolutely groundless accusations are put forward against the Russian side, which are aimed at discrediting Russia in the eyes of the international community" (deny); "The Dutch MH17 investigation is biased, anti-Russian and factually inaccurate" (dismiss). Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on. These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the "firehose of misinformation" approach.

-

Things to look for:

- Amplification of competing narratives
- Competing narratives from the same sources

References

TA02 Objective Planning Techniques

T0005 Center of Gravity Analysis

Part of TA02
Summary: Recon/research to identify "the source of power that provides moral or physical strength, freedom of action, or will to act." Thus, the center of gravity is usually seen as the "source of strength". Includes demographic and network analysis of communities

Disinformation creators will be out doing research on their target communities and target decision makers. What they look for will depend on what they’re doing. Generally will see an initial research phase, with a list of 4-5 things, then may or may not see some A-B testing of messaging to a centre of gravity that then gets honed to a specific audience.

Things to look for:

- A-B testing of messaging, e.g. variations on inauthentic messages, images etc being tried at the same time
- Audience testing of messaging, e.g. messaging being aimed at different audiences over time
- Demographic research in searches

Potential counters:

- Microtarget and countermessage most likely target groups

REferences

T0006 Create Master Narratives

Part of TA02

Summary: The promotion of beneficial master narratives is perhaps the most effective method for achieving long-term strategic narrative dominance. From a "whole of society" perspective the promotion of the society's core master narratives should occupy a central strategic role. From a misinformation campaign / cognitive security perspective the tactics around master narratives center more precisely on the day-to-day promotion and reinforcement of this messaging. In other words, beneficial, high-coverage master narratives are a central strategic goal and their promotion constitutes an ongoing tactical struggle carried out at a whole-of-society level.

By way of example, major powers are promoting master narratives such as:

- "Huawei is determined to build trustworthy networks"
- "Russia is the victim of bullying by NATO powers"
- "USA is guided by its founding principles of liberty and egalitarianism"

Tactically, their promotion covers a broad spectrum of activities both on- and offline.

Things to look for:

- Existing disinformation narratives
- New inauthentic narratives

TA03 Develop People Techniques

T0007 Create fake Social Media Profiles / Pages / Groups

Part of TA03

Summary: Create key social engineering assets needed to amplify content, manipulate algorithms, fool public and/or specific incident/campaign targets.

Computational propaganda depends substantially on false perceptions of credibility and acceptance. By creating fake users and groups with a variety of interests and commitments, attackers can ensure that their messages both come from trusted sources and appear more widely adopted than they actually are.

Examples: Ukraine elections (2019) circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages. EU Elections (2019) Avaaz reported more than 500 suspicious pages and groups to Facebook related to the three-month investigation of Facebook disinformation networks in Europe. Mueller report (2016) The IRA was able to reach up to 126 million Americans on Facebook via a mixture of fraudulent accounts, groups, and advertisements, the report says. Twitter accounts it created were portrayed as real American voices by major news outlets. It was even able to hold real-life rallies, mobilizing hundreds of people at a time in major cities like Philadelphia and Miami.

Things to look for:

- Sets of profiles with the same profile image or profile text

T0008 Create fake or imposter news sites

Part of TA03

Summary: Modern computational propaganda makes use of a cadre of imposter news sites spreading globally. These sites, sometimes motivated by concerns other than propaganda--for instance, click-based revenue--often have some superficial markers of authenticity, such as naming and site-design. But many can be quickly exposed with reference to their ownership, reporting history and advertising details. A prominent case from the 2016 era was the _Denver Guardian_, which purported to be a local newspaper in Colorado and specialized in negative stories about Hillary Clinton.

Things to look for:

- Local news sites that are unknown to local residents
-

Potential counters:

-

References:

- Pink slime

T0009 Create fake experts

Part of TA03

Summary: Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself. For example, in the Jade Helm conspiracy theory promoted by SVR in 2015, a pair of experts--one of them naming himself a “Military Intelligence Analyst / Russian Regional CME” and the other a “Geopolitical Strategist, Journalist & Author”--pushed the story heavily on LinkedIn.

Things to look for:

*

Potential counters:

*

References:

*

TA04 Develop Networks Techniques

T0010 Cultivate ignorant agents

Part of TA04

Summary: Cultivate propagandists for a cause, the goals of which are not fully comprehended, and who are used cynically by the leaders of the cause. Independent actors use social media and specialised web sites to strategically reinforce and spread messages compatible with their own. Their networks are infiltrated and used by state media disinformation organisations to amplify the state’s own disinformation strategies against target populations. Many are traffickers in conspiracy theories or hoaxes, unified by a suspicion of Western governments and mainstream media. Their narratives, which appeal to leftists hostile to globalism and military intervention and nationalists against immigration, are frequently infiltrated and shaped by state-controlled trolls and altered news items from agencies such as RT and Sputnik. Also know as "useful idiots" or "unwitting agents".

Things to look for:

*

Potential counters:

*

References:

*

T0011 Hijack legitimate account

Part of TA04

Summary: Hack or take over legimate accounts to distribute misinformation or damaging content. Examples include Syrian Electronic Army (2013) series of false tweets from a hijacked Associated Press Twitter account claiming that President Barack Obama had been injured in a series of explosions near the White House. The false report caused a temporary plunge of 143 points on the Dow Jones Industrial Average.

Things to look for:

*

Potential counters:

*

References:

*

T0012 Use concealment

Part of TA04

Summary: Use anonymous social media profiles. Examples include page or group administrators, masked "whois" website directory data, no bylines connected to news article, no masthead connect to news websites.

Example is 2016 @TEN_GOP profile where the actual Tennessee Republican Party tried unsuccessfully for months to get Twitter to shut it down, and 2019 Endless Mayfly is an Iran-aligned network of inauthentic personas and social media accounts that spreads falsehoods and amplifies narratives critical of Saudi Arabia, the United States, and Israel.

Things to look for:

*

Potential counters:

*

References:

*

T0013 Create fake websites

Part of TA04

Summary: Create media assets to support fake organizations (e.g. think tank), people (e.g. experts) and/or serve as sites to distribute malware/launch phishing operations.

Things to look for:

*

Potential counters:

*

References:

*

T0014 Create funding campaigns

Part of TA04

Summary: Generate revenue through online funding campaigns. e.g. Gather data, advance credible persona via Gofundme; Patreon; or via fake website connecting via PayPal or Stripe. (Example 2016) #VaccinateUS Gofundme campaigns to pay for Targetted facebook ads (Larry Cook, targetting Washington State mothers, $1,776 to boost posts over 9 months).

Things to look for:

*

Potential counters:

*

References:

*

T0015 Create hashtag

Part of TA04

Summary: Many incident-based campaigns will create a hashtag to promote their fabricated event (e.g. #ColumbianChemicals to promote a fake story about a chemical spill in Louisiana).

Creating a hashtag for an incident can have two important effects:

1. Create a perception of reality around an event. Certainly only "real" events would be discussed in a hashtag. After all, the event has a name!

2. Publicize the story more widely through trending lists and search behavior

Asset needed to direct/control/manage "conversation" connected to launching new incident/campaign with new hashtag for applicable social media sites ie: Twitter, LinkedIn)

Things to look for:

*

Potential counters:

*

References:

*

TA05 Microtargeting Techniques

T0016 Clickbait

Part of TA05

Summary: Create attention grabbing headlines (outrage, doubt, humor) required to drive traffic & engagement. (example 2016) “Pope Francis shocks world, endorses Donald Trump for president.” (example 2016) "FBI director received millions from Clinton Foundation, his brother’s law firm does Clinton’s taxes”. This is a key asset

Things to look for:

*

Potential counters:

*

References:

*

T0017 Promote online funding

Part of TA05

Summary: Drive traffic/engagement to funding campaign sites; helps provide measurable metrics to assess conversion rates

Things to look for:

*

Potential counters:

*

References:

*

T0018 Paid targeted ads

Part of TA05

Summary: Create or fund advertisements targeted at specific populations

Things to look for:

*

Potential counters:

*

References:

*

TA06 Develop Content Techniques

T0019 Generate information pollution

Part of TA06

Summary: Flood social channels; drive traffic/engagement to all assets; create aura/sense/perception of pervasiveness/consensus (for or against or both simultaneously) of an issue or topic. "Nothing is true, but everything is possible." Akin to astroturfing campaign.

Things to look for:

*

Potential counters:

*

References:

*

T0020 Trial content

Part of TA06

Summary: Iteratively test incident performance (messages, content etc), e.g. A/B test headline/content enagagement metrics; website and/or funding campaign conversion rates

Things to look for:

*

Potential counters:

*

References:

*

T0021 Memes

Part of TA06

Summary: Memes are one of the most important single artefact types in all of computational propaganda. Memes in this framework denotes the narrow image-based definition. But that naming is no accident, as these items have most of the important

properties of Dawkins' original conception as a self-replicating unit of culture. Memes pull together reference and commentary; image and narrative; emotion and message. Memes are a powerful tool and the heart of modern influence campaigns.

Things to look for:

*

Potential counters:

*

References:

- https://www.digitaltrends.com/computing/what-is-a-meme/
- Joan Donovan, How memes got weaponized: A short history, MIT Technology Review, 2019
- “Memes to Movements: how the world’s most viral media is changing social protest and power”, An Xiao Mina - book from a disinfo community member
- Know Your Meme: Internet meme database
- https://imgflip.com/memegenerator
- https://www.theodysseyonline.com/memes-explained-by-psychology

T0022 Conspiracy narratives

Part of TA06

Summary: "Conspiracy narratives appeal to the human desire for explanatory order, by invoking the participation of powerful (often sinister) actors in pursuit of their own political goals. These narratives are especially appealing when an audience is low-information, marginalized or otherwise inclined to reject the prevailing explanation. Conspiracy narratives are an important component of the ""firehose of falsehoods"" model.

Example: QAnon: conspiracy theory is an explanation of an event or situation that invokes a conspiracy by sinister and powerful actors, often political in motivation, when other explanations are more probable "

Things to look for:

*

Potential counters:

*

References:

*

T0023 Distort facts

Part of TA06

Summary: Change, twist, or exaggerate existing facts to construct a narrative that differs from reality. Examples: images and ideas can be distorted by being placed in an improper content

Things to look for:

*

Potential counters:

*

References:

*

T0024 Create fake videos and images

Part of TA06

Summary: Create fake videos and/or images by manipulating existing content or generating new content (e.g. deepfakes). Examples include Pelosi video (making her appear drunk) and photoshoped shark on flooded streets of Houston TX.

Things to look for:

*

Potential counters:

*

References:

*

T0025 Leak altered documents

Part of TA06

Summary: Obtain documents (eg by theft or leak), then alter and release, possibly among factual documents/sources.

Example (2019) DFRLab report "Secondary Infektion" highlights incident with key asset being a forged "letter" created by the operation to provide ammunition for far-right forces in Europe ahead of the election.

Things to look for:

*

Potential counters:

*

References:

*

T0026 Create fake research

Part of TA06

Summary: Create fake academic research. Example: fake social science research is often aimed at hot-button social issues such as gender, race and sexuality. Fake science research can target Climate Science debate or pseudoscience like anti-vaxx

Things to look for:

*

Potential counters:

*

References:

*

T0027 Adapt existing narratives

Part of TA06

Summary: Adapting existing narratives to current operational goals is the tactical sweet-spot for an effective misinformation campaign. Leveraging existing narratives is not only more effective, it requires substantially less resourcing, as the promotion of new master narratives operates on a much larger scale, both time and scope. Fluid, dynamic & often interchangeable key master narratives can be ("The morally corrupt West") adapted to divisive (LGBT propaganda) or to distort (individuals working as CIA operatives). For Western audiences, different but equally powerful framings are available, such as "USA has a fraught history in race relations, especially in criminal justice areas."

Things to look for:

*

Potential counters:

*

References:

*

T0028 Create competing narratives

Part of TA06

Summary: Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on.

These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the *firehose of misinformation* approach.

Things to look for:

*

Potential counters:

*

References:

*

TA07 Channel Selection Techniques

T0029 Manipulate online polls

Part of TA07

Summary: Create fake online polls, or manipulate existing online polls. Examples: flooding FCC with comments; creating fake engagement metrics of Twitter/Facebook polls to manipulate perception of given issue. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well

Things to look for:

*

Potential counters:

*

References:

*

T0030 Backstop personas

Part of TA07

Summary: Create other assets/dossier/cover/fake relationships and/or connections or documents, sites, bylines, attributions, to establish/augment/inflate credibility/believability

Things to look for:

*

Potential counters:

*

References:

*

T0031 YouTube

Part of TA07

Summary: Use YouTube as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0032 Reddit

Part of TA07

Summary: Use Reddit as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0033 Instagram

Part of TA07

Summary: Use Instagram as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0034 LinkedIn

Part of TA07

Summary: Use LinkedIn as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0035 Pinterest

Part of TA07

Summary: Use Pinterest as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0036 WhatsApp

Part of TA07

Summary: Use WhatsApp as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0037 Facebook

Part of TA07

Summary: Use Facebook as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

T0038 Twitter

Part of TA07

Summary: Use Twitter as a narrative dissemination channel

Things to look for:

*

Potential counters:

*

References:

*

TA08 Pump Priming Techniques

T0039 Bait legitimate influencers

Part of TA08

Summary: Credibility in a social media environment is often a function of the size of a user's network. "Influencers" are so-called because of their reach, typically understood as: 1) the size of their network (i.e. the number of followers, perhaps weighted by their own influence); and 2) The rate at which their comments are re-circulated (these two metrics are related). Add traditional media players at all levels of credibility and professionalism to this, and the number of potential influential carriers available for unwitting amplification becomes substantial.

By targeting high-influence people and organizations in all types of media with narratives and content engineered to appeal to their emotional or ideological drivers,

influence campaigns are able to add perceived credibility to their messaging via saturation and adoption by trusted agents such as celebrities, journalists and local leaders.

Things to look for:

- “Trading up the chain” (Ryan Holliday term) - genuine influencer amplifying disinformation or information from a known disinformation source.

Potential counters:

- Platforms: Clearly marking known political influences on sources, e.g. marking RT as Russian-owned etc.

References:

*

T0040 Demand unsurmountable proof

Part of TA08

Summary: Campaigns often leverage tactical and informational asymmetries on the threat surface, as seen in the Distort and Deny strategies, and the "firehose of misinformation". Specifically, conspiracy theorists can be repeatedly wrong, but advocates of the truth need to be perfect. By constantly escalating demands for proof, propagandists can effectively leverage this asymmetry while also priming its future use, often with an even greater asymmetric advantage. The conspiracist is offered freer rein for a broader range of "questions" while the truth teller is burdened with higher and higher standards of proof.

Things to look for:

*

Potential counters:

*

References:

*

T0041 Deny involvement

Part of TA08

Summary: Without "smoking gun" proof (and even with proof), the incident creator can or will deny involvement. This technique also leverages the attacker advantages outlined in T0040 "Demand unsurmountable proof", specifically the asymmetric disadvantage for truth-tellers in a "firehose of misinformation" environment.

Things to look for:

*

Potential counters:

*

References:

*

T0042 Kernel of Truth

Part of TA08

Summary: Wrap lies or altered context/facts around truths.

Influence campaigns pursue a variety of objectives with respect to target audiences, prominent among them: 1. undermine a narrative commonly referenced in the target audience; or 2. promote a narrative less common in the target audience, but preferred by the attacker. In both cases, the attacker is presented with a heavy lift. They must change the relative importance of various narratives in the interpretation of events, despite contrary tendencies.

When messaging makes use of factual reporting to promote these adjustments in the narrative space, they are less likely to be dismissed out of hand; when messaging can juxtapose a (factual) truth about current affairs with the (abstract) truth explicated in these narratives, propagandists can undermine or promote them selectively. Context matters.

Things to look for:

*

Potential counters:

*

References:

*

T0043 Use SMS/ WhatsApp/ Chat apps

Part of TA08

Summary: Direct messaging via encypted app is an increasing method of delivery. These messages are often automated and new delivery and storage methods make them anonymous, viral, and ephemeral. This is a diffucult space to monitor, but also a difficult space to build acclaim or notoriety.

Things to look for:

*

Potential counters:

*

References:

*

T0044 Seed distortions

Part of TA08

Summary: Incident creators often try a wide variety of messages in the early hours surrounding an incident or event in order to give a misleading account or impression.

Examples: (2019) China formally arrests Canadians Spavor and Kovrig, accuses them of spying (in retaliation to detention of Hauwei CFO). (2018) The Russian ministry of defence put out a press release, claiming that they had intelligence Syrian rebel forces were about to gas their own people in Idlib province as part of a “false flag” operation to frame the Syrian government.

Things to look for:

*

Potential counters:

*

References:

*

T0045 Use fake experts

Part of TA08

Summary: Use the fake experts that were set up in T0009. Pseudo-experts are disposable assets that often appear once and then disappear. Give "credibility" to misinformation. Take advantage of credential bias

Things to look for:

*

Potential counters:

*

References:

*

T0046 Search Engine Optimization

Part of TA08

Summary: Manipulate content engagement metrics (ie: Reddit & Twitter) to influence/impact news search results (e.g. Google), also elevates RT & Sputnik headline into Google news alert emails. aka "Black-hat SEO"

Things to look for:

*

Potential counters:

*

References:

*

TA09 Exposure Techniques

T0047 Muzzle social media as a political force

Part of TA09

Summary: Use political influence or the power of state to stop critical social media comments. Government requested/driven content take downs (see Google Transparency reports. (Example 20190 Singapore Protection from Online Falsehoods and Manipulation Bill would make it illegal to spread "false statements of fact" in Singapore, where that information is "prejudicial" to Singapore's security or "public tranquility." Or India/New Delhi has cut off services to Facebook and Twitter in Kashmir 28 times in the past five years, and in 2016, access was blocked for five months -- on the grounds that these platforms were being used for anti-social and "anti-national" purposes.

Things to look for:

*

Potential counters:

*

References:

*

T0048 Cow online opinion leaders

Part of TA09

Summary: Intimidate, coerce, threaten critics/dissidents/journalists via trolling, doxing. Examples: Philippines, Maria Ressa and Rappler journalists targeted the Duterte regime, lawsuits, trollings, banned from the presidential palace where press briefings take place; 2017 bot attack on five ProPublica Journalists.

Things to look for:

*

Potential counters:

*

References:

*

T0049 Flooding

Part of TA09

Summary: Flooding and/or mobbing social media channels feeds and/or hashtag with excessive volume of content to control/shape online conversations and/or drown out opposing points of view. Bots and/or patriotic trolls are effective tools to achieve this effect.

Example (2018): bots flood social media promoting messages which support Saudi Arabia with intent to cast doubt on allegations that the kingdom was involved in Khashoggi’s death.

Things to look for:

*

Potential counters:

*

References:

*

T0050 Cheerleading domestic social media ops

Part of TA09

Summary: Deploy state-coordinated social media commenters and astroturfers. Both internal/domestic and external social media influence operations, popularized by China (50cent Army manage message inside the "Great Firewall") but also techniques used by

Chinese English-language social media influence operations are seeded by state-run media, which overwhelmingly present a positive, benign, and cooperative image of China.

Things to look for:

*

Potential counters:

*

References:

*

T0051 Fabricate social media comment

Part of TA09

Summary: Use government-paid social media commenters, astroturfers, chat bots (programmed to reply to specific keywords/hashtags) influence online conversations, product reviews, web-site comment forums. (2017 example) the FCC was inundated with nearly 22 million public comments on net neutrality (many from fake accounts)

Things to look for:

*

Potential counters:

*

References:

*

T0052 Tertiary sites amplify news

Part of TA09

Summary: Create content/news/opinion web-sites to cross-post stories. Tertiary sites circulate and amplify narratives. Often these sites have no masthead, bylines or attribution.

Examples of tertiary sites include Russia Insider, The Duran, geopolitica.ru, Mint Press News, Oriental Review, globalresearch.ca. Examples: (2019, Domestic news): Snopes reveals Star News Digital Media, Inc. may look like a media company that produces local news, but operates via undisclosed connections to political activism. (2018) FireEye reports on Iranian campaign that created between April 2018 and March 2019 sites used to spread inauthentic content from websites such as Liberty Front Press (LFP), US Journal, and Real Progressive Front during the 2018 US mid-terms.

Things to look for:

*

Potential counters:

*

References:

*

T0053 Twitter trolls amplify and manipulate

Part of TA09

Summary: Use trolls to amplify narratives and/or manipulate narratives. Fake profiles/sockpuppets operating to support individuals/narratives from the entire political spectrum (left/right binary). Operating with increased emphasis on promoting local content and promoting real Twitter users generating their own, often divisive political content, as it's easier to amplify existing content than create new/original content. Trolls operate where ever there's a socially divisive issue (issues that can/are be politicized) e.g. BlackLivesMatter or MeToo

Things to look for:

*

Potential counters:

*

References:

*

T0054 Twitter bots amplify

Part of TA09

Summary: Use bots to amplify narratives above algorithm thresholds. Bots are automated/programmed profiles designed to amplify content (ie: automatically retweet or like) and give appearance it's more "popular" than it is. They can operate as a network, to function in a coordinated/orchestrated manner. In some cases (more so now) they are an inexpensive/disposable assets used for minimal deployment as bot detection tools improve and platforms are more responsive.(example 2019) #TrudeauMustGo

Things to look for:

*

Potential counters:

*

References:

*

T0055 Use hashtag

Part of TA09

Summary: Use a dedicated hashtag for the incident (e.g. #PhosphorusDisaster) - either create a campaign/incident specific hashtag, or take over an existing hashtag.

Things to look for:

*

Potential counters:

*

References:

*

T0056 Dedicated channels disseminate information pollution

Part of TA09

Summary: Output information pollution (e.g. articles on an unreported false story/event) through channels controlled by or related to the incident creator. Examples include RT/Sputnik or antivax websites seeding stories.

Things to look for:

*

Potential counters:

*

References:

*

TA10 Go Physical Techniques

T0057 Organise remote rallies and events

Part of TA10

Summary: Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives. Example: Facebook groups/pages coordinate/more divisive/polarizing groups and activities into the public space. (Example) Mueller's report, highlights, the IRA organized political rallies in the U.S. using social media starting in 2015 and continued to coordinate rallies after the 2016 election

Things to look for:

*

Potential counters:

*

References:

*

T0061 Sell merchandising

Part of TA10

Summary: Sell hats, t-shirts, flags and other branded content that's designed to be seen in the real world

Things to look for:

*

Potential counters:

*

References:

*

TA11 Persistence Techniques

T0058 Legacy web content

Part of TA11

Summary: Make incident content visible for a long time, e.g. by exploiting platform terms of service, or placing it where it's hard to remove or unlikely to be removed.

Things to look for:

*

Potential counters:

*

References:

*

T0059 Play the long game

Part of TA11

Summary: Play the long game can mean a couple of things:

1. To plan messaging and allow it to grow organically without conducting your own amplification. This is methodical and slow and requires years for the message to take hold (e.g. China and its constant messaging that Taiwan and Hong Kong are part of one China).

2. To develop a series of seemingly disconnected messaging narratives that eventually combine into a new narrative.

Things to look for:

*

Potential counters:

*

References:

*

T0060 Continue to amplify

Part of TA11

Summary: continue narrative or message amplification after the main incident work has finished

Things to look for:

*

Potential counters:

*

References:

*

TA12 Measure Effectiveness Techniques

References

Also, O'reilly's "4 short links" had this neat bit on source hacking techniques, accompanied by definitions: Source Hacking — In this report, we identify four specific techniques of source hacking: 1. Viral Sloganeering: repackaging reactionary talking points for social media and press amplification; 2. Leak Forgery: prompting a media spectacle by sharing forged documents; 3. Evidence Collages: compiling information from multiple sources into a single, shareable document, usually as an image; 4. Keyword Squatting: the strategic domination of keywords and sockpuppet accounts to misrepresent groups or individuals These four tactics of source hacking work.

Rand Waltman's rumours series

- https://twitter.com/CogSec/status/1271758646485987329?s=20