AMITT TTP Guide

Introduction

About this report

This report contains a description (eventually 1-2 pages long) of each tactic, technique and procedure (TTP) in AMITT (the 'squares' on the AMITT grid), designed for people using AMITT in the field. This includes advice on how to investigate each tactic - e.g. "This incident is using the pump priming tactic, what are the indicators you need to look for, what are the countermeasures you could use"", and how to counter it in the user's context.

This is a companion document to the AMITT Design Guide and the github repository https://github.com/cogsec-collaborative/amitt which contains the master copy of the AMITT models.

Structure of this report

This report contains a section for each tactic stage ("column") of the AMITT framework model. In that section is a description of the tactic stage, then descriptions of disinformation creators' TTPs (the squares on the AMITT framework diagram, aka "red team" techniques), and descriptions of disinformation defenders' TTPs (aka 'countermeasures' or "blue team" techniques). The list of counter ("blue team") techniques are sorted by defence type.

Each technique description includes these fields:

- A description
- Indicators
- Counters
- Examples

Each counter-technique descriptions will include:

- A description
- Who is involved in this counter
- Intended effects
- How to measure
- Examples

Future Work

There's a lot more to populate in this document, including things like indicators for each TTP. CogSecCollab also have many collected suggestions for AMITT changes - these are in the companion document, "Proposed Changes to AMITT TTPs".

TA01 Strategic Planning

TA01 Disinformation Techniques

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

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

- 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.
- 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.

Indicators:

- 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

Counters

- Media: moving from the 24-hour news cycle, so storytelling becomes less of a tactical back-and forth.
- C00020: Delegitimize the 24 hour news cycle (needs media)

Examples

- 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

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.

Indicators:

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

Counters:

- C00026: Shore up democracy based messages (peace, freedom) - make it sexy
- C00031: Dilute the core narrative - create multiple permutations, target / amplify
- C00088: Poison pill recasting of message
- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00022: Inoculate. Positive campaign to promote feeling of safety - to counter ability and fear based attacks
- Mockery. Frequently making fun of the Wumao groups is very effective at defanging their impact. In particular when their "shill" nature is exposed and they are mocked for being robotic unthinking automatons, their messaging loses emphasis. Make jokes about their own limited repertoire of approved messages.

Examples:

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

T0003 Leverage Existing Narratives

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.

Indicators:

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

Counters
- C00031: Dilute the core narrative - create multiple permutations, target / amplify

Examples:

T0004 Competing Narratives

Advance competing narratives connected to the same issue ie: deny an incident, and at the same time dismiss it.
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.

Indicators:

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

Counters:

- C00042: Address truth contained in narratives

Examples:

- MH17 "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).

TA01 Disinformation Tasks

Goal Setting

Population research / audience analysis (Centre of Gravity)

Campaign design (objective design)

TA01 Counters

C00006: Charge for social media (Deny)

Charge money for the use of social media accounts.

- Earliest affected tactic stage: TA01 Strategic Planning.
- Who is involved in this counter: platform_admin:socialmedia. Social media executives, social media admins
- Intended effects: increase the cost of running large-scale disinformation seeding, amplification, and use across multiple channels.
- How to measure: look at botnet markets for changes in pricing, availability etc.
- Examples:

C00007: BetterBusinessBureau (BBB) for news media (Deny)

Create framework for this

C00008: Create shared fact-checking database (Deny)

(factcheckers)

C00009: Educate high profile influencers on best practices (Deny)

(influencers,educators)

C00010: Enhanced privacy regulation for social media (Deny)

(government:policymakers)

C00011: Media literacy. Games to identify fake news (Deny)

(educators,games designers,developers)

C00012: Platform regulation (Deny)

(government:policymakers)

C00013: Rating framework for news (Deny)

- full transcripts, link source, add items, BBB for news

C00014: Real-time updates to fact-checking database (Deny)

(factcheckers)

C00015: Reputation scores for social media users (Deny)

(data_scientist,datastreams)

C00016: Social media as a privilege not right (Deny)

C00073: Educate on how to handle info pollution (Deny)

(educators)
Push out targeted education on why it's pollution

C00017: Media campaign promoting in-group to out-group in person communication / activities (Disrupt)

(media)

C00018: Promote constructive communication by shaming division-enablers (Disrupt)

C00019: Promote playbooks to call out division-enablers (Disrupt)

C00153: Use offensive cyber action (Disrupt)

(infosec)

C00159: Campaign mindset and associated toolbox (Disrupt)

C00205: strong dialogue between the federal government and private sector to encourage better reporting (Disrupt)

(companies,government)

C00020: Delegitimize 24-hour news cycle (Degrade)

(media)

C00021: Encourage in-person communication (Degrade)

C00022: Inoculate. Positive campaign to promote feeling of safety (Degrade)

- to counter ability and fear based attacks

C00023: Promote civility as an identity that people will defend (Degrade)

C00024: Promote constructive narratives (Degrade)

i.e. not polarising. Pro-life, pro-choice, or pro-USA?

C00025: Promote identity neutral narratives (Degrade)

C00026: Shore up democracy based messages (Degrade)

(peace, freedom) - make it sexy

C00027: Create culture of civility (Deter)

C00161: Coalition Building and Third-Party Inducements (Deter)

C00176: Improve Coordination with and feedback from the U.S. private sector (Deter)

C00207: tit-for-tat campaign (Deter)

(government,platforms)

See also: C00009 (Deny)

TA02 Objective Planning

TA02 Disinformation Techniques

T0005 Center of Gravity Analysis

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.

Indicators:

- 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

Counters:

- Microtarget and countermessage most likely target groups
- C00136: Microtarget most likely targets then send them countermessages
- C00036: Infiltrate the in-group to discredit leaders: divide

Examples:

T0006 Create Master Narratives

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.

Indicators:

- Existing disinformation narratives
- New inauthentic narratives

Counters:

- C00031: Dilute the core narrative - create multiple permutations, target / amplify
- C00088: Poison pill recasting of message
- C00023: Promote civility as an identity that people will defend
- C00024: Promote constructive narratives i.e. not polarising. Pro-life, pro-choice, or pro-USA?
- C00008: Create shared fact-checking database (factcheckers)
- C00014: Real-time updates to fact-checking database (factcheckers)
- C00025: Promote identity neutral narratives

Examples:

TA02 Disinformation Tasks

Identify target subgroups

Analyse subgroups

Create master narratives

Decide on techniques (4Ds etc)

Create subnarratives

4chan/8chan coordinating content

TA02 Counters

C00070: Block access to platform. DDOS an attacker (Deny)

C00028: Blockchain audit log and validation with collaborative decryption to post comments (Disrupt)

C00029: Create fake website to issue counter narrative and counter narrative through physical merchandise (Disrupt)

C00030: Develop a compelling counter narrative (truth based) (Disrupt)

C00031: Dilute the core narrative - create multiple permutations, target / amplify (Disrupt)

C00032: Hijack content and link to truth-based info (Disrupt)
(platform)

TA03 Develop People

TA03 Disinformation Techniques

T0007 Create fake Social Media Profiles / Pages / Groups

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.

Indicators:

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

Counters:

- C00012: Platform regulation (government:policymakers)
- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00039: Standard reporting for false profiles
- C00133: Deplatform Account* (platform_admin)
- C00135: Deplatform message groups and/or message boards (platform_admin)
- C00036: Infiltrate the in-group to discredit leaders: divide

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.

T0008 Create fake or imposter news sites

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.

Indicators:

- Local news sites that are unknown to local residents

Counters:

- C00053: Delete old accounts / Remove unused social media accounts (platform_admin,platform_admin:socialmedia,public:account_owners)
- C00070: Block access to platform. DDOS an attacker
- C00008: Create shared fact-checking database (factcheckers)
- C00014: Real-time updates to fact-checking database (factcheckers)

Examples:

- Pink slime
- 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.

T0009 Create fake experts

Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself.

Indicators:

Counters:

- C00133: Deplatform Account* (platform_admin)
- C00008: Create shared fact-checking database (factcheckers)
- C00014: Real-time updates to fact-checking database (factcheckers)
- C00040: third party verification for people

Examples:

- 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.

TA03 Disinformation Tasks

Create personas

Recruit contractors

Recruit partisans

Find influencers

TA03 Counters

C00033: Build cultural resistance to false content (Deny)

C00034: Create more friction at account creation (Deny)

C00035: Friction (Deny)

C00036: Infiltrate the in-group to discredit leaders (divide) (Deny)

C00039: Standard reporting for false profiles (Deny)

C00040: third party verification for people (Deny)

C00150: Call them out (Deny)

C00155: Ban incident actors from funding sites (Deny)

(platform_admin:fundingsites)

C00160: find and train influencers (Deny)

(data_scientist,influencers)

C00197: remove suspicious accounts (Deny)

For example, Facebook. This is active policy on many sites, and comes with a large burden of proof.

C00042: Address truth contained in narratives (Disrupt)

C00043: Detect hijacked accounts and re-allocate them (Disrupt)
(platform_admin,activists,civil_society,money)

C00044: Keep people from posting to social media immediately (Disrupt)
(platform_algorithms)

C00045: S4d detection and re-allocation approaches (Disrupt)

C00085: Demuting content (Disrupt)

C00164: compatriot policy (Disrupt)

C00170: elevate information as a critical domain of statecraft (Disrupt)

C00179: Identify, monitor, and, if necessary, target externally-based non-attributed social media accounts (Disrupt)
Including Russia-based

C00046: Marginalise and discredit extremist (Degrade)

C00047: Coordinated inauthentics (Deceive)

C00189: Ongoing analysis/monitoring of "flagged" profiles (Destroy)

C00048: Name and Shame (Deter)

See also: C00011 (Disrupt)

TA04 Develop Networks

TA04 Disinformation Techniques

T0010 Cultivate ignorant agents

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 known as "useful idiots" or "unwitting agents".

Indicators:

Counters:

- C00136: Microtarget most likely targets then send them countermessages
- C00009: Educate high profile influencers on best practices (influencers,educators)
- C00093: Establish tailored code of conduct for individuals with many followers

Examples:

T0011 Hijack legitimate account

Hack or take over legitimate accounts to distribute misinformation or damaging content.

Indicators:

Counters:

- C00043: Detect hijacked accounts and reallocate them (platform_admin,activists,civil_society,money)
- C00053: Delete old accounts / Remove unused social media accounts (platform_admin,platform_admin:socialmedia,public:account_owners)
- C00133: Deplatform Account* (platform_admin)
- C00135: Deplatform message groups and/or message boards (platform_admin)
- C00045: S4d detection and re-allocation approaches

Examples:

- 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.

T0012 Use concealment

Use anonymous social media profiles.

Indicators:

Counters:

- C00049: Influence literacy training (educators)
- C00050: Anti-elicitation training (educators)
- C00051: Phishing prevention education etc (educators)
- C00052: Infiltrate platforms (activists)

Examples:

- 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.
- Page or group administrators, masked "whois" website directory data, no bylines connected to a news article, no masthead connected to news websites.

T0013 Create fake websites

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.

Indicators:

Counters:

- C00008: Create shared fact-checking database (factcheckers)
- C00014: Real-time updates to fact-checking database (factcheckers)

Examples:

T0014 Create funding campaigns

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.

Indicators:

Counters:

- C00012: Platform regulation (government:policymakers)
- C00070: Block access to platform. DDOS an attacker.
- C00133: Deplatform Account* (platform_admin)
- C00008: Create shared fact-checking database (factcheckers)
- C00014: Real-time updates to fact-checking database (factcheckers)

Examples:

- (2016) #VaccinateUS Gofundme campaigns to pay for Targeted facebook ads (Larry Cook, targeting Washington State mothers, $1,776 to boost posts over 9 months).

T0015 Create hashtag

Many incident-based campaigns will create a hashtag to promote their fabricated event. 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)

Indicators:

Counters:

- C00145: Pollute the data voids with wholesome content (Kittens! Babyshark!)
- C00066: Co-opt a hashtag and drown it out (hijack it back)
- C00088: Poison pill recasting of message
- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00070: Block access to platform. DDOS an attacker.

Examples:

- #ColumbianChemicals to promote a fake story about a chemical spill in Louisiana.

TA04 Disinformation Tasks

Network building

Network infiltration

Identify targets

Susceptible audience members in networks

TA04 Counters

C00049: Influence literacy training (Deny)

(educators)

C00050: Anti-elicitation training (Deny)

(educators)

C00051: Phishing prevention education etc (Deny)

(educators)

C00055: Empower existing regulators to govern social media (Deny)

(government:policymakers,government,platform_admin)

C00056: Leave social media (Deny)

C00057: Privacy standards (Deny)

C00058: Report crowdfunder as violator (Deny)

C00059: Verification of project before posting fund requests (Deny)

This counters funding campaigns

C00152: Name and shame (Deny)

C00157: Build alternative news sources (Deny)

C00174: Free and Fair Press (Deny)

C00060: Legal action against for-profit engagement factories (Disrupt)

(government:policymakers)
Enhanced legal enforcement against for-profit follower/engagement factories.

C00061: Inoculating at language (Disrupt)

C00162: Unravel/target the Potemkin villages (Disrupt)

collect data/map constellations of Russian“civil society”.

C00052: Infiltrate platforms (Degrade)

(activists)

C00053: Remove old and unused social media accounts (Degrade)

(platform_admin,platform_admin:socialmedia,public:account_owners)

Delete or archive unused social media accounts.

C00054: Media literacy training (Degrade)

(educators,libraries,schools,DHS,NGO,platform_outreach,media,community_groups,religious_organisations)

C00062: Free open library sources worldwide (Destroy)

See also: C00011 (Disrupt), C00085 (Disrupt)

TA05 Microtargeting

TA05 Disinformation Techniques

T0016 Clickbait

Create attention grabbing headlines (outrage, doubt, humor) required to drive traffic & engagement.

Indicators:

Counters:

- C00069: Mark clickbait visually

Examples:

- (2016) “Pope Francis shocks world, endorses Donald Trump for president.”
- (2016) "FBI director received millions from Clinton Foundation, his brother’s law firm does Clinton’s taxes”. This is a key asset

T0017 Promote online funding

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

Indicators:

Counters:

- C00068: Expose online funding as fake
- C00088: Poison pill recasting of message
- C00070: Block access to platform. DDOS an attacker
- C00133: Deplatform Account* (platform_admin)
- C00135: Deplatform message groups and/or message boards (platform_admin)
- C00036: Infiltrate the in-group to discredit leaders (divide)
- C00067: Denigrate the recipient/ project (of online funding)
- C00093: Establish tailored code of conduct for individuals with many followers

Examples:

T0018 Paid targeted ads

Create or fund advertisements targeted at specific populations

Indicators:

Counters:

- C00133: Deplatform Account* (platform_admin)
- C00063: Ban political microtargeting (government:policymakers)
- C00065: Ban political ads (government:policymakers)

Examples:

TA05 Disinformation Tasks

TA05 counters

C00063: Ban political microtargeting (Deny)

(government:policymakers)

C00216: Use advertiser controls to stem flow of funds to bad actors (Deny)

(platform_admin:adtech)

C00065: Ban political ads (Disrupt)

(government:policymakers)

C00066: Co-opt a hashtag and drown it out (hijack it back) (Disrupt)

C00067: Denigrate funding recipient/ project (Disrupt)

C00068: Expose online funding as fake (Disrupt)

C00069: Mark clickbait visually (Disrupt)

C00140: "Bomb" link shorteners with lots of calls (Disrupt)

C00141: "Hey this story is old" popup for old URLs (Disrupt)

(platform_algorithms)
Popup when messaging with old URLs.

C00142: "This has been disproved - do you want to forward it" (Disrupt)

(platform_algorithms)

See also: C00011 (Disrupt), C00085 (Disrupt)

TA06 Develop Content

TA06 Disinformation Techniques

T0019 Generate information pollution

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.

Indicators:

Counters:

- C00091: Honeypot social community
- C00071: Block source of pollution
- C00073: Educate on how to handle info pollution. Push out targeted education on why it's pollution (educators)
- C00042: Address truth contained in narratives

Examples:

T0020 Trial content

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

Indicators:

Counters:

- C00137: Pollute the AB-testing data feeds
- C00149: Poison the monitoring & evaluation data
- C00090: Fake engagement system

Examples:

T0021 Memes

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.

Indicators:

Counters:

- C00079: Change search algorithms for hate and extremist queries to show content sympathetic to opposite side
- C00089: Throttle number of forwards
- C00076: Prohibit images in political discourse channels

Examples:

- 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

"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."

Indicators:

Counters:

- C00074: Identify identical content and mass deplatform (platform_admin,platform_admin:socialmedia)
- C00072: Content censorship in non-relevant domains e.g. Pinterest antivax
- C00023: Promote civility as an identity that people will defend
- C00024: Promote constructive narratives i.e. not polarising. Pro-life, pro-choice, or pro-USA?
- C00096: Strengthen institutions that are always truth tellers
- C00025: Promote identity neutral narratives
- C00042: Address truth contained in narratives

Examples:

- 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

T0023 Distort facts

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

Indicators:

Counters:

- C00023: Promote civility as an identity that people will defend
- C00024: Promote constructive narratives i.e. not polarising. Pro-life, pro-choice, or pro-USA?
- C00092: Establish a truth teller reputation score for individuals with many followers
- C00095: Keep score
- C00025: Promote identity neutral narratives

Examples:

T0024 Create fake videos and images

Create fake videos and/or images by manipulating existing content or generating new content (e.g. deepfakes).

Indicators:

Counters:

- C00092: Establish a truth teller reputation score for individuals with many followers
- C00076: Prohibit images in political discourse channels

Examples:

- Pelosi video (making her appear drunk)
- Photoshopped shark on flooded streets of Houston TX.

T0025 Leak altered documents

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

Indicators:

Counters:

- C00074: Identify identical content and mass deplatform (platform_admin,platform_admin:socialmedia)
- C00012: Platform regulation (government:policymakers)
- C00092: Establish a truth teller reputation score for individuals with many followers
- C00036: Infiltrate the in-group to discredit leaders (divide)
- C00202: Set data 'honeytraps'
- C00210: Use encrypted apps for confidential communication

Examples:

- (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.

T0026 Create fake research

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

Indicators:

Counters:

- C00074: Identify identical content and mass deplatform (platform_admin,platform_admin:socialmedia)
- C00094: Force full disclosure on corporate sponsor of research
- C00092: Establish a truth teller reputation score for individuals with many followers

Examples:

T0027 Adapt existing narratives

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."

Indicators:

Counters:

- C00023: Promote civility as an identity that people will defend
- C00024: Promote constructive narratives i.e. not polarising. Pro-life, pro-choice, or pro-USA?
- C00025: Promote identity neutral narratives
- C00042: Address truth contained in narratives

Examples:

T0028 Create competing narratives

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.

Indicators:

Counters:

- C00042: Address truth contained in narratives

Examples:

TA06 Disinformation Tasks

Content creation

Content appropriation

TA06 Counters

C00071: Block source of pollution (Deny)

C00072: Remove non-relevant content (Deny)

E.g. antivax in Pinterest domains. Moderators generally do this already, but there are exceptions, e.g. the Ravelry discussions on Trump-related knitting patterns.

C00074: Identify identical content and mass deplatform (Deny)

(platform_admin,platform_admin:socialmedia)

C00075: normalise language (Deny)

C00076: Prohibit images in political discourse channels (Deny)

C00165: Limit access to alterable documents (Deny)

C00167: Deploy Information and Narrative-Building in Service of Statecraft (Deny)

C00171: social media content take-downs (Deny)

(platform_admin:socialmedia)

C00172: social media page removal (Deny)

(platform_admin:socialmedia)

C00202: Set data 'honeytraps' (Deny)

C00210: Use encrypted apps for confidential communication (Deny)

C00077: Active defence: replay "develop people" (Disrupt)

C00078: Change Search Algorithms for Disinformation Content (Disrupt)

More specifically, change image search algorithms for hate groups and extremists

C00079: Change search algorithms for hate and extremist queries to show content sympathetic to opposite side (Disrupt)

C00080: Create competing narrative (Disrupt)

C00081: Highlight and explain flooding with noise (Disrupt)

Discredit by pointing out the "noise" and informing public that "flooding" is a technique of disinformation campaigns; point out intended objective of "noise"

C00082: Ground truthing as automated response to pollution (Disrupt)

C00084: Steal their truths (Disrupt)

C00219: Add metadata to content - out of the control of the adversary (Disrupt)

C00086: Distract from noise with addictive content (Degrade)

C00087: Make more noise (Degrade)

C00088: Poison pill recasting of message (Degrade)

C00089: Throttle number of forwards (Degrade)

C00090: Fake engagement system (Deceive)

C00091: Honeypot social community (Deceive)

C00092: Establish a truth teller reputation score for influencers (Deter)

TODO add to Definitions: Influencer = individual with many followers.

C00093: Influencer code of conduct (Deter)

Establish tailored code of conduct for individuals with many followers

C00094: Force full disclosure on corporate sponsor of research (Deter)

C00095: Keep score (Deter)

C00096: Strengthen institutions that are always truth tellers (Deter)

See also: C00008 (General), C00014 (General), C00053 (General), C00085 (Disrupt), C00070 (Deny), C00073 (Deny), C00085 (Degrade)

TA07 Channel Selection

TA07 Disinformation Techniques

T0029 Manipulate online polls

Create fake online polls, or manipulate existing online polls. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well

Indicators:

Counters:

- C00136: Microtarget most likely targets then send them countermessages
- C00103: Create a bot that engages / distract trolls (developers)
- C00097: Require use of verified identities to contribute to poll or comment (platform_algorithms)
- C00101: Create participant friction (platform_algorithms)
- C00102: Make repeat voting harder (platform_admin)
- C00009: Educate high profile influencers on best practices (influencers,educators)

Examples:

- Flooding FCC with comments;
- Creating fake engagement metrics of Twitter/Facebook polls to manipulate perception of given issue.

T0030 Backstop personas

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

Indicators:

Counters:

- C00099: Strengthen verification methods (platform_algorithms)

Examples:

T0031 YouTube

Use YouTube as a narrative dissemination channel

Indicators:

Counters:

Examples:

T0032 Reddit

Use Reddit as a narrative dissemination channel

Indicators:

Counters:

- C00107: Content moderation

Examples:

T0033 Instagram

Use Instagram as a narrative dissemination channel

Indicators:

Counters:

Examples:

T0034 LinkedIn

Use LinkedIn as a narrative dissemination channel

Indicators:

Counters:

Examples:

T0035 Pinterest

Use Pinterest as a narrative dissemination channel

Indicators:

Counters:

- C00107: Content moderation

Examples:

T0036 WhatsApp

Use WhatsApp as a narrative dissemination channel

Indicators:

Counters:

Examples:

T0037 Facebook

Use Facebook as a narrative dissemination channel

Indicators:

Counters:

Examples:

T0038 Twitter

Use Twitter as a narrative dissemination channel

Indicators:

Counters:

- C00098: Revocation of "verified" (platform_admin)

Examples:

TA07 Disinformation Tasks

TA07 Countermeasures

Tactic	Technique	Dominant Media	Scope	Type of Engagement	Content Availability	Style	Recommended Content	Title

TA07	T0031 YouTube	Visual	Content	Content	Content	Content	Automatic	Passive / Autoloading
TA07	T0032 Reddit	Text	Direct	User	Public	Conversation	Manual	Active
TA07	T0033 Instagram	Visual	Interest based	Content	Content	Content	Manual	Active
TA07	T0034 LinkedIn	Text	Narrow	User	Content	Content	Manual	Active
TA07	T0035 Pinterest	Visual	Content	Content	Content	Content	Automatic	Passive
TA07	T0036 WhatsApp	Text	Content	User	Private	Content	Manual	Active
TA07	T0037 Facebook	Text	Broad	User	Semi-Private	Content	Automatic	Passive
TA07	T0038 Twitter	Text	Indirect	User	Public	Performance Art	Automatic	Passive
TA07	T0070 Gaming Platforms	Content	Content	Content	Content	Content	Content	Content
TA07	T0071	Content	Content	Content	Content	Content	Content	Content

C00133: Deplatform Account (General)

(platform_admin)

C00135: Deplatform message groups, message boards (General)

(platform_admin)

C00097: Require verified identities to contribute to poll or comment (Deny)

(platform_algorithms)
Users to be verified before answering a poll or commenting.

C00098: Revocation of "verified" (Deny)

(platform_admin)

C00099: Strengthen verification methods (Deny)

(platform_algorithms)

C00107: Content moderation (Deny)

C00110: Monetize centrist SEO by subsidizing the difference in greater clicks towards extremist content (Deny)

(funding)

C00195: Redirect Method (Deny)

C00217: Registries alert when large batches of newsy URLs get registered together (Deny)

(platform_admin)

C00100: Hashtag jacking (Disrupt)

C00105: Buy more advertising than the adversary to shift influence and algorithms (Disrupt)

(money,adtech)

C00106: Click-bait centrist content (Disrupt)

C00109: De-escalation (Disrupt)

C00196: Include the role of social media in the regulatory framework for media (Disrupt)

(government)

C00214: Create policy that makes social media police disinformation (Disrupt)

(government:policymakers)

C00215: Use fraud legislation to clean up social media (Disrupt)

(government:policymakers)

C00101: Create participant friction (Degrade)

(platform_algorithms)

C00102: Make repeat voting harder (Degrade)

(platform_admin)

C00111: Present sympathetic views of opposite side (Degrade)

(media,content_creators)

C00103: Create a bot that engages / distract trolls (Deceive)

(developers)

See also: C00078 (General), C00044 (General), C00012 (General), C00055 (General), C00092 (General), C00028 (General), C00016 (General), C00060 (General), C00085 (General), C00093 (General),

TA08 Pump Priming

TA08 Disinformation Techniques

T0039 Bait legitimate influencers

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.

Indicators:

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

Counters:

- Platforms: Clearly marking known political influences on sources, e.g. marking RT as Russian-owned etc.
- C00093: Establish tailored code of conduct for individuals with many followers
- C00114: Don't engage with payloads (public)

Examples:

T0040 Demand unsurmountable proof

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.

Indicators:

Counters:

- C00112: "Prove they are not an op!"

Examples:

T0041 Deny involvement

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.

Indicators:

Counters:

- C00116: Provide proof of involvement

Examples:

T0042 Kernel of Truth

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.

Indicators:

Counters:

- C00042: Address truth contained in narratives
- C00112: "Prove they are not an op!"

Examples:

T0043 Use SMS/ WhatsApp/ Chat apps

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.

Indicators:

Counters:

- C00012: Platform regulation (government:policymakers)
- C00016: Social media as a privilege not right
- C00121: Tool transparency and literacy for channels people follow.

Examples:

T0044 Seed distortions

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.

Indicators:

Counters:

- C00042: Address truth contained in narratives
- C00118: Repurpose images with new text
- C00119: Engage payload and debunk. Provide link to facts.

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.

T0045 Use fake experts

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

Indicators:

Counters:

- C00113: Debunk and defuse a fake expert / credentials. Attack audience quality of fake expert
- C00133: Deplatform Account* (platform_admin)
- C00135: Deplatform message groups and/or message boards (platform_admin)
- C00092: Establish a truth teller reputation score for individuals with many followers

Examples:

T0046 Search Engine Optimization

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"

Indicators:

Counters:

- C00145: Pollute the data voids with wholesome content (Kittens! Babyshark!)
- C00115: Expose actor and intentions
- C00078: Change Search Algorithms for Disinformation Content. More specifically, change image search algorithms for hate groups and extremists
- C00012: Platform regulation (government:policymakers)
- C00070: Block access to platform. DDOS an attacker.
- C00117: Downgrade de-amplify label promote counter to disinformation

Examples:

TA08 Disinformation Tasks

Anchor trust / credibility

Insert themes

TA08 Pump Priming Counters

C00124: Don't feed the trolls (General)

(public,media)

C00136: Microtarget most likely targets then send them countermessages (General)

C00112: "Prove they are not an op!" (Deny)

C00113: Debunk and defuse a fake expert / credentials. Attack audience quality of fake expert (Deny)

C00114: Don't engage with payloads (Deny)

(public)

C00115: Expose actor and intentions (Deny)

C00116: Provide proof of involvement (Deny)

C00154: Ask media not to report false information (Deny)

(media)

C00204: Strengthen local media (Deny)

(media)

C00188: Newsroom/Journalist training to counter SEO influence (Disrupt)

(media,educators)

C00193: promotion of a “higher standard of journalism” (Disrupt)
(media,educators)

C00203: Stop offering press credentials to propaganda outlets (Disrupt)
(government)

C00117: Downgrade de-amplify label promote counter to disinformation (Degrade)

C00118: Repurpose images with new text (Degrade)

C00120: Open dialogue about design of platforms to produce different outcomes (Deter)

C00119: Engage payload and debunk. Provide link to facts. (Deter)

C00121: Tool transparency and literacy for channels people follow. (Deter)

See also: C00018 (General), C00019 (General), C00048 (General), C00009 (General), C00011 (General), C00008 (General), C00014 (General), C00092 (General), C00028 (General), C00027 (General), C00085 (General)

TA09 Exposure

TA09 Disinformation Techniques

T0047 Muzzle social media as a political force

Use political influence or the power of state to stop critical social media comments. Government requested/driven content takedowns

Indicators:

Counters:

- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00092: Establish a truth teller reputation score for individuals with many followers
- C00027: Create culture of civility
- C00060: Enhanced legal enforcement against for-profit follower/engagement factories (government:policymakers)
- C00093: Establish tailored code of conduct for individuals with many followers

Examples:

- See Google Transparency reports.
- 2019: 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."
- 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.

T0048 Cow online opinion leaders

Intimidate, coerce, threaten critics/dissidents/journalists via trolling, doxing.

Indicators:

Counters:

- C00048: Name and Shame
- C00115: Expose actor and intentions
- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00027: Create culture of civility

- C00093: Establish tailored code of conduct for individuals with many followers

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.

T0049 Flooding

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.

Indicators:

Counters:

- C00044: Keep people from posting to social media immediately (platform_algorithms)
- C00131: Seize and analyse botnet servers (server_admin)
- C00123: Bot control

Examples:

- (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.

T0050 Cheerleading domestic social media ops

Deploy state-coordinated social media commenters and astroturfers. Both internal/domestic and external social media influence operations,

Indicators:

Counters:

-

Examples:

- 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.

T0051 Fabricate social media comment

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.

Indicators:

Counters:

- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00123: Bot control

Examples:

- (2017) the FCC was inundated with nearly 22 million public comments on net neutrality (many from fake accounts)

T0052 Tertiary sites amplify news

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.

Indicators:

Counters:

- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00070: Block access to platform. DDOS an attacker.
- C00123: Bot control

Examples:

- Examples of tertiary sites include Russia Insider, The Duran, geopolitica.ru, Mint Press News, Oriental Review, globalresearch.ca.
- (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.

T0053 Twitter trolls amplify and manipulate

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.

Indicators:

Counters:

- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00144: Buy out troll farm employees / offer them jobs
- C00092: Establish a truth teller reputation score for individuals with many followers
- C00027: Create culture of civility
- C00093: Establish tailored code of conduct for individuals with many followers
- C00123: Bot control

Examples:

- Trolls operate wherever there's a socially divisive issue (issues that can/are be politicized) e.g. BlackLivesMatter or MeToo

T0054 Twitter bots amplify

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.

Indicators:

Counters:

- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00044: Keep people from posting to social media immediately (platform_algorithms)
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00131: Seize and analyse botnet servers (server_admin)
- C00123: Bot control

Examples:

- (2019) #TrudeauMustGo

T0055 Use hashtag

Use a dedicated hashtag for the incident - either create a campaign/incident specific hashtag, or take over an existing hashtag.

Indicators:

Counters:

- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00066: Co-opt a hashtag and drown it out (hijack it back)
- C00055: Empower existing regulators to govern social media (government:policymakers,government,platform_admin)
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00070: Block access to platform. DDOS an attacker.
- C00123: Bot control

Examples:

- #PhosphorusDisaster

T0056 Dedicated channels disseminate information pollution

Output information pollution (e.g. articles on an unreported false story/event) through channels controlled by or related to the incident creator.

Indicators:

Counters:

- C00115: Expose actor and intentions
- C00126: Social media amber alert
- C00120: Open dialogue about design of platforms to produce different outcomes
- C00071: Block source of pollution
- C00073: Educate on how to handle info pollution. Push out targeted education on why it's pollution (educators)
- C00036: Infiltrate the in-group to discredit leaders (divide)
- C00042: Address truth contained in narratives
- C00123: Bot control

Examples:

- RT/Sputnik
- Antivax websites seeding stories

TA09 Disinformation Tasks

Deamplification (suppression, censoring)

Amplification

TA09 Counters

C00122: Content moderation. Censorship? (Deny)

(platform_admin)

C00182: malware detection/quarantine/deletion (Deny)

(infosec)

C00218: Censorship (Deny)

(platform_admin)

C00123: Bot control (Disrupt)

C00125: Prepare the population with pre-announcements (Disrupt)

C00126: Social media amber alert (Disrupt)

C00128: Create friction by marking content with ridicule or other "decelerants" (Disrupt)

(influencers:trusted_authority)

C00151: “fight in the light” (Disrupt)

C00156: Better tell the U.S., NATO, and EU story (Disrupt)

(government,military)

C00169: develop a creative content hub (Disrupt)

C00178: Fill information voids with non-disinformation content (Disrupt)

C00190: open engagement with civil society (Disrupt)

(public)

C00194: Provide an alternative to Russian information by expanding and improving local content. (Disrupt)

C00200: Respected figure (influencer) disavows misinfo (Disrupt)

(influencers)

C00211: Use humorous counter-narratives (Disrupt)

C00212: build public resilience by making civil society more vibrant (Disrupt)

(educators,government)

C00158: Use training to build the resilience of at-risk populations (Degrade)

Actors: educators, media

Examples:

- Immunisation through gameplay “pre-bunking”, e.g. the game https://getbadnews.com/#intro
- Education on specific techniques, e.g. the pineapple pizza education on division tactics
- The Finnish education model
- Other counters being explored by groups like the CredCo media literacy working group

C00184: Media exposure (Degrade)

See also: C00011 (General), C00012 (General), C00018 (General), C00019 (General), C00028 (General), C00085 (General), C00086 (General), C00124 (General, Disrupt), C00133 (General), C00135 (General), C00136 (General), C00140 (General), C00141 (General), C00142 (General)

TA10 Go Physical

TA10 Go Physical Techniques

T0057 Organise remote rallies and events

Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives.

Indicators:

Counters:

- C00048: Name and Shame
- C00088: Poison pill recasting of message
- C00129: Use banking to cut off access
- C00070: Block access to platform. DDOS an attacker.
- C00036: Infiltrate the in-group to discredit leaders (divide)

Examples:

- Facebook groups/pages coordinate/more divisive/polarizing groups and activities into the public space.
- 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

T0061 Sell merchandising

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

Indicators:

Counters:

- C00048: Name and Shame
- C00068: Expose online funding as fake
- C00129: Use banking to cut off access
- C00070: Block access to platform. DDOS an attacker.
- C00067: Denigrate the recipient/ project (of online funding)

Examples:

- Qanon merchandise on Amazon and other sales sites.

TA10 Disinformation tasks

TA10 Counters

C00129: Use banking to cut off access (Deny)

C00130: Mentorship: elders, youth, credit. Learn vicariously. (Deter)

See also: C00012 (General), C00018 (General), C00019 (General), C00028 (General), C00085 (General), C00133 (General), C00135 (General), C00136 (General), C00140 (General), C00141 (General), C00142 (General)

TA11 Persistence

TA11 Disinformation Techniques

T0058 Legacy web content

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.

Indicators:

Counters:

- C00085: Demuting content

Examples:

T0059 Play the long game

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.

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

Indicators:

Counters:

- C00085: Demuting content
- C00088: Poison pill recasting of message
- C00011: Media literacy. Games to identify fake news (educators,gamesdesigners,developers)
- C00042: Address truth contained in narratives

Examples:

- China and its constant messaging that Taiwan and Hong Kong are part of one China.

T0060 Continue to amplify

Continue narrative or message amplification after the main incident work has finished

Indicators:

Counters:

- C00085: Demuting content
- C00147: Make amplification of social media ports expire (e.g. can't like/ retweet after n days) (platform_algorithms)

Examples:

TA11 Disinformation tasks

Retention

Customer relationship

Advocacy / zealotry

Conversion

Keep recruiting / prospecting

TA11 Counters

C00131: Seize and analyse botnet servers (Deny)

(server_admin)

C00137: Pollute the AB-testing data feeds (Disrupt)

C00138: Spam domestic actors with lawsuits (Disrupt)

C00139: Weaponise youtube content matrices (Disrupt)

C00143: (botnet) DMCA takedown requests to waste group time (Degrade)

(public,elves)

C00144: Buy out troll farm employees / offer them jobs (Degrade)

C00145: Fill data voids with wholesome content (Degrade)

Pollute with Kittens! Babyshark!

See also: C00133 (Disrupt), C00135 (Disrupt), C00136 (Disrupt), C00140 (Degrade), C00141 (Degrade), C00142 (Degrade)

TA12 Measure Effectiveness

TA12 Disinformation Techniques

Behaviour changes

Message Reach

Social Media Engagement

TA12 Disinformation Tasks

Evaluation

Post-mortem

After-action analysis

TA12 Counters

C00147: Make amplification of social media ports expire (e.g. can't like/ retweet after n days) (Disrupt)

(platform_algorithms)

C00148: Add random links to network graphs (Degrade)

(needs platform_algorithms)

C00149: Poison the monitoring & evaluation data (General, Degrade)