Chapter 16 Tools

Response Toolkit

The tools you need depend on the size of the response you're planning to run, the number of people involved, and things like whether they already have access to their own specialised tools for things like tracking disinformation narratives. A good basic set of tools will include:

- Incident tracking. The team needs to know which incidents it's responding, where to find information on them, where to add information, and what types of action have been taken already. Incident tracking tools range from a shared spreadsheet (e.g. googlesheets and airtables) to ticketing systems (The League uses D3PO), and case management systems like TheHive.

- Incident note and summary sharing. Shared notebooks (e.g. Googledoc templates) work for this, and some tracking systems (e.g. TheHive) also include shared notes.
- Artefact analysis. We're often starting investigations from single artefacts: text, images, video, domains, groups. We borrow heavily from OSINT toolkits to analyse each of these.
- Social media analysis. At a minimum, you'll need network and text analysis tools. Some of our teams bring their own; otherwise sourcing or creating open-source analysis tools is a good thing.
- Incident technique, artefact and narrative sharing. Techniques, artefacts and narratives are objects of specific importance to an incident: they're the objects that you want to share with responders, like hashtags, groups, and superspreader account ids. Each incident is built on techniques, artefacts and narratives: collecting, annotating, and sharing these is an important part of the teams' work. We've tried a range of tools, from shared spreadsheets (googlesheet templates) to MISP and DKAN for this.
- Incident broadcast. One group can only do so much on its own. Most of our communications to date have been through individual connections and the cross-team tracking system inside the League, but MISP allows for both setting an event to public share, and for emailing event summaries out to a subscriber list. Other possibilities include a public list of non-sensitive incidents, an incidents mailing list etc.
- Large dataset storage. A tracking team will collect a lot of supporting data that isn't artefacts: things like the tweets and accounts associated with a hashtag, or urls and groups that a story appears on. Most of this data isn't part of reports - it's supporting data - but still needs to be stored somewhere, for analysis. We've tried DKAN storage for json, CSV and image files, with sql for other objects of interest, and are investigating other storage methods.

The big idea here is that we can use existing open source threat intelligence tools for disinformation defence.

Incident Tracking Tools

HIVE

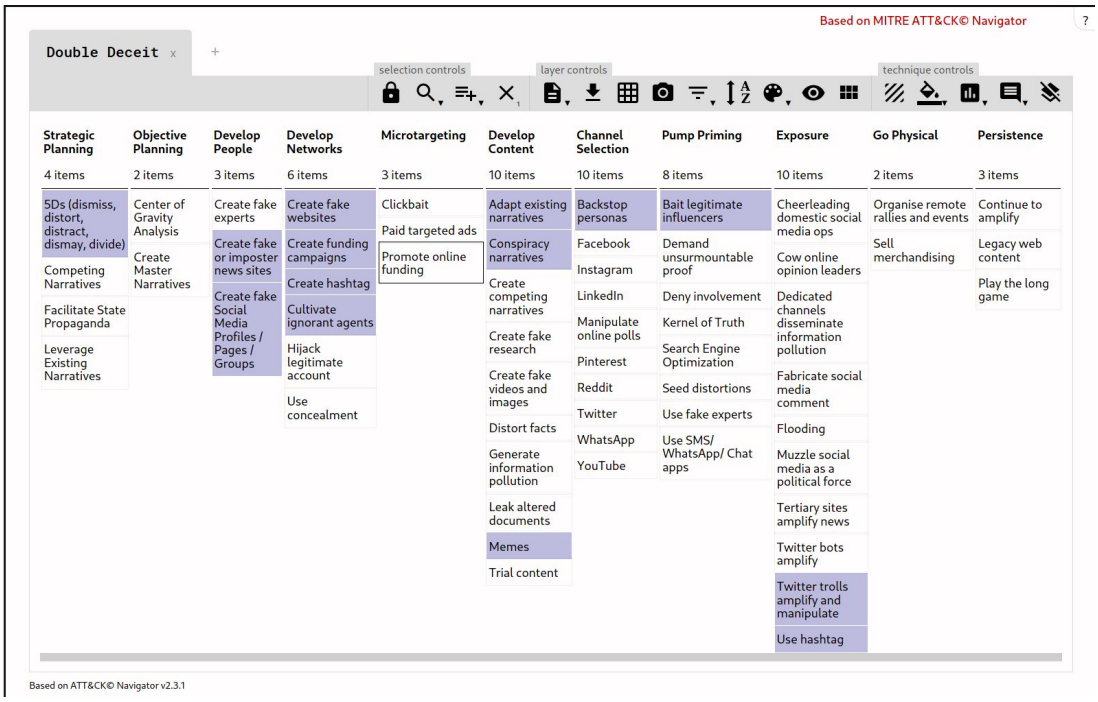
We use Hive to manage our list of incidents, and links from them to the other objects and data connected to incident responses. Check Hive and search for the incident name. All incidents will have the tag “disinformation” and word “Incident” in the title, which should help with searching.

Incident Sharing Tools

The big idea here is that we can use existing open source threat intelligence tools for disinformation defence.

For incident sharing, we've worked with the MITRE ATT&CK toolset, MISP, and OpenCTI.

MITRE ATT&CK toolset



AMITT Framework in the ATT&CK Navigator: Double Deceit Example

The AMITT Framework's ATT&CK-based format means we can reuse ATT&CK tools with it. Having STIX data was important for integration in the community, but not everyone wants to work with STIX JSON directly.

The MITRE ATT&CK navigator (image above) is well-known to most people who've used ATT&CK. It was created for navigation of STIX formatted data, is used for visualisation, red and blue team planning and has exportable layers (that can model adversary capabilities at some point in time). Tools like this are important for usability; MITRE did an excellent job on it and we hope that it will be useful to folks in the cognitive security space.

We've made a small modification to the navigator to support AM!TT; this is available on the CogSec Collab site at https://www.cogsec-collab.org/project/amitt_navigator/

MISP

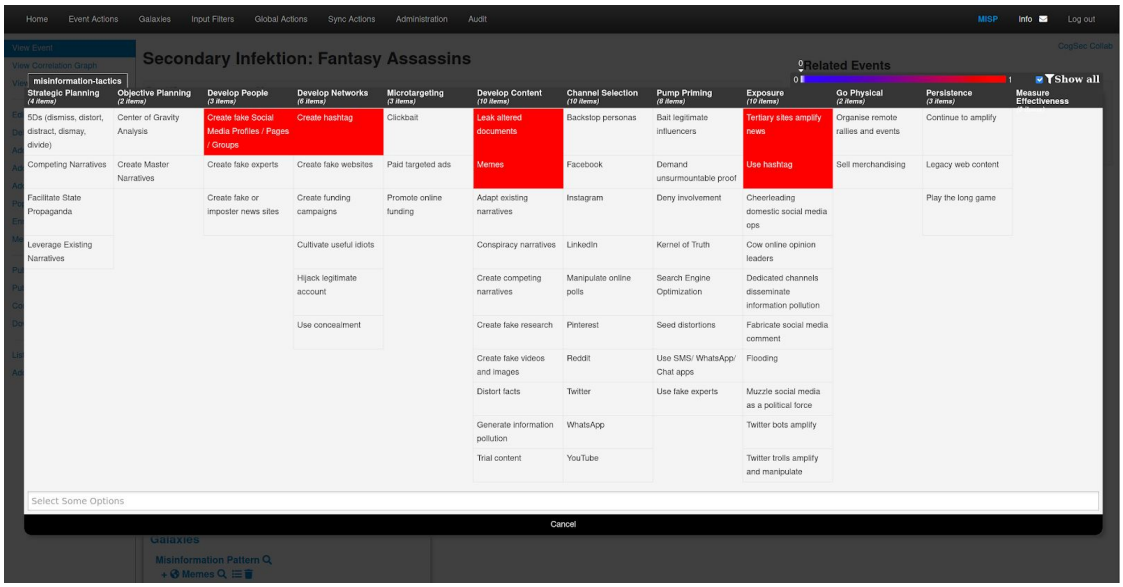
MISP (Malware Information Sharing Platform, https://www.misp-project.org/) is an open-source threat intelligence platform that was originally designed for malware, but is now used with many types of threat and data.

MISP is a community driven, collaborative threat intelligence platform. It's a permanent fixture of the CTI community largely due to its openness, commitment to FOSS, and an awesome community. MISP supports a range of diverse and open communities, and is used by ISAOs and ISACs, and also ad-hoc groups beyond infosec: e.g. MISP is being used to track COVID19 infections.

MISP is used to store and share structured data. It's open and extensible, and its users can easily build enrichment and automation modules for it. It also integrates with lots of other platforms and data formats including STIX. This is why we chose it for influence operations.

A good place to start with MISP is the "MISP Training for COVID" recording, from CIRCL, https://bbb.secin.lu/b/ale-q6v-ecn

Adding an AMITT description to MISP



AMITT Framework Galaxy interface in MISP

We built an AMITT Framework Galaxy in MISP: this now ships with MISP. A galaxy is definitions and corresponding tags, providing contextualising information. As analysts are working through reports, they can attach a technique, navigate and read a definition. For workflow, similar to the AMITT Framework, MISP allows you to click and add corresponding techniques as you work through a report.

Disinformation object types in MISP

We added a set of new object types to MISP, to help with disinformation incident tracking. Objects you might be interested in include:

Object	**Misp**
Facebook group	misc:facebook-group
Facebook page	misc:facebook-page
Facebook account	misc:facebook-account
Facebook post	misc:facebook-post
Twitter account	misc:twitter-account
Twitter list	misc:twitter-list
Twitter post	misc:twitter-post (was misc:microblog)
Blogsite	network:url
Blog account	misc:user-account
Blogpost	misc:blog
Reddit group (subreddit)	misc:reddit-subreddit
Reddit account	misc:reddit-account
Reddit post	misc:reddit-post
Reddit post comment	misc:reddit-comment
YouTube Channel	misc:youtube-channel
YouTube Video	misc:youtube-video
YouTube Playlist	misc:youtube-playlist
YouTube Comment	misc:youtube-comment
Website address	network:url
Hashtag	ADD NEW
Instant message	misc:instant-message
Instant message group	misc:instant-message-group
Narrative	misc:narrative
Image	file:image
Meme	file:meme-image
Individual	misc:person
Event (e.g. protest)	misc:scheduled-event
Location	misc:geolocation

Other MISP objects we might need include: misc:course-of-action, network:email, file:forged-document, file:leaked-document, misc:legal-entity, misc:news-agency, misc:organization, misc:scheduled-event, misc:short-message-service, network:shortened-link, misc:user-account.

Adding an object (tweet etc) to MISP by hand

- Go to MISP
    - Click on the incident ID in the list of events.
- Click on “Add Object” in the left-side column
    - Misc -> microblog for twitter or Facebook posts
    - Fill out the details
    - Click submit
    - Repeat for more objects
- Now you can start playing with the grey bar at the bottom of the event description, and toggle things like the timeline on and off.

Adding an object to MISP via Slack bot

- Slack bots can quickly create and append an object to an event.
- Each bot attempts to modify the MISP event directly. If it lacks permission it will instead create a MISP event extension. Click the icon shown below to switch to extended mode to see the extended event objects appended into the main event.

Twitter Posts

There’s a Slackbot in #4-disinformation that can upload a Twitter post to a MISP event. The bot works like this /misp_twitter $MISP_event_id $post_id

It accepts either a Twitter Status ID or a Twitter post URL as arguments for $post_id

- In the #disinformation channel use the following command to add a Twitter post to the CTI League MISP
    - /misp_twitter <misp event id> <twitter post URL or twitter post ID>
    - Example: /misp_twitter 34 https://twitter.com/NASA/status/1259960728951365633?s=20

BuiltWith Tags

- In the #disinformation channel use the following command to add a Twitter post to the CTI League MISP
    - /misp_builtwith <misp event id> <url or domain name>
    - Example: /misp_builtwith 34 newyorkcityguns.com

Cortex Analysers

Cortex analysers are python-based tools that we can run from MISP, HIVE and Slack. We've primarily used them to speed up getting data into MISP.

Slack to MISP bots

We use slack bots to push artefacts to MISP. We can now add the following object to a MISP event using the following slash commands

- "/misp_reddit_account " - add a Reddit account's details
- "/misp_reddit_comment " - add a Reddit comment
- "/misp_reddit_post " - add a Reddit post
- "/misp_reddit_subreddit " - add a subreddit's details
- "/misp_builtwith " - add builtwith tags
- "/misp_twitter " - add a tweet to MISP

If we want new ones - we can build them, and Roger wrote a handy how-to guide: https://vvx7.io/posts/2020/05/misp-slack-bot/

Adding New Object Types to MISP

If we want new MISP object types, here's how to do that too:

1. Create the new object folder
   1. Git clone https://github.com/MISP/misp-objects
   2. Go into repo folder objects. It contains a subfolder for every misp object type
   3. Copy one of the existing object folders; rename the copy to the new object you want
   4. Go into the new object's folder. You'll find one file in here: definition.json. Open it for editing
2. Set basic data
   1. Get a new UUID from https://www.uuidgenerator.net/ - replace "uuid" in definition.json with this new one
   2. Set "version" to 1
   3. Set "name" to the same as the new folder name (nb use "-" not "_")
   4. Set "description" to something descriptive
   5. "Meta-category" is usually "misc"
3. Set attributes. Go through attributes. For each one, set:
   1. "Description": something descriptive
   2. "Misp-attribute": see [https://www.circl.lu/doc/misp/categories-and-types/](https://www.circl.lu/doc/misp/categories-an

d-types/). You'll probably use "text" a lot. The difference between url and link? url isn't trusted; link is trusted (this signals whether something is safe to click on).

   3. "Ui-priority": just leave this as default (1 is always okay)

4. These attributes aren't mandatory, but are useful
   1. "Multiple": set this to "true" if you allow multiple of this attribute (e.g. hashtags)
   2. "disable_correlation": true, - stops MISP trying to correlate this attribute - set this on things like language to stop MISP from wasting time
   3. "to_ids" - makes exportable via api - set to false as needed (most attributes don't need it)
5. Set the list of attributes that an object must have one of to exist
   1. List these in "requiredOneOf"
6. Check the new object is valid
   1. Run validate_all.sh
   2. Run jq_all_the_things.sh
7. Push your change back to the MISP objects repo (or to Roger for sanity-checking)

Disinformation object categories in MISP

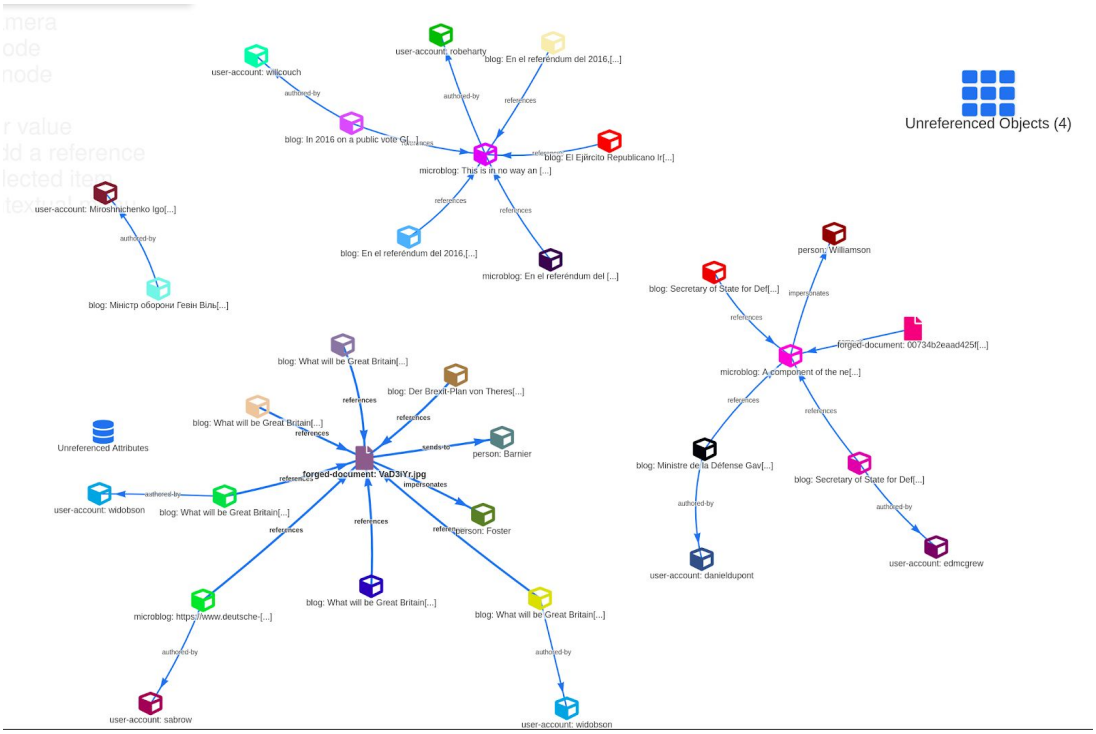
Owner org	Id	Clusters	Tags	#Attr.	Email	Date	Info
CogSec Collab	19	Misinformation Pattern Create fake or imposter news sites	pink slime	1340	info@vvx7.io	2020-01-30	U.S. Pink Slime
CogSec Collab	20	Misinformation Pattern Memes Leak altered documents Tertiary sites amplify news Use hashtag Create fake Social Media Profiles / Pages / Groups Create hashtag	DFRLab-dichotomies-of-disinformation:primary-target="GB" DFRLab-dichotomies-of-disinformation:primary-disinformant="RU" DFRLab-dichotomies-of-disinformation:platforms-social-media="facebook" DFRLab-dichotomies-of-disinformation:content-topic="government" DFRLab-dichotomies-of-disinformation:content-topic="elections" DFRLab-dichotomies-of-disinformation:methods-tactics="sockpuppets"	296	info@vvx7.io	2020-01-31	Secondary Infektion: Fantasy Assassins

MISP incident description with both DFRLab and AMITT tags

We had STIX objects in MISP for e.g. threat actors, but we don't have taxonomies for things like the types of threat actor.

We fixed this by adding the DFRlab's Dichotomies of Disinformation Taxomony tags. This wasn't quite what we needed for tactical work, so we started working with NATO on a cutdown set.

Disinformation relationship types in MISP



MISP event graph for Sekondary Infektion

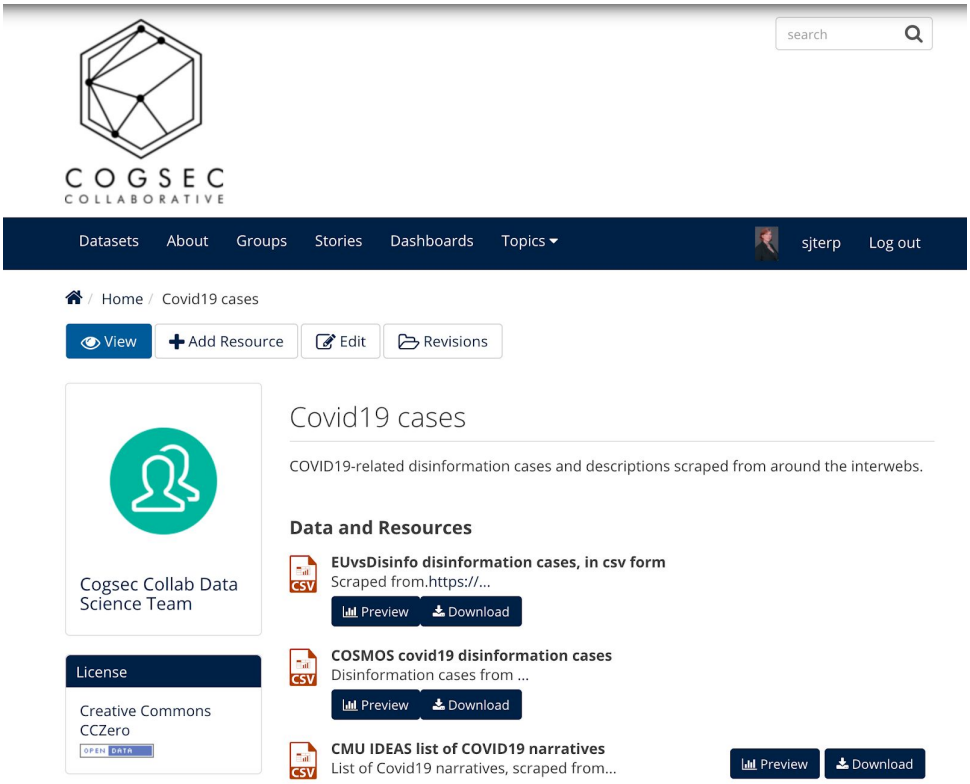
Finally, we added object-to-object relationship types to MISP to help with describing disinformation. MISP is graph-based, and these become useful when investigating and sharing relationships between objects.

The important thing is that the data we share tells a story. The AMITT framework summarises behaviour; the fancy tags (DFRlab dichotomies etc) help describe the event and provide context on what we're seeing, and MISP objects help us represent the relationships between things: Who posted a blog post, who was mentioned in a news articles, who is the registered owner of a domain etc.

Ultimately these are the things we're aiming to build and share. Not a flat list of indicators, but a model of how the adversary operated.

Large Data Storage Tools

DKAN



CogSecCollab DKAN

DKAN is a data warehouse tool - it's where we store large datasets and their descriptions,for analysts to use.

Analysis Tools

Gephi

Viewing networks with Gephi

This is a manual process with instructions created from Andy Patel's video at https://www.youtube.com/watch?time_continue=17&v=AqlT0khVuZA

- Get Gephi from https://gephi.org/users/download/ - install it.
- Start Gephi.

- Click on top menu>file>“import spreadsheet”. Grab User_user_graph.csv - use all defaults
- Top menu: Go to data laboratory, “copy data to another column”, click ‘id’, click okay.
- Go to overview. RHS: Run modularity algorithm, using defaults
- RHS: Run average weighted degree algorithm
- LHS: Click color icon, then partition, modularity class. Open palette, generate, unclick “limit number of colors”, preset=intense, generate, okay
- LHS: Select “tt”, ranking, weighted degree, set minsize=0.2, choose 3rd spline, apply
- LHS: Layout: OpenOrd, run. Then forceatlas2, run. Try stronger gravity, and scaling=200
- Top menu: Preview - select “black background”, click “refresh”. Click “Reset zoom”

Gephi has an API - these tasks could be automated.

Python scripts

We use python a lot (just look at the github repo…). Here are some useful resources:

- Learn python the hard way
- ACTION: SJ add notes on python and data science - Pablo-level friendly

Other analysis tools

We’ve mentioned a bunch of tools above. Some basic tools:

- Most data scientists use Python and Jupyter notebooks. You’ll see a lot of these - the basic Anaconda install comes with most of the things we use https://www.anaconda.com/distribution/
- Data gathering:
    - Reaper https://github.com/ScriptSmith/reaper https://github.com/ScriptSmith/socialreaper https://reaper.social/ - scrapes Facebook, Twitter, Reddit, Youtube, Pinterest, Tumblr APIs
- Network analysis and visualisation: there are many tools for this.
    - Gephi is a good standalone tool https://gephi.org/users/install/
    - Networkx is a useful python library
- URL analysis
    - Builtwith.com
- Image analysis
    - Reverse image search: tineye.com, Bellingcat guide
    - Image search: bing.com, yandex.com
    - Image text extraction: bing.com, yandex.com
- Data storage / Threat Intelligence tools
    - DKAN https://getdkan.org/
    - MISP https://www.misp-project.org/

Disinformation-specific tools:

- Indiana University has a set of tools at https://osome.iuni.iu.edu/tools/
    - Botometer: check bot score for a twitter account and friends https://botometer.iuni.iu.edu/#!/
    - Hoaxy: check rumour spread (uses Gephi) https://botometer.iuni.iu.edu/#!/
    - Botslayer https://osome.iuni.iu.edu/tools/botslayer/
- Bellingcat made a list of useful tools
    - Bellingcat's really big tools list - worth reading if you need a specific OSINT tool