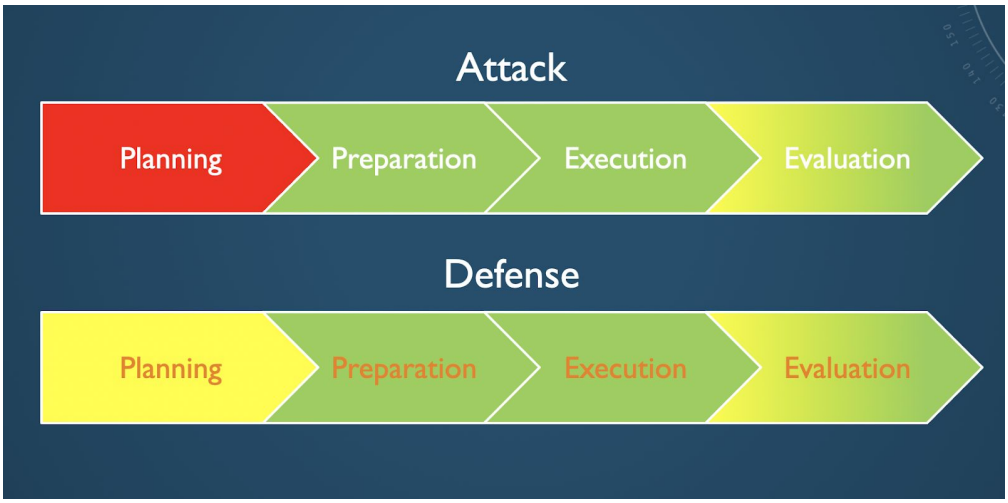
AMITT Frameworks: User Guide



1 Ways to Work with AMITT

AMITT is designed for rapid sharing of disinformation threat intelligence, over the same systems used by information security professionals, but that's not the only thing you can do with it. This section covers uses and tools, including:

- Offensive planning
- Defensive planning
    - Red teaming and planning
    - Intelligence analysis and tracking
    - Active defence and countering
- Sharing AMITT data
- Tools (including MISP) for disinformation tracking

We've used the AMITT framework to decompose different misinformation incidents into stages and techniques, so we can start looking for weak points in the ways that incidents are run, and in the ways that their component parts are created, used and put together. We've also used it to analyse what's possible in terms of algorithm use and other automations.

2 Sharing Disinformation Data with AMITT

2.1 Coordinating Responses

We need to tie this all together. Whole-system attacks often need whole-system responses. We've seen campaign creators use different types of accounts (bot, troll, cyborg, 'useful idiots' etc) across multiple platforms, topics and geographies; responses need to be across platforms, and will often be a mix of different blue team TTPs. This will need coordination across different groups, potentially through disinformation SOCs and ISAO-like bodies.

2.2 Making Tactics and Techniques Easy to Share

Online disinformation doesn't exist in a vacuum. The same types of framework that help campaign creators can also help with their removal. For instance, the easy access to demographic datasets that make micro targeting easy could be countered with stronger use of privacy laws and individual counters against online privacy invasions.

2.2.1 Sharing Formats

Checking parent models is also useful because this gives us formats for our counter objects— which is basically that these are of type "mitigation", and contain a title, id, brief description and list of techniques that they address. Looking at the STIX format for course-of-action gives us a similarly simple format for each counter against tactics — a name, description and list of things it mitigates against.

We want to be more descriptive whilst we find and refine our list of counters, so we can trace our decisions and where they came from. A more thorough list of features for a counter list would probably include:

- id
- name
- brief description
- list of tactics can be used on
- list of techniques can be used on
- expected action (detect, deny etc)
- who could take this action (this isn't in the infosec lists, but we have many actors on the defence side with different types of power, so this might need to be a thing)
- anticipated effects (both positive and negative — also not in the infosec lists)
- anticipated effort (not sure how to quantify this — people? money? hours? but part of the overarching issue is that attacks are much cheaper than defences, so defence cost needs to be taken into account)

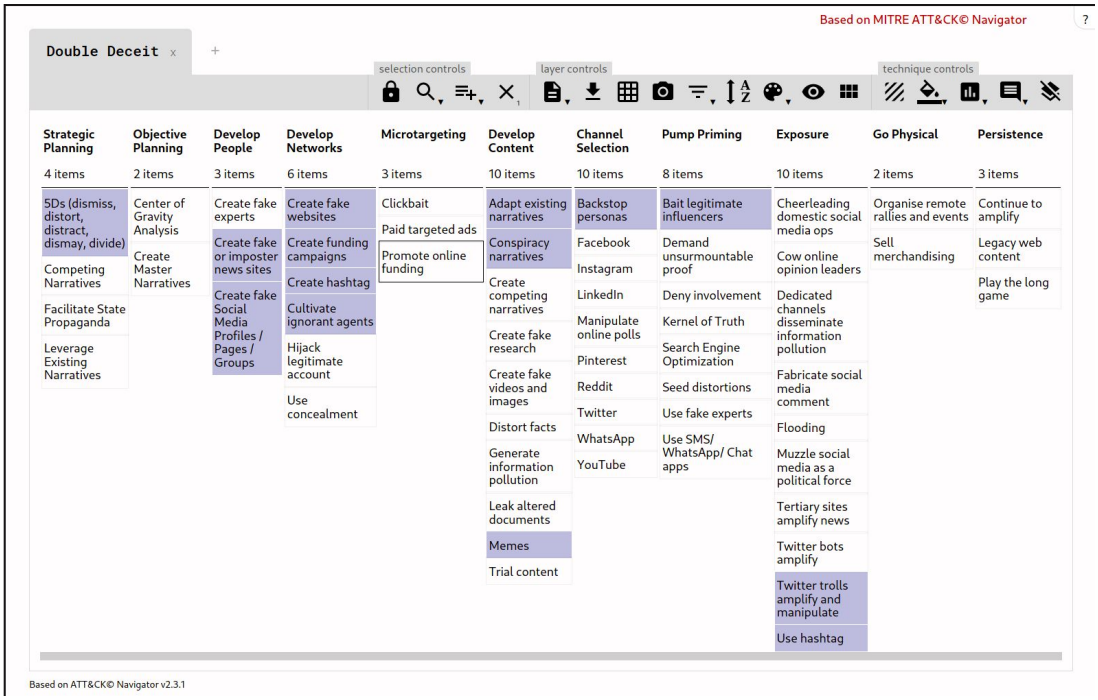
And be generated from a cross-table of counters within incidents, which looks similar to the above, but also contains the who/where/when etc:

- id
- brief description
- list of tactics it was used on
- list of techniques it was used on
- action (detect, deny etc)
- who took this action
- effects seen (positive and negative)
- resources used
- incident id (if known)
- date (if known)
- counters-to-the-counter seen

3 Using Tools with AMITT

AMITT is designed to be used with a suite of other disinformation tools and processes, including the MISP open-source threat intelligence toolset. This section covers disinformation adaptations to MISP and other toolsets.

3.1 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/

3.2 STIX Viewers

STIG (https://github.com/idaholab/STIG) is a useful GUI-based tool for drawing and sharing STIX graphs outside the larger tools like MISP.

Stixview https://github.com/traut/jupyter-widget-stixview is a useful way to display STIX graphs from within Jupyter/ Python.

3.3 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.

CogSecCollab have added the Misinformation Pattern Galaxy (AMITT), the DFRlab Dichotomy of Disinformation Pattern Galaxy, and other cogsec-related object templates - facebook-post, twitter-post, etc to MISP.

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

4 Using AMITT Frameworks in MISP

MISP is used to store and share the artifacts and indicators of Cognitive Security incidents.

Objects in MISP can be thought of as STIX Domain Objects (SDOs). Relationships in MISP can be thought of as STIX relationship objects (SROs).

4.0.1 MISP Object Templates

The MISP objects we've created, and prior objects relevant to disinformation, are listed below. The code for MISP objects, the AMITT framework in MISP, and the DFRLab Dichotomy of Disinformation can be found in the MISP Project GitHub repo.

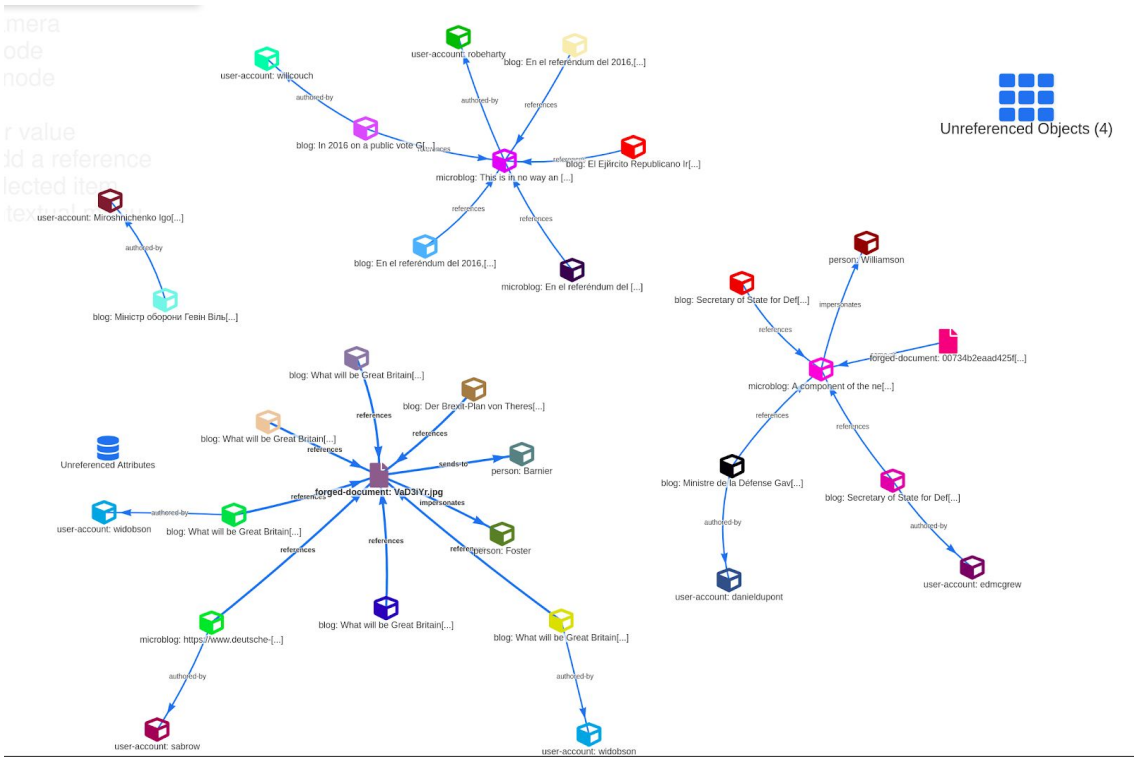
Object	Misp
Facebook group	misc:facebook-group
Facebook page	misc:facebook-page
Facebook account	misc:facebook-account
Facebook post	misc:facebook-post
Twitter account	misc:twitter-account
Twitter list	misc:twitter-list
Twitter post	misc:twitter-post
Blogsite	network:url
Blog account	misc:user-account
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
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

4.0.2 MISP Relationships

MISP Object relationships (think STIX Relationship Objects) define the relationship between all objects. These relationships let us describe how the pieces fit together. MISP relationships are found here: https://github.com/MISP/misp-objects/blob/main/relationships/definition.json

We can graph MISP relationships as shown below. This is one of the incidents in the Secondary Infektion campaign.



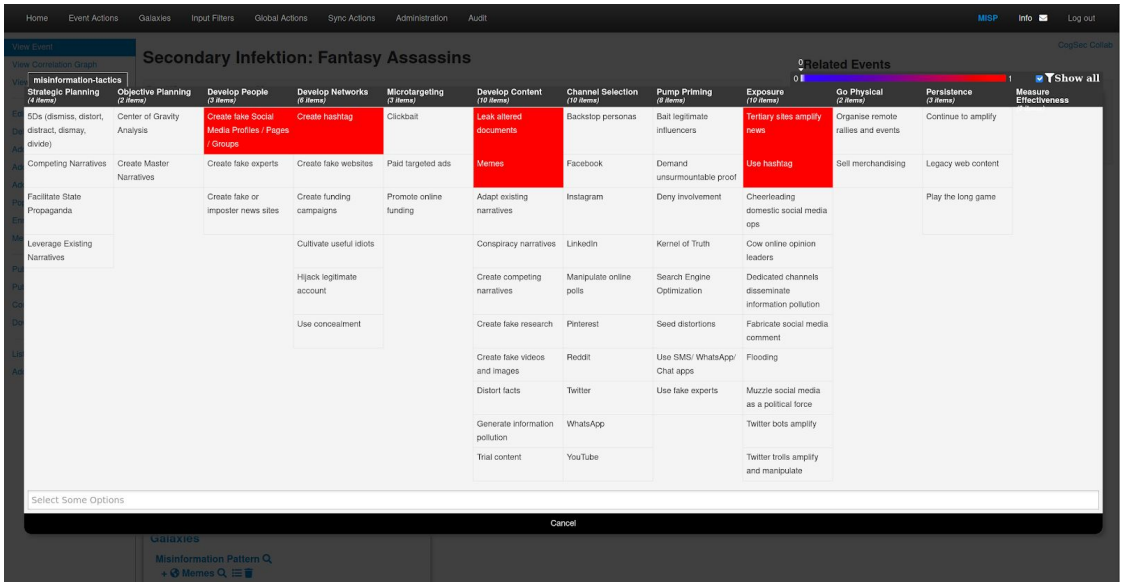
We can modify the objects/relationships to fit our specific needs. Since the MISP Project typically accepts PRs within a few days, it makes iterating over a data model fairly painless.

4.0.3 Example: The Narrative Object

The Narrative object stores a description of a narrative ("Bill Gates' C19 vaccines contain mind-control microchips") but it does not tell us anything about how that narrative relates to other entities (blog posts, persons, merch, etc).

So why use a Narrative object? It lets us store more information than MISP event tags, and keeps the UI cleaner (less wear on analysts). Artifacts within an incident might relate to different narratives, and we want to be deliberate in communicating which objects belong to what. What issues might you face with using narratives (and any other object) this way? Objects are a set of attributes and all attributes are automatically correlated via literal string matching. This works well for infosec artifacts but is more complicated with influence operations where totally unrelated campaigns might routinely reference the same persons, sites, etc. The immediate challenge with using Narratives is that in order to correlate two distinct incidents we must use a standard Narrative definition. This is an open problem.

4.0.3.1 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.

4.0.4 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.

4.0.5 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.

4.0.5.1 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

4.0.6 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.

4.0.7 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/

4.0.7.1 Adding New Object Types to MISP

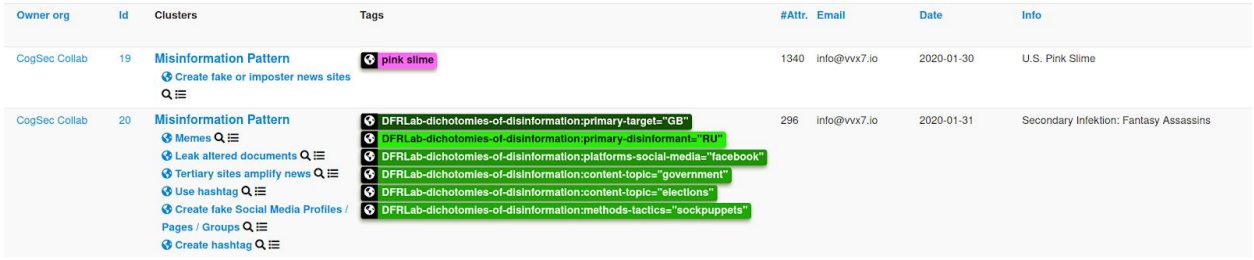
If we want new MISP object types, here's how to do that too:

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

c. “Ui-priority”: just leave this as default (1 is always okay)

4. These attributes aren’t mandatory, but are useful
    a. “Multiple”: set this to “true” if you allow multiple of this attribute (e.g. hashtags)
    b. "disable_correlation": true, - stops MISP trying to correlate this attribute - set this on things like language to stop MISP from wasting time
    c. "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
    a. List these in “requiredOneOf”
6. Check the new object is valid
    a. Run validate_all.sh
    b. Run jq_all_the_things.sh
7. Push your change back to the MISP objects repo (or to Roger for sanity-checking)

4.0.8 Disinformation object categories in MISP

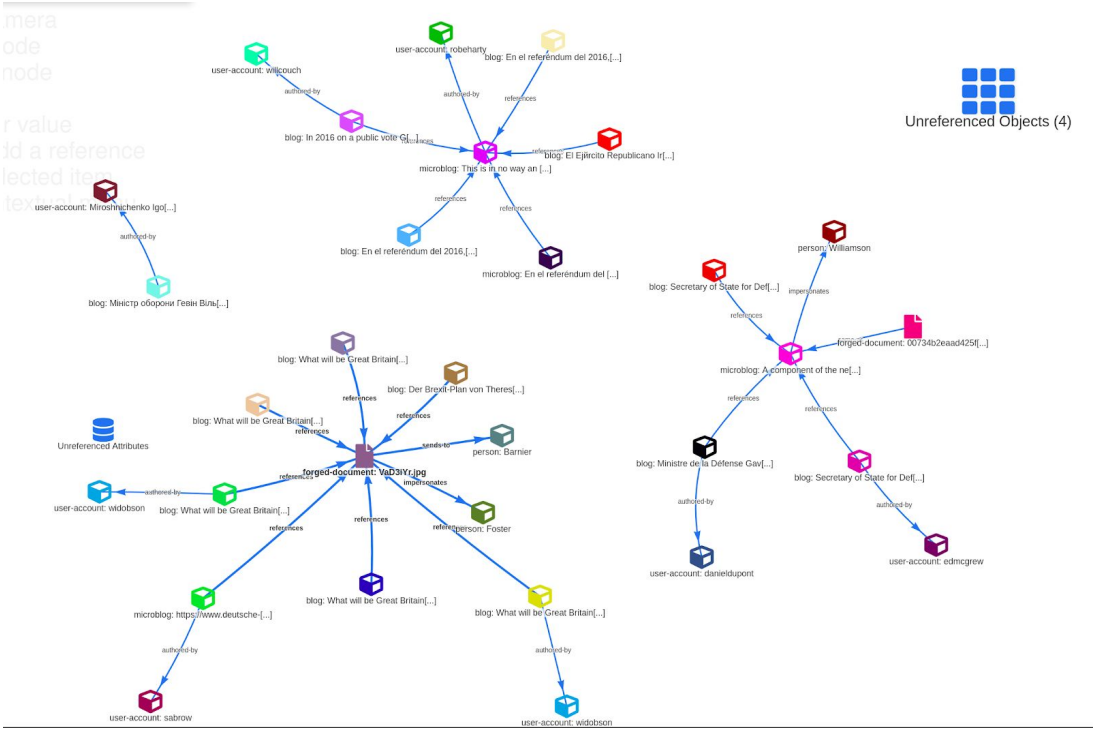


MISP incident description with both DFRLab and AMITT tags

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.

4.0.9 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.

5 AMITT for disinformation analysis

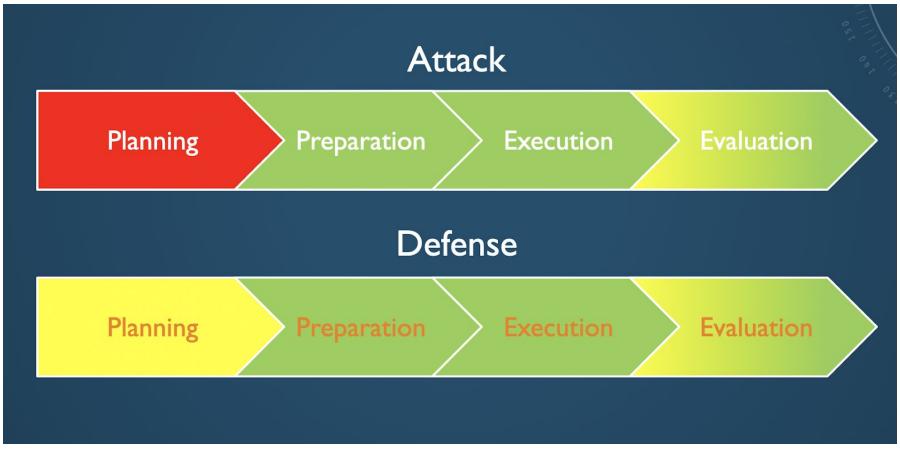


Figure 9.1 AMITT Phases and automation

5.1 Introduction

One of the advantages of the AMITT framework is that it allows an analyst to drill down to the most minute details of how a tactic, technique, or procedure is executed and can be countered while simultaneously allowing decision makers to make strategic decisions without becoming bogged down in the minutia of an individual action. In the early stages of planning, strategic thinkers may ask if a particular technology is the right fit for a given plan. Unfortunately, it's more likely that a decision maker will attempt to shoehorn a technology to their particular use-case.

This chapter will examine how a technology, in this case artificial intelligence (AI), can be examined for use in misinformation attacks and defense. The examination will be conducted from the vantage point of a strategy as opposed to a tactical action. In this context, strategy is an idea which guides employment of numerous resources or actions to achieve a desired end-state. A tactical action, by comparison, is the employment of

resources and actions to support the achievement of a larger strategy. To summarise, tactical actions are time and resource limited and are in support of a larger, overarching strategy. One of the advantages of strategic thinking is it allows a planner to abstract away a lot of details and niche cases. At a minimum, this kind of strategic analysis helps to identify what things may be of most use and seed further detailed discussions.

At the strategic level, AMITT identifies four phases for a misinformation operation: planning, preparation, execution, and evaluation (Figure 9.1). The rest of this chapter will examine what each phase entails and how AI may be used to automate actions in that phase for both offense and defense.

5.2 Planning Phase

5.2.1 Offensive Misinformation

The planning phase requires two tasks to be completed: strategic planning and objective planning. Strategic planning is an inherently human decision and centers around the question of why the misinformation operation is being conducted. If the operation is successful, what is to be gained or accomplished? As strategic goals are a human desire for change, automation is not of use and AI is not well suited to assisting in this task.

Objective planning requires that a center of gravity analysis be conducted on the target. It is critical to note that there is one center of gravity. The center of gravity is the keystone from which every other facet of the target grows. Identifying the center of gravity for a target population requires in-depth understanding of society being targeted. Social norms, community norms, biases, and identity help form and inform the center of gravity. This kind of social analysis cannot be directly automated.

Where automation may help is in gathering large amounts of data to allow for broad scoping. By using automation and AI it's easy to collect information which will allow for identification of subjects of interest to the population as well as sentiment analysis for the population. This data will require further qualitative analysis to include "binning" before it is useful.

5.2.2 Countering Misinformation

One of the advantages defenders have in the battle of misinformation is their knowledge of themselves, their groups, and their society. Defenders know their own center of gravity and they know what must be protected. Likewise, defenders know what functions and objectives are critical and what normal behavior looks like making detection of anomalous activity feasible. As such, AI becomes a plausible tool in the planning phase by enabling the detection of anomalous activity and serving as an early warning system of possible attack.

5.3 Preparation Phase

5.3.1 Offensive Misinformation

The preparation phase is the phase where necessary resources are developed. Network development in the preparation phase includes understanding existing social networks as well as cultivating "useful idiots" to unknowingly propagate misinformation payloads. AI can automate these analyses through the use of social media analysis. AI is also useful for microtargeting. As a matter of fact, social media services are purpose-built for micro-targeting of advertisement; their entire business model is built on this capability. If we ignore laws about false advertising, the difference between advertising and misinformation is merely intent.

AI can also be tremendously useful in generating and honing message content. While the use of AI to generate deep fake videos is well-discussed in the open press, the use of systems like GPT-3 (Generative Pre-trained Transformer 3) to generate text narratives has gone largely undiscussed outside of academic circles. Further, using the advertising tools provided social media networks, AI has become remarkably adept at conducting A-B testing to determine which of two messages is most effective and using that information to generate the next iteration of messaging content.

5.3.2 Countering Misinformation

The defensive tactic most often discussed to counter misinformation is to provide counter narratives. In this sense, defenders can take advantage of automation in many of the same ways as attackers. Network analysis will allow for the identification of influencers which may help populate and transmit positive narratives. Network analysis also helps identify which groups may be susceptible to misinformation campaigns and therefore may be good targets for a prophylactic round of messaging by defenders. Finally, AI can be useful for A-B testing and honing of defensive messaging.

5.4 Execution Phase

5.4.1 Offensive Misinformation

The execution phase is where messaging reaches target audiences. AI can be used to identify existing and emerging influencers for pump priming. The use of AI bots to amplify misinformation is, however, a mistake as numerous computation methods exist for identifying bots and the messages they're currently spreading. Spotlighting attack infrastructure is a sure way to let defenders get the upper hand and deny needed resources to attackers. Smarter chatbots enabled by technologies such as GPT-3 can

automate answering challenges to messaging as well as responding to queries from targeted audiences. Finally, AI is useful in continued A-B testing as well as in the effort to persist at the forefront of the target audience's mind.

5.4.2 Countering Misinformation

AI is of use in countering a misinformation campaign in its execution phase. Most current AI efforts concentrate on the use of AI to identify misinformation, but don't address the psychological facts of audiences having ingested misinformation. Misinformation works, in part, because it plays to pre-existing biases in the target audiences. By the time a target audience has been infected with misinformation, defenders must overcome cognitive dissonance, cognitive friction, and likely cognitive easing. This means that simply pointing out something isn't true is unlikely to have a significant effect.

The use of AI for fact checking has presented challenges, but does not make it useless. Considerations of whether the AI should assume an open-world or closed-world system will provide vastly different results and may be suitable in some cases. Likewise, known models for cascade-based and time-based propagation of misinformation are suitable for automation in AI systems. The use of AI to create deepfakes produces numerous anomalies that may be detectable by an AI. Mathematical anomalies in file content created by their creation are easily detectable by AIs. Likewise, medical anomalies can be detected by AIs. Micro-changes in complexion due to the heart pumping are easily detectable by AIs and the lack of such in a regular rhythm is a good indicator of altered media.

5.5 Evaluation Phase

5.5.1 Offensive Misinformation

As offensive campaigns continue, it is necessary to measure the effectiveness of ongoing efforts. AI is useful for gathering large amounts of data for measuring effectiveness and again for A-B testing of parallel efforts. While AI bots may be used for keeping the existence messages persistent, they are as easily detectable as they were in earlier phases. Worse, it's likely that now that the attack has executed, defenders have been alerted and are now actively looking for signs of attacker infrastructure. AI enabled evaluation enables for a rapid evaluation of current efforts and generation and testing of new content for rapid execution of additional iterations.

5.5.2 Countering Misinformation

The use of AI by defenders in the evaluation phase is useful in all of the same ways that it is for attackers. AI can enable the collection and evaluation of measures of effectiveness, help conduct A-B testing of counter narratives, and help speed the next iteration of the next effort. One advantage is that defenders don't necessarily mind if their infrastructure is highlighted to attackers as they have at least perceived legitimacy. There is a danger, however, that the discovery of bots to spread information may be leveraged by an attacker by re-contextualizing the narrative in saying that legitimate authorities are trying to muffle dissenting voices.

5.6 Conclusion

While the AMITT framework allows for highly detailed, component-wise analysis and countering of misinformation attacks, it also allows for the abstraction of details for a more

holistic analysis of misinformation attacks and defense at the strategic level. This strategic level analysis may be used to seed discussion of the appropriateness of tools in conducting/countering misinformation as well as the efficacy of such tools at various phases of the misinformation kill-chain.