1. Chapter 1: Introduction to the Disinformation Team

This is the big book of disinformation response for the CTI League's disinformation team. We're embedded within the CTI League, and track disinformation using similar tools and techniques to the rest of information security, but there are some things that we do a little differently. Hence this book.

1.1. The CTI League

The CTI League is a community of cyber threat intelligence experts, incident responders and industry experts working to neutralize all cyber threats looking to exploit the Covid19 pandemic. It identifies, analyzes and neutralizes all threats but at this most sensitive time is prioritizing front-line medical resources and critical infrastructure. The League's April 2020 report is https://cti-league.com/2020/04/21/cti-league-inaugural-report/ and its activities are listed in the playbook.

The disinformation team is tasked with finding coordinated inauthentic activities ("disinformation campaigns"), and the objects and people attached to them, and using known ways (some of which we have to invent ourselves) to expose, disrupt or stop their operations.

1.2. Glossary

We all come from different disciplines: words like "campaign" have different meanings to a military, an adtech or a tech person (and if you're all three, you get to fight about definitely with yourself). There are also committees dedicated to defining what words like "disinformation" and "misinformation" mean, and the differences between them.

We ain't got time for that here. This glossary is our latest best effort at definitions for some of the words we use a lot between us, and what we (mostly) think we mean when we say them.

- **Cognitive Security**: The top layer of security, alongside Physical-security and Cyber-security. The art and practice of protecting against hacks that exploit cognitive weaknesses, especially cognitive hacks that are online and/or in large numbers of people. One of the reasons the MisinfoSec crowd started talking about Cognitive Security (including rebranding as the CogSecCollab) in 2020 is a belief that, in order to deal with things like disinformation, we need to focus on the thing we're protecting. That means working on reducing disinformation, but also on boosting good information when we see it.
- **Misinformation**: false content, where that content could be text, images, video, voice etc. Misinformation does not have to be deliberately generated (e.g. my mother might forget my favorite colour)
- **Disinformation**: deliberate attempt to deceive online. There is usually intent to deceive with disinformation, and the content itself might be true, but in a deceptive context (e.g. fake users, fake groups, mislabelled images, doctored videos etc). Claire Wardle's work on the differences between misinformation and disinformation is still some of the best.
- **Campaign**: Campaigns are long-term efforts to change or confuse populations.
- **Incident**: Incidents are coordinated inauthentic activity that are carried out as part of a campaign. The "coordinated" implies either an instigator of some form with motives (geopolitics, money, ideology, attention, etc.) or some form of collective deliberate behaviour around it, like flooding a hashtag. That activity usually lasts for a short period of time because the narratives, artefacts, and other aspects can be picked up and continued by people who aren't driving an incident - and this is often part of an incident or campaign's goals.
- **Narrative**: Narratives are the "stories" that are being used to change minds, confuse people etc. Narratives are part of incidents - each incident might have multiple narratives involved, or just one, but there's usually an identifiable narrative somewhere in there, that you can use to see if there are related incidents already tracked or dealt with etc. The other thing about narratives is that they, like incidents, have lifetimes. Some narratives appear as a result of a world or local event (or upcoming or anticipated event), and are only useful whilst that event is in peoples' minds.
- **Artefact**: Artefacts are the objects that you can 'see' connected to a disinformation incident or campaign. They're the text, images, videos, user accounts, groups, hashtags etc that you use to get a picture of an incident or campaign.

Other terms related to this work:

- **Astroturfing**: creating a fake grassroots movement with an obfuscated sponsor or orchestrating group

1.3. Styles and formats

- We use ISO8601 format for dates where possible: yyyy-dd-mm (see https://www.w3.org/QA/Tips/iso-date)

- When referencing specific times related to incidents, explicitly declare the timezone or use UTC

1.4. Other places to look for information

There's a lot to learn about disinformation, misinformation, and how they fit into cognitive security / infosec in general - there's a separate BigBook of Cognitive Security for all that. This BigBook is the practical one.

We've added lists at the end of this document (here), to books and papers about disinformation, to other teams doing this, sources of data, tools etc. And CogSecCollab is also collecting information in its documentation repo, which was used to seed this document.

For all things CTI Disinformation, start at the Team Readme.

1.5. How Disinformation fits into the League

1.5.1. Activities

Reading through the CTI League handbook, the league stresses *"Our members prioritize efforts on helping hospitals and healthcare facilities protect their infrastructures during the pandemic and creating an efficient channel to supply these services". We should do this.*

It lists services as:

1. Neutralize malicious activities in the cyber domain with takedown, triaging, and escalation relevant information for sectors under threats.
2. Prevent attacks by supplying reliable, actionable information (IoCs, vulnerabilities, compromised sensitive information and vulnerabilities alerting).
3. Support the medical sector and other relevant sectors with services such as incident response and technical support.
4. Act as clearinghouse for data, a connection network and a platform for facilitating those connections

There are disinformation equivalents to these:

1. **Neutralise**: This is the disinformation takedown, triage and escalation work listed under disinformation incident response below.
2. **Prevent**: This is work that we could be doing - collating and supplying disinformation IoCs and vulnerabilities to the organisations, especially the health organisations, that we work with. For example, if we identify that a "Reopen $STATE" campaign is attempting to organize another "Operation Gridlock" incident, we can alert state, city, and county officials, as well as any hospitals in the target area.
3. **Support**: We've seen few direct cognitive security attacks on medical facilities so far. We have seen attacks directed at high-profile medical individuals and general attacks.

We can assess the possibility of direct attack, and ways to be ready for that. For example, we could prepare resources that could be used in countering campaigns that target COVID-19 field hospitals (such as the Javitz Center field hospital in NYC).

4. **Clearinghouse**: We have connections established, but haven't built ourselves as a clearinghouse yet. We could. We could also coordinate this work with those who are focusing on response and countercampaigns (the “elves” who fight the “trolls”).

For the neutralisation part, the league lists as examples:

- Infrastructures used by a threat actor that is exploiting the pandemic – malicious command and control server / DDoS servers / domains / IPs / etc.
- Exploiting legitimate services (such as open port in a legitimate website or compromised website used by hackers) and relevant to our stakeholders can be used to deploy attacks

The disinformation equivalents here would include:

- Hashtags, groups, networks, botnets, information routes, etc used by disinformation actor groups to create and run incidents. We can map several of these ahead of time, monitor them for new events forming (e.g. qanon checkins etc), and also file abuse complaints to registrars etc, notify companies hosting botnets and command and control accounts etc.
- Medical events (e.g. vaccination rollouts) that we know will trigger disinformation incidents

For prevention and support, the league lists examples:

- Alerting about vulnerabilities / compromised information and infrastructure to our stakeholders
- Creating a database of malicious indicators of compromise for blocking (via both MISP and GitHub repository)
- Alerting about trends and uneventful events regarding the pandemic in the cyber domain
- Creating a database of hunting queries for alerting systems.
- Create a safe and secure infrastructure for CTI League activities
- Create reports dedicated for the stakeholders and update them about ongoing trends of attack vectors regarding their organizations, such as significant information from underground-based platforms (darknet).

This is more detailed work, but as we track more incidents and become more familiar with the methods and tools used by incident creators, some measure of prevention activities become possible.

1.5.2. Channels and Bots

We have potential inputs, outputs and help across the other CTI league channels, beyond our own channel #4-disinformation.

- #2 channels are useful for finding us the people and places we need to get assistance, to report to (e.g. to find a specific Twitter group representative), to request takedowns etc.
- #3 channels are supplementary input data
- #4 channels are other teams (e.g. darknet) who work alongside us sometimes on the same artefacts
- We could add outputs to #5 channels
- #6 channels could become useful in future.