

COVID-19 Harm Reduction

[Team Mission and Goals](#)

[Data Preparation Activities](#)

[Health-related Harm Reduction](#)

[Extremist Groups](#)

[Group Tracking](#)

[Narrative Tracking](#)

[Handovers to other teams \(including CogSecCollab\)](#)

[Incident Response Activities](#)

[Incident Response](#)

[Active Incidents](#)

[Timeline](#)

[Countermeasures](#)

[Tool Development Activities](#)

[Content Coverage](#)

[Bots](#)

Team Mission and Goals

Our mission is to help prevent harm directly related to COVID-19 disinformation.

Our goals to support that mission include getting information and evidence so we can send escalations to law enforcement, takedown notices to platforms, alerts to organisers, local media etc, and social media outputs via our influencers.

The activities we do support those goals, and include things like

- monitoring for public safety issues that we can report before they become harmful;
- chasing down disinformation tactics and counters;
- mapping harmful narratives as they emerge;
- monitoring known disinformation feeder channels.

Our outputs are outputs to law enforcement (/Lenew reports), the other actions we take, messages in this slack channel, and google docs.

What we do needs to be within this framing: are we working to help prevent harm?

Data Preparation Activities

Health-related Harm Reduction

Our group's focus is on harm reduction as it relates to disinformation.

Specifically, our attention is best allocated to narratives which are likely to be most harmful in the coming months and beyond, and issues related to COVID-19 that will play into accelerationist narratives.

We expect a second wave of COVID-19 as a result of anti-lockdown protests and Black Lives protests. The number of people affected will be hard to gauge as health complications due to teargas, poor testing, and volatility are likely to affect the outcome. These matters will be complicated by high unemployment, social issues, fear of being tested and linked to the protests, and a hyper-partisan media landscape.

Our short list of important narrative subject matter includes:

- Blame on a particular group for the second wave
- Antivax conspiracies
- Putting people back in contact risk
- Immediate harm intended around protests

Activity: map the hashtags, known urls, amplifiers, groups etc for: medical disinfo, antivax, 5g etc where it overlaps Covid/medical, and all the other narratives that we've seen feeding into and feeding off Covid19

Extremist Groups

COVID-19 harm reduction gets a little fuzzy as extremist groups get involved in the narratives.

In the CTI League, we're interested in these groups and their content only as it relates to COVID-19 disinformation. Tracking and engaging these groups for other reasons is out of scope.

Activity: continue mapping of extremist groups

Activity: list the orgs already mapping longer-term harms, so team knows that work is covered / can go help those orgs if compelled.

Activity [comment01][comment02] track artefacts (groups, accounts, hashtags etc) that switched from Covid19 to protests and are likely to switch back to Covid19.

Group Tracking

We're continuing the work we've done mapping extremist groups, hashtags, etc., because they're part of the Covid19 disinfo landscape and aren't going away.

Going forward, our main focus will return to groups who actively spread COVID-19 disinformation. We'll continue to aggregate actor profiles, hashtags, URLs, amplifiers, etc for:

- Medical disinfo
- Antivax
- 5G (as it overlaps Covid/medical)

Narrative Tracking [comment03]

COVID-19 narratives will be tracked across all previously monitored groups and those specifically focused on COVID-19 disinformation.

We're interested in:

- Narratives crossing over between groups
- Narratives with high likelihood of causing harm

Handovers to other teams (including CogSecCollab)

The CTI League Disinformation Admins [comment04] may decide to focus on a particular incident or campaign which would normally be out of scope. Such incidents will be moved to CogSec Collab Slack.

We want to avoid fighting on multiple fronts. There may be cases we simply cannot ignore a particular issue, but we should acknowledge it comes at the expense of working on the process and tools required to build out additional deployments.

Where possible we should consider handing off our findings to organizations who may be willing to work with us or have capabilities in place to use the information we provide.

Activity:manage the separation of concerns between our mission of immediate safety, with the team's desire to literally fight nazis. If needed: spin up a new team in CogSecCollab for this, work on primers and find teams and links in places like ADL that need our specialist skills, and have leads from CDC to bridge people across to that. Write something that says "we're not directly doing this, but if you want to, here are the resources"? Maybe write a larger resource pack over at CSC?

Incident Response Activities

Incident Response

Active Incidents

We need team members to easily know about live tasks and active incidents via Slack. Team members should be able to:

- View list of incident tasks
- Add an incident task
- Modify task priority/severity
- Open/close incident
- Keyword/observable search tasks
- Close a task

Suggestions for tools include bots and D3PO or TheHive. At the moment, we're using the Slack pins in #4-disinformation to do this and [THREAD HERE](#).

TASK FOR IM LEAD: Need to do better job getting leading words to flag certain posts, which could eventually be turned into a bot or something but it would help as we all review things

- INVESTIGATE
- CLOSED
- ACTION
- DECISION
- ~~CROSSOUT~~

Timeline

We need to track the history of narratives that the team is seeing.

- First seen, last seen
- Key metrics
 - engagement
- Detection time
 - How long does it take us to notice after some threshold of engagement

We need some way to know when to stop chasing an incident (once hashtags start downtrending, are below some signal/noise ratio, below some engagement level, OBE, etc)

Countermeasures

We were finding "anarchist bus" disinformation within 30 minutes of it reaching small town facebook groups, message boards etc this week: could we have countered it there?

What counters are we willing to use within CTI League?

- Counter narratives

- Pollution (kpop stans)

Who is elevating counter (decision and/or handoff)? [comment05]

- May not want this open for all to see - we might want to establish something like “action officers” “accountability officers”
 - Possibly team leads but as this grows we may want to break the action officer out to their own team

Tool Development Activities

Content Coverage

- Current capabilities vs future capabilities
- In-scope vs out-of-scope

What platforms can we look at programmatically?

What are we collecting from each platform?

What tools do we have to compare findings across platforms easily?

We have misp and hive to store data in, but want to make them more accessible via spack. Next is what can we get accessibility into: e.g. scraping facebook. Need to build scrapers for social media platforms to SQL/DKAn etc. See the Kanbans. (look at the Team README) - if you’ve got code, talk to [Name Redacted], [Name Redacted] etc.

- identifying analyst leads per platform to help new analysts
-

Bots

Need to lat how our bots work. If you have to log into MiSP or Hive to do work, its cumbersome and slow - too many URLs; thinking, archiving; need to speed that out... lots of quality of live improvement conversations. How can we make it easier to contribute and get data where it needs to go on platforms.

TheHive IR Bots

Wayback archive

MISPTwitter

- Can we create a @ alias for the teams? (Example if you want to flag if for collection/analysis or review for incident??) [comment06]

Analyst support

E.g. jupyter notebook support - can sign into our web app for this
Mac/unix, being able to spin up a virtual machine with all the tools in.
(can ask the CSC data science team)

Action: data science training

Action: training signup?? Messaging?

[Name Redacted] training on cognitive bias

Peopleing

if you haven't taken the survey since it's official launch on May 22nd, do this here:
<https://docs.google.com/forms/d/e/1FAIpQLSew0nj6vzBtk7tEzIhnW5upAC6MxA0hA05tb6QwOI2WICZVug/viewform> any answers before then have been deleted

Action: retake survey if you need to

Dec 2023: Comments added below here as part of PII removal

- [comment01] Does that mean we don't bother moving forward with the right-wing extremist 1-pager or just nothing beyond that?
- [comment02] Would this mean status?? Active vs Dormant
- [comment03] Any way we can get a printout (daily) to a pin in slack channel (managers or triage) of current/active narratives from all sources?
- [comment04] Is this admins or managers?
- [comment05] Sanity check here too
- [comment06] Is this ok for this forum or??