# 2020-07 CTI disinfo team log

# Sticky

These are running notes on the CTI disinfo team. They're a log of what we're trying to do, as we're trying to do it. They're also a log of our team meetups.

## Disinformation Meetups

- Every weds and sat 4pm PST/ 7pm EST /OMG elsewhere
- Recorded
- See Training folder in Googledrive
- See Team README for meeting link

## Hi Newbies!

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

- Team: in Slack #4-Disinformation
- Leads: [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted], [Name Redacted]
- Process: in team README
- How-tos: in Big Book of Disinformation Response
- Tech: HIVE, MISP, DKAN, Googledrive, Python, github, bots

# Log

## 2020-07-01

What happened in the past week:

Incidents

- New incident: Million Masks March
- Closed incidents: Obamagate, Guo, BlackLives
- How do we get data out to other places? Other orgs using MISP… pull to CSC… export to json/CSV/xml and email… can trigger email notifications to people who sign up - might be fastest way.
- Flash alerts to other disinfo groups is possible. Can lead that. Post in their Slacks til we get a better system set up. Email alert, with “sign into MISP to get details”.

Tech

- Parler API client
- Data in Hive and Slack - making its way into MISP; need to find someone willing to push data to MISP; TL;DR copypasting into MISP.

Dox/training:

- Awesome training with [Name Redacted], [Name Redacted] last week… cool actively supporting that… Doing “dilemma consultancy protocol” today…
- Cleaning up training doc… need the training recordings into googledrive
- Disinfo data science to hand over

Outreach

- Hackathon in less than 2 weeks. Prepare!

Training:

- TheHive - Is it making our lives easier? Has it failed?
- [Name Redacted] presentation:
    - Incident response helps us frame the problem.
        - Workflows frame a problem, define procedures, indicate progress.
        - Hive = list sane minimum investigation steps, guardrails, quick reference to links and materials.
        - Case = IOCs, IODs, notes, tasks
    - So far used
        - Base template “disinformation incident” with base tasks “create misp, create dkan, tell people in channel”
        - Task groups: phases, tactics, IR lifecycle.
    - Task is title, group, description (markdown), assignee
    - Create tasks, merge templates.
- Clarifying questions
    - What’s the back end that makes HIVE workflows work?
    - Where this is working smoothly, what’s the type of interaction that people have with this? Typically used to optimize - e.g. read data, run cortex analyses etc.

Default observable types are atomic indicators; things like twitter post (which are collections of atomic indicators) can't be represented easily - need to be flattened etc.

- Other questions:
    - Relationship between HIVE and MISP? MISP is record of authority - use it to present public-facing threat intelligence to community; everything in there should meet some minimum standard. Hive is where we get work done; can throw junk in, work through findings; when happy can push only the things we're happy about to MISP. [Name Redacted] wrote integration for Hive so we can export Hive observables and AMITT galaxies to MISP… default export covers only some types of observable. Click on "responders->misp" to get these. To deal with getting the right observables across, mark them as IOCs.
    - What should be in MISP, what should be in HIVE? e.g. can do Maltego as cortex analyses in HIVE, then mark the interesting things in there. Same with BuiltWith finding a bunch of unrelated sites. Cortex and automated responses happen in HIVE; hand-curated data still goes up to MISP.
    - Action: add that to training - the team already looks and finds relevant data, we write that down in the BigBook.
    - Added to hackathon: create proper subcases, or merge natively.
    - Could we do Slack to HIVE notes as a bot? Could start a thread with a boilerplate initial post… e.g. START HIVE xxx DISCUSSION or call slackbot from thread.
    - ACTION: id cortex analysers for this
    - What do we want to automate? [Name Redacted] listed some, also look in BigBook sections on actions for URLs, hashtags, Facebook pages etc.
    - ACTION: Jupyter notebook integration into Hive?
    - Relationship with Cortex? What's the output format? Json that's transformed into html2 template comes back. Idea for tool that pulls up hive case, shows all jobs run related to it. Can do this - split data out from cortex, send to another service.
    - DKAN: thoughts on export to DKAN? Grant's the DKAN person - recording of DKAN training going up soon.
    - Pulling stuff from Slack threads: [Name Redacted] has bot to extract URLs from a thread; is a good shell for this. Could use Hive Emoji to trigger this. Isn't in League repo yet - [Name Redacted] will add asap.
- Responses/ Next Steps from [Name Redacted] (plus anything that was most helpful)
    - Confirming about friction using platform. Next step: build tooling we need; if we can't do that, rethink our case management tool.

Also, everyone's welcome to the happy hour

## 2020-07-08

Team meeting

- Incidents
- Process and Training
- Tools
- Hackathon!!!!
- AOB

Team work

- EU/NATO/MITRE
- Migrate BigBook:
    - Gitbooks?  Good to have reviews of changes etc
    - Also has an inline IDE too
- How is bigbook helpful? What would make it useful to you?
    - First time, helped with scope of what this group is doing
    - [Name Redacted] - DM email to [Name Redacted] to get access to BigBook
- Tools: needs
    - more data science tools
- Tools: Hive
    - MISP going in right direction, but state of HIVE not great. Cortex analysers etc. Need to optimise for speed…
    - HIVE at moment being used as big googledoc with objects thrown in.
    - HIVE only useful because of cortex analysers
    - Can use cortex analysers off the MISP, elsewhere.
    - MISP can send to users every time a new event is created.
- Tools: alerting to end users?
    - CERTs use MISP for this - email alerts
- Tools:
    - Keep MISP clean, only the objects we need to communicate go in there
    - Have an Elastic or somesuch to hold the other data.  Reuse the Slackbot mappings to create Elastic containers, visualisations etc.
- Tools:
    - Jupyter notebooks - can standardise and have other people using them.
    - Notebooks already in the github, and will be some in the trainings
- Move from Hive to MISP, notebooks, Elastic, D3PO bots.
- D3PO tasks, e.g. “see this facebook group, go find all the groups connected to it” is a good short task that could be done over a couple of hours - [Name Redacted] to run training on each of these small tasks (and make sure they’re in the BigBook?)
- Newbie!
    - @disinfo-admin:
        - [Name Redacted] does training, processes
        - [Name Redacted] tools plus being cool
        - [Name Redacted] Doctor and Commander
        - [Name Redacted] Data Scientist
        - [Name Redacted] does people stuff
        - [Name Redacted] runs incident response

    - Triage channel: fill out the disinfo team survey
- Q: what can an academic do?

## 2020-07-29 Team meeting: the road ahead

Topics for discussion:

- Check-in
- Covid-19 Disinfo response - next steps
    - It feels like a lost cause, for the most part
    - It's possible that we could effectively counter specific campaigns against individuals (e.g., Fauci) or institutions like hospitals
    - Anti-vaxx might be a better area to start focus
        - We have a good idea of what's going to be used
        - We can start staging counters now
            - What archetypes do we want to target
            - Can we utilize CTI connections for directing counters
            - We've been largely focused on response. How do we reach out to people who are responsible for targeting counters and get ahead of the game?
            - Are we working directly in service of critical life saving institutions, or are we focusing more on general public response? Both?
        - How can we support pro-vaccination campaigns?
            - Reach out to [Name Redacted] on this front
    - It feels like now that we've got a team in place, we're pivoting to strategic response
        - How do we engage people, and how do we keep people engaged?
        - What are our strategies?
        - Trial some before/after testimonials of COVID that can be used for pro-vaccination campaigns -- This is Dan, Dan got COVID, don't be like Dan, get the vaccine
    - Next actions:
        - Reach out to folks working for H-ISAC, state depts of health, get their input at the next wednesday meeting
            - Who is doing this and how?
                - [Name Redacted], talking to his wife and also through CTI H-ISAC folks
        - Talk to [Name Redacted] re: how we achieve those goals (influencing platforms to respond faster, etc.)
            - Wait on this until after talking to H-ISAC folks
        - Assemble a Social Media Justice League -- high-follower accounts who can help interrupt campaigns
            - Who is doing this and what are they doing?

- assemble a proof of concept (dank pro-vaxx meme) in the #memetic-warfare channel in Cogsec Collab Slack
- [Name Redacted], reaching out to [Name Redacted] et al with POC to see how they feel about it

- Where do we go from here?
  - Other disinformation areas to defend against
    - U.S. Presidential Election, for example -- What does the threat model for the election space look like?
      - The traditional ones
        - Voting locations
        - Voter registration
        - Election date
          - How do we encourage turnout, especially among young people and underrepresented groups?
      - Covid-specific ones
        - Attacks against USPS / Attacks against legitimacy of vote-by-mail
          - Trump Administration is already trying to do this
          - Pro: USPS regularly ranks #1 in trust of gov’t institutions
          - Counter: Trust your letter carrier to get your ballot where it needs to go
            - Campaigns by individual postal employees
            - Humanize it to defang the attacks
          - Next actions: take this stuff to Deb, find more people to be engaged with this work
        - Misinfo re: when absentee ballots have to be returned
          - Meme the shit out of the date (Nov. 3)
        - Uncertainty re: when the winner will be declared due to large number of absentee ballots
          - Counter: PSA campaign that it’s going to take at least a few days to count if there’s a high number of absentee ballots
        - Election insecurity
          - Misinfo re: where absentee ballots have to be returned
          - What happens if a recount is needed?
          - Next action: poke around CTI for the folks focusing on this, and make sure they’re in Cogsec Collab
            - Bring them into a meeting to discuss what their concerns and areas of focus are
        - Bonus nightmare: this is going to happen *EVERYWHERE*, so how do we respond locally?

- Census
    - Threat space
        - Minorities and immigrants are afraid to fill out their census forms because they are afraid of getting deported
            - You can fill out the census without dropping personal info
            - Orgs are already doing GOTC work, how can we support them?

Red team Wednesday:
Question for discussion: If I were an evil bastard, how would I instigate all of the above?

Anti-vaxx:

- Campaigns:
    - Vaccines cause Autism / testicular shrinkage / etc.
    - What herd immunity actually means?
    - Vaccines contain live viruses, are impure, etc. (they're trying to make you sick)
    - The virus ain't that bad -- in re. Measles
    - This is absolutely untested and you're playing russian roulette
    - Microchips in the vaccine (method of control, mark of the beast, etc.)
    - Targeting specific brands or groups (specific vaccine, health care chains like Walgreens, CVS, etc.)
    - The vaccine won't work on $MINORITY / has intentional negative effects for $MINORITY
    - Actual rollout == an unannounced stage IV trial (half of you are gonna get a placebo, don't do their work for them)
    - Poisoning the well -- the data was corrupted by Russia/China/somebody, and the vaccine is thus suspect
        - See Johns Hopkins "Tuskegee" Guatemalan vaccine tests
- Scenarios
    - 1 country pulls ahead on vaccine candidate
        - Russia has a vaccine! Now what?
        - Put the stage IV trial campaign into play
        - Drum up the price for export to create another Russian niche economy
        - Use as a potential way to avoid sanctions/launder money
    - 2 countries pull ahead on rival vaccine candidates
        - Research data is tainted and can't be trusted
            - China has been cooking their research and academic papers
            - Compare and contrast externally visible numbers with data out of US and UK
        - Questioning the supply chain:
            - Russia developed the vaccine, but it was produced in India, and India's QC is shoddy, so is it actually safe?
            - China has put toxic stuff in their consumer products (melamine in baby formula), how can you trust anything they make?
            - Can you distribute it to the end destinations in a way that is verifiable and safe?
        - Edge cases
            - Have you tested on people who might have the standard set of severe side effects?
- Potential platforms for these?
    - NextDoor (Jesus.)
    - MumsNet (British)

        - Facebook
        - Instagram
        - WhatsApp (private groups)

Election security

- Campaigns
    - Election day is Monday for Democrats, Tuesday for Republicans
    - Your vote doesn't actually matter
    - Prematurely call the results of the election due to absentee voting
    - "If you vote for Biden, that puts you on a list for being associated with Antifa"
    - Someone sends out fake absentee ballots and they get routed to the circular file
        - Already happening re: [Name Redacted]
    - "Here, I'll take your ballot in for you, don't seal it"
    - Can't trust the Post Office
        - Have to get through the carriers first
    - Can't go vote because long lines, no machines, etc.
- Vectors:
    - Facebook
    - Nextdoor
    - U.S. Postal Service
    - Instagram

A few more ideas and resources from Mike

- Resources:
    - "The Vaccine Trust Problem" from NYTimes The Daily Podcast
        - 50% of Americans are hesitant or would not take the vaccine
- Ideas
    - We need strategies for neutralizing disinfo
    - We need proactive messaging targeted to people based on their concerns and their identities.
    - List of concerns/archetypes for vaccine skeptics, vaccine hesitancy, and anti-vaxxers
        - Vaccine Skepticism
            - Waves seen with MMR vaccine and autism as well as Smallpox vaccine
            - Texans for vaccine choice
            - People who resent PHARMA
            - Crunchy granola parenting movement
            - African-American and Latinx communities bc of things like Tuskegee experiments, being used as cannon fodder for rich white people
        - Vaccine Hesitancy

  - People who normally get all vaccines but are skeptical of the COVID vaccines in particular
    - Lack of Faith in President Trump
      - He or his friends will profit
      - Operation Warpspeed is not following proper safety steps and protocols
      - Operation Warpspeed is too rushed
  - Shift to individualism endangers idea of vaccine as an expression of altruism and protection of others. Protects those who can’t be vaccinated
- Anti-Vaxx