2020-06 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
- Format
    - 30 mins team coordination
    - 30 mins team training
- 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]
- Process: in team README
- How-tos: in Big Book of Disinformation Response
- Tech: HIVE, MISP, DKAN, Googledrive, Python, github, bots

Log

2020-06-06

Team catchup:

- COVID-19 Harm Reduction
- 2 pager on spotting disinformation

2020-06-10

Team catchup

- Memetic warfare session
- Defining narratives
    - [Name Redacted]: “Stories you tell yourself
    - [Name Redacted]: “Interconnected set of ideas that come together and influence how you interpret the meaning of things”

2020-06-17

[Name Redacted] on narratives.

- Disinfo talking points are extremely consistent and endlessly repetitive.
- Strategy: Explain - encapsulate - saturate.
    - Simple authoritative fact sheets on hard issues. Clear resonant talking points, hashtags, memes.
- Audience: confused, “low info liberal”, allies (for building an amplification network).
- Three teams:
    - Monitoring - current, emerging and likely future hot topics.
    - Messaging - Research, build simple explainers, create resonant talking points
    - Distribution - allies, platform etc
    - (also infrastructure and process, and advisory board)
- Current status
    - Have: Website in progress, slack, docs and processes; 2 explainers, volunteers
    - Need: editors (to own topics), writers room volunteers (for regular weekly writers room), design skills, social media help, alliances, modest funding.
- Deliverables
    - Explainers (2 done: vote by mail and antifa, 7 in progress)
    - Talking points
    - Network

- How to help
    - Follow twitter and snapchat @realityteam11
    - Join team info@realityteam.org
    - Help connect to other people
- Questions to Deb on [Email Redacted]

Facilitate:

- Clarifying questions
    - Q: can we amplify other groups' content? A: yes, and that's critical. If build a network, needs to be multidirectional, not just us ("Catalog effect").
    - Q: prime directive is to do counter-messaging, and create alternatives ("positive grounding narratives").
    - Q: proactive vs reactive. What's the relationship with that? Starting with both, or reactive first, or proactive because can control those narratives. Right now, trying both, but glacial progress. Currently have list of topics, e.g. "what is systemic racism"... current alternative narratives aren't strong on e.g. "what does it mean to be a global leader"... will need to discuss prioritisation in the Writers' room.
    - Q: templates for explainers - is the same template good for proactive and reactive? When things are templatised, people learn to read them more easily, and they're faster to build. E.g. takeaways, then Q&A, then repeat takeaways, then references and further reading.
    - <Q: "a factual summary". Facts are difficult>
    - Q: design skills, or meme skills? Both, but someone who can make templates legible and clear; also work on the logo. Looks count not just for clarity, but also identity and attachment.
- Then probing questions (question assumptions, get at deeper ideas)
    - Q: Gave example of 20-year-old son searching for info but doesn't know who to trust. Why is this template more convincing to them, why would it resonate with them? A: a few things - the key takeaways. Empathy that confusion is a normal response to these topics. Also goal to have these as simple as possible. Narratives: usually have a narrative hierarchy, with key takeaways at the top… the rest of the Q&A is to flesh out and explain why these takeaways… make takeaways simple and repeated enough so they stick. Short message with virality of a meme - sized between a meme and a factsheet. Ideally, with key talking points used as memes of their own. Narrative, rhetoric, propaganda, marketing: repetition is truth.
    - Q: decentralised, want to be governed by a community. Lines up with cogsec approach - TI as a service where it's necessary; lines up with that operational mode. A: first concept was bad guys have a very effective network; RT etc put together talking points, and they all coordinate around these things, with a mature process and network. First idea was a good-guy analogue to that. Part of this is an invitation - "would you like to be part of this network", CTI style. "X Team" = so anyone in public can be part of the Reality Team… layers of this network

    - Q: Interesting about this is not just counter-messaging, but also building the network. Important to respond to counter-counter messaging. Don't have a way to stress test if a narrative will take off, and how to deal with counters. See this in Asia: narrative formed, counter, then come back with new narrative. How is team going to deal with Discredit moves? A: programmatic advertising to stress test, AB-test narratives etc - Facebook makes this easy to do. Haven't thought so much about counters to this. Having a core message creates positive against this. [Name Redacted] doing work on cognitive hardening - "how does this truth vary from the truths I've already learned", and Truth resilience. A: reading about deprogramming cults… cognitive security… [Name Redacted]: want to use as canaries/ social listening - becoming a target can be helpful.
    - Q: scope = beyond Covid ([Name Redacted] has colleagues who can help). Focus on US election is in here.
    - Q: group is homogeneous - how getting extensive diverse groups into this process? And people from different topics? A: CTI isn't the only group [Name Redacted] talking to. Other groups include former government types.
    - Q: is this a network of networks (aggregating other networks), or a network unto itself? A: there are a lot of fellow travellers - if this group could be touchstone for those, coordinate, be friendly facilitator across domains, would be very powerful. Not trying to build a selfish network asset, but a way to get info to as many people as possible. Network of networks good guy analogue of badguys.
    - Q: scale. Hackers do small agile things fast; this is larger scale, how do we get that to work together? A: place for all those things - writers room as rapid response. AOL standard used to be dollar cost scaleable: create something so can do more stuff with more people… but fun memes stuff isn't mutually exclusive. Should be able to put out some stuff every night.
- Then discussion and observations
    - (Q: network - you build this on trust. And you get that from results)
    - Decentralised, nimble, scaleable networks of networks. Playing field is laid out the way it is right now because lots of different entities had money and aligned interests, and reinforced each other. What we're seeing now is the result of lots of people throwing money at the same problem accidentally. Reality (the thing) has an advantage, but we need to spend time drowning out the voices trying to drag people away from reality.
    - We might not agree on reality - reality isn't reality… it's perception of reality. There is no Truth… use "consensus"?
    - Try an experiment - people clicking on a colour map, pointing at the colour of the sky… then do social media experiment telling people it's orange, get 2 clusters now? Then later, without experiment, go back to 1 peak? Challenge is competing with a well-organised network.
    - Internal narratives influence the meaning of things, and nobody has the same internal narratives… but "what is antifa and are they coming on buses" are topics with a legitimate amount of complicated stuff that can collapse down so people

can understand better - might interpret in different ways, but a lot of space between what's in the disinfo space and what most people agree is real.
- Follow-ups… DM [Name Redacted] in slack, or email [Email Redacted]

2020-06-24 Issues and Fixes meeting

Group cohesion

- Poor communication - 36 people in the triage team; who are they, what are they looking at, what are they up to?
- Could: talk to people in triage more
- Could: rename 4-disinformation to 4-disinformation-discussion
- Could: push all chat to 4-disinfo unless it's sensitive
- Could: explicitly name our norms. There's the CTI code of conduct. Could run a training activity around group norms.

Channel expectations and norms

- We don't set the norms of each channel: managers vs triage vs disinfo. Hate to loose the sense of unity, of common purpose - want to come back to that… once understood difference between disinfo, triage, managers, cogsec, knew where to put things.
- Managers issue with helping people be helpful without blowing things up. Lots of energy, but needs to be channeled. [Name Redacted] suggested how do we drop stuff from Twitter into channel - there are confusions about where things go… we need to fix that.
- Opsec concerns - people need to be careful about what they're contributing to and how. e.g. can't see Kanbans without GitHub account.
- Could: list difference between channels, enforce that.
- Could: talk to people about patterns of interactions and challenges.
- Could: set norms. Where do we drop twitter links. Do we thread or not thread? Ask [Name Redacted] for help. (She's now the BigBook editor)

Incident management

- Management - putting out fires is wrong way to run incidents. Burn out concern.
- Current style = monitor twitter, respond on interesting things. Should have master narratives and stick to them.
- Covid: need to sit down, define what we work on, what the milestones are. Incident ends when we answer questions, not when people get bored… [Name Redacted] and [Name Redacted] can help with what those benchmarks look like.
- Jumping on things quickly, rapidly iterating - works if that's the target; but if it's everything, it's too much for 5 people
- Have to focus on covid-related disinfo. Protest falls under that because of things like getting tested. Have to shift focus back to covid
- Could: Measure incident tasks - e.g. did a, b, c this time, could do d, e next time.

- Could: pre-triage things that come into triage, so we only post things that are sensitive or relevant to incidents there.
- Could: shift focus back to covid
- Could: set up a temporary warroom at cogsec for protests etc. e.g. set up and use the CSC_incubator slack

Pace of progress

- "we don't get anything done".
- Could: measure our pace.

Not providing adequate tooling for triage

- No "here's some useful toys, get up and running now" in triage.
- Jupyter notebooks, more bots are a good idea. Ask people to start building stuff?
- Could: post regular updates on tools
- Could: add existing notebooks and other tools
- Could: [Name Redacted] ask triage for help on data science notes

Team meeting starts

- [Name Redacted] - [Name Redacted] doing more editing on BigBook (lead editor!)
- [Name Redacted] writing tactical disinformation data science doc - https://docs.google.com/document/d/1PZnfbZXBxor3rdg_Rik9yC5QbP-JoAjx1IfVyue676g/edit#
- Speaking - we need to do more of this, and by we, we mean not just [Name Redacted]! [Name Redacted] can help with this; [Name Redacted] mentors at BsidesLV.
- [Name Redacted] - writing subtechniques for AMITT

@channel
We've had amazing engagement in #4 Disinformation in the last several weeks around COVID as well as several other topics like the George Floyd Protests, and Far-right disinfo. We've also had a lot of new folks joining the team. In the spirit of supporting that awesomeness, @disinfo_leads wanted to provide a few updates. (Apologies for the length of the post. Please do read all the way through though.)

1. We have a new channel: the #disinformation-random and it's an awesome place to learn from each other about all non-COVID-related Disinfo! (more on that below)

2. We have Channel descriptions to help everyone know what goes where, clear up any confusions, and make it easier to engage in the channels.

Our Disinfo Channels are:

- Disinfo-Managers

    - Leads channel: A place for @disinfo_leads to coordinate and discuss how we run the disinformation team.
- Triage
    - Vetted channel: A place to work on sensitive data and incidents. Triage has access to the full CTI disinformation toolkit and write access to the BigBook.
    - You can join Triage by filling out the disinformation team survey (link), and saying that you'd like to join Triage.
    - If we see something that doesn't fit here, we'll suggest you put it in 4-Disinfo or Random, then delete it.
- 4-Disinfo
    - Open channel: A place for anyone in the league who wants to learn, engage, and share about Covid-related disinformation and disinformation techniques. Also a place for anyone who wants to help with incident tasks (e.g. data gathering). Has access to open tools like MISP and the bots and read-only access to BigBook.
    - We handle difficult content. There's an expectation this will appear in our incidents - we use threads so you don't have to look at these. If you think something might be triggering, write a line with a Content Warning saying it might be difficult, then add the thing in a thread.
    - If we see something inappropriate in here, we'll suggest you put it in Random, then delete it.
- Random
    - Open channel: Where you put anything that doesn't fit into the above channels. Drop resources and observations in here and chat about disinfo. It's fine to discuss other types of disinformation and other areas affected beyond COVID, but please don't run non-CTI incidents here (CogSecCollab is working on providing support for that).
    - If we see something inappropriate in here (e.g. non-threaded disturbing content), we'll flag it, then delete it. We want to keep everyone safe.

- Examples
    - A fun post about disinformation in the gas industry = Random
    - Non-medical political disinformation = Random
    - Extremist disinformation = Random, unless they're part of a disinfo incident
    - An alert about a (non-sensitive) potential new incident = 4-Disinfo
    - Articles on health-related disinfo = 4-Disinfo
    - Cool tools and ideas = 4-Disinfo (unless sensitive)
    - Announcements = 4-Disinfo
    - News from other groups = 4-Disinfo
    - "How's everyone doing" check-ins = 4-Disinfo and Triage
    - An alert about a (sensitive) potential new incident = Triage
    - A post about a sensitive incident that we need to keep in triage = Triage

Channel Norms

- Follow the League code of conduct https://cti-league.com/cti-league/code-of-conduct/

- Don’t put disinformation into the disinformation channel without a warning that it is disinformation
- OPSEC
    - Defang your urls (i.e., www[.]google[.]com)
- Threading
    - We should keep anything potentially triggering in threads
    - Incidents should be threaded
    - Incident threads use keywords to help manage and analyze them, e.g.
        - NEW RUMOR
        - NEW INCIDENT
        - DEEP DIVE COLLECTION
        - DEEP DIVE ANALYSIS
        - ACTION
        - ACTIVE
- Content Warnings: Live by the rule of “First, do no harm”
    - You can use “CW” to indicate that there’s a content warning
    - Types of content that require content warnings: Violence, Hatred, self harm, etc.

2020-06-27 Team meet and training: threat hunting with AMITT framework

THreat hunting with AMITT Framework

- Slides: 2020-06-27_Threat_Hunting_with_AMITT_Framework
- [Name Redacted] talking through AMITT; [Name Redacted] on threat hunting, team working through an incident with this
- A lot of our work til now has been putting out fires, but AMITT is designed for more than that - is for understanding adversary behaviour and how to counter that. Natonstates to script kiddies need to think about what victory looks like, how to do it, was the mission a success?
- Can dive down further - and that’s where we see AMITT tactics. The three we’re looking at today are preparation type techniques: creating accounts and networks, and choosing the channels the incident will be staged on
- We don’t want to be chasing artefacts… want to deconstruct what am incident looks like. If we find a specific type of actors and groups, that gives us hints on what we need to be looking for next
- Develop people: 3 ways to get accounts: create, buy, or steal: each of these leaves behind artefacts: creation dates, IPs, timezones… for bought, might be darknet evidence for stolen might be on have1beenpwned or complaints about it online.
- Once you have an account, how is it being used? Will it be backstopped? The quality, the amount of work put into the accounts, give us an idea of the resources available to the incident.

- Networks: Accounts are useful without followers, so need to develop a network of people who will consume signals. NEtworks are cross-platform bridges: often the same individuals doing similar things. E.g. looking at Boogaloos across instragram, reddit, twitter, they used the same hashtags, memes etc - which they needed to do, to work. Can look at how they act, what their norms are, their languages, and their activities in the networks.
- Channels: TI in infosec we have a lot of logs, e.g. powershell logs. If you only look at the big ones, you miss a lot of stuff: cogsec is the same, e.g. looking at instagram, twitter is right of boom - that's not where things start, like the chans. There's work to be done on finding those primary sources. When we look at blogs, we're not just doing it for fun. When we ask what the target audience is, we don't just mean twitter, we want 50 different audiences too. That's where channel selection comes in.
- Everything comes back to the domains. Social media is data in transit; domains is data at rest - and needed if the object is money or power (because can monetise with clicks etc, can control etc)
- Disinformation hunting: important because we want to understand staging environments etc. So we want to look at these three areas, ask very general questions, test and correct them, then do this work at scale.
- Keeping this high level, want to think about this differently, to create our hunting hypotheses.
- Tools etc: we have a lot of work to do building scrapers. We need to prioritise the platforms of interest to us - e.g. if we're talking about antivaxxers, we need to understand the nature of their sites and interactions.
- Tactic/technique based playbooks: we've started some of this work in Hive, but need to make sure this is current.
- CVE: we have people in DarkNet who are good at this, want to get some of them interested in this application.

Questions on using the AMITT framework

- CVE? Countering violent extremism
- Hierarchical AMITT
- Why does this matter? MITRE: threat-informed defence… not enough to defend against a threat if we don't understand it. People plan in the same way, develop accounts in the same way etc.
- What's pink slime? Networks of fake websites

[Name Redacted] on threat hunting

- Can detect where… then build that narrative of what happened from the beginning…
- E.g. if you have pump priming, kernel of truth - you have here's what you know, here's what you need to find out. You develop a hypothesis - I started here, have twitter and blogposts, then start to ask questions, develop a story. If you can't develop stary, can't get other people to buy in on why it's an issue. In 2016 election, had an issue with that - didn't have the language, couldn't tell the story.

- E.g. show difference between intention to disrupt with resources, and script kiddies. Also map actions and counters. E.g. countering cheapfake is going to be the same most of the time, so don't need to recreate it each time; so based on resources and timeline can go "how can we counter this now"... need bumpers, a reference point to id what we have so far, build hypothesis… we're not trying to prove the hypothesis, we're trying to disprove it. Read "structured analytic techniques" by Richard Heuer. Powerful… timebox it, make sure have right inputs, whittle down from impossible to real. Do things like have competing hypotheses, hypothesis generation…
- ACH is a big one… https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art11.html
- also argument mapping https://www.reasoninglab.com/argument-mapping/

Mask example

- E.g. we see an image - can do a reverse image search
- Who shared it?
- What are the hashtags on it - what else was shared on those hashtags?
- Have we seen those hashtags before (e.g. wwgwga is qanon)
- Has to be able to scale - easiest way to scale is through hashtags
-