README: Training notes and log

Introduction

Upcoming Trainings and Discussions (7pm EDT)

- Wednesday 7/1 Intro the Hive: Incident Management with [Name Redacted]
- Saturday 7/4 Disinfo Data Science with [Name Redacted]

Training requests

Training requests list:

- Countermeasures
    - Memetic warfare (and/or shitposting)
- End to end tech use
- Sources - where to find alerts, fill gaps, other efforts etc
- Narrative detection
- Sections from the BigBook
- Tracking foreign vs domestic disinformation
- Keeping it safe and segregated from work stuff
- Disinformation beyond the US: Expanding beyond our US-Centric Worldview

Available training

- OpSec for the CTI League Disinfo Team
- Hive (BigBook step-by-step) (Video coming soon)
- MISP (BigBook step-by-step) (Video coming soon)
- Cortex (BigBook step-by-step coming soon) (Video coming soon)
- Digital harms (Slide Deck)
- TTPs (Slide Deck)
- Threat Hunting with the AMITT Framework (Slide Deck)
- Countermeasures (Slide Deck)
- Disinformation beyond the US: Expanding beyond our US-Centric Worldview (slide deck)

Log

2020-05-08 Reading Group notes: MyTel

https://medium.com/dfrlab/facebook-shut-down-commercial-disinformation-network-based-in-myanmar-and-vietnam-d8c07c518c04

- Goes through tactics and techniques used, and also the forensic analysis used
    - “Coordinated inauthentic” = behaviour rather than content. Like malicious insiders - same behaviour-based detection needed.
    - Building groups around the pages - reputation
    - Had a specific way they wanted to grow

    - Marketing - lot of disinformation teams started in marketing; using social network KPIs, e.g. reach, targetted demographics etc - Facebook ads gives you a toolkit for this
    - At what level is *who* responsible for continuing to spread disinfo; *who* is responsible to the users? Needs something like the Paris agreement
- Business-level disinformation, but if it's a state-owned enterprise, is it a state-run disinformation campaign? Hard to tell difference between state and enterprise. And then you get joint ventures; companies offering up data - e.g. bio-economies.
- Takedowns - can they be done without input from state actors?
    - Depends on perspective. E.g. ISPs can block things w/o government interdiction
    - E.g. CTI have ISPs - have vulnerable hosts, can block and mitigate some of the risk… Google/Facebook putting banners with information on is part of that trend of industry stepping up
    - But… China not cut and dried industry vs state line, Russia can take down internet etc

2020-05-23 Training: discussion on non-USA Covid19 disinformation

Intro

- New training format: more professional learning on wednesday; more discussion-based on saturdays
- Today - looked at less US-based, less anglophone-based
- Starting by looking at the questions we want to ask, then world, then middle east and asia

Questions: what do we want to know?

- [Name Redacted]: what's currently happening with misinfo targetted at africa and middle east. Given there's a lot going out of Nigeria with 419 scams, and Russians used Ghana as proxies in a campaign a few months ago - what's focussed specifically at Africa?
- [Name Redacted]: building a map or graph for displaying organisingcategorising narratives - most of that has been western centric; don't think should change that much, many of the narratives should change, just some of the actors change; maybe go country by country, region by region, see what are the topics? What do we have in the way of translators or resources in other countries? E.g. african countries - language, idiosyncrasies in that culture.
    - [Name Redacted]: have connections to groups round the world. M: Maybe use english because of colonialism? [Name Redacted]: No - e.g. in Ghana mostly tribal languages used.
- [Name Redacted]: what are the prominent channels in each country? What are the mechanisms used, and what's been most effective in the past?
    - [Name Redacted]: is this like forensics - could we get access to artefacts that we can't in other countries? E.g. SMS datasets.

- [Name Redacted]: antivax - how has it spread to other countries since last year, how, what are the flows, are there any localisations?
- [Name Redacted]: as we go

[Name Redacted] overview on world
- TL;DR go read the Comprop reports
- And there's a new section in the BigBook for this

middleeast actors and history
- Disinformation campaigns have always been in the middle east. Defining moment was 2011 arab spring and Syrian civil war: first social media event that got all the players doing digital and sm manipulation; russians coming in, delegating tactics to the syrian regime, leading some of the efforts. Most of the pro-Assad effort was led by the russians. Also seen in CTI world with the Syrian Electronic Army (which was actually Russian) and its information efforts, which were also Russian-led. Saw Russians slowly take over platform after platform with pro-syrian narratives.
- In disinfo world, prominent asset is [Name Redacted] - pro-Assad propagandist; unclear who this persona is, but is a very live persona, probably developed by the russians - also active in the MH17 and other campaigns.
- Syrian civil war also drew in other actors with interest there - probably Iran, and iranian arms in the middle east: Hezbollah, Houthi movement in Yemen, Shiite, pro-iranian elements. Difficult sometimes to distinguish between iranian, russian, syrian efforts based on narrative analysis alone (without forensics); theres a lot of overlap between the narratives: anti-US, anti-israel, pro-Assad, pro-iran, anti-Isis, blaming Isis on west etc. Have to look at different styles of disinformation, or actual forensics.
- Other regimes picked up - moderate regimes, which are still authoritarian, developed their own IO capabilities, for domestic means, to counter iranian destabilisation efforts, and against regional foes (not just iranians)... Sunni regimes: Egypt, Saudi Arabia under MBS, UAE (Bahrian, Oman less active); they usually work through third parties like commercial digital media companies that do campaigns for them; focus on domestic, but main event that sparked IO in middle east was 2017 feud between Qatar and Saudi? Celebrated anniversary - trolling campaign; claimed coup in Qatar? Just died down. Were handling it well, now a second wave hitting them. Many IO in arabic and middle east in past 2 years were part of this conflict. Most attributed to Saudi, UAE, sometimes Egypt. One to Qatar - very sophisticated actor with strong state media outlets that manages to stay under the radar.
- Another big actor in past few years is Turkey. Nobody talks about it a lot. Has strong tradition of IO, intel ops. Most of its efforts in past few years against its kurdish minority. False flag campaigns to pin Isis bombings on kurds, or to pin bombings against kurdish demos on ISA. Now active in Libya; run campaigns in northern africa against rivals: Egypt and UAE. (M: also leaked about Kashoggi to the press; did amplify this story)
- Covid19: Saw rivals trying to run campaigns that leaders were trying to hide true numbers, and had covid themselves. Died down now - Covid19 is so bad in both places, e.g. Qatar has 20k cases? UAE is just behind? Mostly foreign workers - is serious, so

they don't want to play with fire and start rumours that can hit them back. Still seeing info campaigns e.g. fighting in libya, but not so much covid related. Iranians focussed on playing the victim, trying to fight the sanctions, and lift some of the sanctions; lots cyberattacks. Haven't seen any attempts to amplify US, UK etc movements. MiddleEast actors are preoccupied with their own area.

Near-peer adversaries

- Semiconductor between china and us. Hasn't really kicked off - lot of it going back and forth. US has Taiwanese semiconductor manufacturing company building factory in USA. Is evolving over time. See this amplify. Over last 5 years… near-peer adversaries (russia, china...) - focus used to be regional, now focus farther out, push regional conflicts and get more people involved. What Covid's done for all of them (Russia, China, DPRK, Iran) has sped up their modus operandi and ops tempo, showed their hands more than before.
- Merged operations/ tactics? Shared interests, and enemy of my enemy is my friend. China tried to be heroes, level playing field, its not us its them, and that narrative's been knocked down. E.g. 5g: was "the US is trying to keep us out"; Covid showing what they're capable of - e.g. Italy, the information campaign, fake videos "italians happy we're providing aid" and that wasn't real. Advancing faster - if you can push an adversary to go faster, there are more opportunities for them to mess up; influence, strategic objectives; e.g. hong kong backlash is there. They push on the offensive when it gets harder at home, to divert attention. E.g. when 2nd wave hit, they pushed externally. Can track numbers of virus and effects at home; see offensive and push e.g. venezuela coup, covid 5g in NL when gets bad enough. Could look at timeline of when the pushes happen relative to crisis at home. E.g. push to avert eyes out of home, so eyes aren't on when they respond.
- Q: convergence of narratives. If have cyber operation running, may have strategic targets don't want to share with allies, but if running an IO, it's in my interests to copypaste narratives from allies, amplify each other's messages. Will we see more of this from russia, china etc, to keep US busy, keep our hands full. Starting to see that line drawn, similar to cold war - west vs everyone else is the fear. Seeing convergence of some of the big players. E.g. Russia behaviour in WW2. If that big a target, only benefits to have shared interest, willing to collaborate on shared objectives. Didn't really see this before 2015; some russia-iran some other bleedover, but now russia bleedover into venezuela, amplifying factions because pro-non-democracy. Watching China belt and road; Open; India-Pakistan, trying to build out infrastructure, africas, americas: have more at stake there; if US gains influence there, whilst not directly regional, because of increased economic they're trying to build there, will push more.. If can align with belt and road - if see strategic objectives, can see what they're likely to start hitting.

Shares

- Twitter and Teargas
- https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Thoughts:

- Look at how China looks at this: they look at this as IO directed at them. In terms of dynasty, where US thinks in term of decade, if that. Middle East is rooted a lot further back too? This is dangerously close to orientalism.
- On Covid19 - big disparity between chinese narratives and narratives we're tracking in us. E.g. tendency to blame US. Also China won't go Antivax, or anti-WHO. Easy to differentiate between the different narratives. Chinese narratives will be seen as counter-attacks, counter-narratives, e.g. incompetence dealing with the virus. Some amplification of russian e,g, RT/Sputnik; Russians using e.g. global news and chinese narratives. Renewed attacks on legislation in HongKong: HongKong and Taiwan seen as domestic areas; HK likely to be a focus in next few weeks. Most chinese IO in past few months blew up in their faces / backfired: Italian operation backfired (wanted europeans to say how much more responsible, benevolent they are), HK backfired (wanted to quell demonstrations) because poorly executed - in style of chinese cyberattacks.
- "so maybe that is something we look at too to triage, what is their No-Go points it helps narrow down who may or may not. there is the possibility of this having the opposite effect of false flags I think the backfire is important because they are having to move at a speed they are not used to"

Feedback before wednesday

- Documentation work goes into the operational kanban
- BigBook editors: anyone who hasn't been through disinfo checking goes to comment-only til we get them through onboarding.

2020-06-10 Discussion: Memetic Warfare and Shitposting

Quick Updates

- Leads
- People
    - Onboarding and offboarding lists (see spreadsheet).
        - Bigger lead effort on member activity - if members haven't participated in certain amount of time, are looking at that harder, considering booting them if not many messages, effort.
        - Larger holistic view on CTI application vs disinfo survey answers. If they didn't match, gave pause. E.g. github repos with stars but empty. [Name Redacted] a pause because maybe looking for hot topic? Members with password breaches - can we trust them?
    - Newbie channel message (see Ohad message below)

        - Thanks for editing [Name Redacted], [Name Redacted], [Name Redacted]. Going to [Name Redacted] at end of today.
- Tech
    - What are our most-wanted data sources? Will petition dev channel to build scrapers.
    - Work on AMITT subtechniques is ongoing. Send me your notes/ideas.
- Process, documentation, training
    - Want to start moving on Operational Kanban (quick review)
    - Give us more pretty graphics
    - Eventbot - being used by AI Village to manage team calls and reminders. Seems to work well: can we get it? https://support.geteventbot.com/hc/en-us (but not this one https://techcrunch.com/2020/04/29/eventbot-android-malware-banking/)
- Incidents and incident management
    - More protest stuff, inc Atlanta Black Panthers
    - Need to pivot to Covid19 - second wave narratives are starting (blame)
    - Need to get ahead on data work (e.g. groups, sites)
- Outreach
    - CTI Darknet
    - CTI - other teams are getting set up… we're still the most process-oriented team… seeding that
    - Guest demos, visitors, lectures?

Looking for people to come in to talk about Data Science and Data Tracking

Narrative: Stories we tell ourselves
[Name Redacted]
Registered Realityteam.org
Explainers > Memes
BLM and George Floyd
Project Lincoln, 11 Films and Midas Touch: highly produced videos, not very mimetic, highly political
We may be able to draw those out
American flag and Confederate flags
Nascar statement on the Confederate Flag
Topic areas that we want to push back on

- Vote by mail
- Antifa

Topic areas mirror the narrative list and expected narratives? Including crossover narratives?
Master narratives list is Covid19_Master_narratives_list.xlsx

Start with FAQs and use them to build memes
Activities interested in pursuing

1. Calm cool and collected here are the key takeaways with citations
    a. Addresses not-on-twitter population that gets overwhelmed and confused

b. Top line talking points people can take away and remember

Link to [Name Redacted] doc White Hat Disinfo Response Team Quick Summary

Process: Editor per topic
Then to Writer's Room

Development of talking points that should be shared in common
More important than memes in some ways
Imagery as a way to support the words
Those resonant messages that are the crux of the issue
Getting the words into people's vocabulary
Need those talking points coming from many different places at once
Need to build ally and amplification network
No value in deeply resonant messaging if nobody hears it
Repetition is truth

[Name Redacted] is currently putting together the portfolio
Amplify the work of others
Ally network is really essential
If we can get funny folks in, all the better

Aside: History of the World
DDay Fuckery Factory
MisinfoSec Group
Misinfosec working group inside credco that built AMITT
Created CogSecCollab to continue that work in 1 place
[Name Redacted] from Crisis Mappers
[Name Redacted] from Mutual friends
[Name Redacted] and SJ started
TedX Disinfo team
CogSec Collab builds tools that support many teams
CTI League was seeded with CogSecCollab folks
CTI League does not do team like politics

Next steps:

- Add these to meme template sites and let the team have at it (also let everyone else have at it)

- Flesh out research room and writer's room

2020-06-20 Discussion: Identifying outliers with [Name Redacted]

Establish Baseline of Current Threat Landscape
Capabilities + Intent
What are you seeing?
What assumptions have you made?
Biases and sources
Persistent threats

- Known Bots
- Sources
- Tips
- Canaries (accounts and hashtags)
    - Look at your factions. Any outliers in who is pushing what narratives

Regular threat streams (Collection)

- Feeds
- Subscriptions
- Platforms
    - Establish the biases they have
    - Document those to communicate to team
- Disinformation Streams
    - UI Dashboards
    - botometer

In case you miss something, the feeds allow you to go back and find it
Cast your net wide and be able to filter from there

Persistent and repeatable Monitoring

- Develop repeatable methodology
    - Identify data sources to monitor - GoogleNews, Twitter, Facebook, other news aggregation sites
    - Create Saved or formatted searches per platform -
    - Twitter = #Disinformation, COVID, QANON, Boogaloo
    - Google = Google Hack formatted w/ time parameter
    - "Disinformation AND COVID when=1d"
    - Utilize other platform collection resources
    - Tweetdeck
    - CrowdTangle

Outlier/New Narrative
Watch for the following

- Merging and/or Reemerging Narrative's - narratives being pushed by usually opposed groups, or old ones that are reactivating
- Local or World Events - ex: protests, reopen, change in area's open phase for COVID (memorial day, 15 June, etc.)
- Anomalous or significant-sized online activity - Watch trending hashtags

Analyze Outlying Narratives

- Evaluate source biases - State media, opinion article, social media, etc
- Find additional sources with same or competing narratives
- Compare and contrast findings
    - What is the same? Is this fact or opinion?
    - What is different? Why is it different?
    - What is the intent/agenda? Political, influence, harm, confuse, distract, disrupt
- How could this be used for bad? (hypothesis)
- What would the impact be if narrative is leveraged for bad?

Automating things
[Name Redacted] Minions pulling from Twitter 5-Disinformation-Data
Gephi Graphs [Name Redacted] github

[Name Redacted] notes:
[Name Redacted] training on incident threat analysis

- TI = capabilities and intent. C without I = operational threat; I-C = aspirational threat.
- First, establish the baseline. What the current is - otherwise can't find the outliers. Cyber, car, etc
- Baseline - a lot of this is manual at the moment. E.g. a news source giving tips - lots of those have subscriptions; better if they come to you.
- Monitoring - need repeatable methodology
    - We also have tips as a threat stream
    - We can also pull form the other groups that are monitoring, e.g. UIndiana dashboards, bolometer etc
    - news aggregation vs disinformation aggregation

    - Google dorks, google hacks. https://en.wikipedia.org/wiki/Google_hacking. Lists of google dorks are interesting https://www.exploit-db.com/google-hacking-database
- Dashboards:
    - Why crowdtangle? Can get Facebook, multiple streams, api etc
    - https://tweetdeck.twitter.com/ is free, but limited
    - https://blog.hubspot.com/marketing/social-media-dashboard-tools
- Outlying narratives
    - Source biases, e.g. TASS, RT
    - How could this be used for bad?

CoronaPalooza example

- Trump planned rally in Tulsa on Juneteenth
- Example: tweetdeck
    - Grab, r-click, “copy link to this tweet"
- Google: saved searches - e.g. “covid and disinformation when:1d"
    - Check that daily
    - Twitter: a lot of people calling out stuff using hashtag #disinformation
    - (Saved stories - what are these?)
- hashtags
    - Back in 2011 saw people hijacking each others’ hashtags - look at intent
    - The Gephi code works for hashtags too - use andypatel.py code to get the files needed for this
- Action: add to hackathon code: getting the [Name Redacted] scraper plus Gephi code into a web app, so we can use that quickly (as a bot). Also add in Facebook data equivalent. NB AP gives last day - need a different scraper for further back.
- Nice to haves: automate some of this collection, e.g. find something in trending hashtags that want to pull a feed of. Maybe every 3 hours - look at, not in platform (e.g. hootsuite, twitter).
- Also tool need: want to monitor for upcoming events, known groups and domains. Twitter uses t.co urls - is there some way to unpack these? If it’s news sites, then RSS feeds, article scrapes (there are sites that do this), and most news sites have twitter feeds too.
- Using Jupyter? Inputs… download these, execute this… playbook… can pipe from Slack to Jupyter, load the Jupyter web app.
- Capabilities now; wanted inputs; wanted outputs; what do we want to do now; how manipulate data; output for action; automate collection and make available to everyone, with consistent evaluation of that data (e.g. daily with raw summary, next steps, data gaps)

Next steps

- Lead/triage conversation about Jupyter notebooks
- Diving into examples with incidents, get people starting to use these strategies

- Take current capabilities (BigBook chapter 6), handle artifacts, grow out Jupiter notebooks (6, 7), and analysis in 8; some of 4.

2020-07-04 Disinfo Data Science with [Name Redacted]

Next steps:
[Name Redacted]: tldr on CTI: Actionable…?
[Name Redacted]: Jupyter Notebooks
[Name Redacted]: We have a growing database on [Name Redacted] minions
[Name Redacted]: Elastic Search, possible hackathon thing
[Name Redacted]: Data entry bottleneck
[Name Redacted]: Need to standardize data ingestion
What works best for the data scientists?
[Name Redacted]: Do we have a good enough handle of the schemas?
Push-shift has mappings
JSON file that maps JSON keys to a data type
Admin of the elastic cluster is where the dragons are

[Name Redacted]: Mapping strategies to AMITT TTPs
Text classification, network analysis, deep fake
Enumerate and overlay on the matrix
In MITRE ATTCK you have the mitigations overlays
Would be useful to have that for AMITT

Are we going to look at the use of bots or LP elves as countermeasures? Is that within our wheelhouse?
Precedent for the use of bots for repair
Commons Bot look at boundaries where people split apart, identity them and try to bring them together
Look for data voids and drop things into them so there's something to be found
Need a place to host jupyter notebooks
Given space on the CTI League servers
Need [Name Redacted] to pull out what he's thinking about
Look at the needs of our customer base, pull [Name Redacted] in
Who in LE, hospitals, people who receive our product: what do they need?

What does resilience work look like?
How do we help medical orgs and individuals become less vulnerable to disinformation based attacks?
Rubber ducking with [Name Redacted], code-alongs
[Name Redacted] can built out jupyter notebooks and scrapers, just needs to know what the requirements and outputs are
Strategy sessions

Counters

Mask a symbol for everything that's broken

What can you meme?
What will resonate?

What would be effective enough to matter that isn't psyops?
Marketing, guidance, leadership, advisement

Wear a mask to own the libs
Relate it to election concerns and voting

Santa Claus wearing the mask
Getting people
Mixing religion and consumerism
Last supper

Joblessness
Powerlessness

Symbols of control and power for the powerlessness
How do you empower someone by wearing the mask?
Crabs in a bucket