CTI Specific BigBook Pages

Book chapters:

Chapters already checked:

- README - clean
- Chapter0 introduction - clean
- Chapter1 the team - clean
- Chapter2 looking after yourself - clean
- Chapter3 disinformation - clean
- Chapter 3a covid disinformation - clean
- Chapter 4 - clean
- Chapter 5 - clean
- Chapter 6 - clean
- Chapter 7 - clean
- Chapter 8 - clean
- Chapter 9 - clean
- Chapter 10 - clean
- Chapter 11 - clean

[The League’s April 2020 report](https://cti-league.com/2020/04/21/cti-league-inaugural-report/) describes how CTI operates, and its activities are detailed in the internal document "CTI League playbook".

---
description: 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.

For all things CTI Disinformation, start at the [Team Readme][Link Redacted]).

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.

Getting help

[team readme]([Link Redacted])

Team leads can be reached by pinging @disinfo-leads.

To get involved in Triage, [fill out the disinformation survey.](https://docs.google.com/forms/d/e/1FAIpQLSew0nj6vzBtk7tEzlhnW5upAC6MxA0hA05tb6Qw0l2WlCZVug/viewform)

Process

[incidents spreadsheet](https://docs.google.com/spreadsheets/d/1PAfipi5e1oxb6tw_gSe-OZfpb_2b3un9ZTpYtqtF1TQ/edit#gid=0)

[googledrive INCIDENTS folder](https://drive.google.com/drive/u/2/folders/1xOScRf-uU0Lem_m4HvVs3Gp8rPQoTzAY)

Alert feeds
* Alerts from disinformation team members
* The covid19activation slack group \(the Tedx team feed\)
* The covid19disinformation slack group \(the Atlantic Council team feed\)
* CTI League Phishing inputs - maybe not so much; lots false positives
* Phone honeypots
* disinfo@ctileague.org - reporting hotline
* Feeds potential from other groups - e.g. peacetechlabs have offered a feed
* Mitre covid19 feed - might be in wrong direction; needs to be symmetric
* Sniff EuVsDisfo - is slow \(narrative based\) – [Name Redacted] dataset/ data stream list
* Sniff hamilton68 dashboard for themes
* Sniff botnet feeds for themes
* Set up reporting from Facebook, twitter etc
* Ask Facebook for feeds from them
* New data coming into the DKAN

At the moment, all the team's feeds are manual; team members check other slack channels etc, or CTI League members post alerts in the 4-disinformation slack channel.

* CTI League is Covid19. Do we just cover Covid19? No - can include politics. Don't care about aliens though.
* Anybody in the disinformation team can start an incident, but the group decides what it reports on.

Outputs to:
- [\#3-medical-sector-supporting](https://covid-19-cti.slack.com/archives/C0100EWMLNR)

- [\#4-takedown-request](https://covid-19-cti.slack.com/archives/CVC7WJBH9)
- LeNew

Data inputs for DKAN

* Potential starts of incidents
  * Feeds from messenger dms \(about 30\) - on personal facebook/messenger
  * Data in covid19disinfo team slack repository channel
  * Data in covid19activation disinfo-watch channel
  * <sms honeypots>
  * <emails to disinfo email address>
  * <feeds from other groups>
* Analysis datasets
  * Covid5g twitter data \(5 directories\) - on pc
* Supporting datasets
  * Narrative lists \(CMU etc\)
  * Narrative descriptions \(EuVsDisinfo etc\)

Tools

Hive is at [https://hive.thlab.ninja/index.html\#!/cases](https://hive.thlab.ninja/index.html#!/cases)

Our main MISP instance is https://covid-19.iglocska.eu - we share this with the whole of the CTI League.

1.1 CTI Disinformation Reading Group

We have a reading group! We meet Fridays at 4pm PST/ 7pm EST. [Name Redacted] is running the group.
https://us02web.zoom.us/j/85454323080?pwd=bjNnVE1RY3pmSVhFaWd3UXR1YUVHUT09

1.1.1 Reading Schedule

* Friday May 8th 2020: ARTICLE [Facebook shut down commercial disinformation network based in Myanmar and Vietnam](https://medium.com/dfrlab/facebook-shut-down-commercial-disinformation-network-based-in-myanmar-and-vietnam-d8c07c518c04)
* Friday May 15th 2020: NO READING GROUP MEETING
* Friday May 22nd 2020: BOOK Thomas Rid's "[Active Measures](https://us.macmillan.com/books/9780374287269)" Chapter 1 & 2
* Friday May 29th 2020: ARTICLE [\(Bellingcat\) Uncovering A Pro-Chinese Government Information Operation On Twitter and Facebook: Analysis Of The \#MilesGuo Bot

Network](https://www.bellingcat.com/news/2020/05/05/uncovering-a-pro-chinese-government-information-operation-on-twitter-and-facebook-analysis-of-the-milesguo-bot-network/)
* Friday June 5th 2020: ARTICLE [Unpacking China's Viral Propaganda War](https://www.realclearinvestigations.com/articles/2020/03/30/unpacking_chinas_viral_propaganda_war_122988.html)

1.1.2 Meeting Notes

* Friday May 8th 2020
[Notes](https://docs.google.com/document/d/1HPss41cGRiYHyDbnGYh5RU7siq9JaH-mYvTjP2rheA0)

Current platform safety guidelines

1.3.1 Platform trust and safety policies

Pinterest community guidelines:

* “Hateful activities. Pinterest isn’t a place for hateful content or the people and groups that promote hateful activities. We limit the distribution of or remove such content and accounts, including:
  * Slurs or negative stereotypes, caricatures and generalisations
  * Support for hate groups and people promoting hateful activities, prejudice and conspiracy theories
  * Condoning or trivialising violence because of a victim’s membership in a vulnerable or protected group
  * Support for white supremacy, limiting women’s rights and other discriminatory ideas
  * Hate-based conspiracy theories and misinformation, such as Holocaust denial
  * Denial of an individual’s gender identity or sexual orientation, and support for conversion therapy and related programmes
  * Attacks on individuals including public figures based on their membership in a vulnerable or protected group
  * Mocking or attacking the beliefs, sacred symbols, movements or institutions of the protected or vulnerable groups identified below
* Protected and vulnerable groups include: people grouped together based on their actual or perceived race, colour, caste, ethnicity, immigration status, national origin, religion or faith, sex or gender identity, sexual orientation, disability, or medical condition. It also includes people who are grouped together based on lower socio-economic status, age, weight or size, pregnancy or ex-military status.
* Misinformation. Pinterest isn’t a place for misinformation, disinformation or mal-information. We remove or limit distribution of false or misleading content that may harm Pinners’ or the public’s well-being, safety or trust, including:

  * Medically unsupported health claims that risk public health and safety, including the promotion of false cures, anti-vaccination advice, or misinformation about public health or safety emergencies
  * False or misleading content about individuals or protected groups that promotes fear, hate or prejudice
  * False or misleading content that encourages turning individuals, groups of people, places or organisations into targets of harassment or physical violence
  * Conspiracy theories
  * False or misleading content that impedes an election’s integrity or an individual's or group's civic participation, including registering to vote, voting and being counted in a census
  * Content that originates from disinformation campaigns
  * Factual information that’s published or deliberately modified to erode trust or inflict harm, such as changing or omitting context, date or time
  * Fabricated or meaningfully manipulated visual or audio content that erodes trust or causes harm
* Harassment and criticism. Pinterest isn’t a place to insult, hurt or antagonise individuals or groups of people. There are good reasons to express criticism, but we may limit the distribution of or remove insulting content to keep Pinterest a positive, inspiring place; this includes:
  * Manipulated images intended to degrade or shame
  * Shaming people for their bodies or assumed sexual or romantic history
  * Sexual remarks about people’s bodies and solicitations or offers of sexual acts
  * Criticism involving name-calling, profanity and other insulting language or imagery
  * Mocking someone for experiencing sadness, grief, loss or outrage
* We’ve also put together [some resources \(opens in a new window\)](https://help.pinterest.com/article/report-harassment-and-cyberbullying) for you to protect yourself.”

HIVE workflows

(Adding an object workflow to a Hive Incident - don’t use this yet)

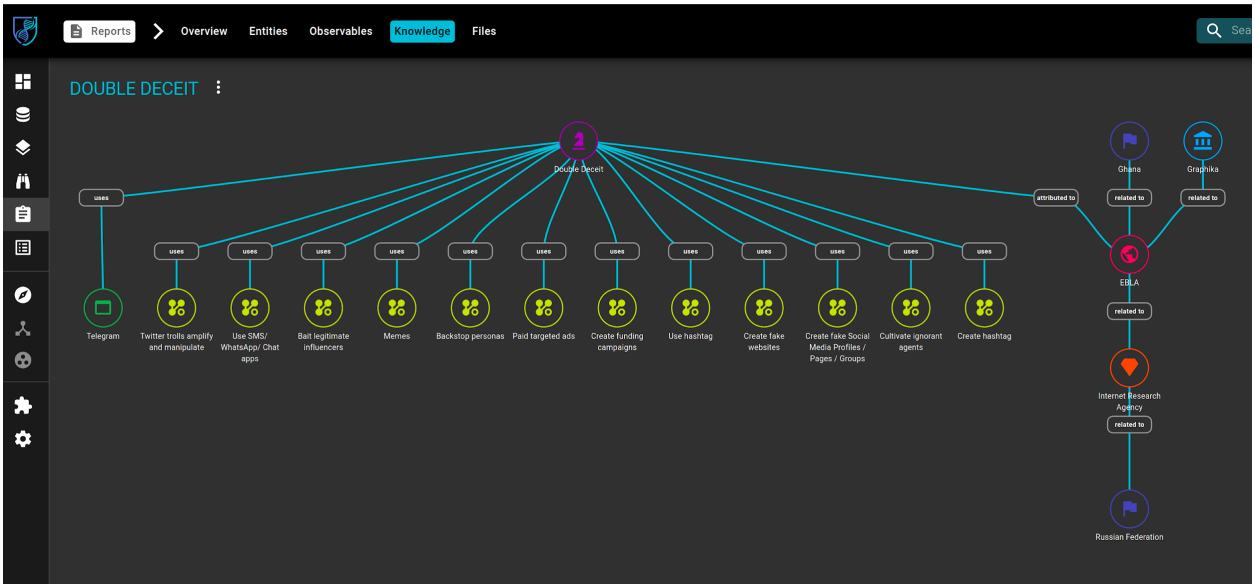
Adding a new workflow to a case:

1. Assume the current Case ID is (A).
2. Create a new Case (B) selecting the workflow Case Template you wish to add to Case (A).
3. Open Case (A) and click "merge".
4. Select "By Number" and add Case ID (B).

OpenCTI - OPEN THREAT INTELLIGENCE PLATFORM

The other open threat intelligence platform we worked on is OpenCTI. It's a report-based knowledge graph. It's an ANSSI and CERT-EU project and now a LUATIX product. It's new, but advancing rapidly. With OpenCTI, we can take reports, blog posts, etc, add event information to them and track that data and its origin. https://www.opencti.io

- STIX 2.0
- Knowledge graph
- Report based
- MISP integration



AMITT in OpenCTI looks like this. This is Double Deceit, showing relations to IRA, Grafika (who broke the story) etc. Everything in here is Stix data. This report only shows the relationship of the actor to capabilities. We could also add in URLs and other data. OpenCTI integrates with MISP. We can stream data into OpenCTI from MISP.

AM!TT + Atomic Threat Coverage

We looked at atomic threat coverage briefly on the playbooks page. We've done AM!TT techniques with this. We need to go deeper for next steps, and make significant modifications to handle effects, and the critical parts of a disinformation campaign, and assemble them into more game-theoretic playbooks where we can suggest actions based on the target. We can also send outputs to Confluence so they're easy to play with.

- Done: AM!TT Techniques
- Next: AM!TT Counters
- Playbooks are assembled from sets of counters
- Markdown, Confluence, API, …
- https://github.com/atc-project/atomic-threat-coverage

Old process

- Add a row to the incidents spreadsheet
- Add an incident case to HIVE
- Create an incident event in CTI League's MISP
- Add notes to the Hive case, and observables to the Hive case
- We coordinate with responders individually at the moment, but we're also working on tech alerts:
    - MISP: we add to the MISP so others can read and act on the incidents in it
    - IRs: we're working on this