C0 About This Book

TL;DR The Fast Route

Every chapter in this book contains detailed instructions on how we do the things we do, why we do them, and ways to look for more information about that. When the sticky stuff hits the rotating thing, there isn't time to read through all that, so each chapter will also start with a "TL;DR" section, containing the basics needed to get set up and running.

Introduction

Where This Book Came From

These are chapters from the Big Book of Disinformation Response, as used in the CTI League's Disinformation threat intelligence team for its Covid19 disinformation response. We have modified the chapters from their original form by removing CTI-specific notes and adding in other notes that might help other teams who are engaging in similar work.

We've written a lot of text during our Covid19 disinformation response, and we're realizing that there's a lot of stuff we haven't explained. So we're writing it down. And making stuff clearer and cleaner to use as we test and explain it. This document is those explanations. When we finish, it should contain notes on:

* What disinformation is, for threat intelligence (TI) people
* How to run distributed disinformation TI teams
* Suggested data standards for that
* Suggested tools for that
* Resources that could help with disinformation threat sharing and response

Distributed Disinformation Defense

This book is about the things we need to build, test and document to create truly distributed disinformation defenses. That includes the tools, techniques and resources for threat sharing and response as part of threat-informed defence, how to use those resources in communities, and how other communities (e.g. MLsec and other parts of information security) might help with this.

The first big idea is that disinformation campaigns are a large-scale distributed, asymmetric threat, and we need a large-scale, collective, distributed, asymmetric response to them. This includes:

- joining together all the individual responses,
- connecting community alerts to responders,
- making it easy,
- making it possible to build groups for free,
- connecting new groups to the existing information security response system

The next big idea is that near-real-time distributed disinformation response is easier if you can share information and data quickly, and the MISP threat intelligence platform, lightly extended, lets you do that.

This is systems work, and most systems contain people, processes, algorithms, data, and insights. Of all these, the most important part is the people. Steven from the CS-ISAO pointed out that what we've accidentally built is a Security Operations Center (SOC) for disinformation - over time, we'll adapt the nomenclature in this book to more closely match that.

Contributors

We are community. We have been part of many communities on this journey, helped form communities and organizations, and have many people to acknowledge and thank for the work in these guides. Many people have been part of the BigBook efforts, and will be acknowledged here if they don't want to remain in the shadows.

CogSecCollab

The Cognitive Security Collaborative is a volunteer community of academics, researchers, technologists, students, journalists, and engineers, all working on the intersection of infosec and misinformation.

Its mission is to bring together information security researchers, data scientists, and other subject-matter experts, in order to create and improve resources for the protection and defense of the cognitive domain. Specifically in 2020, CogSecCollab is concentrating on building the tools and techniques that groups need to counter disinformation campaigns.

CogSecCollab officially formed in January 2020 from the Credibility Coalition's Misinfosec Working Group and the Misinfosec slack discussion channel, which built on work started in SOFWERX and the Hackers community.

- Before 2019, we were raising awareness that there was an intersection between infosec and disinformation / information operations.
- In 2019, we built the AM!TT Framework, an infosec-based description framework for influence operations, and started models of influence operation countermeasures.
- In 2020, we're building tools, processes and community to support community-based responses to counter disinformation campaigns.

CogSecCollab also convenes the MISP disinformation sharing community, which is focused on influence operations. The community is listed in the MISP communities page on https://www.misp-project.org/.

The CTI League

The CTI League is a community of cyber threat intelligence experts, incident responders and industry experts working to neutralize all cyber threats looking to exploit the Covid19 pandemic. Formed in April 2020, the CTI League identifies, analyzes and neutralizes all threats. At this most sensitive time, the CTI League is prioritizing front-line medical resources and critical infrastructure.

The CTI disinformation team is tasked with finding coordinated inauthentic activities (“disinformation campaigns”), and the objects and people attached to them, and using known ways (some of which we have to invent ourselves) to expose, disrupt or stop their operations.

The CTI League’s disinformation team is embedded within the CTI League, and tracks disinformation using similar tools and techniques to the rest of information security. However, there are some things that we do a little differently, which is how we ended up writing a book.

Covid19Activation and Covid19Disinformation

We work alongside other teams. Covid19Activation was started by TEDx fellows to track Covid19 information and disinformation, and has worked tirelessly on this. Covid19Disinformation was started jointly by CogSecCollab and Andy Carvin from the Atlantic Council's DFRlab team as a community disinformation tracking team (Andy is one of the original crisismappers). Covid19Disinformation fell fallow as the CTI League team built up, but provided many of the baseline processes for the CTI League's Disinformation team.

Fellow Travelers

Tool adaptations and trials, specifically the MISP and AMITT adaptations, were the work not just of the CogSecCollab and CTI League teams. We were joined in this work by teams from NATO, DHS, MITRE, RRM Canada, EEAS, MISP, CIRCL and Belgium, specifically in the MISP disinfo sharing community. These are our wider community.

Crisismappers, Old and New

Ten years ago, some of the CogSecCollab leads worked in and with the community data teams that responded to the Haiti 2010 earthquake, ran globally-distributed but locally-focused teams, and created processes and tools for what became the crisismapping movement. Crisismappers changed the ways that disaster response and development agencies managed both data and the way that they worked with people on the ground. We see many parallels between that work, and the work of creating and sustaining community-supported disinformation response.

Helpful info

Glossary

We all come from different disciplines: words like "campaign" have different meanings to a military, adtech or tech person (and if you're all three, you get to fight about definitions with yourself). There are also committees dedicated to defining what words like "disinformation" and "misinformation" mean, and the differences between them.

We ain't got time for that here. This glossary is our latest best effort at working definitions for some of the words we use a lot between us, and what we (mostly) think we mean when we say them.

- Cognitive Security: The top layer of security, alongside Physical-security and Cyber-security. The art and practice of protecting against hacks that exploit cognitive weaknesses, especially cognitive hacks that are online and/or in large numbers of people. One of the reasons the MisinfoSec crowd started talking about Cognitive Security (including rebranding as the CogSecCollab) in 2020 is a belief that, in order to deal with things like disinformation, we need to focus on the thing we're protecting. That means working on reducing disinformation, but also on boosting good information when we see it.
- Misinformation: false content, where that content could be text, images, video, voice, etc. Misinformation does not have to be deliberately generated (e.g. my mother might forget my favorite color)
- Disinformation: deliberate attempt to deceive online. There is usually intent to deceive with disinformation, and the content itself might be true, but in a deceptive context (e.g. fake users, fake groups, mislabeled images, doctored videos, etc). Claire Wardle's work on the differences between misinformation and disinformation is still some of the best.
- Campaign: Campaigns are long-term efforts to change or confuse populations.
- Incident: Incidents are coordinated inauthentic activity that are carried out as part of a campaign. The “coordinated” implies either an instigator of some form with motives (geopolitics, money, ideology, attention, etc.) or some form of collective deliberate behavior around it, like flooding a hashtag. That activity usually lasts for a short period of time because the narratives, artifacts, and other aspects can be picked up and continued by people who aren’t driving an incident - and this is often part of an incident or campaign’s goals.
- Narrative: Narratives are the “stories” that are being used to change minds, confuse people, etc. Narratives are components of incidents. Each incident might have multiple narratives involved or just one, but there’s usually an identifiable narrative somewhere in there. You can use narratives to see if there are related incidents that have already been tracked or dealt with. Narratives, like incidents, have lifetimes. Some narratives appear as a result of a world or local event (or anticipated event), and are only useful while that event is in peoples’ minds.
- Artifact: Artifacts are the objects that you can 'see' connected to a disinformation incident or campaign. Artifacts are the text, images, videos, user accounts, groups, hashtags, etc. that you use to get a picture of an incident or campaign.

- Astroturfing: creating a fake grassroots movement with an obfuscated sponsor or orchestrating group

Other places to look for information

There’s a lot to learn about disinformation, misinformation, and how they fit into cognitive security / infosec in general. There are separate books being written about that. This BigBook is the practical one.

We’ve added lists at the end of this document, under References, that will point you to books and papers about disinformation, other teams doing this, sources of data, tools, etc. In addition, CogSecCollab is collecting information in its documentation repo, which was used to seed this BigBook.