0. The Big Book of Disinformation Defence

Introduction

This is a guide for teams building risk-based defences against disinformation. It contains notes on:

- Disinformation as an information security risk
- How to run distributed disinformation defence teams
- How Infosec, MLsec, and other disciplines can help
- Tools, techniques and resources

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

This is systems work, and most systems contain people, processes, algorithms, data, and insights. Of all these, the most important part is the people. 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. We describe this work as building Security Operations Centers (SOCs) for disinformation.

Every chapter in this guide is self-contained, and starts with a "TL;DR" summary.

Contributors

This book started as chapters from the CTI League's “Big Book of Disinformation Response”. We’ve removed CTI-specific notes and migrated AMITT-specific notes to the AMITT Design Guide.

Communities that contributed to this work include MisinfoSec, CogSecCollab, CTI League, Crisismappers, and other disinformation response communities.

CogSecurityCollab 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. It’s a volunteer community of academics, researchers, technologists, students, journalists, information security researchers, data scientists, and engineers, working on the intersection of infosec and misinformation. Its mission is to create and improve resources for cognitive security communities.

CogSecCollab mentors and works alongside other disinformation defence communities. The CTI League is a community of cyber threat intelligence experts, incident responders and industry experts working to identify, analyze and neutralize cyber threats. The CTI League’s disinformation team tracks disinformation using similar tools and techniques to the rest of information security. Covid19Activation was started by TEDx fellows to track Covid19 information and disinformation. Covid19Disinformation was started as a community disinformation tracking team, and was the trial community for this work. Teams from NATO, DHS, MITRE, RRM Canada, EEAS, MISP, CIRCL and Belgium, convened by the CogSecCollab-led MISP disinfo sharing community worked on tool adaptations and trials.

Ten years ago, some of the CogSecCollab leads responded to the 2010 Haiti earthquake, running globally-distributed but locally-focused data teams, and creating processes and tools for crisis mapping. Crisismappers changed the ways that disaster response and development agencies managed data and worked with people on the ground. There are parallels between that work, and the work of creating and sustaining disinformation response communities.

Glossary

Words like "campaign" have different meanings to military, adtech, and tech people. These are our working definitions for common words in disinformation:

- **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).
- **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

The References chapter includes links to books and papers about disinformation, disinformation response teams, data sources and tools.

If you say you're working on disinformation, people around you will often quietly ask how they can help, and where they can get more information about it. Good introductions that you can show your mum and other people who ask include:

- The War on Pineapple: Understanding Foreign Interference in 5 Steps
- Bad News Game
- The Dark(er) Side of Media: Crash Course Media Literacy #10
- Web Literacy for Student Fact-Checkers – Simple Book Production

Although that doesn't cover everything we do, those references between them give a good introduction to what we're dealing with, and some of the things that everyone can do to help mitigate them.