Left-of-Boom MisinfoSec: Were Four Big Steps Behind

Sara-Jayne Terp
Bodacea Light Industries / Portland, OR
sarajterp@gmail.com

John F Gray
MentionMapp / Vancouver, Canada
john@mentionmapp.com

Abstract

The structure and propagation patterns of misinformation incidents have many similarities to those seen in information security. The Credibility Coalitions MisinfoSec Working Group has analysed the similarities and adapted information security standards (e.g. ATTCK) to create the AMITT (Adversarial Misinformation and Influence Tactics and Techniques) framework. AMITT includes the left-of-boom misinformation activities that are often missed by other analyses, where ”left of boom” covers activity before an incident is widely visible to the public. This note covers some of the steps typically seen in left-of-boom misinformation.

1 Introduction

Misinformation incidents are large-scale neuron hacks powered by hijacked and distorted narratives, using the deliberate promotion of false, misleading or mis-attributed information. The structure and propagation patterns of misinformation incidents have many similarities to those seen in information security. The Credibility Coalitions MisinfoSec Working Group has analysed the similarities and adapted information security standards (e.g. ATTCK) to create the AMITT (Adversarial Misinformation and Influence Tactics and Techniques) framework.

AMITT gives misinformation analysts and response organisations ways to identify, describe, communicate, disrupt and counter the techniques, tactics and procedures (TTPs) used in misinformation incidents. In particular, AMITT covers the left-of-boom misinformation activities that are often missed by other analyses, where ”left of boom” is a term from explosives response, meaning the time before an attack a period when you still have time to prepare and avert a crisis. This note covers some of the steps typically seen in left-of-boom misinformation.

2 Why information security people care about misinformation

Misinformation incidents are about hacking neurons and the narratives powering them. Historically some of the best hackers have been better at manipulating people than they are at writing code. Social engineering is a key component of most misinformation incidents.

This type of hacking is not about exploiting information/data like password credentials, credit card numbers, or stealing IP; its about influencing opinion and manipulation of public perception. Human vulnerabilities are being exposed by hacking minds, emotions and narratives at scale.

Were evolving the information security conversation by recognizing the importance of having a cognitive security framework. Misinformation needs to be confronted at the same scale of response as traditional information security.

There are lessons to learn from the past, and these are key to informing our misinfosec models/ framework today, but its also time to get past 2016, bots and collusion. Our adversaries are multiple state actors, their proxies, for-hire-actors (putting information operations in reach of smaller nation-states), and domestic actors operating to deflect/misdirect attribution (see the Alabama Senate campaign experiment).

3 How stage-based infosec models can help with misinformation

Stage-based models describe the points where a misinformation incident can be disrupted, at the individual technique level, the stage level and the procedure (route through a set of stages) level.

Several models from different disciplines could be used, but none of them are right enough to cover the variety of current and evolving misinformation incidents. Marketing, psyops and the cyber killchain models have all been suggested, but each cover of different point of view on an incident; models tailored to misinformation (Department of Justices Malign Foreign Influence Campaign Cycle, Ben Deckers misinformation propagation models, and Clint Watts work on Advanced Persistent Manipulators, Renee DiRestas model) are each either tailored to a specific type of incident (e.g. Russia on USA), or are at levels (strategy, technique) that are less useful for development of counters. Our model was cross-checked against each of these.

Our earlier work was on adapting the ATTCK framework, which covers the right of boom part of the Cyber Killchain model. This works because right-of-boom is where the visible artefacts are (such as the work of social bots, trolls, phoney Facebook groups, and imposter news sites) but we extended it to left-of-boom to cover the time periods before damage has been done and is being done.

4 Why we need left-of-boom strategies and techniques

There are four big steps left-of-boom in the Cyber Killchain that need to become a focus of attention:

- Reconnaissance - searching the social space, and/or using well established OSINT tools and techniques - advantage attacker; they have access to data and when combined with anonymity deception it makes target gathering and profiling too easy.

- Weaponization - the proliferation of free/inexpensive tools also makes content creation easier than ever. The deep history of psyops still applies today, by wrapping rumor innuendo in a grain of truth and mixing in a dose of outrage, doubt, conspiracy and even humour, clickbait is easily weaponized. With AI/deep cheap-fake videos and audio, and image manipilation deception is now delivered at scale.

- Delivery - multi-platform digital distribution one to one/one to few/one to many/many to many WhatsApp (see Indian and Brazilian elections), Tinder (Jeremy Corbyn UK election campaign use of bots) to Facebook, YouTube, Twitter, BlackHat SEO (RT are masters at getting news at/near the top of news search rankings.)

- Exploitation - bots operate to amplify the message and/or juice the metrics manipulating the algorithms to make content look popular/viral. While trolls and the useful/willing idiots are covering the landscape with bait (baiting journalists, politicians, business leaders and just Jane and Joe Q public)... truth doesnt matter, facts are whatever you want them to be. At the volume of supply (headlines) speed of consumption, and shallowness of engagement sources are irrelevant, and verification is unwarranted because its feeding deeply entrenched human biases.

Our adversaries have a four-step advantage (planning, developing, testing, recruiting) over misinformation responders and response organisations. Their objectives are cognitive and the vectors of delivery are social potential successful responses to attacks must be crafted in the context of these varied actors, targets, messages, goals and networks. Focusing on each left-of-boom step, we will be better able to detect, disrupt, deny and potentially disable emerging misinformation operations, by making online spaces (such as 4Chan, 8chan and GAB) less easy and more costly for our adversaries to operate in.