Misinformation: We're Four Steps Behind Its Creators

John F Gray[1] and Sara-Jayne Terp[2]

[1] Mentionmapp Analytics, Canada

john@mentionmapp.com

[2] Bodacea Light Industries, USA

Abstract. Our earlier work described misinformation incidents as a series of tactic stages. This paper discusses the work needed to determine those stages, including whether we need more than one model for misinformation. We describe our methodology and work on which stages are appropriate for misinformation tracking, and our extension of earlier work to "left of boom" (before a misinformation incident is visible to its targets) misinformation stages.

Keywords: Misinformation, Information Security, Framework

1. Introduction

We use "misinformation incident" to refer to 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 Coalition's Misinfosec Working Group ("MisinfosecWG") is analyzing those similarities, including adapting information security framework standards to give better ways to describe, identify, disrupt and counter the techniques, tactics and procedures (TTPs) used in misinformation incidents.

In [1], we built a strawman framework (figure 1), based on the ATT&CK framework (used by the infosec community to share information about incidents), and described how we were populating it by analyzing known misinformation incidents.

Initial Access	Create Artefacts	Insert Theme	Amplify Message	Command And Control
Account takeover	Steal existing artefacts	Create fake emergency	Repeat messaging with bots	Create fake real-life events
Create fake group	Deepfake		Create fake argument	
Parody account			Buy friends	
Deep cover				

Figure 1: ATT&CK-based strawman

Concentrating on the ATT&CK framework made sense when we started doing this work—it was detailed, well-supported, had useful concepts like being able to group related techniques together under each stage, and covered the artifacts (messages, botnets etc) seen by a system defender. But even with data, we were still discussing what the stages of the misinformation model should be (and whether there was one model or a family of models), and ATT&CK doesn't cover the 'left of boom' work that a misinformation incident creator does before releasing messages, images etc., so we also started work mapping other potential frameworks onto misinformation incidents. We cover that work here.

2. Creating a master list of misinformation stages

We looked exclusively at stage-based models (models that divide an incident into a sequence of stages, e.g. 'recon'). We found many models to choose from, but none of them were 'right enough' for general misinformation incidents. Figure 2 maps the stages in the models of most interest to us.

Marketing 1	Marketing 2	Cyber Killchain	Psyops phases	Justice Department	Bruce Schneier
		RECON	1. Planning	Research (target environment)	
Market research	Market research		2. Target audience analysis		Find the cracks
Campaign design	Campaign design		3. Series development		Seed distortion
		WEAPONIZE		Position (infrastructure + networks)	Wrap narratives in kernels of truth
Content production	Content production		4. Product development and design, 5. Approval	Produce (content)	
Awareness	Exposure	DELIVER	6. Production, distribution, dissemination	Publish (content dissemination)	Build audiences
	Discovery				
Interest/Consideration	Consideration				
Conversion/Purchase	Customer relationship	EXPLOIT			
		CONTROL			
		EXECUTE			
Loyalty/Retention	Retention	MAINTAIN			
Advocacy				Amplify (media saturation)	Cultivate "useful idiots"
					Deny involvement
			7. Evaluation	Calibrate (assessment +retooling)	Play the long game

Figure 2: Comparing stage-based models

Central to this is the Cyber Killchain model (figure 3), which is the parent model of the ATT&CK framework. ATT&CK adds more detail to the last 3 stages of the Cyber Killchain: these "right of boom" stages happen after bad actors gain control of a network and start damaging it; the other cyber kill chain stages are "left-of-boom".

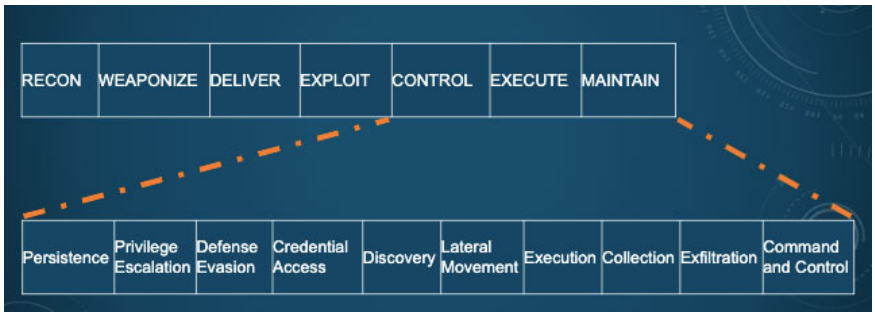

Figure 3: *Cyber Killchain stages (top), ATT&CK framework stages (bottom)*

Digital marketing funnels (figure 4) describe the 'customer journey' of the end consumer of a marketing campaign, moving from seeing an online image, video etc to taking an interest, then building a relationship with a brand/idea/ideology and advocating it to others. The model point of view is a key consideration: the people targeted by a misinformation incident, the people delivering it, or the people defending against it? We suggest the creator/attacker point of view for misinformation models, because each attacker stage, including the ones less-visible to a defender, can potentially be disrupted. Digital marketing could be useful in describing radicalization and including an advocacy stage: this mirrors other models' use of amplification and 'useful idiot' stages, adding the idea that an 'infected' node in the system isn't just repeating a message but might be or become a command node too. Marketing funnels are "right of boom", so we've added marketing planning and production stages (market research, campaign design, content production) to see if they could be useful to describing and disrupting an attacker's game plan.

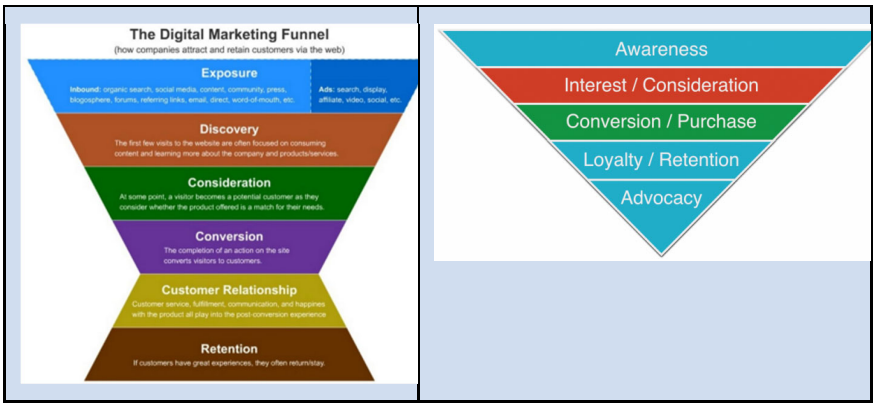

Figure 4: Digital marketing funnels [4] [5]

The psyops model (figure 5) point of view is as an incident creator (or campaign creator - building a group of related incidents), controlling every stage, from planning through to evaluation, with human-hierarchy-aware things like getting sign-offs and permissions, but with little visibility of end-consumer-specific considerations (these are bundled under “production, distribution, dissemination.”) The evaluation stage is useful: one of the strengths of working at scale online is the ability to test hypotheses and adapt quickly at all stages, and when running a campaign, after-action reviews can be invaluable in learning and adjusting higher-level tactics (e.g. the list of stages, the target platforms, the most effective narrative styles and assets) between incidents.

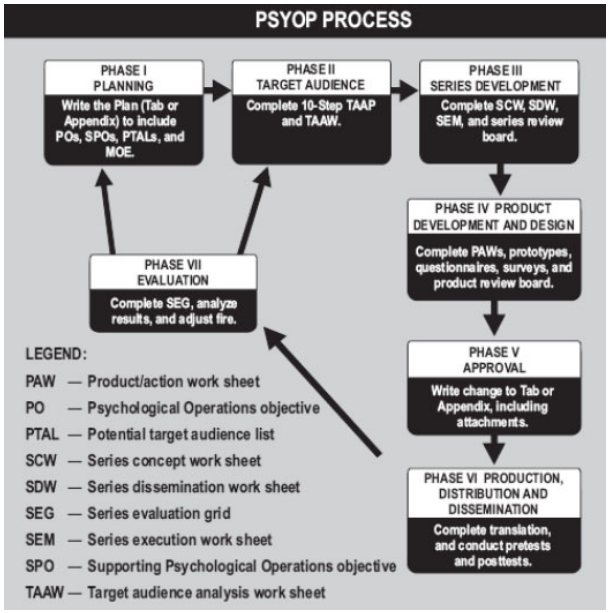

Figure 5 Psyops model [6]

The DoJ misinformation model (figure 6) clearly presents what each stage looks like from both the attacker and defender points of view (the end consumer isn't of much interest here). It's a solid description of early IRA incidents, yet is arguably too passive for recent incident types: it's a great example of how we can create models that work well for some but not all of the misinformation incidents that we've seen or expect to see.

Figure 2: The Malign Foreign Influence Campaign Cycle

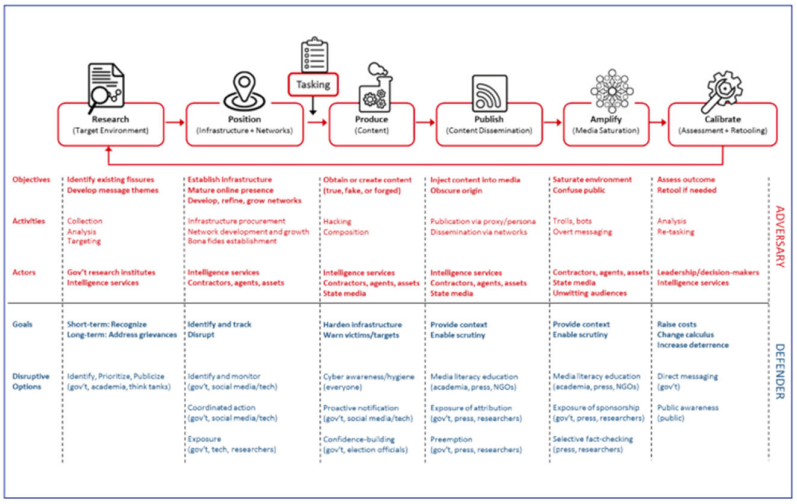

Figure 6: DoJ misinformation model [7]

There are other models. Ben Decker's models look at misinformation campaigns as a series of handoffs between groups on different platforms, from the originators of content, to command and control signals, posting content to social media platforms, amplifying narratives with social media messages, to professional media. This has too many groups to fit neatly onto a marketing model, and appears to be on a different axis to psyops and DoJ models, but still seems important.

3. Looking "left of boom"

Left of boom is the most valuable place to disrupt any incident. Using cyber killchain stages, we have:

- **Reconnaissance -** The attacker has the advantage here, with easy access to social space and OSINT data, combined with anonymity and deception making mass target information gathering and profiling cheap, easy and low risk.
- **Weaponization -** There's a proliferation of free/inexpensive tools to create content (rumors, lies, outrages, conspiracies) and generate memes/images/audio and video (although it isn't vital to use originals). Historical psyops principles still apply today, e.g. wrapping rumor &

innuendo in a grain of truth, using outrage, doubt, conspiracy and humor, and exploiting existing themes/, seams and social polarities.

- **Delivery -** Can distribute to multiple platforms distribution as 1:1, 1:few or 1:many; platforms range from WhatsApp, Twitter, Tinder [8] to Facebook, YouTube and BlackHat with search engine optimization (RT.com are masters at getting news at/near the top of news search rankings).
- **Exploitation -** bots amplify content to make it look popular/viral in metrics; trolls and "useful idiots" lay bait for journalists, politicians, business leaders and the public. At the volume of supply, speed of consumption, and shallowness of engagement for much of the audience, sources are irrelevant, and verification is unwarranted particularly when it's feeding deeply entrenched human biases.

Responses left-of-boom include disrupt, co-opt, deny and displace. Applying these to the recon stage, we have potential actions including:

- **Disrupt** - build honeypots to help find the actors and trace them home; get adversary to reveal themselves
- **Co-opt** - create and deploy personas with counter narratives and information
- **Deny** - remove the narrative power in the space. Note that this doesn't equal censorship, but a removal of artificial positions of strength
- **Displace** - create models of community, identity and trust that move bot- and troll-like behaviors away. Note that this doesn't mean purging anonymity.

4. Conclusions and Future Work

We will continue to refine our misinformation stage models, both bottom-up from our analysis of known incidents, and top-down by combining other models of interest, before testing our next strawman (or strawmen if we have multiple models) on new data.

We'll continue working towards the joined-up responses that we hope will use these standards, and we note with encouragement the increase in discussion for collaboration, "fusion-centers" (government, tech companies, academics, citizens, experts etc) since we started this work.

5. References

1. Walker, C, .: Misinfosec: applying information security paradigms to misinformation campaigns. W3 Workshop on Misinformation (2019).
2. Schneier, B.:, (2019).
3. Sterling, B.: The Hacker Crackdown (2019).
4. https://moz.com/blog/building-your-marketing-funnel-with-google-analytics
5. https://www.singlegrain.com/marketing-funnels/how-to-build-a-social-media-marketing-conversion-funnel/
6. https://2009-2017.state.gov/documents/organization/148419.pdf
7. https://www.justice.gov/ag/page/file/1076696/download
8. https://www.wired.co.uk/article/tinder-political-bots-jeremy-corbyn-labour