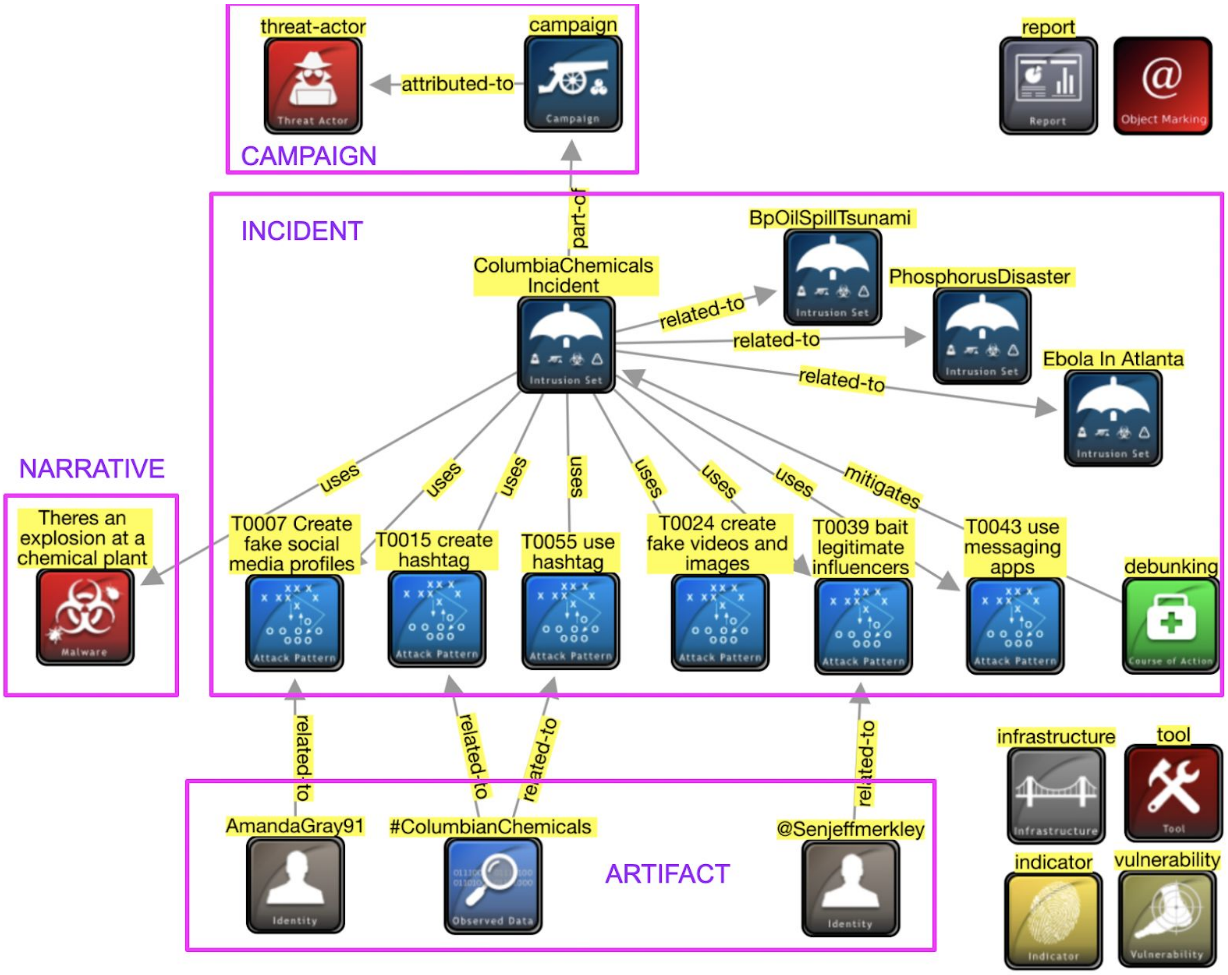
AMITT Use Cases

Introduction

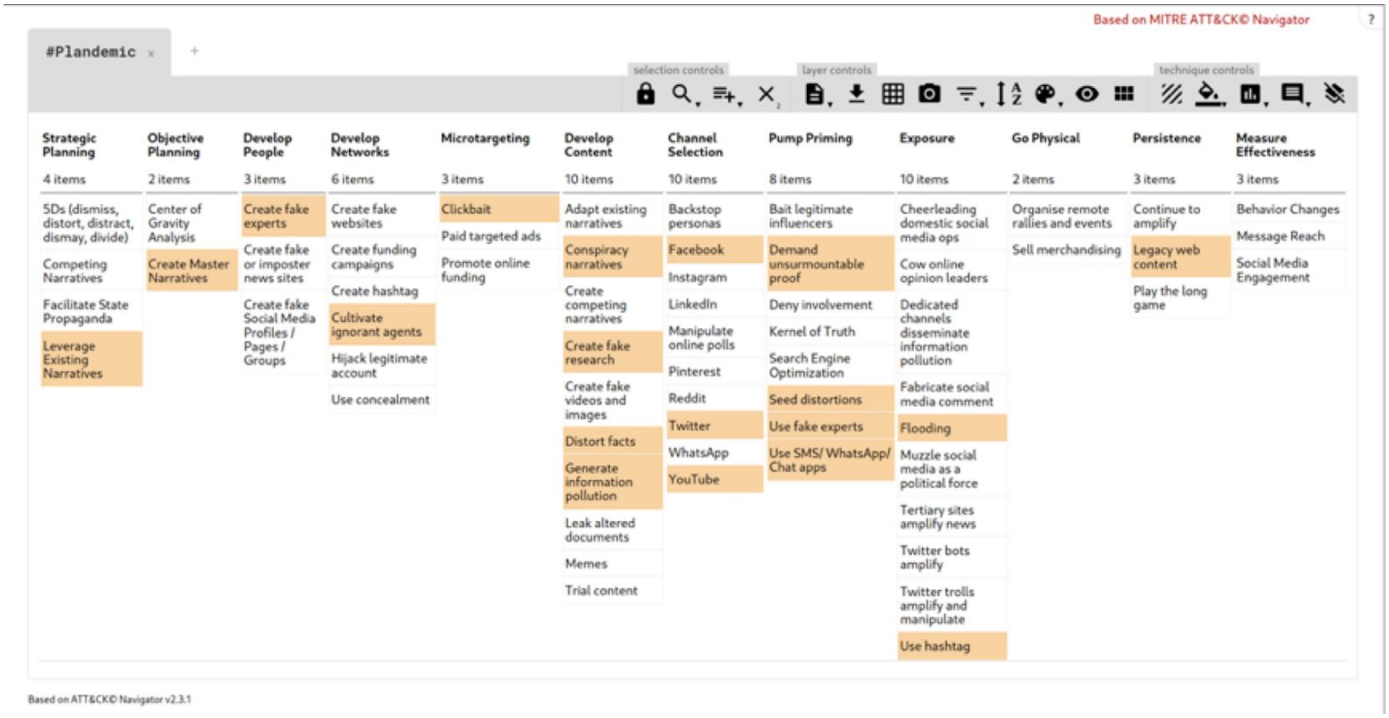
This report shows examples of the AMITT disinformation standards set - AMITT STIX, AMITT Framework TTPs, and AMITT Counter TTPs, in action.   There's also a companion document - the AMITT Incident List - that describes the incident data used to create the original AMITT models.

I00006 Columbian Chemicals



STIX for Columbian Chemicals

Plandemic



Strategic Planning	Objective Planning	Develop People	Develop Networks	Microtargeting	Develop Content	Channel Selection	Pump Priming	Exposure	Go Physical	Persistence	Measure Effectiveness
4 items	2 items	3 items	6 items	3 items	10 items	10 items	8 items	10 items	2 items	3 items	3 items
5Ds (dismiss, distort, distract, dismay, divide)	Center of Gravity Analysis	Create fake experts	Create fake websites	Clickbait	Adapt existing narratives	Backstop personas	Bait legitimate influencers	Cheerleading domestic social media ops	Organise remote rallies and events	Continue to amplify	Behavior Changes
Competing Narratives	Create Master Narratives	Create fake or imposter news sites	Create funding campaigns	Paid targeted ads	Conspiracy narratives	Facebook	Demand unsurmountable proof	Cow online opinion leaders	Sell merchandising	Legacy web content	Message Reach
Facilitate State Propaganda		Create fake Social Media Profiles / Pages / Groups	Create hashtag	Promote online funding	Create competing narratives	Instagram	Deny involvement	Dedicated channels disseminate information pollution		Play the long game	Social Media Engagement
Leverage Existing Narratives			Cultivate ignorant agents		Create fake research	LinkedIn	Kernel of Truth	Fabricate social media comment			
			Hijack legitimate account		Create fake videos and images	Manipulate online polls	Search Engine Optimization	Flooding			
			Use concealment		Distort facts	Pinterest	Seed distortions	Muzzle social media as a political force			
					Generate information pollution	Reddit	Use fake experts	Tertiary sites amplify news			
					Leak altered documents	Twitter	Use SMS/ WhatsApp/ Chat apps	Twitter bots amplify			
					Memes	WhatsApp		Twitter trolls amplify and manipulate			
					Trial content	YouTube		Use hashtag			

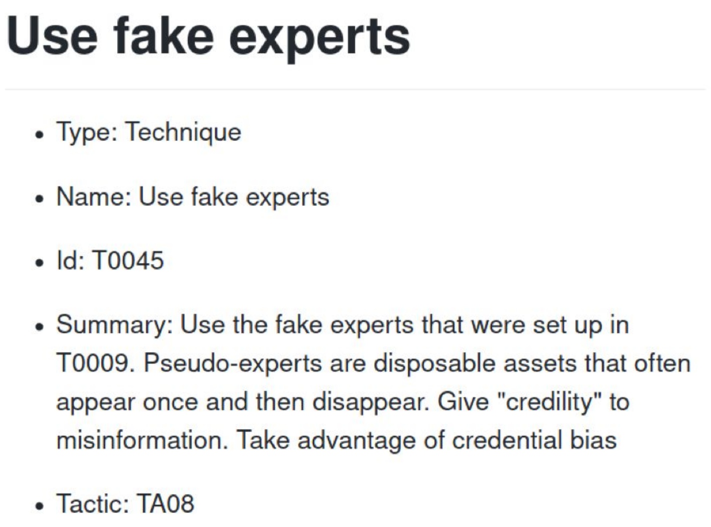
Based on ATT&CK© Navigator v2.3.1

AMITT TTPs for Plandemic incident

The AMITT framework was built to be practical. We need to be able to translate our findings into an actionable story.

Plandemic is a debunked conspiracy theory video which makes some false claims about the nature of COVID-19. Despite high production quality the self reported cost to produce the film was less than $2000. Zach Vorhies, an individual associated with QAnon, claims to be the social media marketer behind the viral success of the video. NYT reported his GoFundMe campaign titled “Help me amplify Pharma Whistleblower Judy Mikovits.”

We can map out this small, but successful, operation in the AMITT framework to help us understand what capabilities the actor has and potentially how they’re resourced. As with ATT&CK, we can start building an understanding of actors' capabilities over time.



Use fake experts

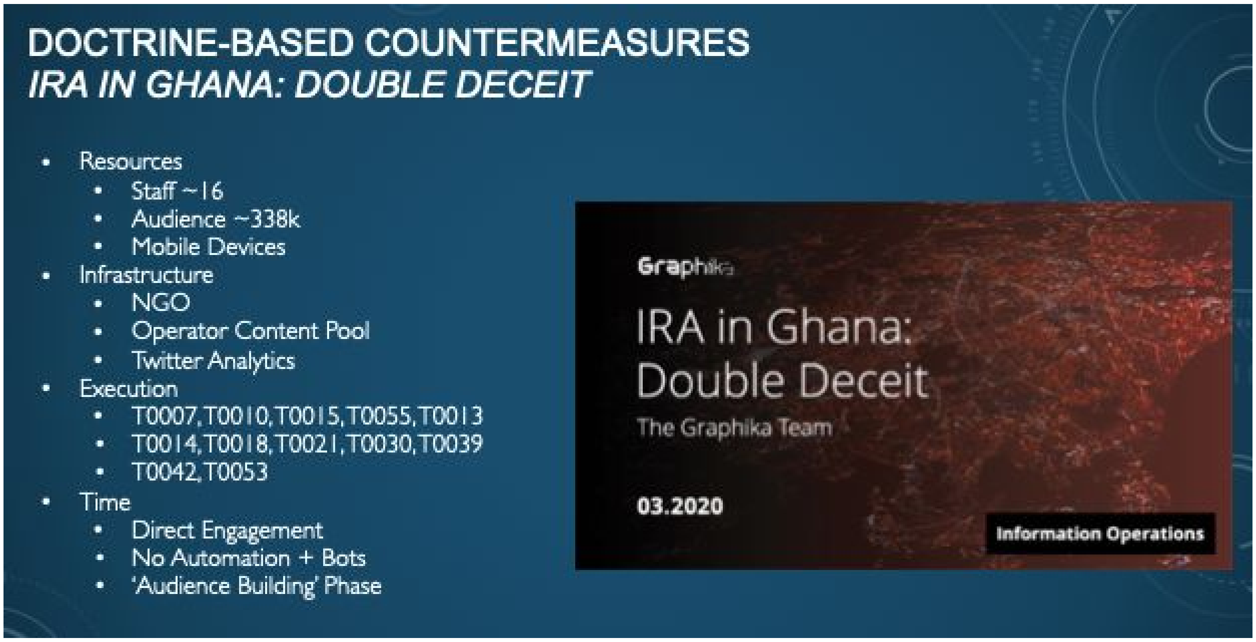
- Type: Technique
- Name: Use fake experts
- Id: T0045
- Summary: Use the fake experts that were set up in T0009. Pseudo-experts are disposable assets that often appear once and then disappear. Give "credility" to misinformation. Take advantage of credential bias
- Tactic: TA08

Technique T0045, used in Plandemic

Plandemic exploited credential bias, and relied heavily on AMITT technique T0045: use fake experts. The "expert" here was Judy Mikovits. Some of the narratives used included that vaccines contain Covid19 virus, masks activate Covid19 virus, and that the Plandemic video was exposing scientific and political elites.

Fake experts are interesting because their credentials lend credibility to outrageous claims. Fake experts use their credential suspend disbelief. Fake experts create an illusion of “another side” of the argument (anti-vaxx, climate change, etc.). It’s an effective technique in part because it's a human story. It plays into the narrative of a lone researcher, an outsider, bravely facing off against the scientific and political elites who seek to destroy her and her reputation to maintain the status quo, and it’s a story that’s cast her as a victim.

Double Deceit



DOCTRINE-BASED COUNTERMEASURES

IRA IN GHANA: DOUBLE DECEIT

- Resources
  - Staff ~16
  - Audience ~338k
  - Mobile Devices
- Infrastructure
  - NGO
  - Operator Content Pool
  - Twitter Analytics
- Execution
  - T0007,T0010,T0015,T0055,T0013
  - T0014,T0018,T0021,T0030,T0039
  - T0042,T0053
- Time
  - Direct Engagement
  - No Automation + Bots
  - 'Audience Building' Phase

Graphika

IRA in Ghana:
Double Deceit

The Graphika Team

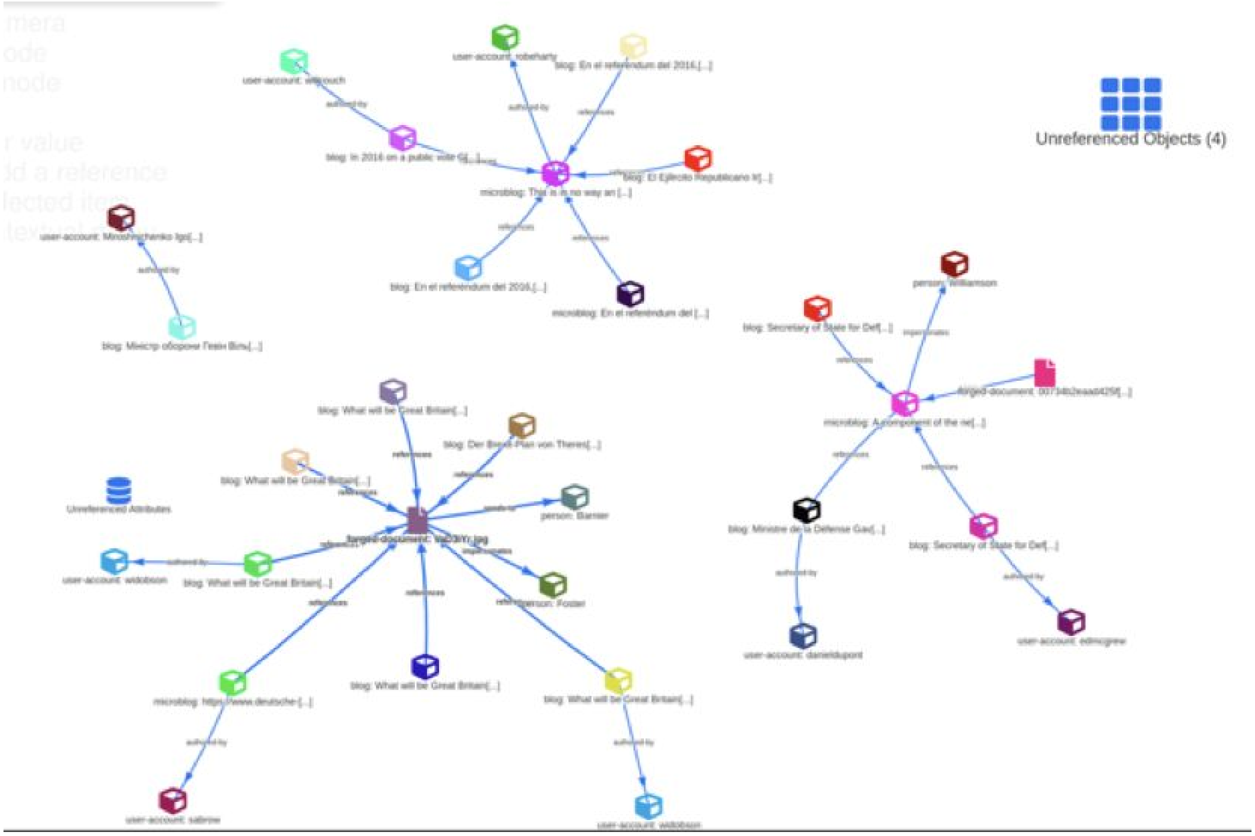
03.2020

Information Operations

We saw the use of T0010 (Cultivate ignorant agents) in the Double Deceit incident. This technique was used by EBLA, registered as an NGO in Ghana, doing NGO charity work on the ground in Ghana (stationary to students). Except it's a Russian front. They hired local youth to post on social media. These people were not aware that they were part of a Russian troll farm. They also attempted to co-opt legitimate US influencers, to retweet their messages. Content was not political, and this appeared to be audience building.

We believe this is associated with the IRA. It appears to have been a failure.

Sekondary Infektion


user-account: robeharty
blog: En el referéndum del 2016,[...]
user-account: willcouch
authored-by
references
blog: In 2016 on a public vote G[...]
microblog: This is no way an [...]
blog: El Ejército Republicano Ir[...]
user-account: Miroshnichenko Igo[...]
authored-by
blog: En el referéndum del 2016,[...]
microblog: En el referéndum del [...]
blog: Міністр оборони Гевін Віль[...]
Unreferenced Objects (4)
person: Williamson
blog: Secretary of State for Def[...]
impersonates
forged-document: 00734b2eaad425f[...]
microblog: A component of the ne[...]
blog: Ministre de la Défense Gav[...]
blog: Secretary of State for Def[...]
user-account: danieldupont
user-account: edmcgrew
blog: What will be Great Britain[...]
blog: Der Brexit-Plan von Theres[...]
blog: What will be Great Britain[...]
Unreferenced Attributes
person: Barnier
forged-document: ...jpg
user-account: widobson
blog: What will be Great Britain[...]
person: Foster
microblog: https://www.deutsche-[...]
blog: What will be Great Britain[...]
blog: What will be Great Britain[...]
user-account: sabrow
user-account: widobson

AMITT STIX for Sekondary Infektion