AMITT Framework - COVID-19 Disinformation Response

SJ TERP
ROGER JOHNSTON

EU ATT&CK Workshop, May 19th 2020

Cognitive Security Collaborative

bring together information security researchers, data scientists, and other subject-matter experts

to create and improve resources

for the defense of the cognitive domain

MISP Disinformation Sharing Community!

https://cogsec-collab.org/

COGSEC
COLLABORATIVE

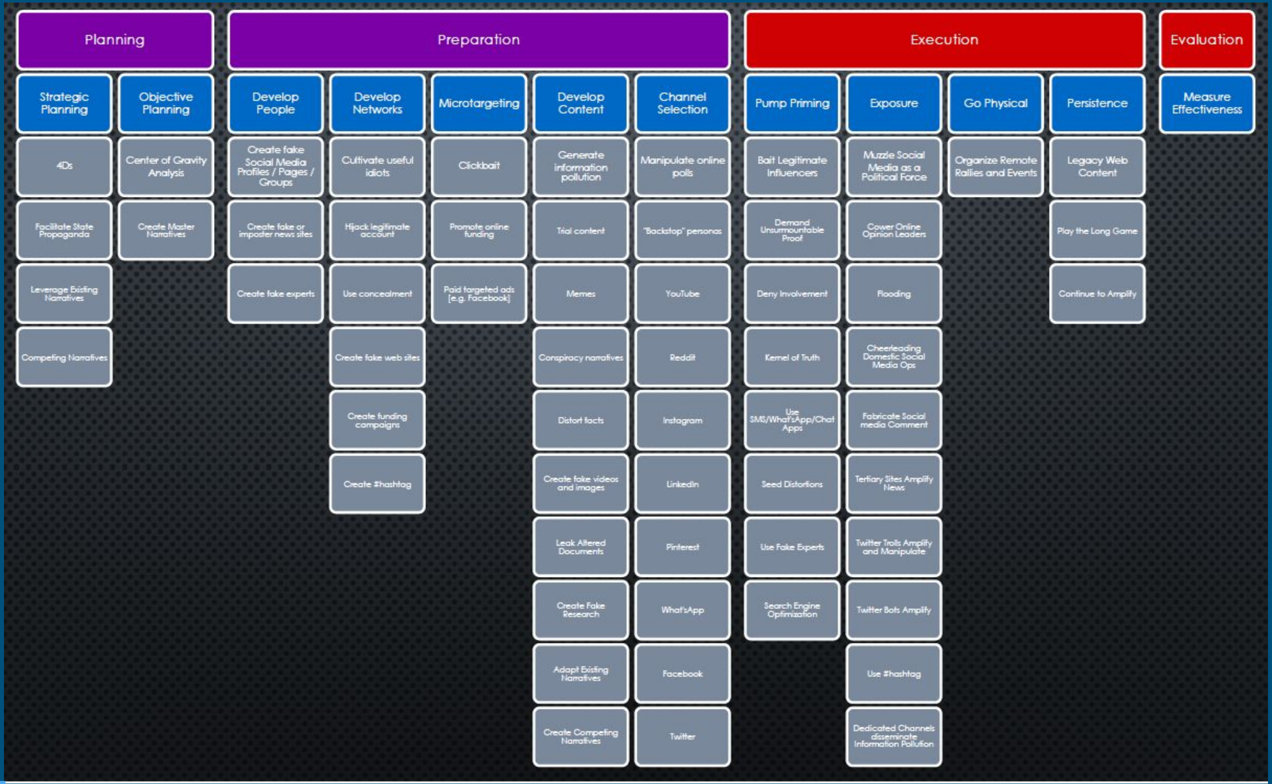
Disinformation

deliberate promotion… of false, misleading or mis-attributed information

focus on creation, propagation, consumption of misinformation online

we are especially interested in misinformation designed to change beliefs in a large number of people

AMITT Framework



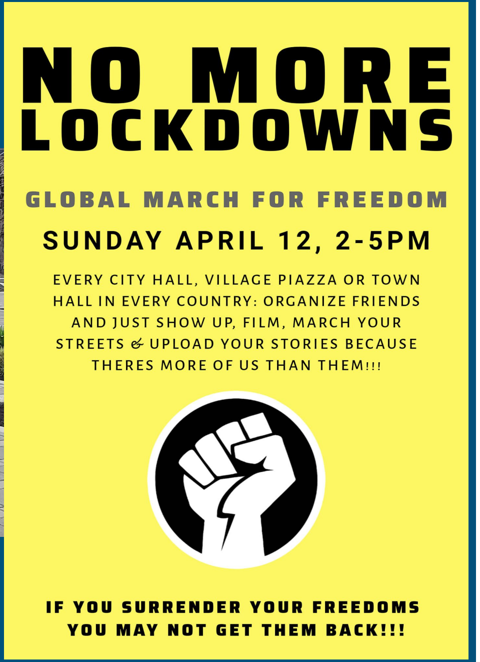
Planning		Preparation					Execution				Evaluation
Strategic Planning	Objective Planning	Develop People	Develop Networks	Microtargeting	Develop Content	Channel Selection	Pump Priming	Exposure	Go Physical	Persistence	Measure Effectiveness
4Ds	Center of Gravity Analysis	Create fake Social Media Profiles / Pages / Groups	Cultivate useful idiots	Clickbait	Generate information pollution	Manipulate online polls	Bait Legitimate Influencers	Muzzle Social Media as a Political Force	Organize Remote Rallies and Events	Legacy Web Content	
Facilitate State Propaganda	Create Master Narratives	Create fake or imposter news sites	Hijack legitimate account	Promote online funding	Trial content	"Backstop" personas	Demand Unsurmountable Proof	Cower Online Opinion Leaders		Play the Long Game	
Leverage Existing Narratives		Create fake experts	Use concealment	Paid targeted ads [e.g. Facebook]	Memes	YouTube	Deny Involvement	Flooding		Continue to Amplify	
Competing Narratives			Create fake web sites		Conspiracy narratives	Reddit	Kernel of Truth	Cheerleading Domestic Social Media Ops			
			Create funding campaigns		Distort facts	Instagram	Use SMS/What'sApp/Chat Apps	Fabricate Social media Comment			
			Create #hashtag		Create fake videos and images	LinkedIn	Seed Distortions	Tertiary Sites Amplify News			
					Leak Altered Documents	Pinterest	Use Fake Experts	Twitter Trolls Amplify and Manipulate			
					Create Fake Research	What'sApp	Search Engine Optimization	Twitter Bots Amplify			
					Adapt Existing Narratives	Facebook		Use #hashtag			
					Create Competing Narratives	Twitter		Dedicated Channels disseminate Information Pollution			

@bodaceacat @VV_X_7

Incidents

#WeWontStayHome

Photo: Lake Country Calendar, Vernon, BC, Canada



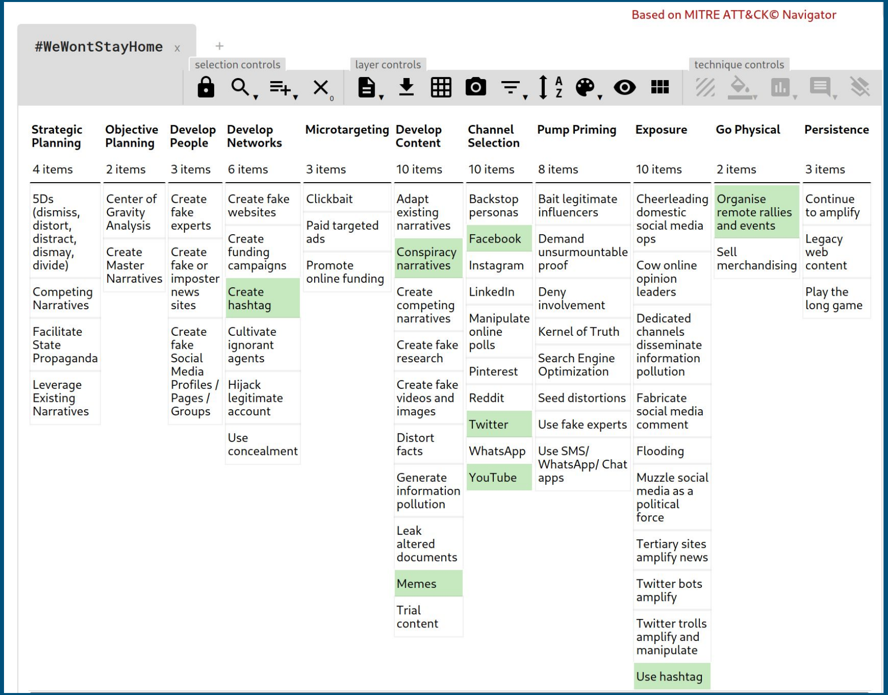
NO MORE LOCKDOWNS

GLOBAL MARCH FOR FREEDOM

SUNDAY APRIL 12, 2-5PM

EVERY CITY HALL, VILLAGE PIAZZA OR TOWN HALL IN EVERY COUNTRY: ORGANIZE FRIENDS AND JUST SHOW UP, FILM, MARCH YOUR STREETS & UPLOAD YOUR STORIES BECAUSE THERES MORE OF US THAN THEM!!!

IF YOU SURRENDER YOUR FREEDOMS YOU MAY NOT GET THEM BACK!!!



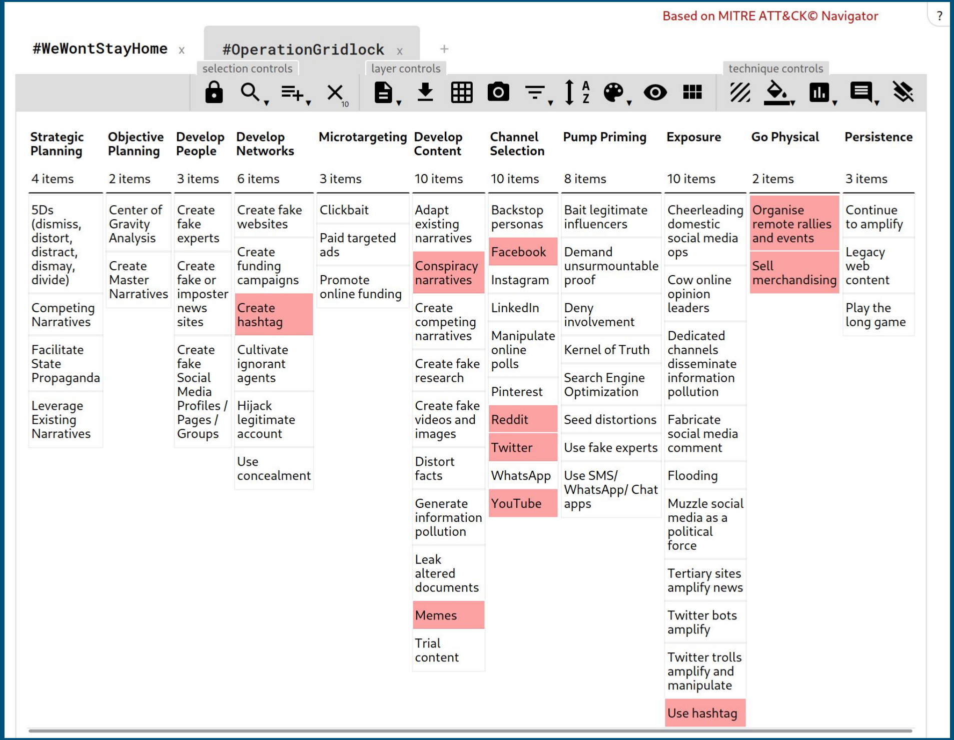
Based on MITRE ATT&CK© Navigator

Strategic Planning	Objective Planning	Develop People	Develop Networks	Microtargeting	Develop Content	Channel Selection	Pump Priming	Exposure	Go Physical	Persistence
4 items	2 items	3 items	6 items	3 items	10 items	10 items	8 items	10 items	2 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
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
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
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		

@bodaceacat @VV_X_7

#OperationGridlock

Photo: The State News, Lansing, Michigan, USA

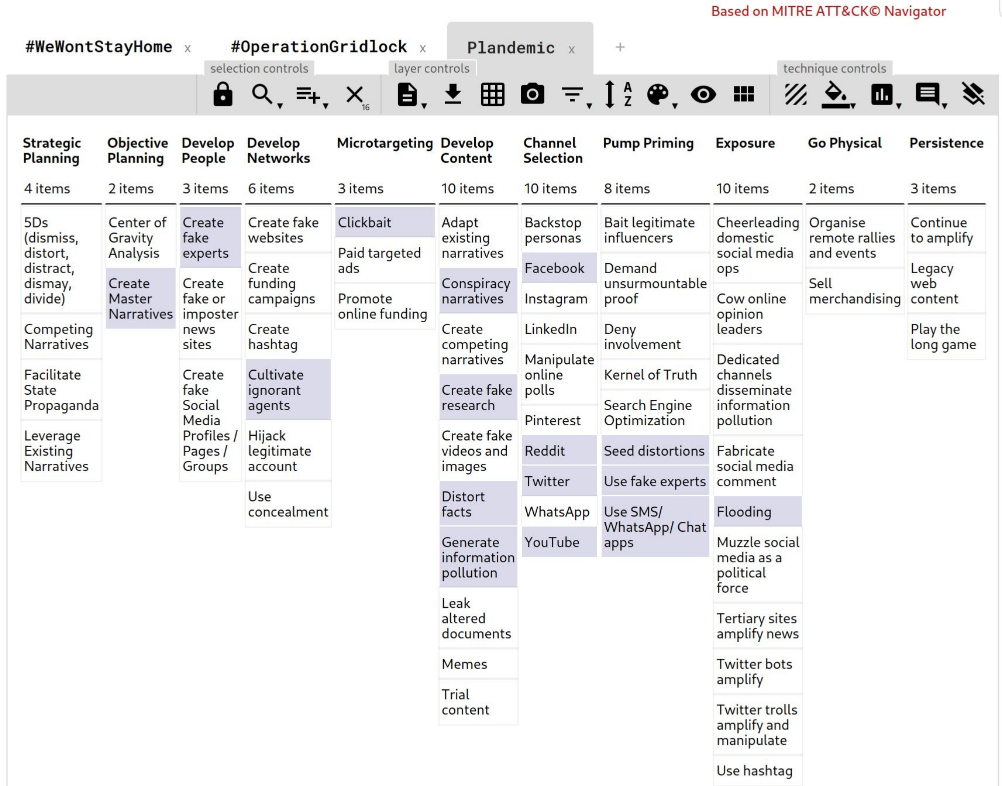


Strategic Planning	Objective Planning	Develop People	Develop Networks	Microtargeting	Develop Content	Channel Selection	Pump Priming	Exposure	Go Physical	Persistence
4 items	2 items	3 items	6 items	3 items	10 items	10 items	8 items	10 items	2 items	3 items
5Ds (dismiss, distort, distract, dismay, divide)	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
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
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
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		

@bodaceacat @VV_X_7

Plandemic

Photo: NBC News, Salem, Oregon, USA



Based on MITRE ATT&CK© Navigator

Strategic Planning	Objective Planning	Develop People	Develop Networks	Microtargeting	Develop Content	Channel Selection	Pump Priming	Exposure	Go Physical	Persistence
4 items	2 items	3 items	6 items	3 items	10 items	10 items	8 items	10 items	2 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
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
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
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		

Countermeasures

Reactive Countermeasures

- Takedown Requests
  - Censorship
  - Violation of ToS
- Law Enforcement Escalations
  - Go Physical

Playbooks

Collection & Analysis

- So far...
  - Collection
  - Processing
  - Analysis
- In progress
  - Counters
- Task tracking
  - TheHive Case templates
  - Workflows are merged to parent

Thank You

EU ATT&CK Community

MITRE Engenuity

MISP Project

TheHive Project

Atomic Threat Coverage

@bodaceacat @VV_X_7