



# Misinformation: We're Four Steps Behind Its Creators

John Gray and Sara "SJ" Terp

Comparative Approaches to Disinformation (Harvard Oct. 2019)

TO CATCH UP WE NEED  
A TRANS-DISCIPLINARY  
COMMUNITY APPLYING

- A FRAMEWORK
- A COMMON LANGUAGE

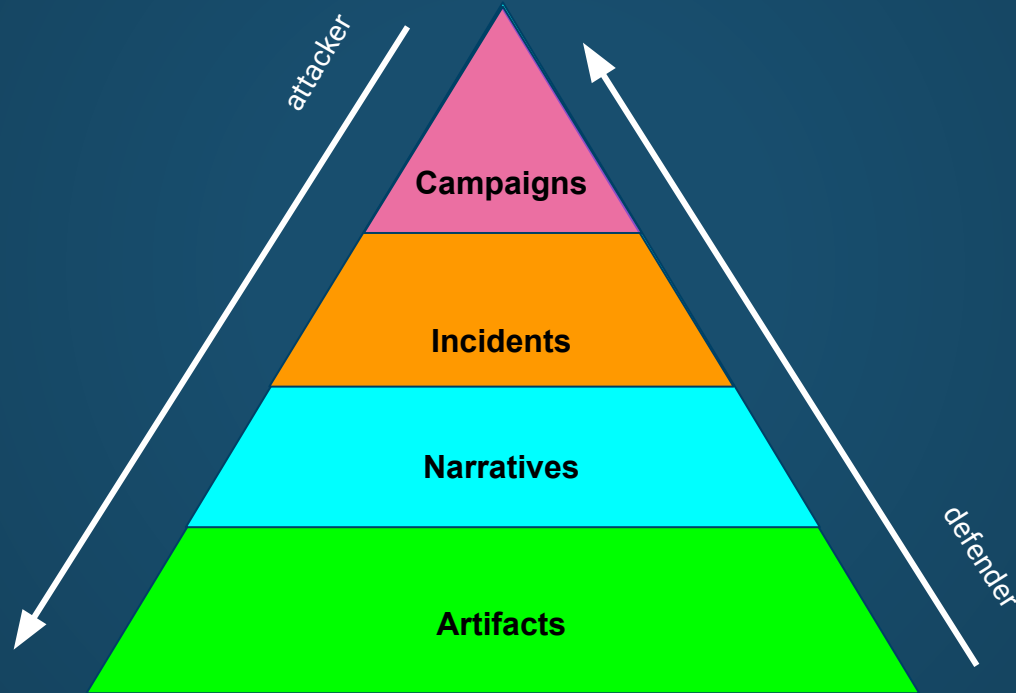
*the infrastructure behind  
misinfosec and what we  
can do with it*



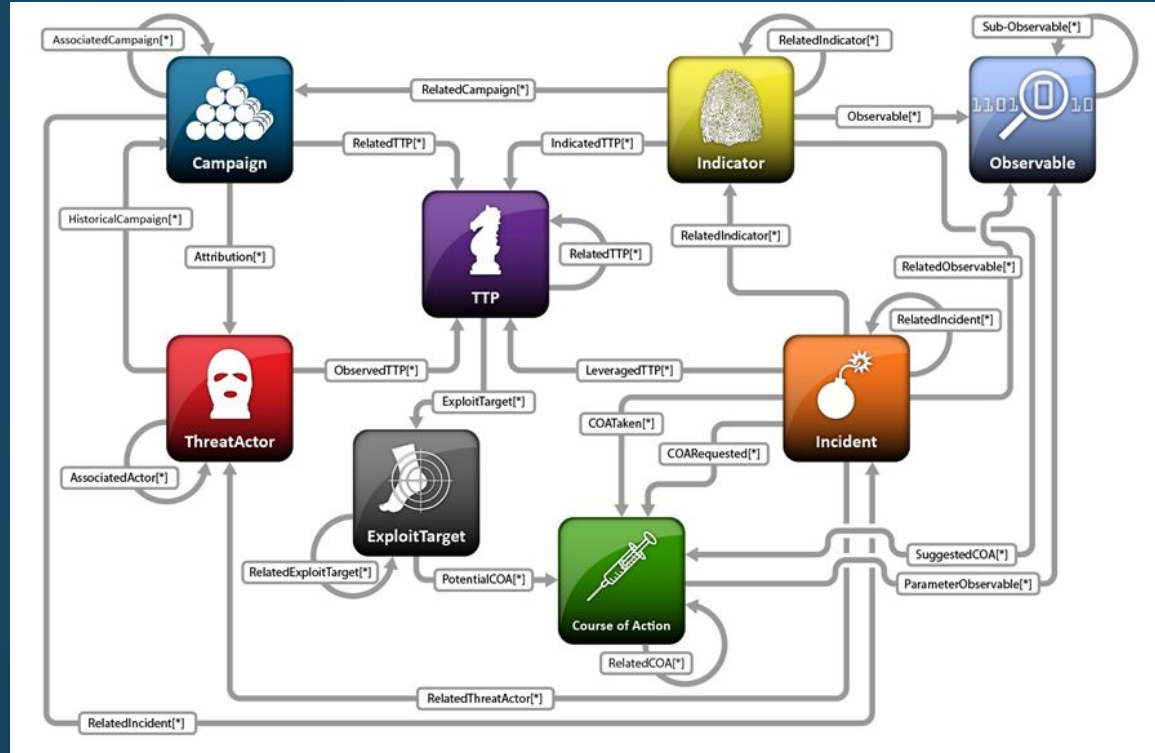
# CREATING A COMMON LANGUAGE

“We use misinformation attack (and misinformation campaign) to refer to the deliberate promotion of false, misleading or mis-attributed information. Whilst these attacks occur in many venues (print, radio, etc), we focus on the creation, propagation and consumption of misinformation online. We are especially interested in misinformation designed to change beliefs in a large number of people.”

# MISINFORMATION PYRAMID



# INFOSEC HAS THINGS WE CAN USE



# STAGE-BASED MODELS ARE USEFUL





# WE EXTENDED THE ATT&CK FRAMEWORK

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Rem
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-pa
Accessibility Features	Binary Padding				Application Deployment Software
Appinit DLLs	Code Signing		Credential Manipulation	File and Directory Discovery	Exploitation of Vulnerability
Local Port Monitor	Component Firmware				
New Service	DLL Side-Loading		Credentials in Files	Local Network Configuration Discovery	Logon Scripts
Path Interception	Disabling Security Tools		Input Capture	Local Network Connections	Pass the Hash
Scheduled Task	File Deletion		Network Sniffing		

# Version 1.0 AMITT (Adversarial Misinformation & Influence Tactics & Techniques) 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 Unmountable Proof	Cover 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/WhatsApp/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	WhatsApp	Search Engine Optimization	Twitter Bots Amplify			
					Adapt Existing Narratives	Facebook		Use #hashtag			
								Dedicated Channels disseminate Information Pollution			



# MISINFOSEC COMMUNITIES

**misinfosec**

**CREDIBILITY  
COALITION**



- Industry
- Academia
- Media
- Community
- Government
- Infosec

# Misinfosec: The Way Ahead

- Continue to grow a trans-disciplinary community
- Support the Cognitive Security ISAO
- Contribute at [misinfosec.org](https://misinfosec.org)
  
- Continue to build an alert structure (ISAC, US-CERT, Interpol, Industry, etc.)
- Continue to refine TTPs and framework
- STIX data science layer - connect to framework