AMITT: ATT&CK-based Standards for Misinformation Threat Sharing

Sara “SJ” Terp and John Gray (co-chairs)
Credibility Coalition Misinfosec Working Group

MITRE ATT&CKcon October, 2019

Credibility Coalition: Who We Are

Is a research community of journalists, researchers, academics, students, policy-makers, technologists and engaged non-specialists that fosters collaborative approaches to understanding the veracity, quality and credibility of online information that is fundamental to civil society.

Credibility Coalition: What We Do

CredCo aims to develop common standards for information credibility by incubating activities and initiatives that bring together people and institutions from a variety of backgrounds. Currently supporting these working groups:

- MisinfoSec
- The UX of Credible Content
- Health Misinformation
- Do Indicators Translate?
- Credibility Literacy
- Responding to Memes and Images

Misinfosec Working Group: People

Academics

Tom Taylor (ASU)
Courtney Crooks (GTRI)
Renee diResta (Stanford)
Chau Tong (UW Madison)
Nitin Agarwal (U Arkansas Little Rock)

Government

Pablo Breuer (USSOCOM)
Daniel Black (NATO)

Others

Connie Moon Sehat (HacksHackers)
Jenny 8 Lee (HackersHackers)
Scott Yates (Certified Content)
Antonio White

Companies

Christopher Walker (Marvelous)
John Gray (Mentionmapp)
SJ Terp (CogSecTech)
Olya Gurevich (Marvelous)
Maggie Engler (GDI)
David Perlman (CogSecTech)
Ed Bice (Meedan)
An Xiao Mina (Meedan)
Zach (Guardians)
Pukhraj Singh
Kat Lo

Mission

The CredCo Misinfosec Working Group (“wg-misinfosec”) aims to develop a framework for the understanding of organized communications attacks (disinformation, misinformation and network propaganda).

Specifically we would like to promote a more formal and rigorous classification of:

- Types of information-based attacks; and
- Types of defense from information-based attacks

Mission continued...

Among the operating assumptions of the group will that social and cognitive factors can "scale up and down" within the framework—facilitating some definitional and procedural crossover in both the construction of a framework for understanding these attacks and in their detection. In this sense scales might be formulated as:

- ACTIONS: What are the atomic "actions" in propaganda attacks?
- TACTICS: How do actions combine to form larger events, including more complex actions and "attacks"?
- STRATEGY: How do the instances of attacks and actions combine to form "campaigns".

Mission continued...

The main objectives of the group will be to:

- Define major terms of art at focal points on the scale, with an emphasis on descriptive or procedural rigor;
- Outline the state-of-the-art "Blue Team" options for defense and counter-attack

WG Timeline

Dec 2018 Jan 2019	WG established & mission statement
Feb 2019	Wrote WWW paper
Mar 2019	Created incidents list
Apr 2019	Created techniques list
May 2019	Red Team Workshop
Jun 2019	Refined AMITT

Jul 2019	AMITT repo goes live
Aug 2019	BlackHat presentation
Sep 2019	STIX SEPs go in
Oct 2019	Populating counters list
Nov 2019	Blue Team Workshop
Dec 2019	Refine counters

First 6 months:

- Collected and analyzed over 63 incidents
- Developed a STIX-inspired format for incident reporting
- Created AMITT, a stage-based framework for misinformation reporting and response
- Published AMITT as an open source project on Github

Current 3 months:

- Collect and analyze misinformation counters
- Convene in DC to organise counters and do blue team incident planning
- Get STIX formats adopted worldwide
- Get AMITT used by reporting and responding organizations
- Find AMITT a regular ‘home’

THE NEED

The only defense against the world is a thorough knowledge of it.

- John Locke

COMPONENTWISE UNDERSTANDING AND RESPONSE

- Lingua Franca across communities
- Defend/countermove against reused techniques, identify gaps in attacks
- Assess defence tools & techniques
- Plan for large-scale adaptive threats (hello, Machine Learning!)

COMBINING DIFFERENT VIEWS OF MISINFORMATION

- Information security (Gordon, Grugq, Rogers)
- Information operations / influence operations (Lin)
- A form of conflict (Singer, Gerasimov)
- [A social problem]
- [News source pollution]

DOING IT AT SCALE

- Computational power
- Speed of analysis
- Lack of framework
- Systems theory and emergence of characteristics
- Cognitive friction
- Cognitive dissonance

https://www.visualcapitalist.com/wp-content/uploads/2018/05/internet-minute-share2.jpg

CREATING MISINFOSEC COMMUNITIES

misinfosec

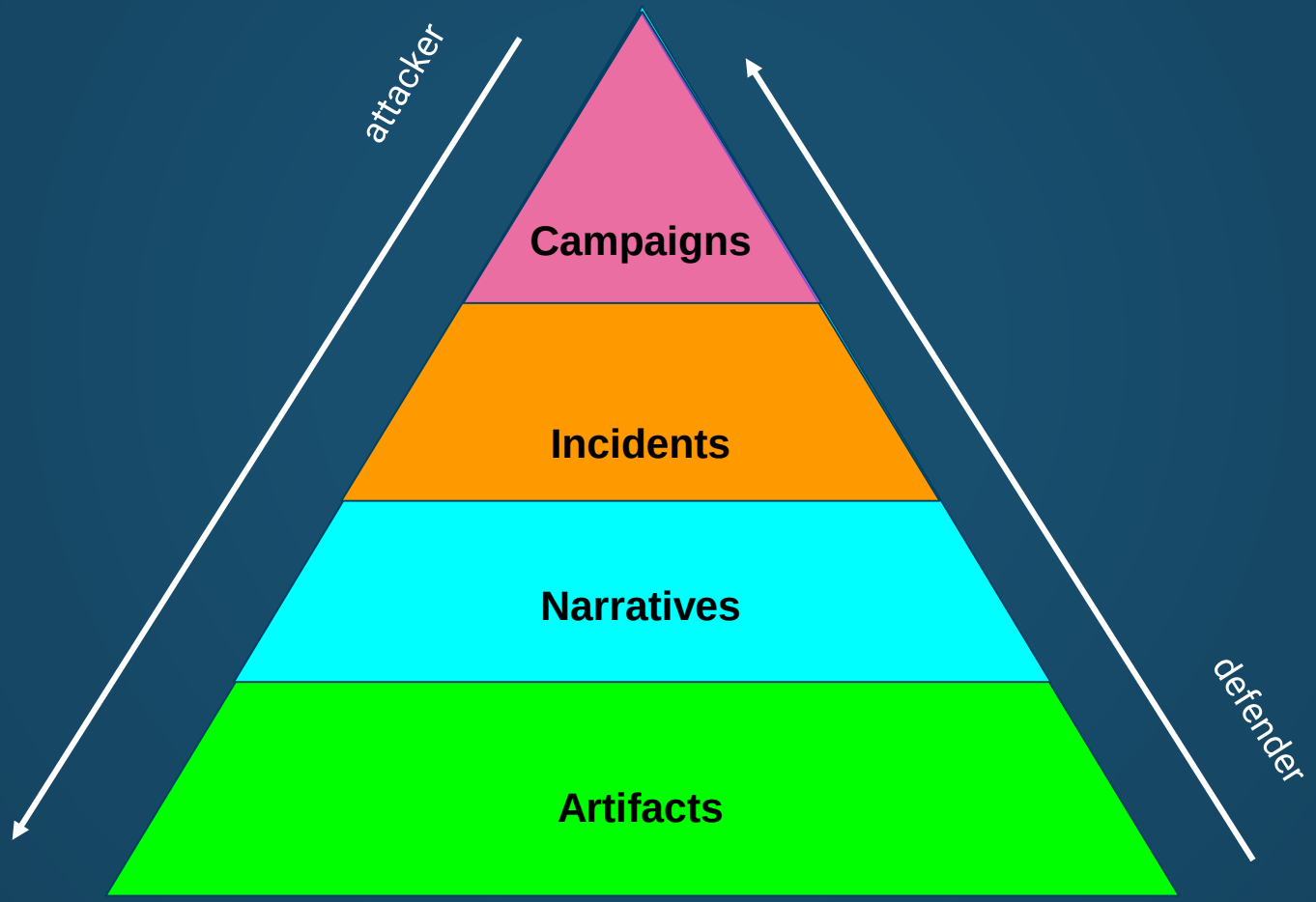
CREDIBILITY COALITION

PEOPLE-CENTERED INTERNET

IACI INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOS

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

CONNECTING MISINFORMATION ‘LAYERS’



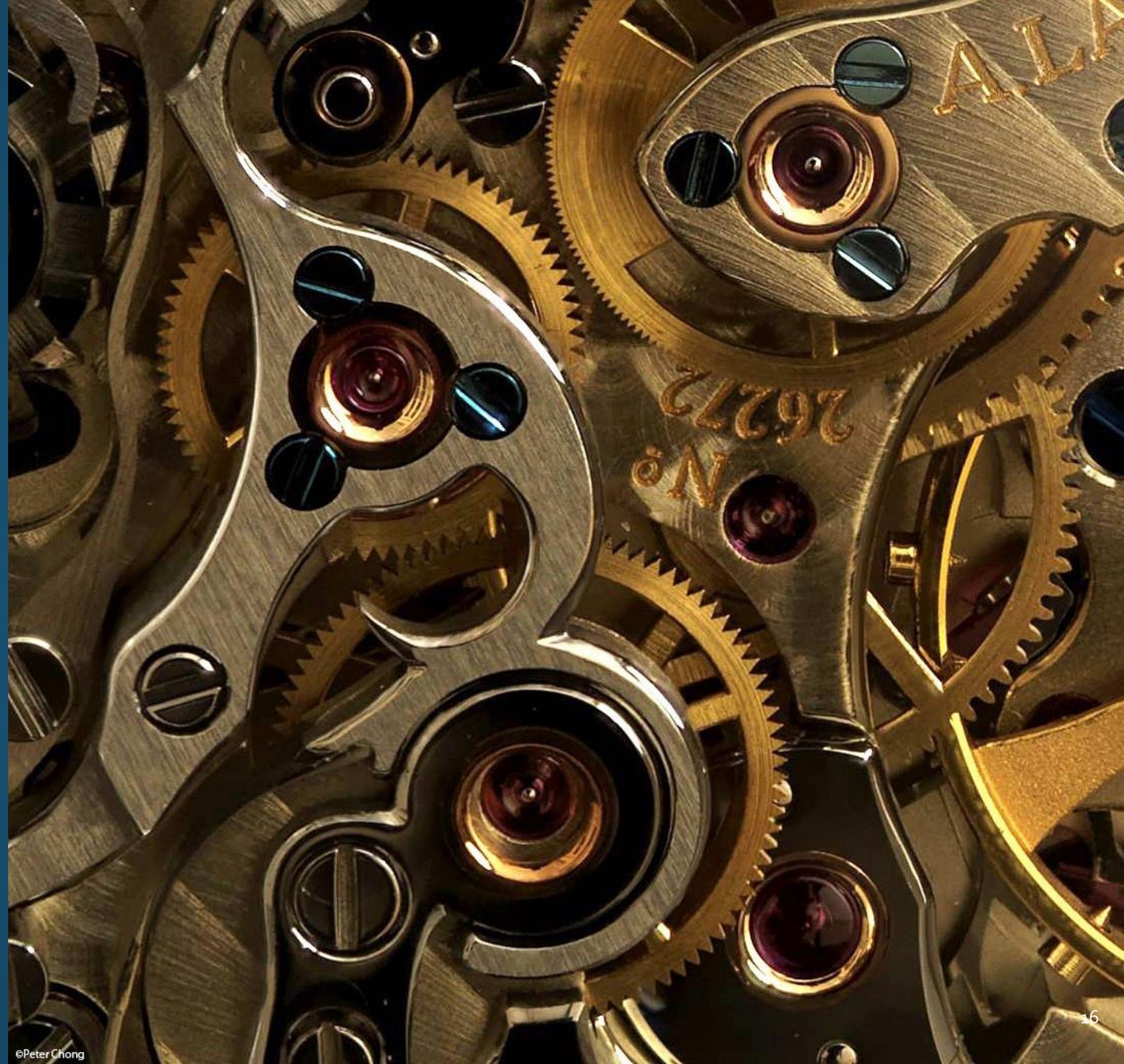
WHAT WE BUILT

All warfare is based on deception.

- Sun Tzu

All cyberspace operations are based on influence.

- Pablo Breuer



STAGE-BASED MODELS ARE USEFUL

RECON	WEAPONIZE	DELIVER	EXPLOIT	CONTROL	EXECUTE	MAINTAIN

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control

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	
Local Port Monitor		Component Firmware			Exploitation of Vulnerability
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery	
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections	Pass the Hash

POPULATING THE FRAMEWORK: HISTORICAL ANALYSIS

- Campaigns
  - e.g. Internet Research Agency, 2016 US elections
- Incidents
  - e.g. Columbia Chemicals
- Failed attempts
  - e.g. Russia - France campaigns

HISTORICAL CATALOG: DATASHEET

- Summary: Early Russian (IRA) “fake news” stories. Completely fabricated; very short lifespan.
- Actor: probably IRA (source: recordedfuture)
- Timeframe: Sept 11 2014 (1 day)
- Presumed goals: test deployment
- Artefacts: text messages, images, video
- Related attacks: These were all well-produced fake news stories, promoted on Twitter to influencers through a single dominant hashtag -- #BPoilspilltsunami, #shockingmurderinatlanta,
- Method:

1. Create messages. e.g. “A powerful explosion heard from miles away happened at a chemical plant in Centerville, Louisiana #ColumbianChemicals”
2. Post messages from fake twitter accounts; include handles of local and global influencers (journalists, media, politicians, e.g. @senjeffmerkley)
3. Amplify, by repeating messages on twitter via fake twitter accounts

- Result: limited traction
- Counters: None seen. Fake stories were debunked very quickly.

FEEDS INTO TECHNIQUES LIST

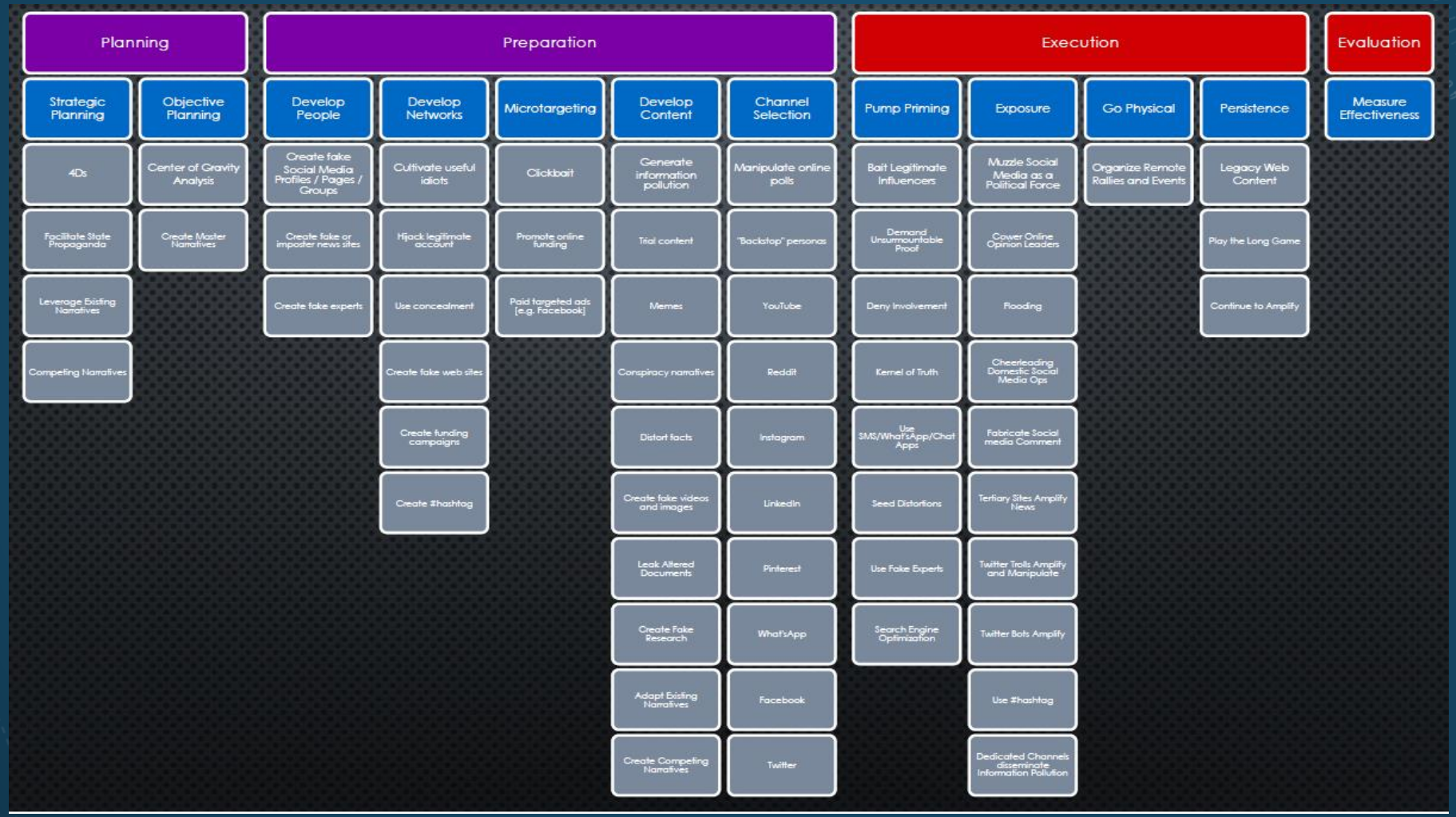
Paid targeted ads

- Type: Technique
- Name: Paid targeted ads
- Id: T0018
- Summary: Create or fund advertisements targeted at specific populations
- Tactic: TA05
- Incidents:

Incident	Descriptions given for this incident
I00002 #VaccinateUS	buy FB targeted ads
I00005 Brexit vote	Targeted FB paid ads
I00017 US presidential elections	Targeted FB paid ads

DO NOT EDIT ABOVE THIS LINE - PLEASE ADD NOTES BELOW

AMITT (Adversarial Misinformation and Influence Tactics and Techniques) Framework



AMITT PHASES AND TACTIC STAGES

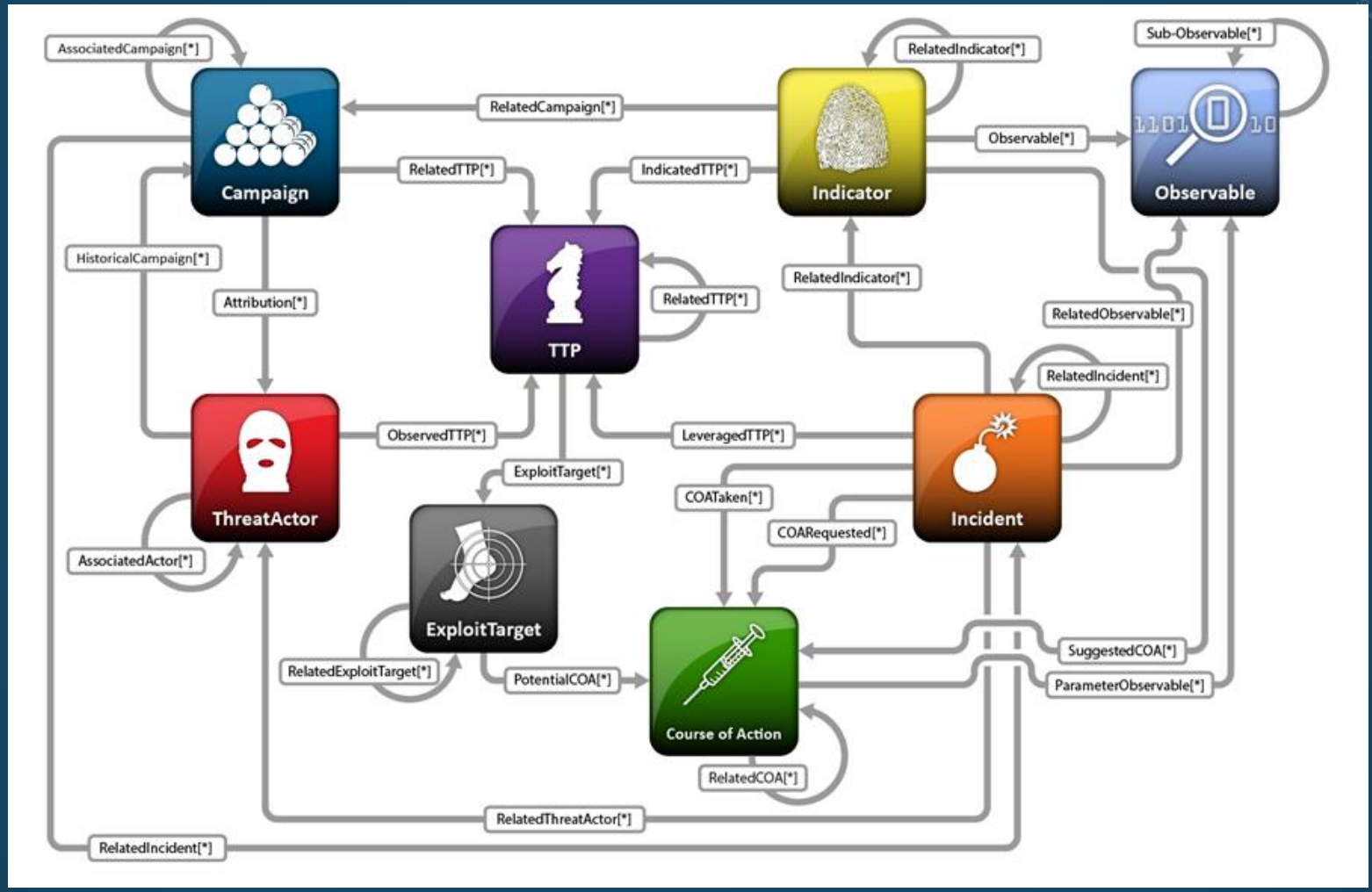
Planning	Strategic Planning
	Objective Planning
Preparation	Develop People
	Develop Networks
	Microtargeting
	Develop Content
	Channel Selection

Execution	Pump Priming
	Exposure
	Go Physical
	Persistence
Evaluation	Measure Effectiveness

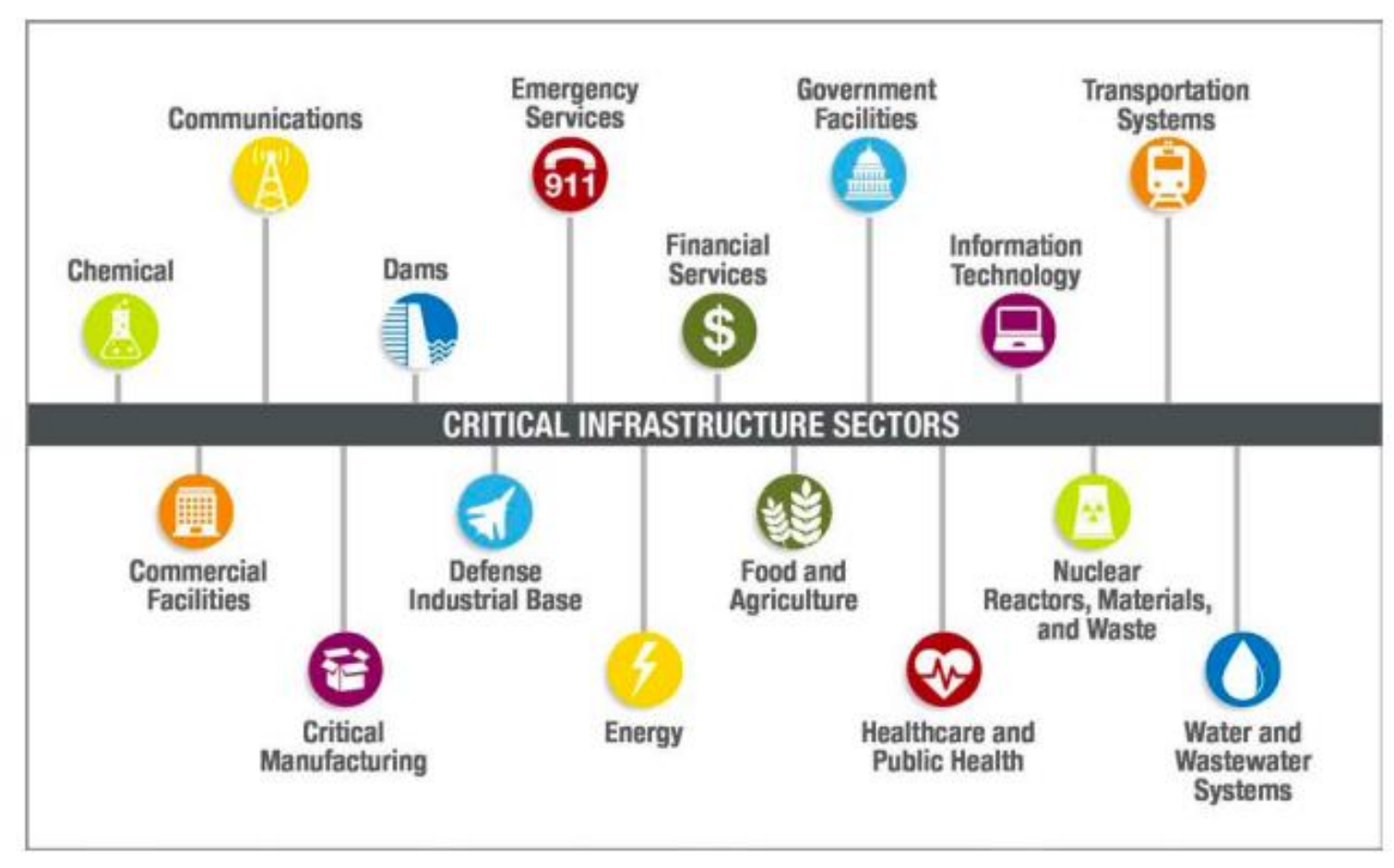
AMITT STIX

Misinformation STIX	Description	Level	Infosec STIX
Report	communication to other responders	Communication	Report
Campaign	Longer attacks (Russia's interference in the 2016 US elections is a "campaign")	Strategy	Campaign
Incident	**Shorter-duration attacks, often part of a campaign**	**Strategy**	**Intrusion Set**
Course of Action	Response	Strategy	Course of Action
Identity	Actor (individual, group, organisation etc): creator, responder, target, useful idiot etc.	Strategy	Identity
Threat actor	Incident creator	Strategy	Threat Actor
Attack pattern	Technique used in incident (see framework for examples)	TTP	Attack pattern
Narrative	**Malicious narrative (story, meme)**	**TTP**	**Malware**
Tool	bot software, APIs, marketing tools	TTP	Tool
Observed Data	artefacts like messages, user accounts, etc	Artefact	Observed Data
Indicator	posting rates, follow rates etc	Artefact	Indicator
Vulnerability	Cognitive biases, community structural weakness etc	Vulnerability	Vulnerability

STIX GRAPHS (STIG)



INTELLIGENCE SHARING AND COORDINATION BODIES



Moving forward

- Focus on Blue Team research and exercises which thorough explore the space of potential inoculations and counter-attacks.
- Propose AMITT as the basis of new misinformation response centers, including ISAOs (Information Sharing and Analysis Organizations) and ISACs (Information Sharing and Analysis Centers)
- Test AMITT against new incidents - both historical incidents that we haven't included in it, and new incidents as they emerge.

Part of this work is to find existing response populations who could use the framework and determine the training and adaptations they need to be able to use it themselves. This will make the framework more useful both to them and to future potential users

AMITT UPDATES AT http://misinfosec.org