AMITT and other Misinfosec-based Misinformation Standards

SJ TERP

Oct 22nd 2019

Who “we” are

AM!TT
misinfosec

misinfosec

CREDIBILITY COALITION

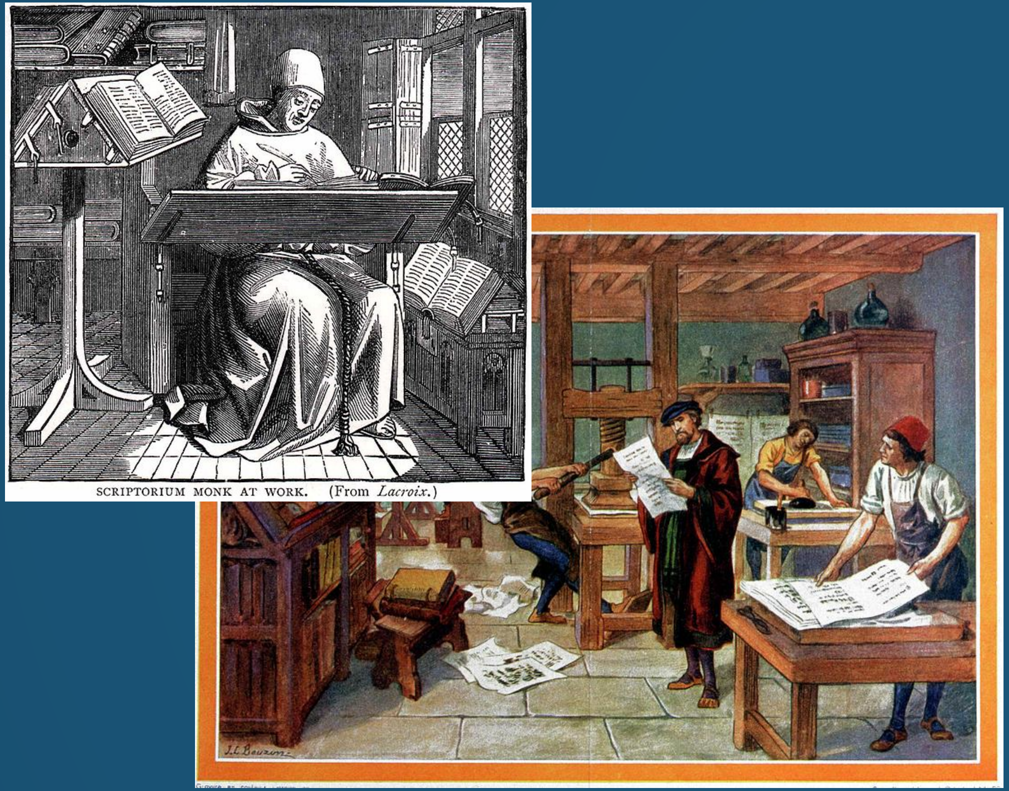
PEOPLE-CENTERED INTERNET

NATION-STATES AND INFLUENCE

War is an act of force to compel the enemy to do our will

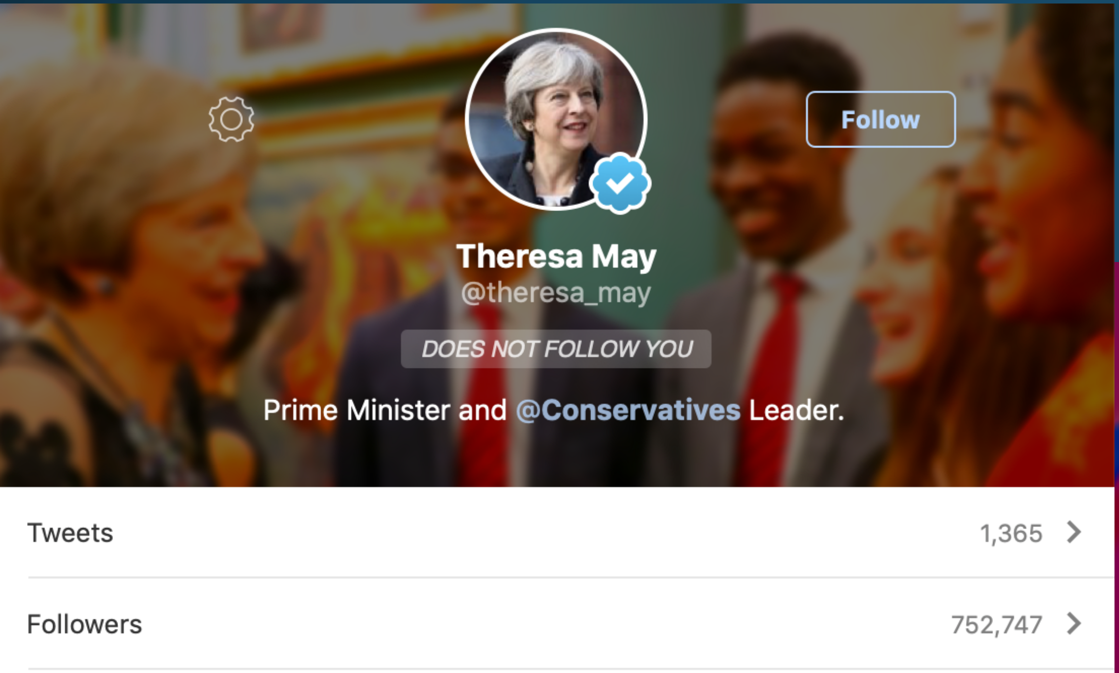
- *Clausewitz*

EVOLUTION OF INFORMATION



SCRIPTORIUM MONK AT WORK. (From *Lacroix*.)

EVOLUTION OF INFORMATION



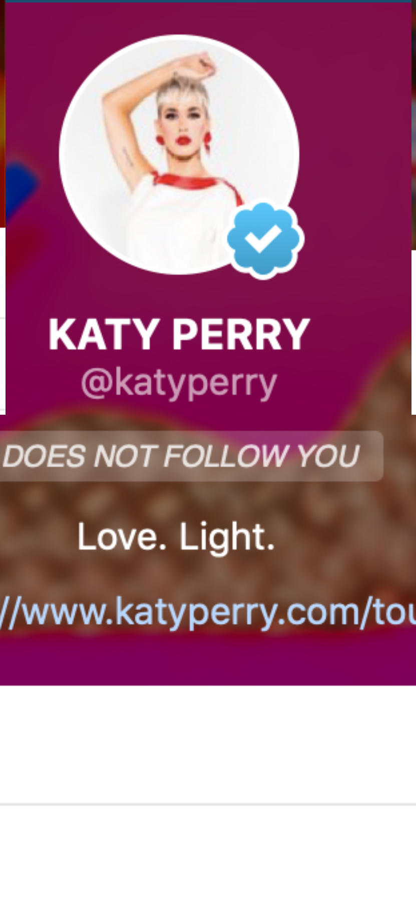
Follow

Theresa May
@theresa_may

DOES NOT FOLLOW YOU

Prime Minister and @Conservatives Leader.

Tweets	1,365
Followers	752,747



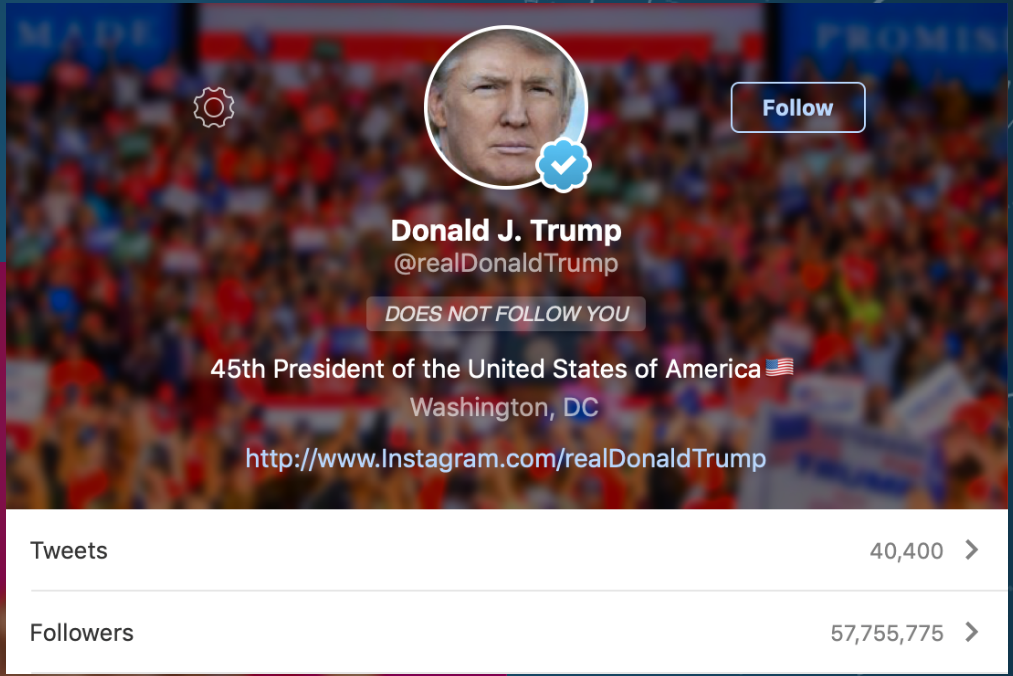
KATY PERRY
@katyperry

DOES NOT FOLLOW YOU

Love. Light.

http://www.katyperry.com/tour

Tweets	9,357
Followers	106,945,008



Follow

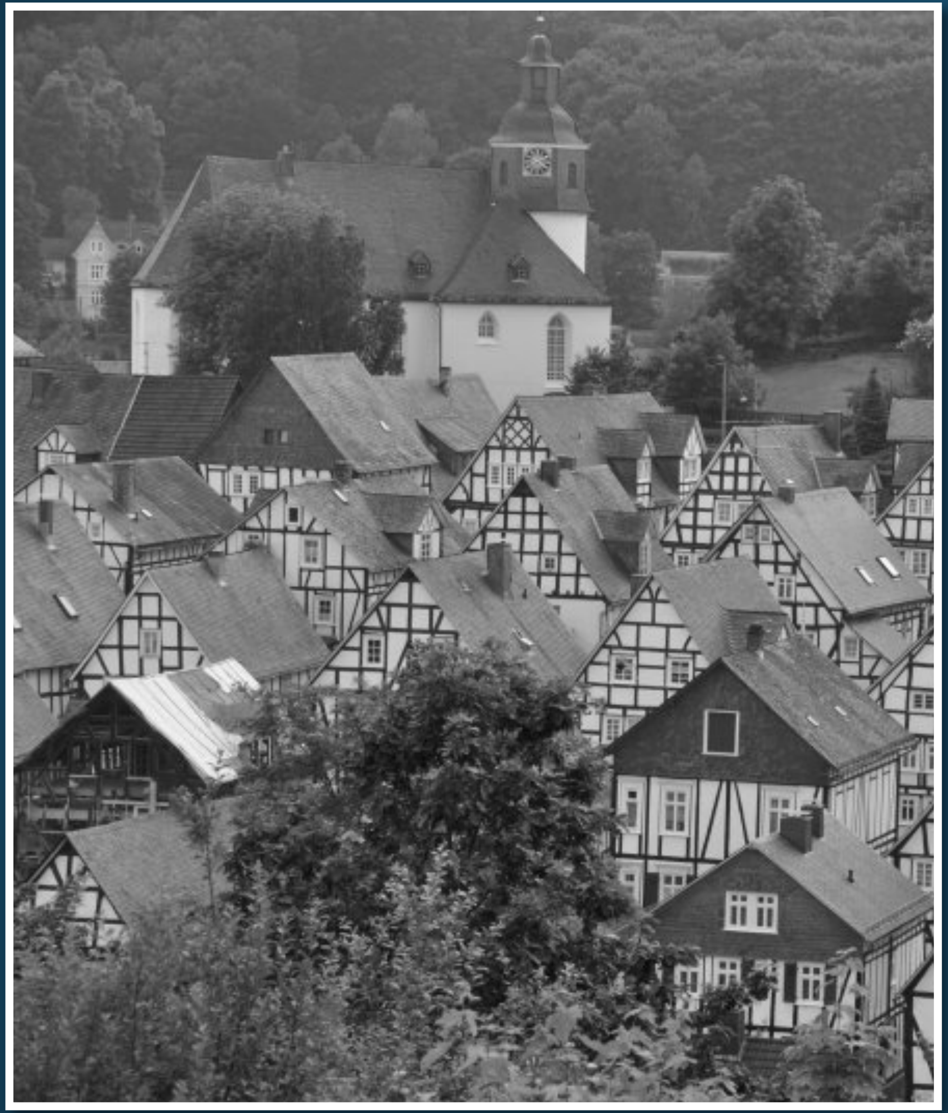
Donald J. Trump
@realDonaldTrump

DOES NOT FOLLOW YOU

45th President of the United States of America 🇺🇸
Washington, DC
http://www.Instagram.com/realDonaldTrump

Tweets	40,400
Followers	57,755,775

WESTPHALIAN SOVEREIGNTY



Each nation has sovereignty over its own territory and domestic affairs

Principal of non-interference in another country's domestic affairs

Each state is equal under international law

NATIONAL INSTRUMENTS OF INFLUENCE

Resources available in pursuit of national objectives…

Diplomatic

Informational

Military

Economic

…and how to influence other nation-states.

BUSINESS INSTRUMENTS OF INFLUENCE

Resources available in pursuit of corporate objectives…

Business Deals & Strategic Partnerships

PR and Advertising

Mergers and Acquisitions

R&D and Capital Investments

INFORMATION THREATS

Democracy

- Require common political knowledge
  - Who the rulers are
  - Legitimacy of the rulers
  - How government works
- Draw on contested political knowledge to solve problems
- Vulnerable to attacks on common political knowledge

Autocracy

- Actively suppress common political knowledge
- Benefit from contested political knowledge
- Vulnerable to attacks on the monopoly of common political knowledge

THE NEED

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

- John Locke

COMPONENTWISE UNDERSTANDING AND RESPONSE

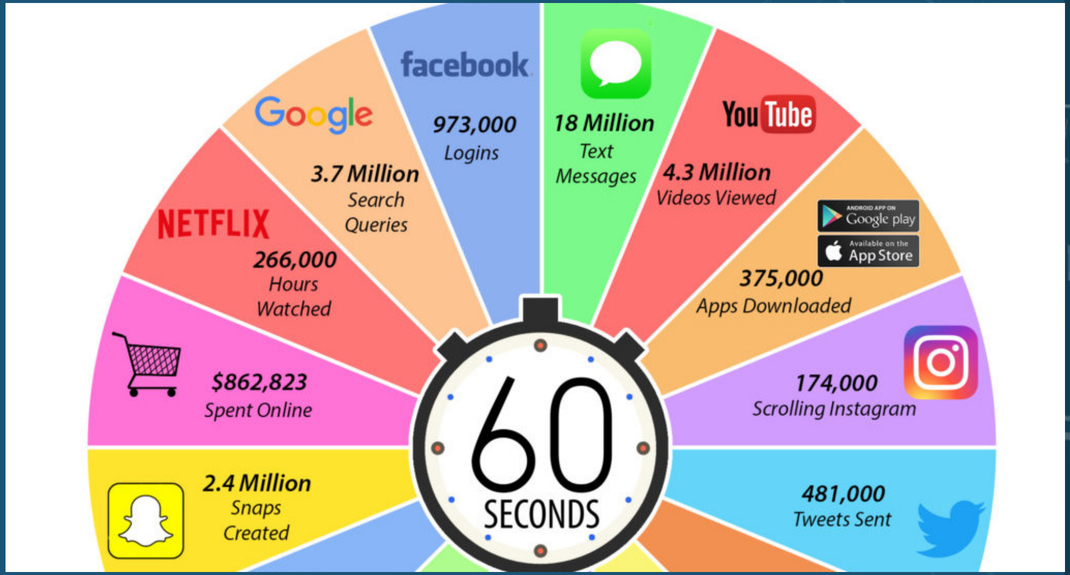
- Lingua Franca across communities
- Defend/countermove against reused techniques, identify gaps in attacks
- Assess defence tools & techniques
- Plan for large-scale adaptive threats (hello, Machine Learning!)

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

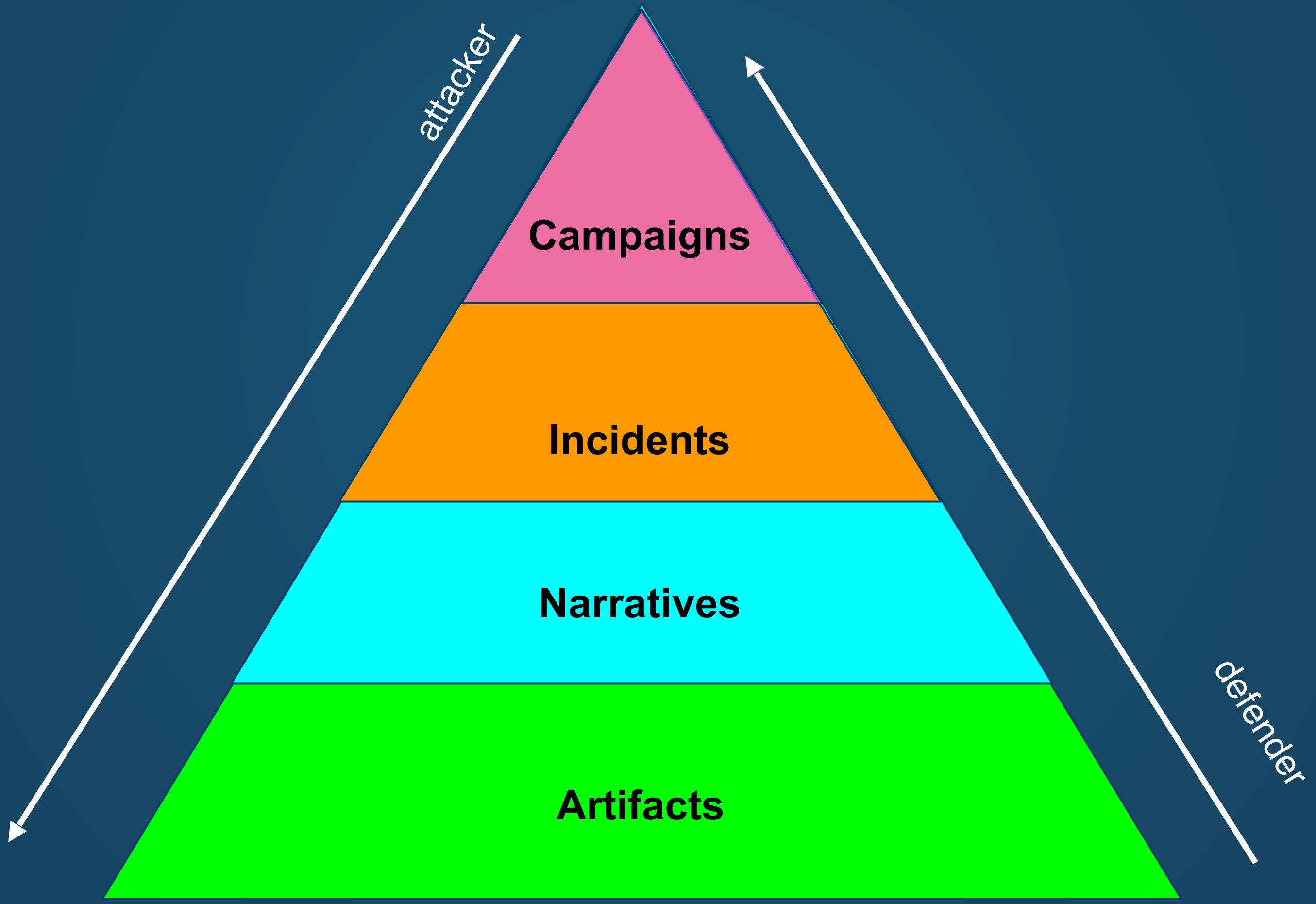
CREDIBILITY
COALITION

PEOPLE-CENTERED
INTERNET

IACI
INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOS

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

CONNECTING MISINFORMATION ‘LAYERS’



Our original spec for AMITT

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

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".

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

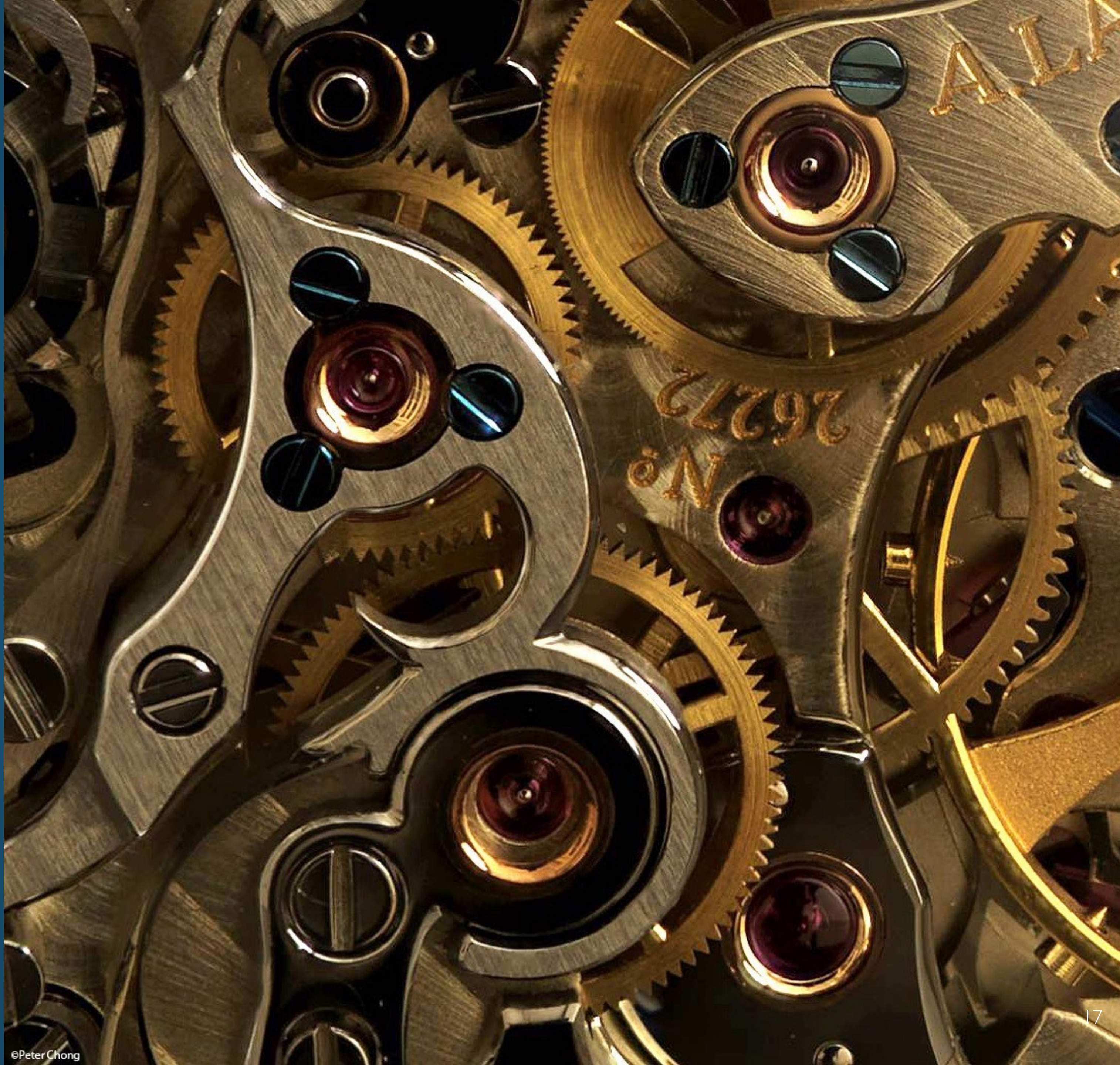
WHAT WE BUILT

All warfare is based on deception.

- *Sun Tzu*

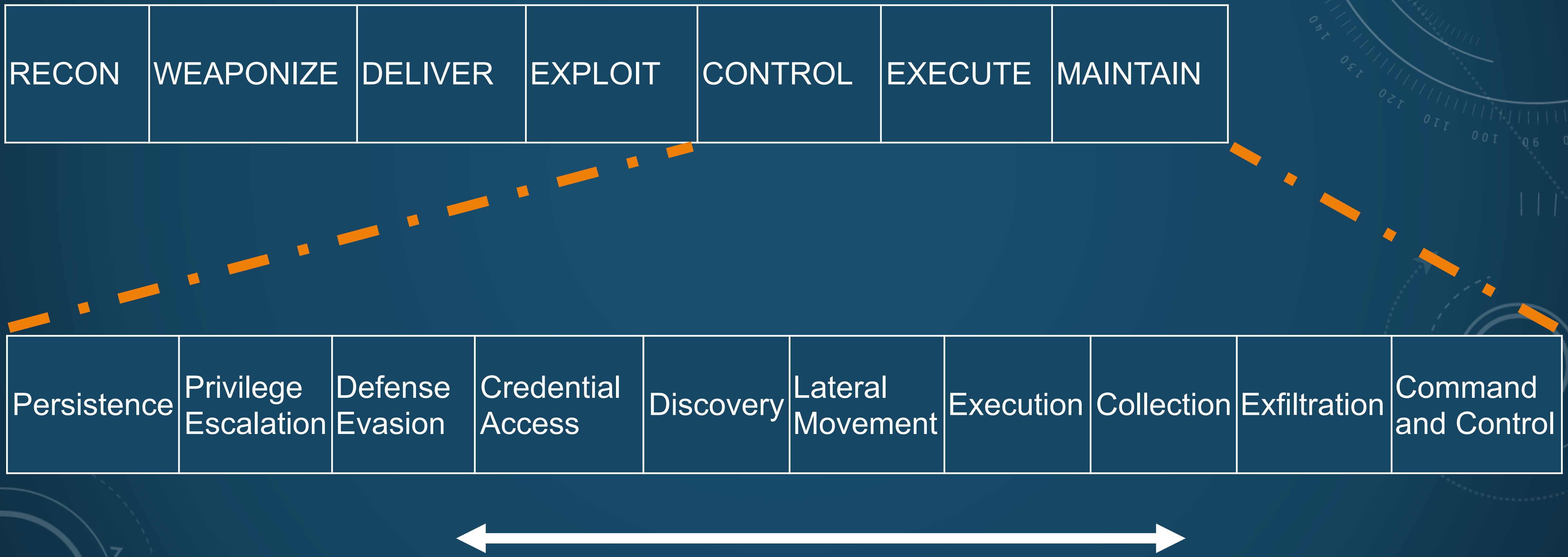
All cyberspace operations are based on influence.

- Pablo Breuer



©Peter Chong

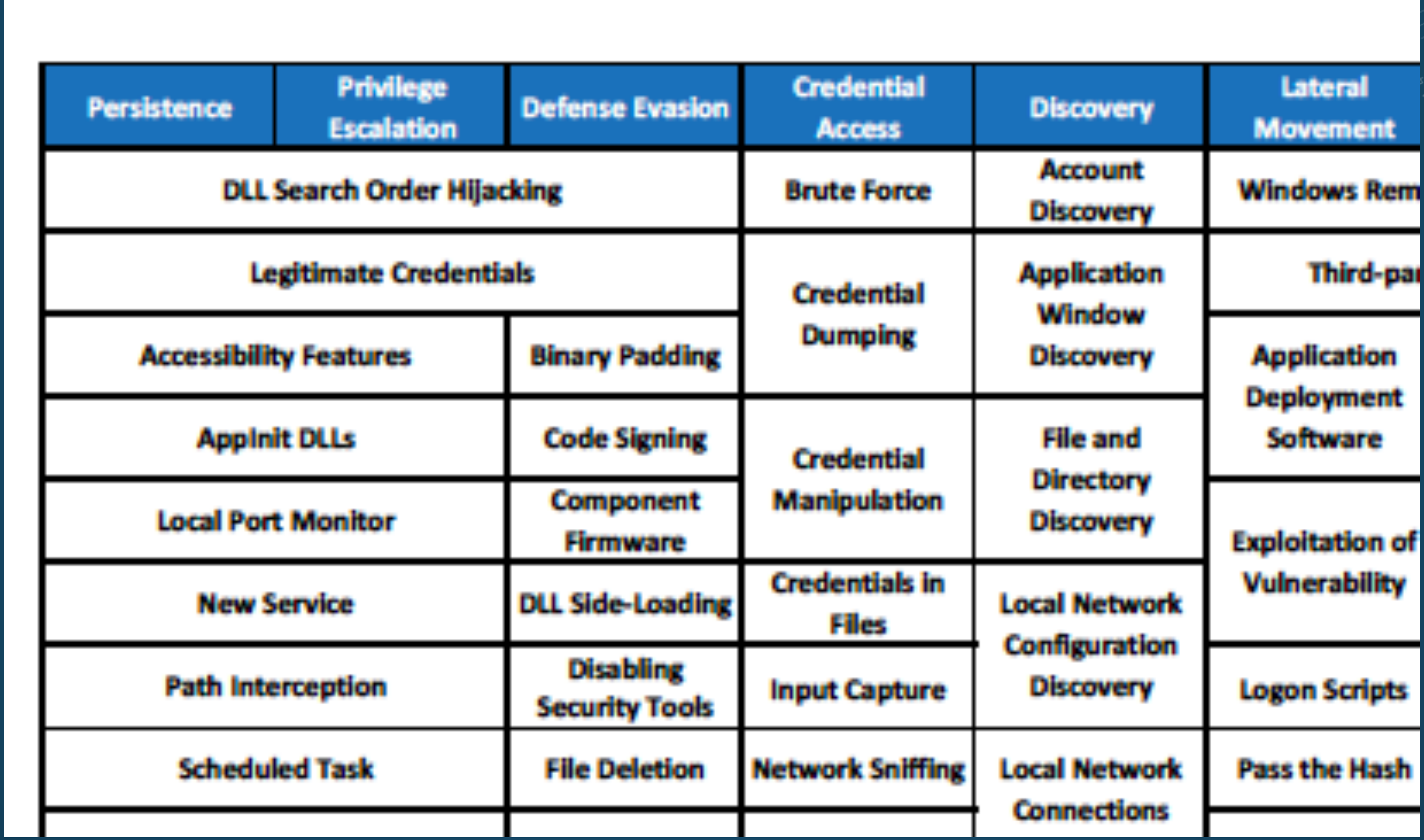
STAGE-BASED MODELS ARE USEFUL



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

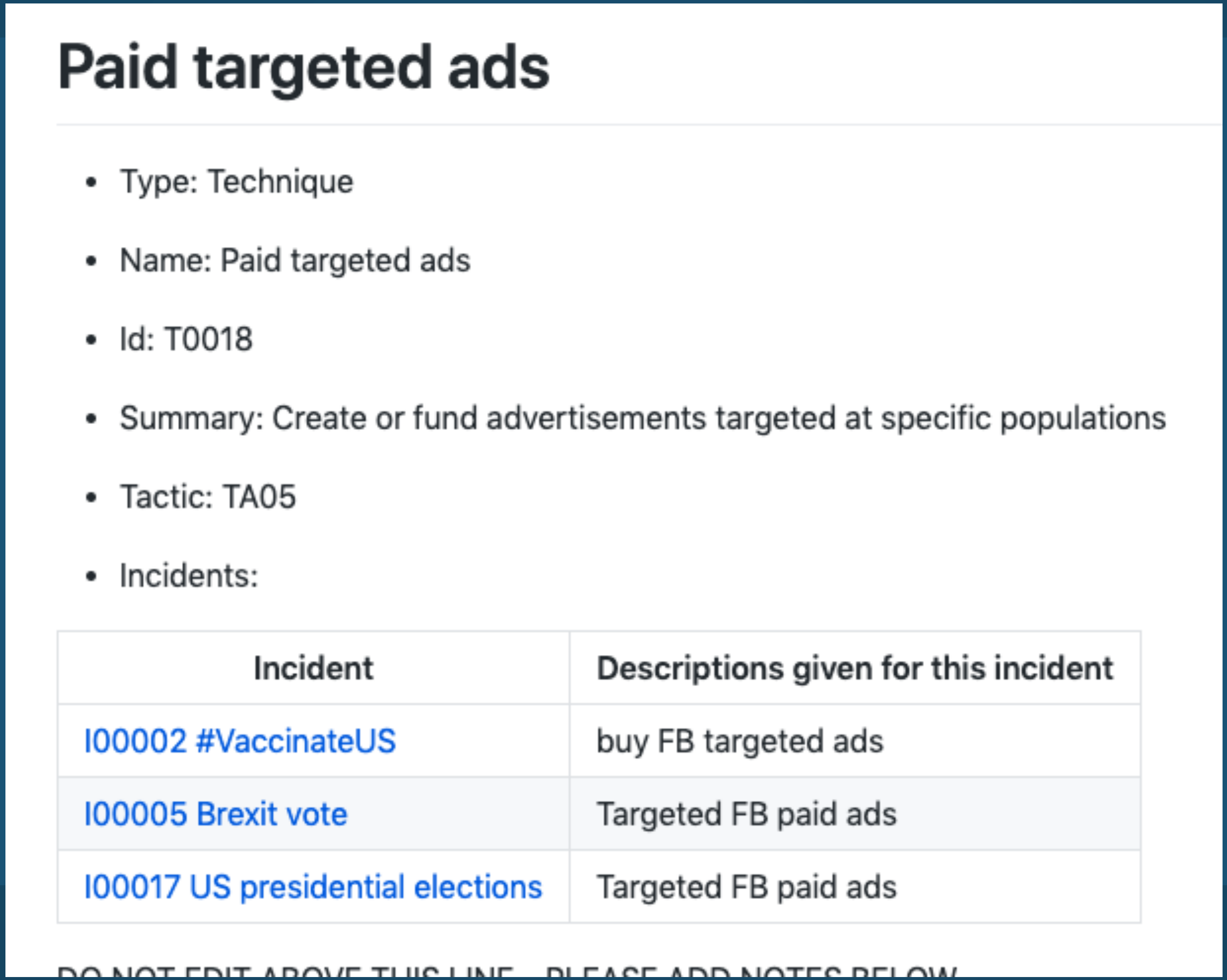
- Summary: Early Russian (IRA) “fake news” stories. Completely fabricated; very short lifespan.
- Actor: probably IRA (source: recordedfuture)
- Timeframe: Sept 11 2014 (1 day)
- Presumed goals: test deployment
- Artefacts: text messages, images, video
- Related attacks: These were all well-produced 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

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/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			
					Create Competing Narratives	Twitter		Dedicated Channels disseminate Information Pollution			

AMITT PHASES AND TACTIC STAGES

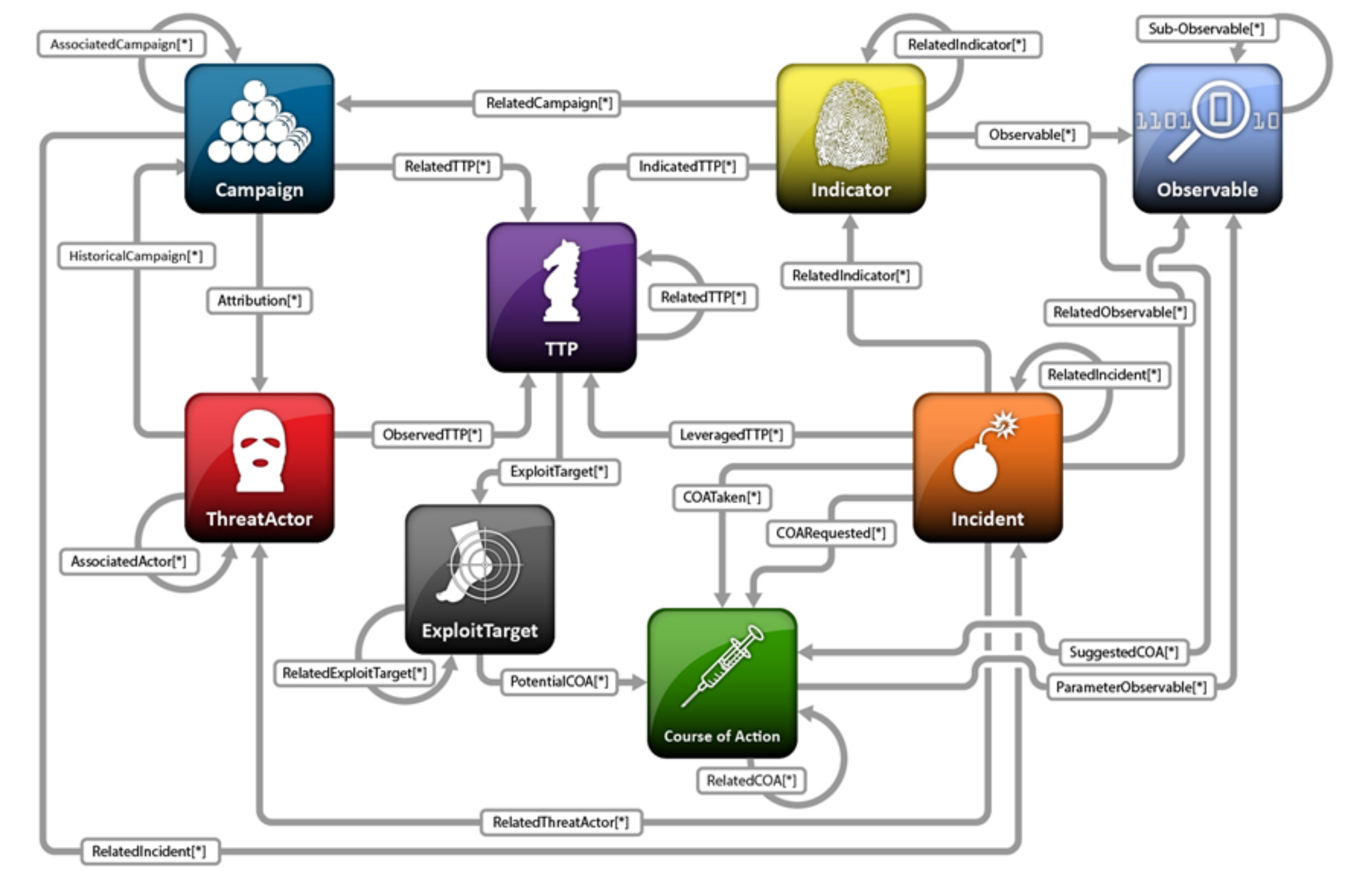
Planning	Strategic Planning
	Objective Planning
Preparation	Develop People
	Develop Networks
	Microtargeting
	Develop Content
	Channel Selection

Execution	Pump Priming
	Exposure
	Go Physical
	Persistence
Evaluation	Measure Effectiveness

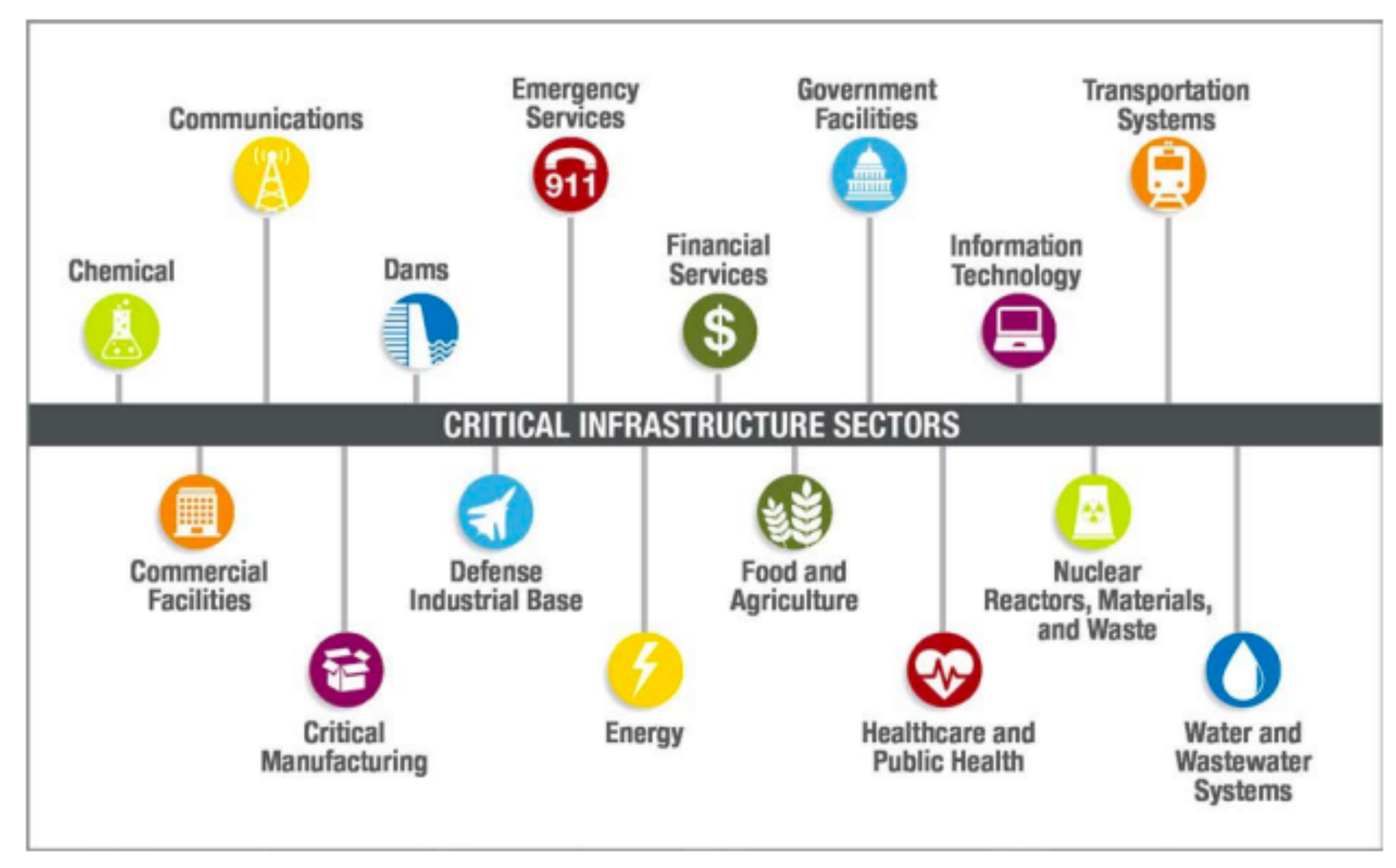
AMITT STIX

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



AMITT UPDATES AT http://misinfosec.org

Misinfosec moving forward

Community

- Support the Cognitive Security ISAO
- Continue to grow the coalition of the willing
- Contribute at misinfosec.org

Tech

- Continue to build an alert structure (ISAC, US-CERT, Interpol, Industry, etc.)
- Continue to refine AMITT framework and TTPs
- Build and connect STIX data science (“artefact” and “narrative”) layers

AMITT moving forward

- Blue Team research and exercises to explore potential inoculations and counters.
- 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

THANK YOU

Sara “SJ” Terp

MisinfosecWG / CogSec Technologies

sarajterp@gmail.com

@bodaceacat

REFERENCES

- A Room With a View. "Lord Haw Haw - Germany Calling." 04 May 2016. *YouTube.* 10 December 2018. <https://www.youtube.com/watch?v=yl3IjZ5Ut9g>.
- Boucher, Tim. "Adversarial Social Media Tactics." 10 August 2018. *Medium.* 26 December 2018. <https://medium.com/@timboucher/adversarial-social-media-tactics-e8e9857fede4 >.
- Bruce, Schneier. "Information Attacks Against Democracy." 21 November 2018. *Schneier on Security.* 15 January 2019. <https://www.schneier.com/blog/archives/2018/11/information_att.html?fbclid=IwAR3I6zYAWUmzdkPwWbX6KI-mbKPRG2gS25E5sSch_5celRUHfEaNTGerIRU>.
- Buzzfeed Video. "You Won't Believe What Obama Says in This Video." 17 April 2018. *YouTube.* 04 December 2018. <https://youtu.be/cQ54GDm1eL0 >.
- Visual Capitalist. *Visual Capitalist.* 14 May 2018. 25 January 2019. <https://www.visualcapitalist.com/wp-content/uploads/2018/05/internet-minute-share2.jpg >.
- Wahrheitsbewegung . "Obama erklärt in kürze die Neue Welt Ordnung 2016 ^^." 26 May 2014. *YouTube.* 04 December 2018. <https://www.youtube.com/watch?v=YfRtbIQ1kTw&feature=youtu.be>.
- Zou, Xinyl and Zafarani, Reza. "Fake News: A Survey of Research, Detection Methods, and Opportunities." 2 December 2018. *Cornell arXiv.* Document. 20 January 2019. <https://arxiv.org/pdf/1812.00315.pdf>.