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

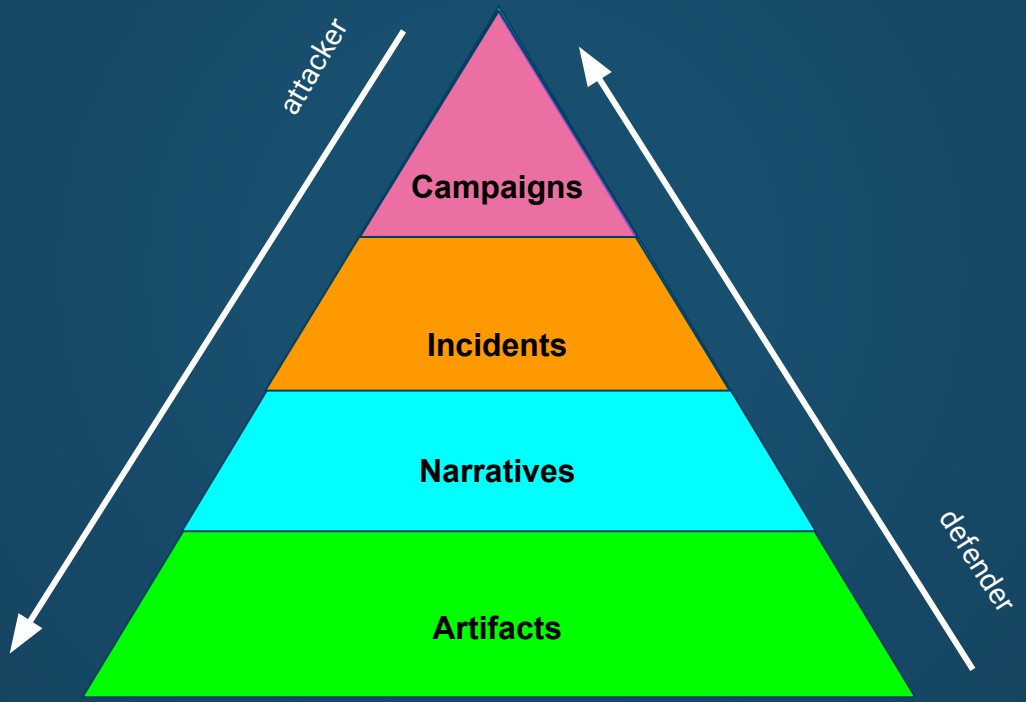
- A FRAMEWORK
- A COMMON LANGUAGE

the infrastructure behind misinfosec and what we can do with it

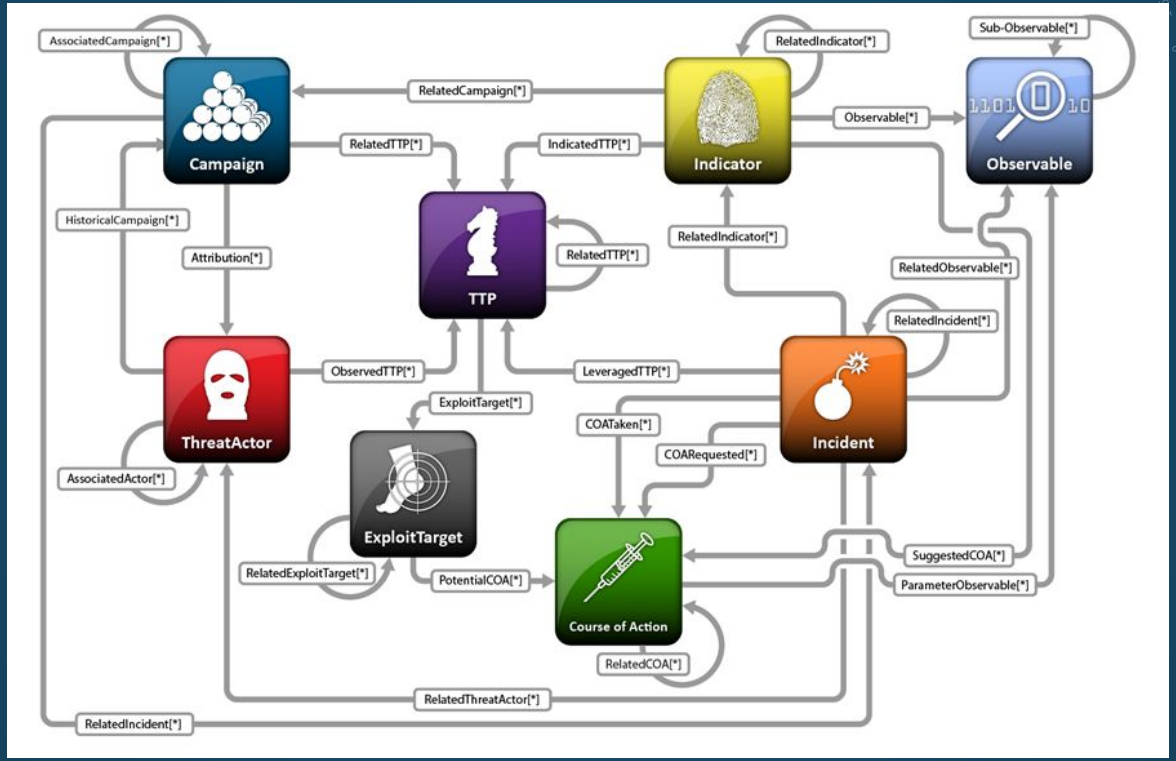
CREATING A COMMON LANGUAGE

“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.”

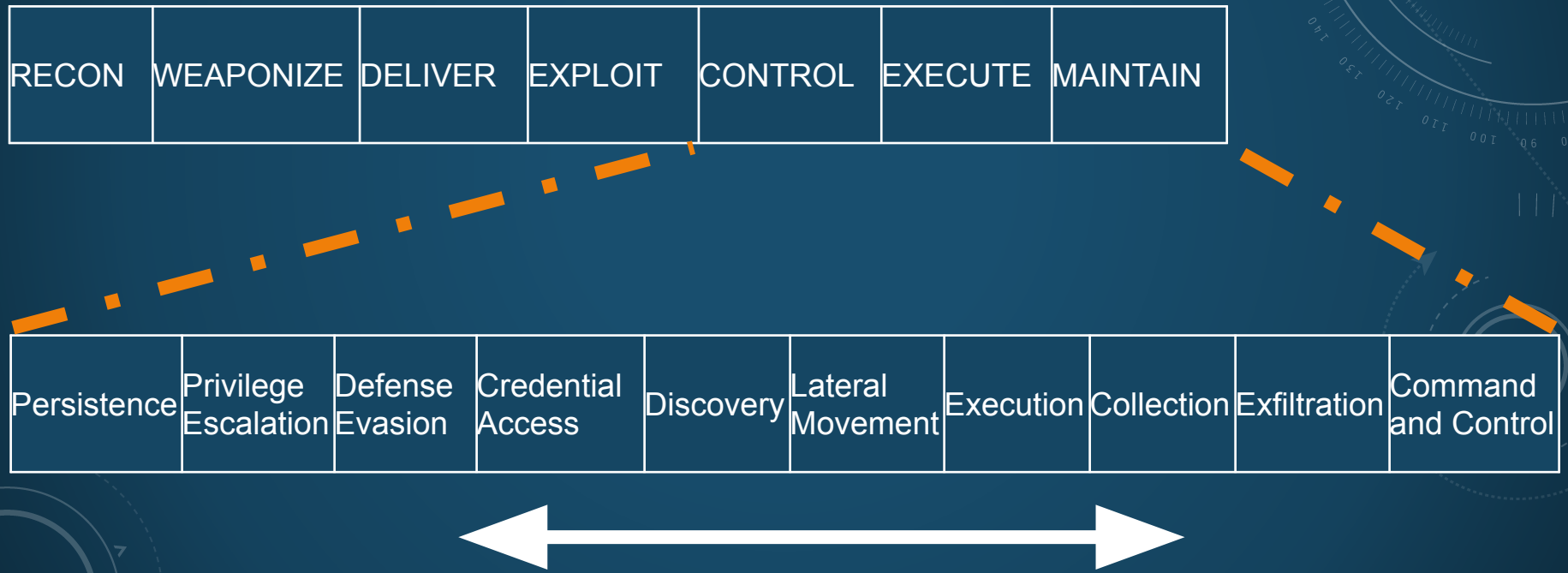
MISINFORMATION PYRAMID



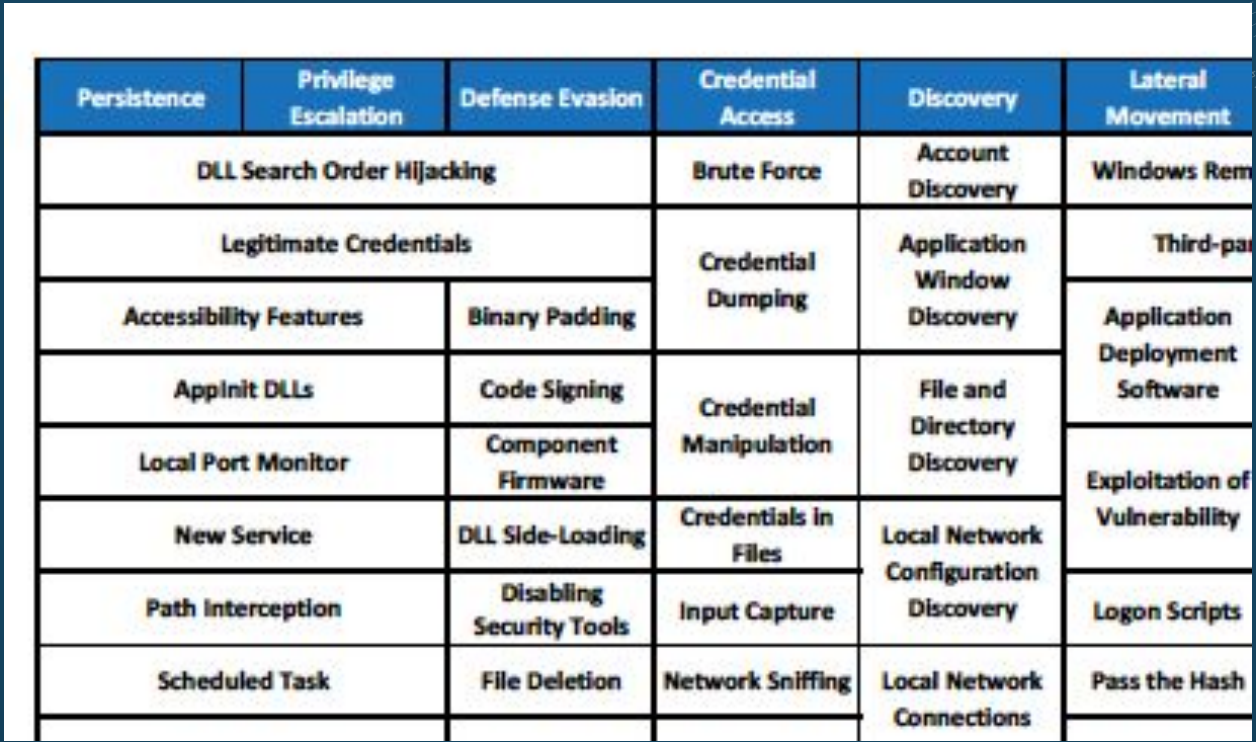
INFOSEC HAS THINGS WE CAN USE



STAGE-BASED MODELS ARE USEFUL

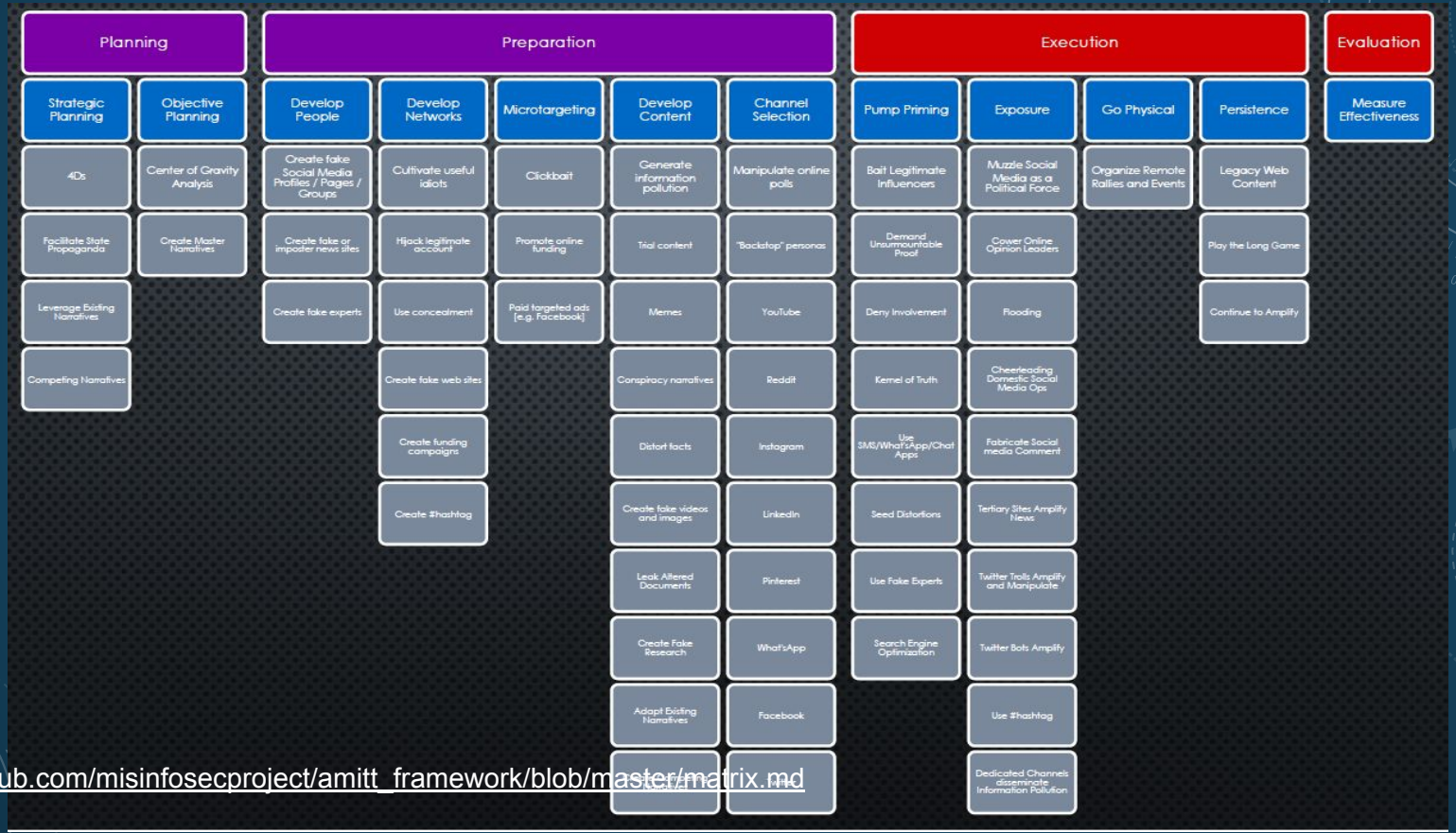


WE EXTENDED THE ATT&CK FRAMEWORK



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	
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

Version 1.0 AMITT (Adversarial Misinformation & Influence Tactics & Techniques) Framework



https://github.com/misinfosecproject/amitt_framework/blob/master/matrix.md

MISINFOSEC COMMUNITIES

misinfosec

CREDIBILITY COALITION

PEOPLE-CENTERED INTERNET

IACI
INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOS

- 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

- 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