Real-World Cases of Disinformation During Cyber Crises: Example Ghostwriter

DI.CASES.3 Stephen Campbell

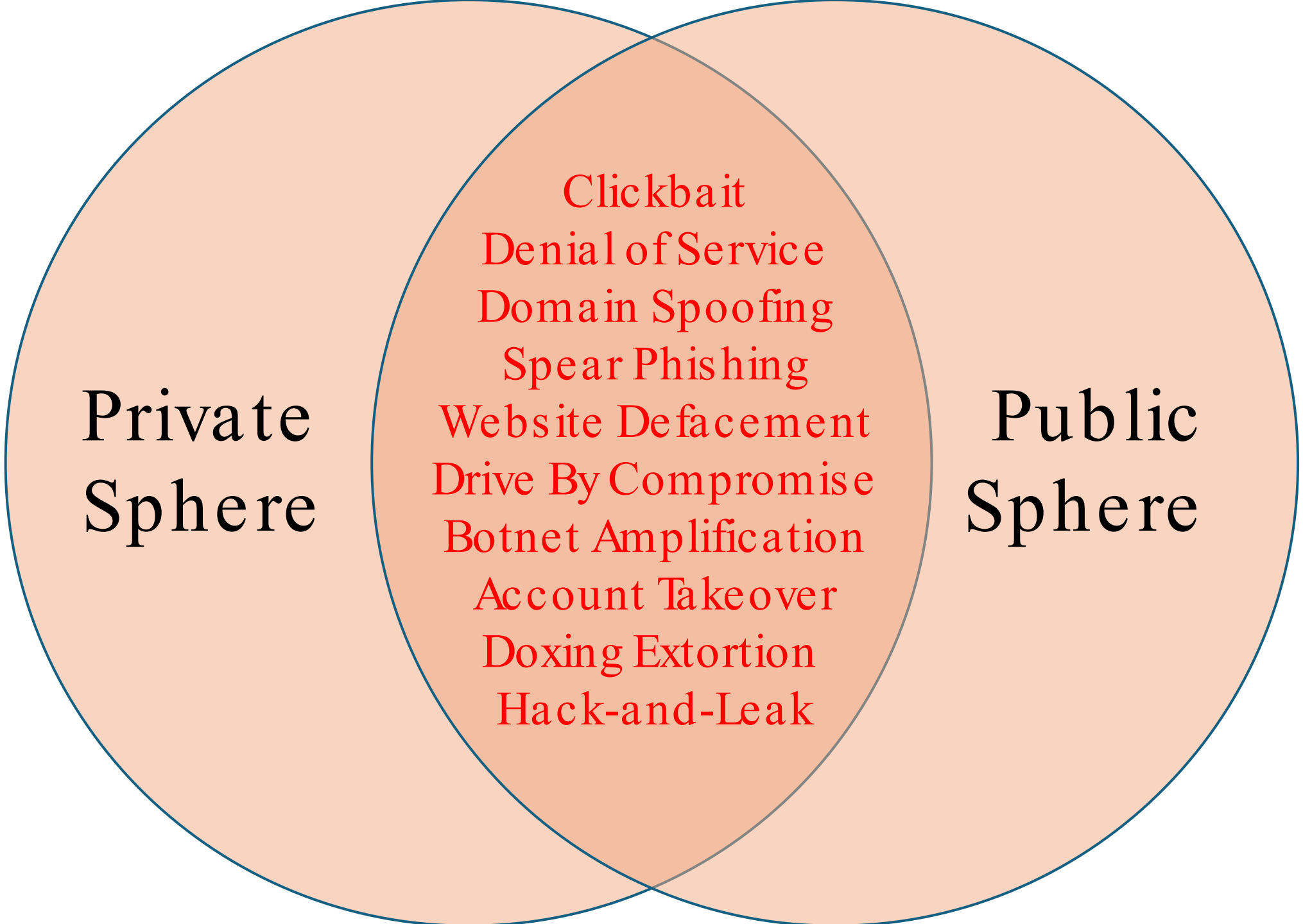
EU CYBERNET SUMMER SCHOOL 2025

Cyber Crisis Management: Navigating Disinformation and Cyber Attacks in the AI Era

EU CyberNet

Federal Foreign Office

Funded by the European Union


Private Sphere
Clickbait
Denial of Service
Domain Spoofing
Spear Phishing
Website Defacement
Drive By Compromise
Botnet Amplification
Account Takeover
Doxing Extortion
Hack-and-Leak
Public Sphere

Cyber Tactics Used in Hybrid Operations

RESOURCE DEVELOPMENT:

The adversary is trying to establish resources they can use to support operations.

Techniques:
Acquire infrastructure;
Compromise accounts;
Compromise infrastructure;
Develop capabilities;
Establish accounts;
Obtain capabilities;
Stage capabilities

INITIAL ACCESS:

The adversary is trying to get into your network.

Techniques:
Drive-by compromise;
Explot Public-Facing application;
External remote services;
Hardware additions; Phishing;
Replication though removable media; Supply chain compromise;
Trusted relationship;
Valid accounts

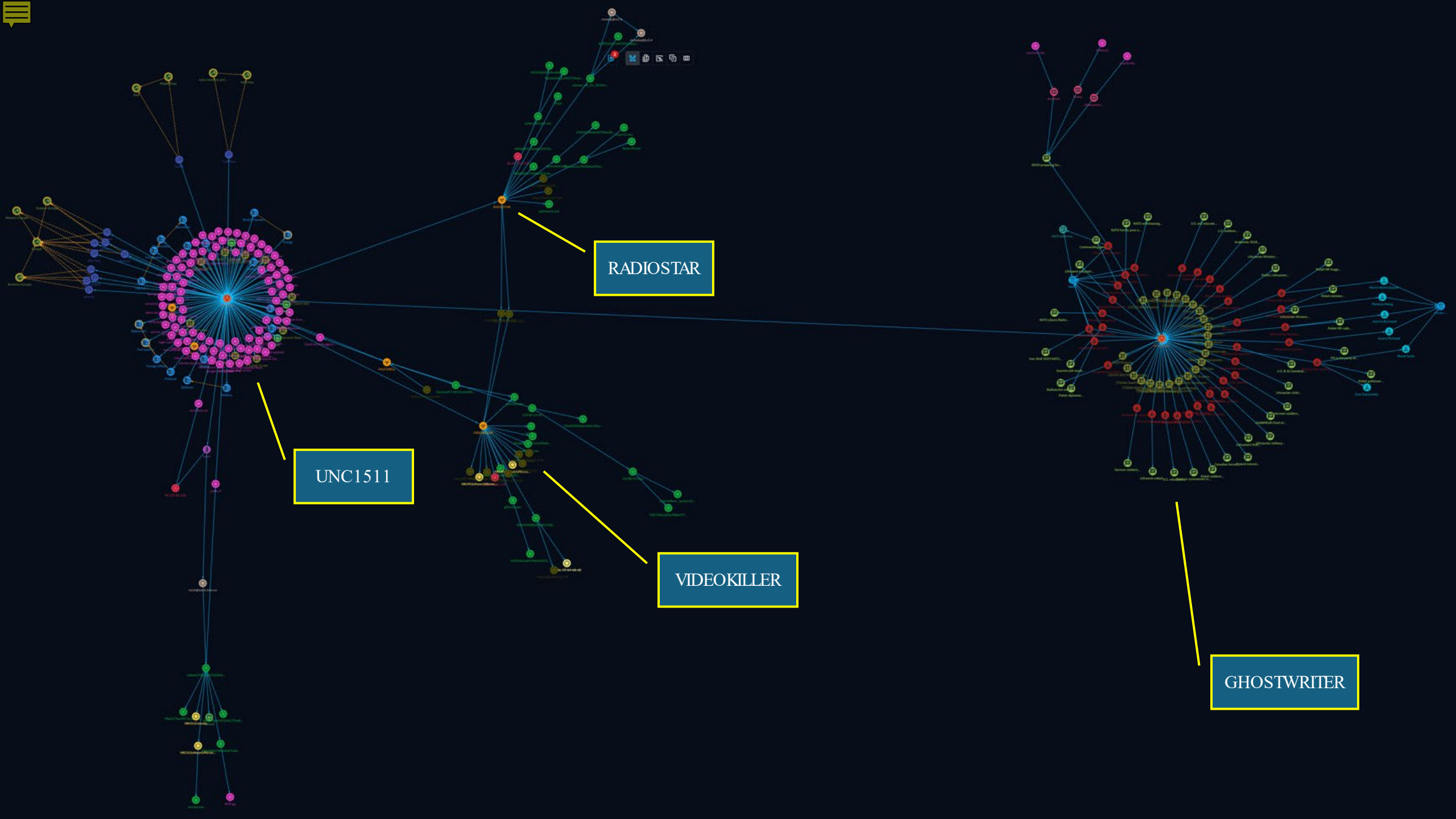
IMPACT:

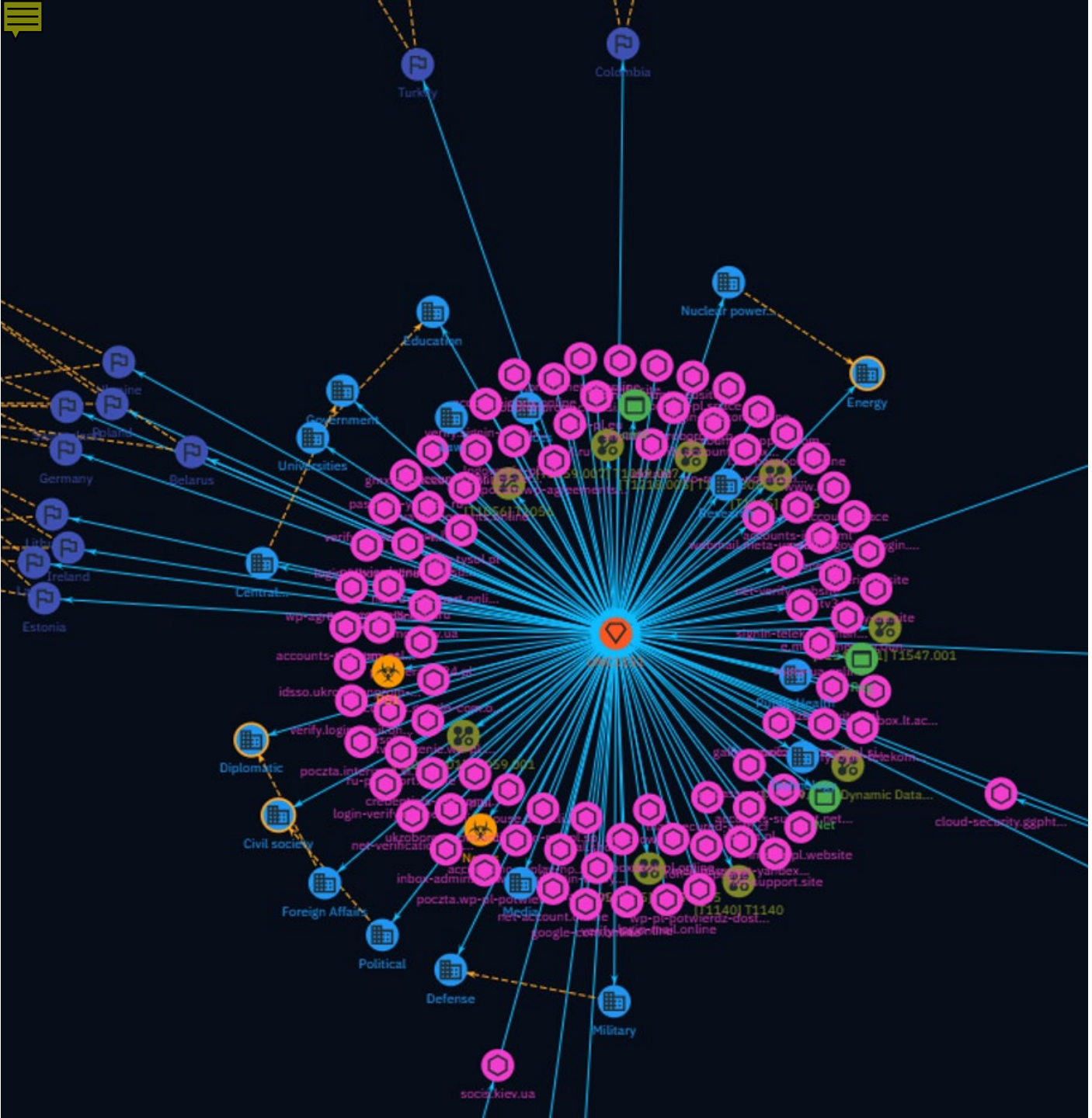
The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Techniques:
Account access removal;
Data destruction;
Data encrypted for impact;
Data manipulation; Defacement;
Disk wipe; Endpoint denial of service; Firmware corruption;
Inhibit system recovery;
Network denial of service;
Resource hijacking; Service stop;
System shutdown/reboot

Cyber Techniques Supporting Influence Tactics

CONTENT	INFRASTRUCTURE	DISSEMINATION
TA06 – Develop Content TA02 – Plan Objectives TA14 – Develop Narratives	TA16 – Establish Legitimacy TA07 – Select Channels and Affordances TA15 – Establish Social Assets	TA17 – Maximize Exposure
Obtain information that can be used (also altered) in information incidents/operations	Obtain data (e.g. e-mails addresses) that can be used to disseminate information (e.g. information flooding)	
Develop content e.g. deep fakes	Establishing legitimacy by creating new (fake) accounts or compromising existing accounts	
Carry out actions that support specific narratives e.g. stealing voter registration data	Compromise websites (e.g. news outlets) to display fake information	


RADIOSTAR
UNC1511
VIDEOKILLER
GHOSTWRITER

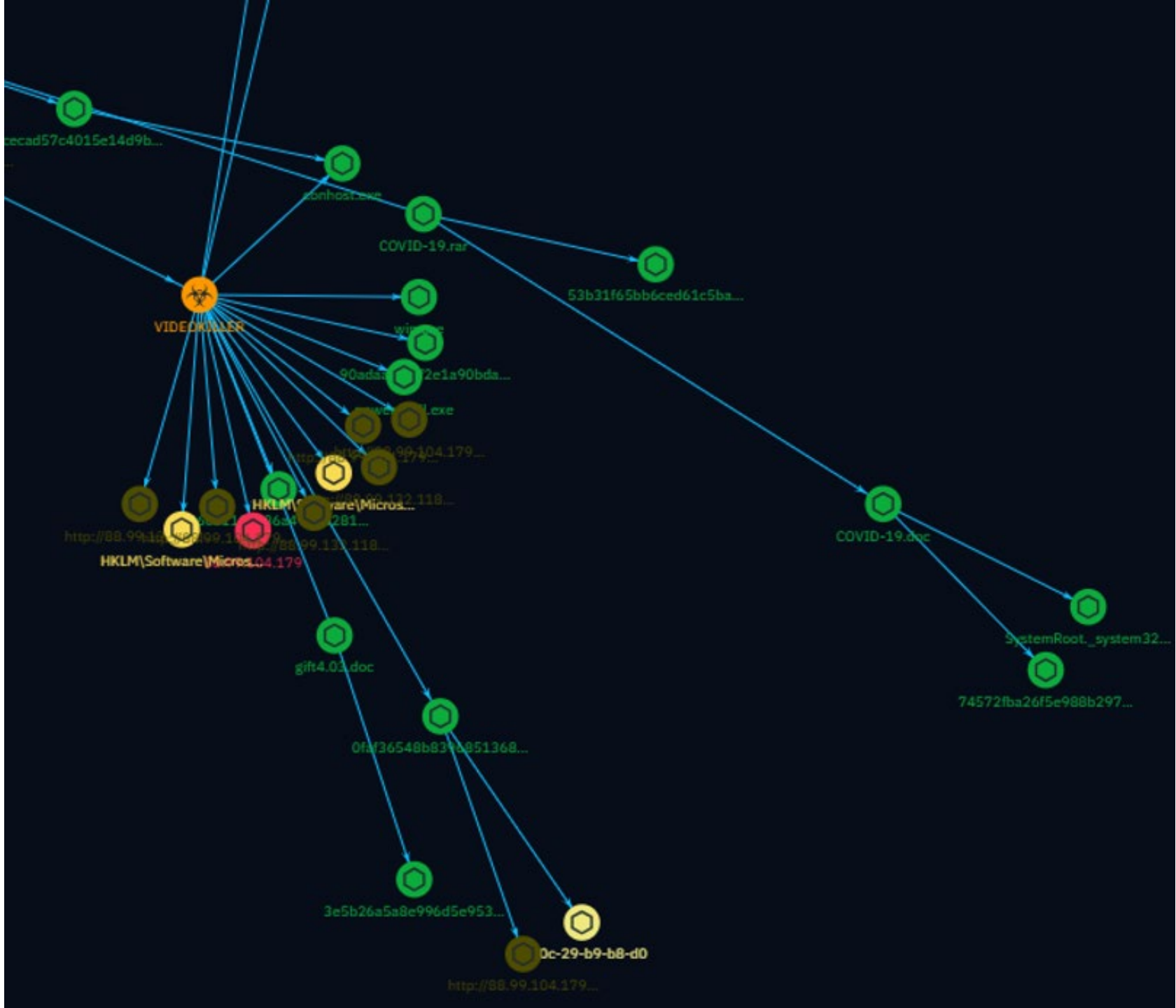


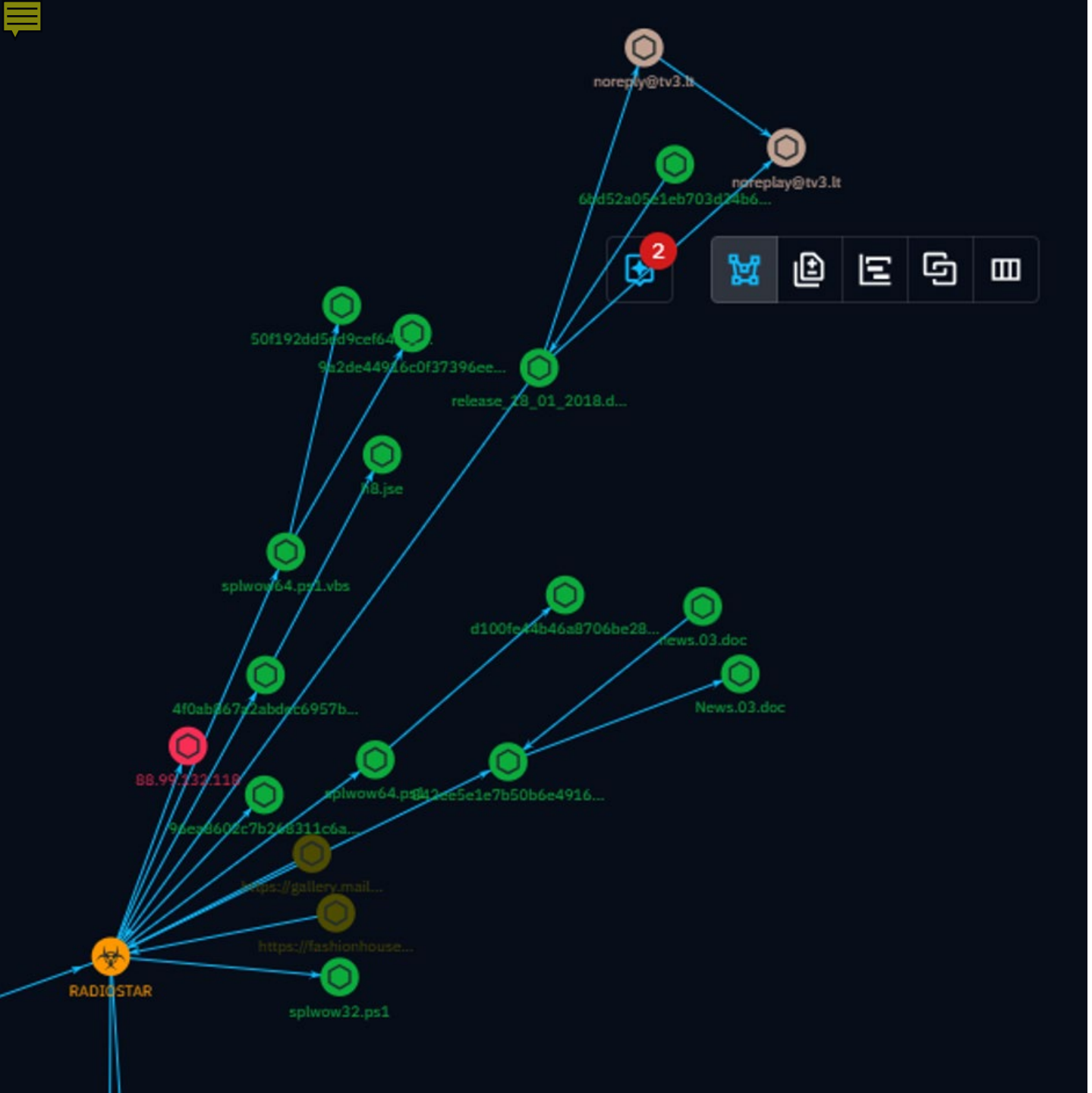
UNC1511

- Intrusion Set responsible for credentials harvesting and malware distribution
- Pink icons are phishing sites
- Green icons are ATT&CK TTPs
- Light blue icons are targeted sectors
- Dark blue icons are targeted countries
- Orange icons are malware

VIDEOKILLER

- Malware dropped after user clicks on a document in email promising a gift
- A.NET backdoor masquerading as conhost.exe
- Maintains persistence by modifying the registry
- Purpose believed to be espionage



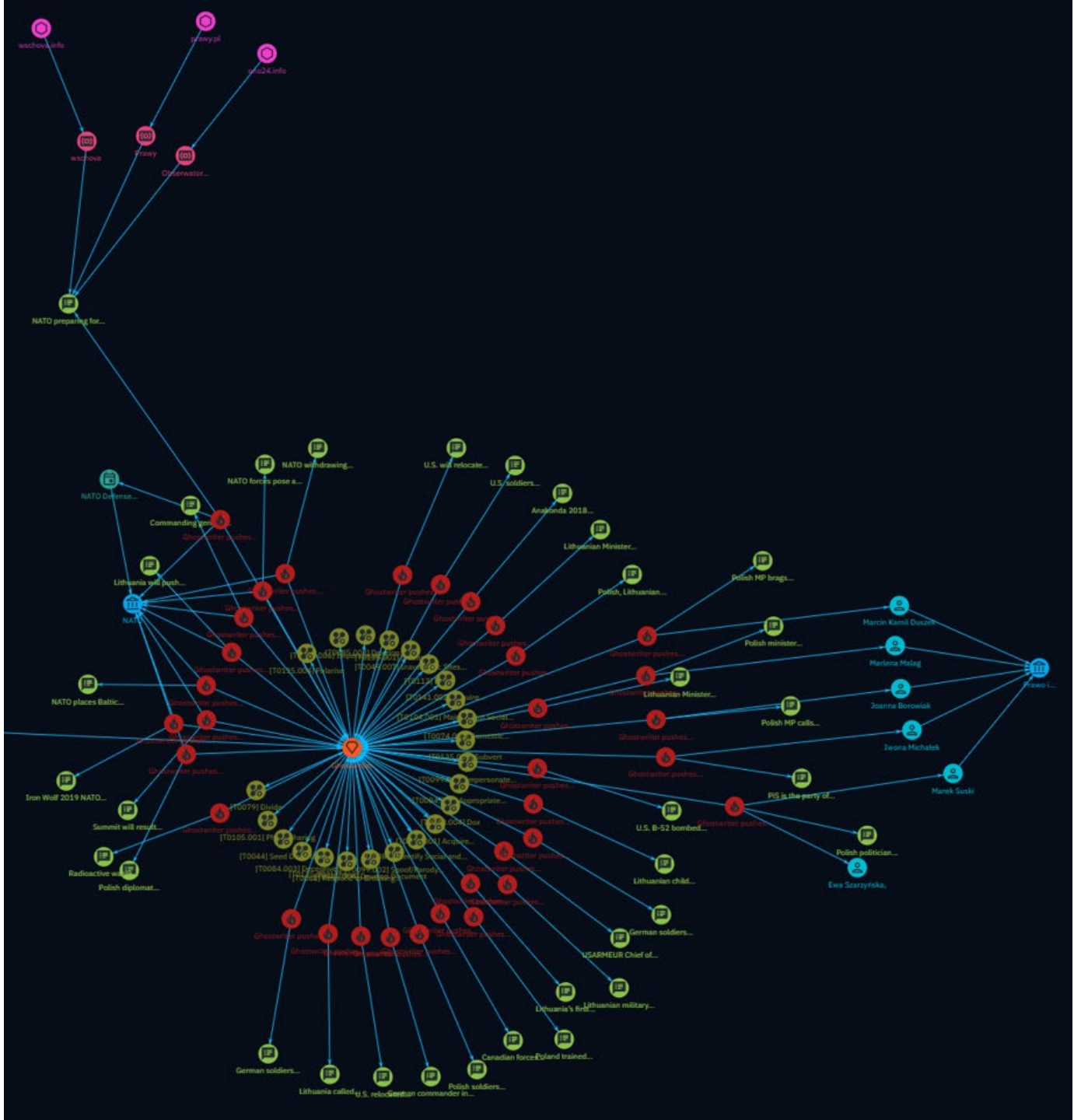


RADIOSTAR

- Malware dropped after user clicks on a document claiming to be a press release
- A PowerShell backdoor downloaded via a VBS script
- Maintains persistence by modifying the registry
- Purpose believed to be espionage

GHOSTWRITER

- Intrusion Set aiming to discredit the Polish government and weaken support for NATO in the Baltics
- Publishes forged documents on hacked media and government websites
- Amplifies forged documents using hacked social media accounts of leading politicians
- Inner icons in green arer DISARM techniques
- Red icons are incidents
- Light green icons are false narratives
- Light blue icons are targets



mandiant_ghostwriter_update_report

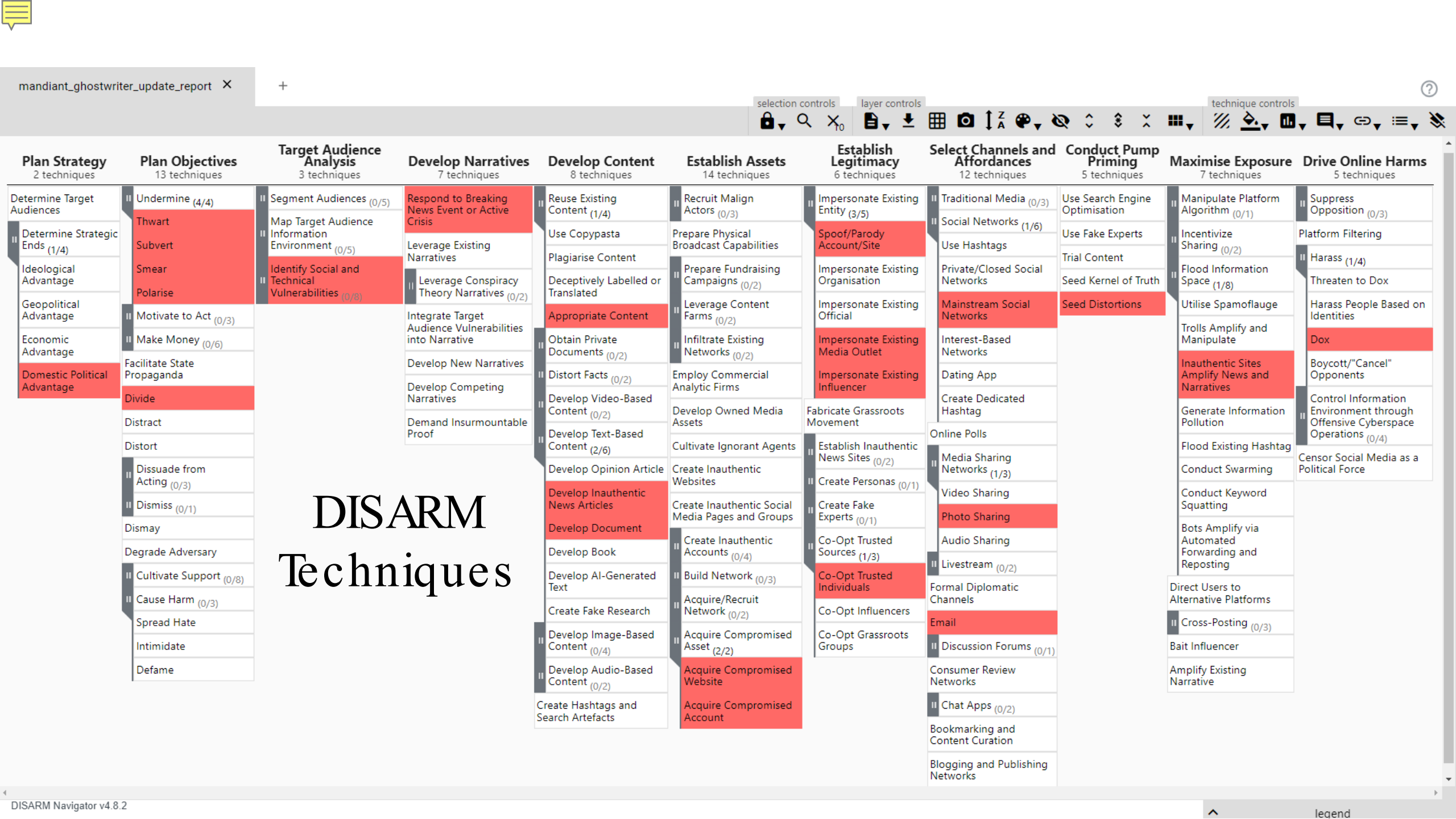
selection controls | layer controls | technique controls

Resource Development 8 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 14 techniques	Defense Evasion 13 techniques	Credential Access 17 techniques	Command and Control 18 techniques	Impact 14 techniques
Acquire Access	Content Injection	Cloud Administration Command	BITS Jobs	BITS Jobs	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Account Access Removal
Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (3/10)	Boot or Logon Autostart Execution (1/1)	Build Image on Host	Brute Force (0/4)	Communication Through Removable Media	Data Destruction
Compromise Accounts (2/3)	Exploit Public-Facing Application	AppleScript	Registry Run Keys / Startup Folder	Debugger Evasion	Credentials from Password Stores (0/6)	Content Injection	Data Encrypted for Impact
Cloud Accounts	External Remote Services	AutoHotKey & AutoIT	Browser Extensions	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Data Encoding (0/2)	Data Manipulation (0/3)
Email Accounts	Hardware Additions	Cloud API	Compromise Host Software Binary	Deploy Container	Forced Authentication	Data Obfuscation (0/3)	Defacement (0/2)
Social Media Accounts	Phishing (1/4)	JavaScript	Create Account (0/3)	Direct Volume Access	Forge Web Credentials (0/2)	Dynamic Resolution (0/3)	Disk Wipe (0/2)
Compromise Infrastructure (1/8)	Spearphishing Attachment	Network Device CLI	External Remote Services	Execution Guardrails (0/1)	Input Capture (0/4)	Encrypted Channel (0/2)	Endpoint Denial of Service (0/4)
Botnet	Spearphishing Link	PowerShell	Hijack Execution Flow (1/1)	Exploitation for Defense Evasion	Modify Authentication Process (0/9)	Fallback Channels	Financial Theft
DNS Server	Spearphishing via Service	Python	Dynamic Linker Hijacking	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Interception	Hide Infrastructure	Firmware Corruption
Domains	Spearphishing Voice	Unix Shell	Implant Internal Image	Hide Artifacts (0/12)	Multi-Factor Authentication Request Generation	Ingress Tool Transfer	Inhibit System Recovery
Network Devices	Replication Through Removable Media	Visual Basic	Modify Authentication Process (0/9)	Hijack Execution Flow (1/1)	Network Sniffing	Multi-Stage Channels	Network Denial of Service (0/2)
Server	Supply Chain Compromise (0/3)	Windows Command Shell	Office Application Startup (0/6)	Dynamic Linker Hijacking	OS Credential Dumping (0/8)	Non-Application Layer Protocol	Resource Hijacking
Serverless	Trusted Relationship	Container Administration Command	Power Settings	Masquerading (0/9)	Steal Application Access Token	Non-Standard Port	Service Stop
Virtual Private Server		Deploy Container	Pre-OS Boot (0/5)	System Binary Proxy Execution (1/14)	Steal or Forge Authentication Certificates	Protocol Tunneling	System Shutdown/Reboot
Web Services		Exploitation for Client Execution	Server Software Component (0/5)	CMSTP	Steal or Forge Kerberos Tickets (0/4)	Proxy (0/4)	
Develop Capabilities (0/4)		Inter-Process Communication (1/3)	Traffic Signaling (0/2)	Compiled HTML File	Steal Web Session Cookie	Remote Access Software	
Establish Accounts (0/3)		Component Object Model		Control Panel	Unsecured Credentials (0/8)	Traffic Signaling (0/2)	
Obtain Capabilities (0/7)		Dynamic Data Exchange		Electron Applications		Web Service (0/3)	
Stage Capabilities (0/6)		XPC Services		InstallUtil			
		Native API		Mavinject			
		Serverless Execution		MMC			
		Shared Modules		Mshta			
		Software Deployment Tools		Msiexec			
		System Services (0/2)		Odbcconf			
		User Execution (0/3)		Regsvcs/Regasm			
		Windows Management Instrumentation		Regsvr32			
				Rundll32			
				Verclsid			

ATT&CK Techniques

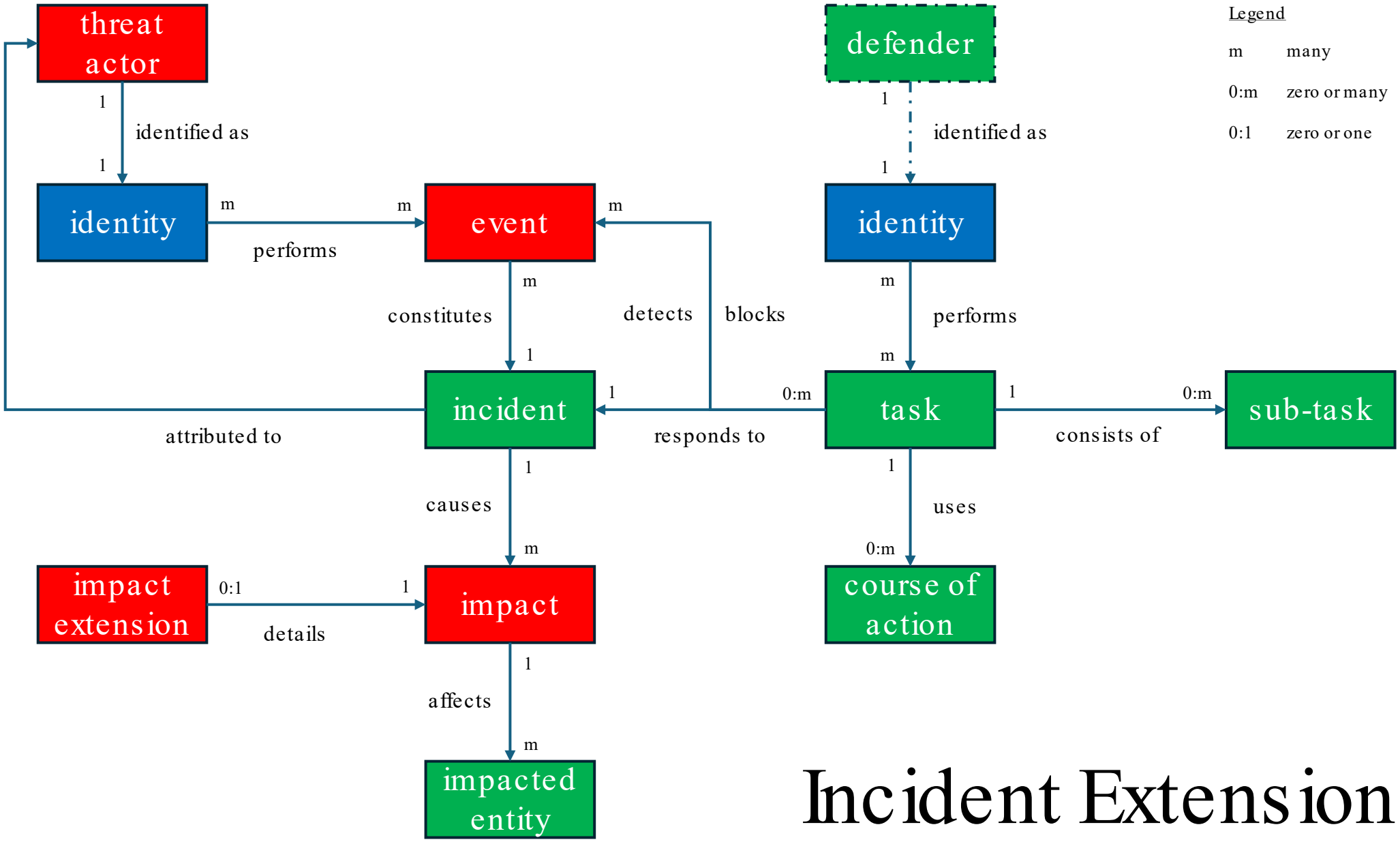
MITRE ATT&CK® Navigator v5.0.1

legend

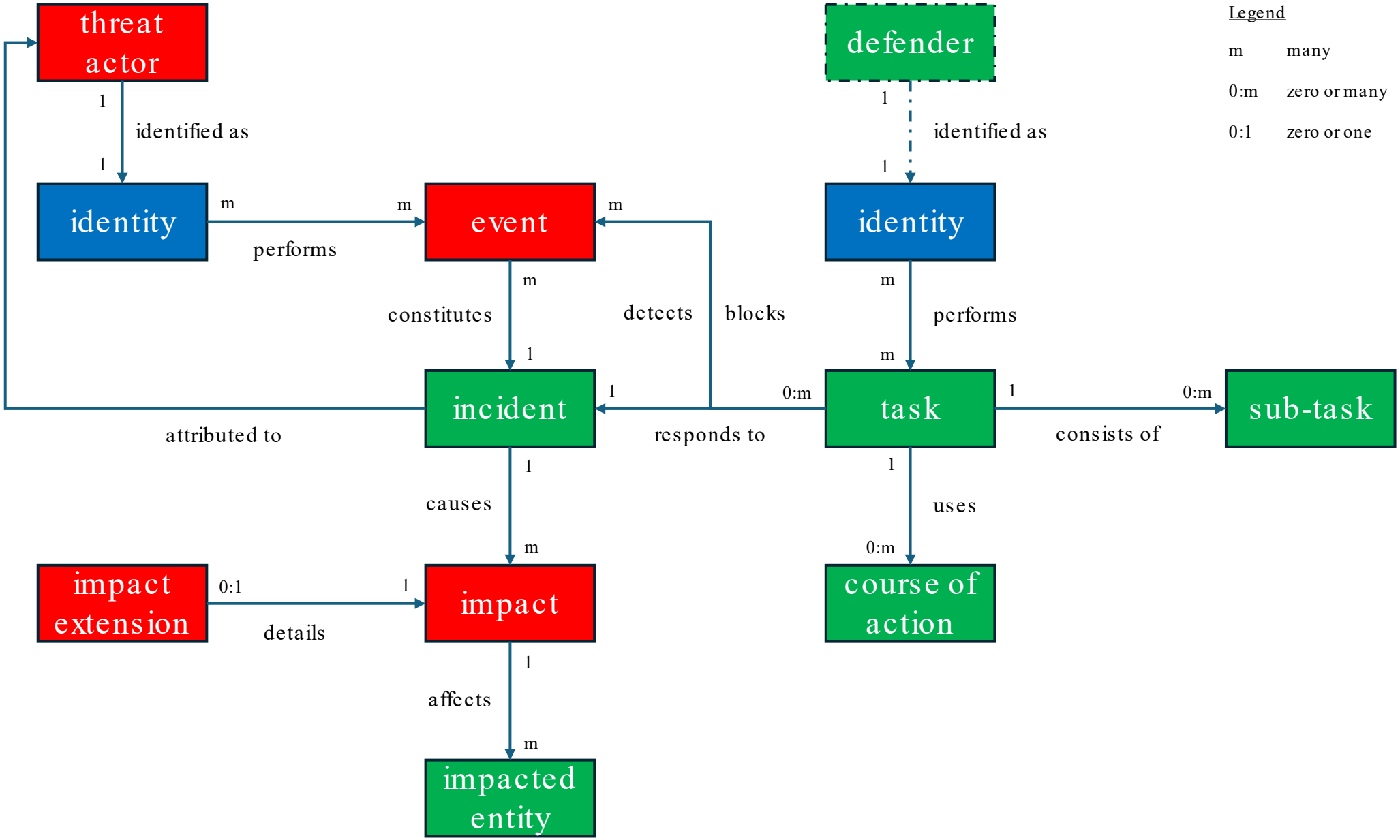

mandiant_ghostwriter_update_report
selection controls
layer controls
technique controls
Plan Strategy
2 techniques
Determine Target Audiences
Determine Strategic Ends (1/4)
Ideological Advantage
Geopolitical Advantage
Economic Advantage
Domestic Political Advantage
Plan Objectives
13 techniques
Undermine (4/4)
Thwart
Subvert
Smear
Polarise
Motivate to Act (0/3)
Make Money (0/6)
Facilitate State Propaganda
Divide
Distract
Distort
Dissuade from Acting (0/3)
Dismiss (0/1)
Dismay
Degrade Adversary
Cultivate Support (0/8)
Cause Harm (0/3)
Spread Hate
Intimidate
Defame
Target Audience Analysis
3 techniques
Segment Audiences (0/5)
Map Target Audience Information Environment (0/5)
Identify Social and Technical Vulnerabilities (0/8)
Develop Narratives
7 techniques
Respond to Breaking News Event or Active Crisis
Leverage Existing Narratives
Leverage Conspiracy Theory Narratives (0/2)
Integrate Target Audience Vulnerabilities into Narrative
Develop New Narratives
Develop Competing Narratives
Demand Insurmountable Proof
Develop Content
8 techniques
Reuse Existing Content (1/4)
Use Copypasta
Plagiarise Content
Deceptively Labelled or Translated
Appropriate Content
Obtain Private Documents (0/2)
Distort Facts (0/2)
Develop Video-Based Content (0/2)
Develop Text-Based Content (2/6)
Develop Opinion Article
Develop Inauthentic News Articles
Develop Document
Develop Book
Develop AI-Generated Text
Create Fake Research
Develop Image-Based Content (0/4)
Develop Audio-Based Content (0/2)
Create Hashtags and Search Artefacts
Establish Assets
14 techniques
Recruit Malign Actors (0/3)
Prepare Physical Broadcast Capabilities
Prepare Fundraising Campaigns (0/2)
Leverage Content Farms (0/2)
Infiltrate Existing Networks (0/2)
Employ Commercial Analytic Firms
Develop Owned Media Assets
Cultivate Ignorant Agents
Create Inauthentic Websites
Create Inauthentic Social Media Pages and Groups
Create Inauthentic Accounts (0/4)
Build Network (0/3)
Acquire/Recruit Network (0/2)
Acquire Compromised Asset (2/2)
Acquire Compromised Website
Acquire Compromised Account
Establish Legitimacy
6 techniques
Impersonate Existing Entity (3/5)
Spoof/Parody Account/Site
Impersonate Existing Organisation
Impersonate Existing Official
Impersonate Existing Media Outlet
Impersonate Existing Influencer
Fabricate Grassroots Movement
Establish Inauthentic News Sites (0/2)
Create Personas (0/1)
Create Fake Experts (0/1)
Co-Opt Trusted Sources (1/3)
Co-Opt Trusted Individuals
Co-Opt Influencers
Co-Opt Grassroots Groups
Select Channels and Affordances
12 techniques
Traditional Media (0/3)
Social Networks (1/6)
Use Hashtags
Private/Closed Social Networks
Mainstream Social Networks
Interest-Based Networks
Dating App
Create Dedicated Hashtag
Online Polls
Media Sharing Networks (1/3)
Video Sharing
Photo Sharing
Audio Sharing
Livestream (0/2)
Formal Diplomatic Channels
Email
Discussion Forums (0/1)
Consumer Review Networks
Chat Apps (0/2)
Bookmarking and Content Curation
Blogging and Publishing Networks
Conduct Pump Priming
5 techniques
Use Search Engine Optimisation
Use Fake Experts
Trial Content
Seed Kernel of Truth
Seed Distortions
Maximise Exposure
7 techniques
Manipulate Platform Algorithm (0/1)
Incentivize Sharing (0/2)
Flood Information Space (1/8)
Utilise Spamoflauge
Trolls Amplify and Manipulate
Inauthentic Sites Amplify News and Narratives
Generate Information Pollution
Flood Existing Hashtag
Conduct Swarming
Conduct Keyword Squatting
Bots Amplify via Automated Forwarding and Reposting
Direct Users to Alternative Platforms
Cross-Posting (0/3)
Bait Influencer
Amplify Existing Narrative
Drive Online Harms
5 techniques
Suppress Opposition (0/3)
Platform Filtering
Harass (1/4)
Threaten to Dox
Harass People Based on Identities
Dox
Boycott/"Cancel" Opponents
Control Information Environment through Offensive Cyberspace Operations (0/4)
Censor Social Media as a Political Force
DISARM Techniques
DISARM Navigator v4.8.2
legend

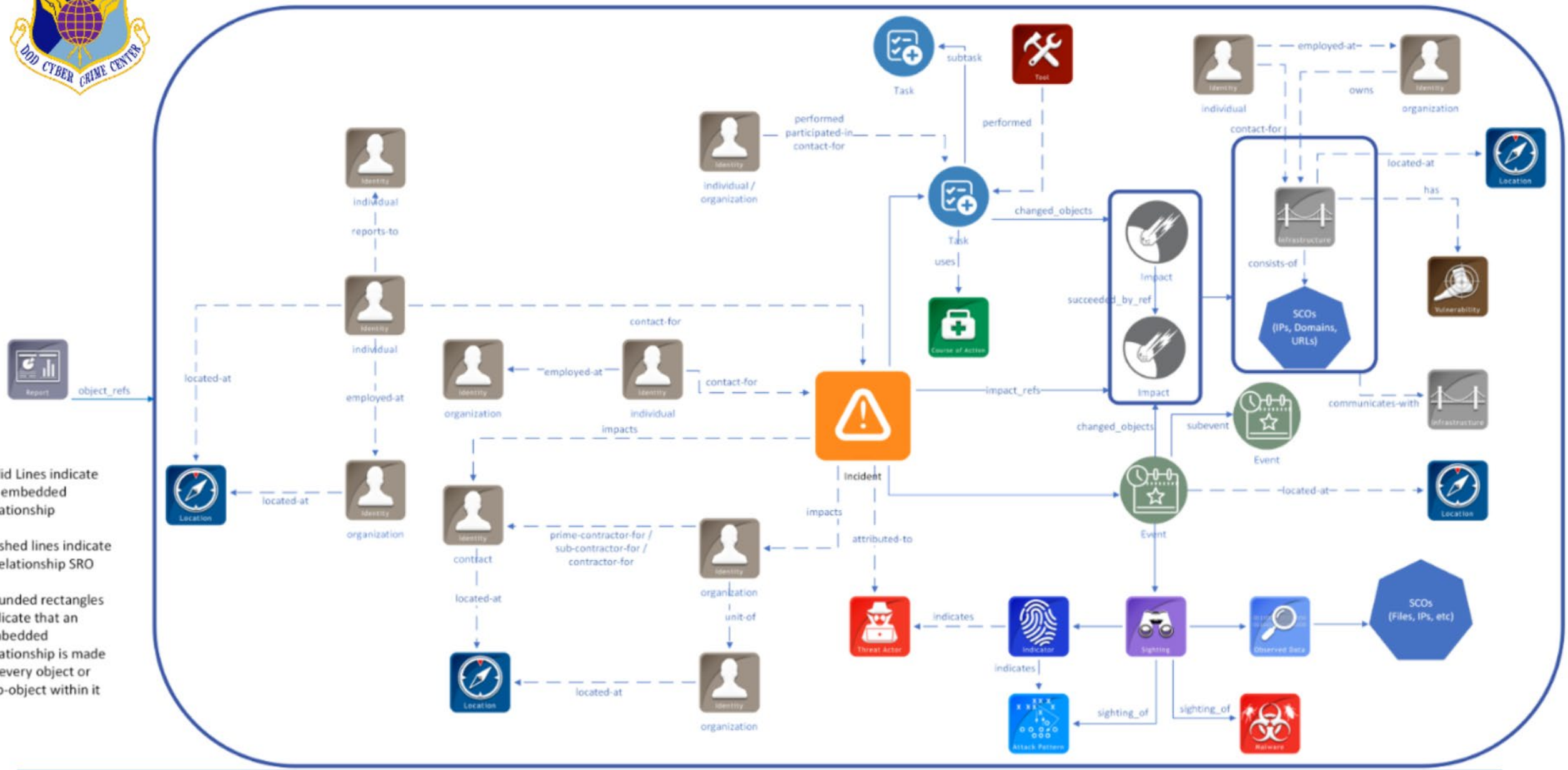
Gap Analysis

- Clashes with incident extension suite
  - Use “Incident Attack” or “Information Operation” instead of “Incident”?
  - Proposed “Real-World Event” SDO?
- Overlap between “Channel” and “Domain”, “URL”, “Account”
  - Defining “Channel”: platforms vs. community vs. account
  - Need “Platform type” open vocabulary
  - Properties differ - subtype-extensions for different platforms?
  - How do we minimize redundancy and trivial SROs?
- Threat actor
  - “Intrusion Set” -> “Manipulation Set”?
  - Need new relationships to model proxies e.g. outsources, sponsors, directs etc
  - Need “Threat Actor individual” and associated relationships e.g. employs
  - Need SRO for “attributed-to” with properties for levels of attribution and associated taxonomy, and embedded relationships to sighings / observations



Incident Extension Suite


threat actor
identified as
identity
performs
event
constitutes
detects
blocks
incident
attributed to
responds to
causes
impact extension
details
impact
affects
impacted entity
defender
identified as
identity
performs
task
consists of
sub-task
uses
course of action
Legend
m many
0:m zero or many
0:1 zero or one

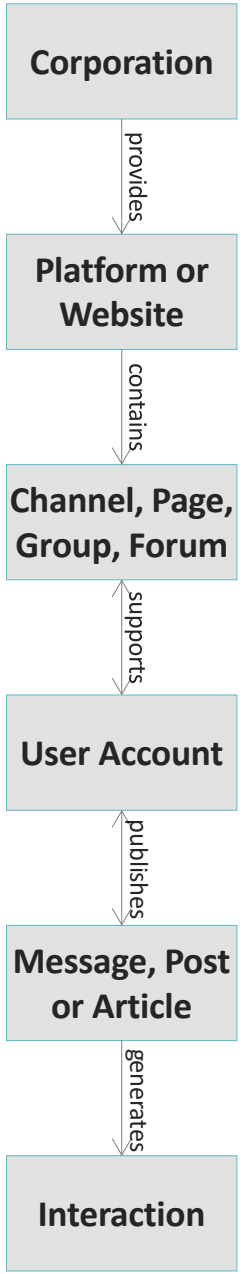


Solid Lines indicate an embedded relationship

Dashed lines indicate a relationship SRO

Rounded rectangles indicate that an embedded relationship is made to every object or sub-object within it

Refining Channel



Technology companies and internet service providers

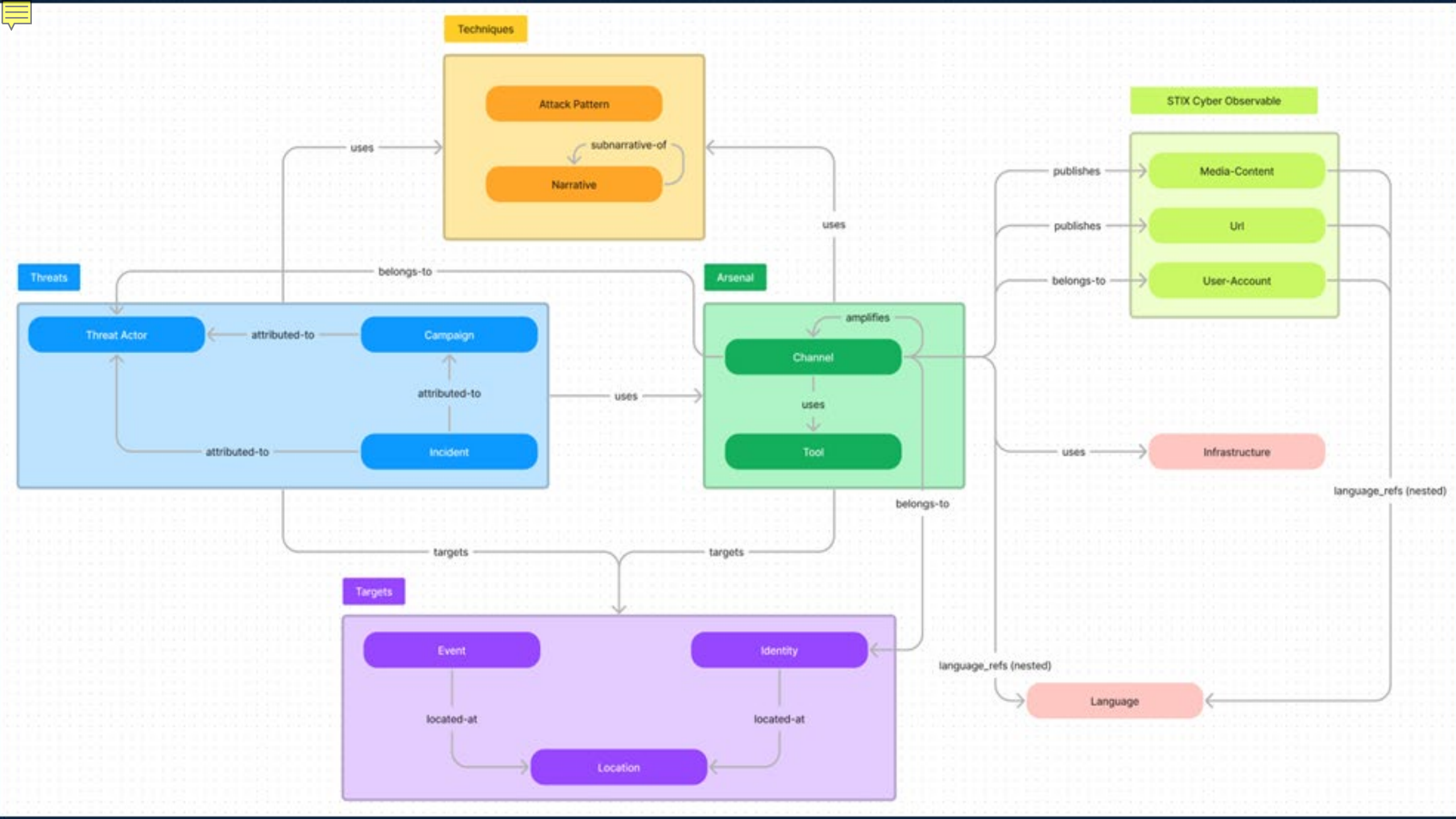
Need platform-type-ov. Include offine media such as TV? If so would the layer below be “program”?

How do we define this layer of the structure? SIOC uses “container” but channel is more intuitive.

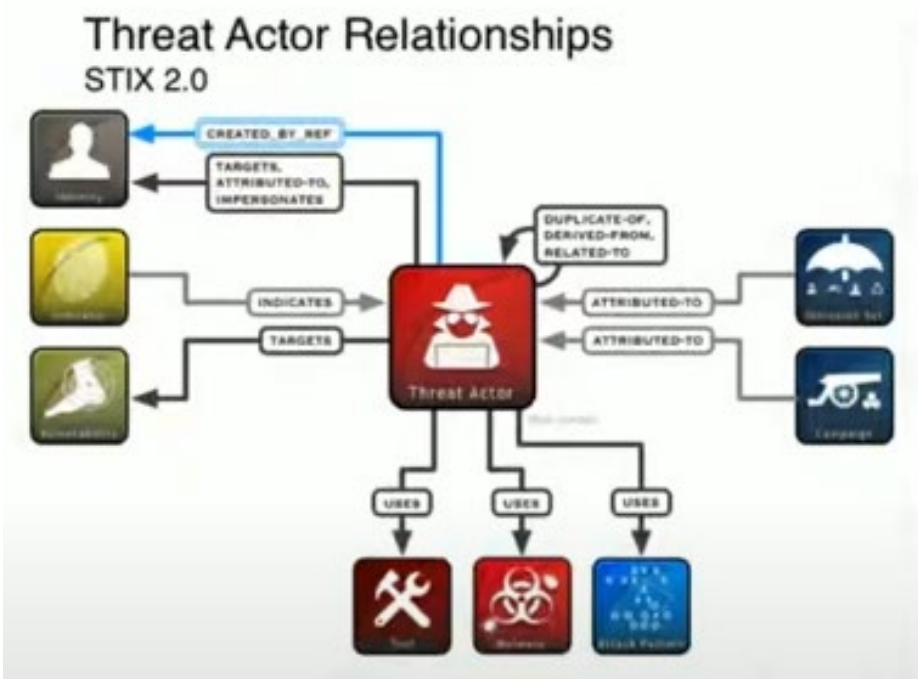
Can we extend the “account” SCO with properties to model profiles, validation, followers etc?

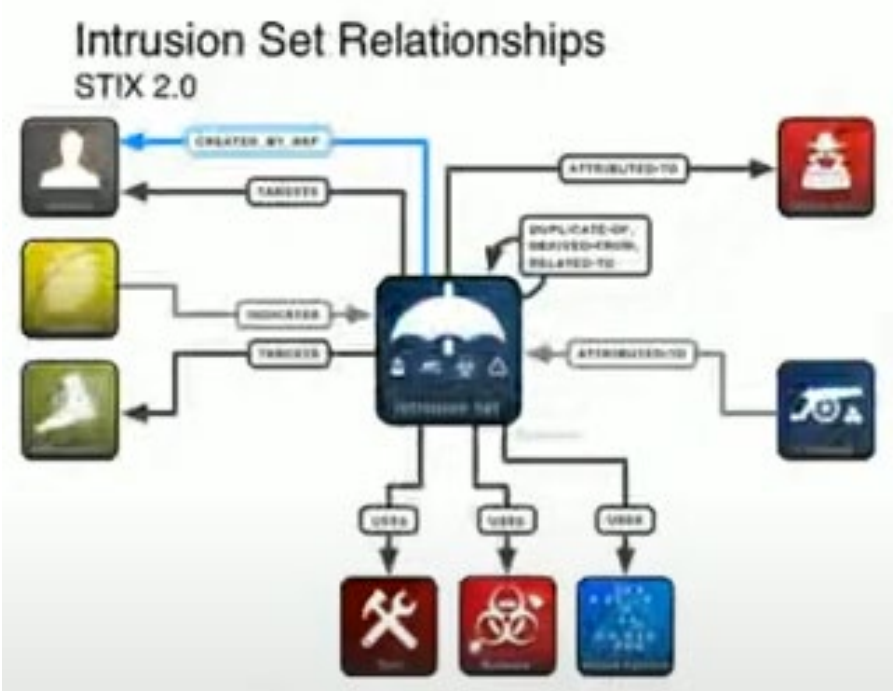
The container for a post is separate from its media-content e.g. it may have a tweet ID

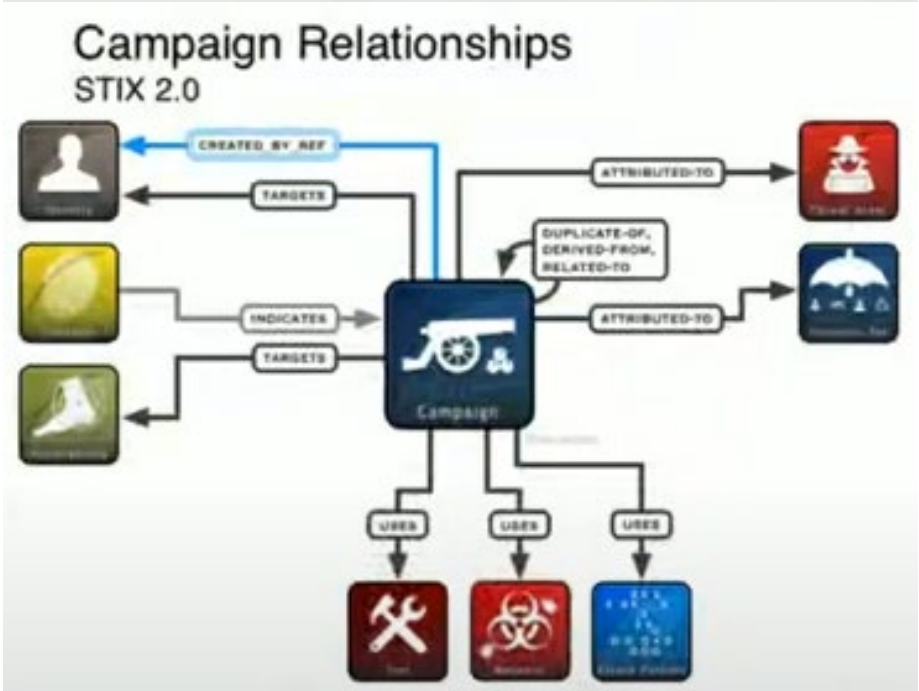
Comments, likes, shares, retweets are special types of posts; perhaps a post-type-ov would suffice


Techniques
Attack Pattern
subnarrative-of
Narrative
uses
uses
STIX Cyber Observable
publishes
Media-Content
publishes
Url
belongs-to
User-Account
Threats
belongs-to
Arsenal
Threat Actor
attributed-to
Campaign
amplifies
Channel
attributed-to
uses
uses
Tool
attributed-to
Incident
uses
Infrastructure
language_refs (nested)
belongs-to
targets
targets
Targets
Event
Identity
language_refs (nested)
located-at
located-at
Language
Location


STIX 2.0 Threat Actor Summary
Threat Actor Labels
Goals
Motivations
Activist
Competitor
Crime Syndicate
Criminal
Hacker
Insider Accidental
Insider Disgruntled
Nation State
Sensationalist
Spy
Terrorist
Sophistication Level
None
Minimal
Intermediate
Advanced
Expert
Innovator
Strategic
Threat Actor
Resource Level
Individual
Club
Contest
Team
Organization
Government
Identity Class
individual
group
organization
class
unknown
Role
Agent
Director
Independent
Infrastructure Architect
Infrastructure Operator
Malware Author
Sponsor
Accidental
Coercion
Dominance
Ideology
Notoriety
Organizational Gain
Personal Gain
Personal Satisfaction
Revenge
Unpredictable


Threat Actor Relationships
STIX 2.0
CREATED_BY_REF
TARGETS, ATTRIBUTED-TO, IMPERSONATES
DUPLICATE-OF, DERIVED-FROM, RELATED-TO
INDICATES
TARGETS
ATTRIBUTED-TO
ATTRIBUTED-TO
Threat Actor
USES
USES
USES


Intrusion Set Relationships
STIX 2.0
CREATED_BY_REF
TARGETS
ATTRIBUTED-TO
DUPLICATE-OF, DERIVED-FROM, RELATED-TO
INDICATES
TARGETS
ATTRIBUTED-TO
USES
USES
USES


Campaign Relationships
STIX 2.0
CREATED_BY_REF
TARGETS
ATTRIBUTED-TO
DUPLICATE-OF, DERIVED-FROM, RELATED-TO
INDICATES
TARGETS
ATTRIBUTED-TO
Campaign
USES
USES
USES