



# Hands on Threat Modeling with Open CTI

*Stephen Campbell and Julian Neylan DISARM Foundation*

EU CYBERNET SUMMER SCHOOL

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



Federal Foreign Office



Funded by  
the European Union

# Access Open CTI

## Specific Real World Examples

Recent Cases of Disinformation

Recent Cyber Incidents with Disinformation

Historic Cyber Incidents with Disinformation

LetsData Alerts

## Tools to Investigate Disinformation

Bellingcat's Online investigation Toolkit

EU Disinfo Lab Tools to Monitor Disinformation

EU Disinfo Lab AI Disinfo Hub

NewsGuard AI Tracking Center

DISARM Foundation's OpenCTI Instance

## Incident Databases

Cyber Incidents

FIMI Incidents

AI Incidents



<https://scampb06.github.io/ss25/>

# Case Study RRN

RRN is a Russia attributed campaign designed to weaken European support for Ukraine by insisting that sanctions are ineffective, Ukrainian forces are unethical and that Russophobia is prevalent

Detected since spring/summer 2022, active through at least mid-2023



# Features of the Campaign

1. Cloned websites (sites pretending to be 20 Minutes, Le Monde, Le Parisien, Le Figaro, and even the French MFA)
2. Social assets (Twitter and Facebook Accounts) especially bots
3. Satirical Cartoons

# Example fake website



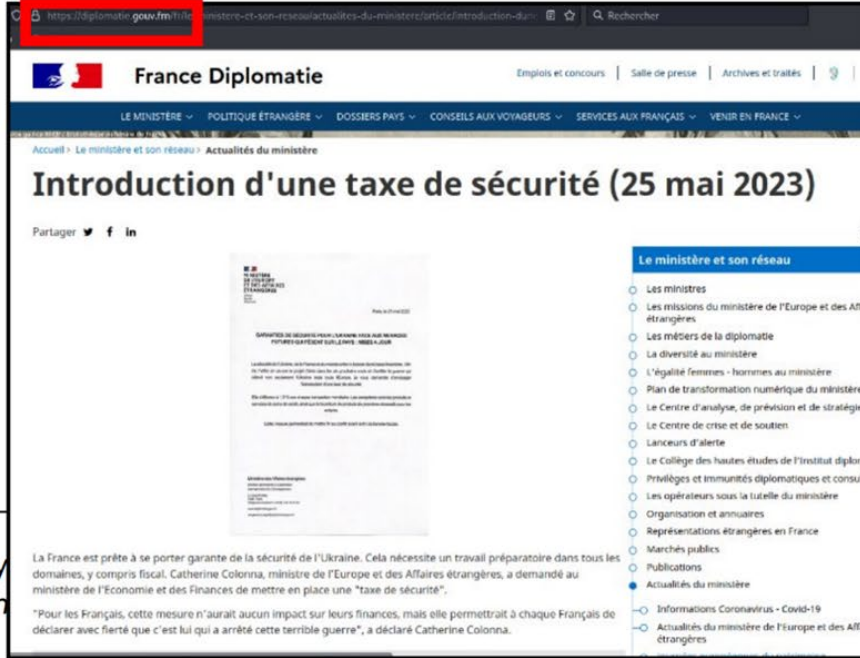
Article published on the typosquatted version of 20 Minutes  
(source: 20minuts[.]com)



Article published on the RRR website (source: rrr[.]world)



# French Government impersonated



32 Germany  
33 leparisien

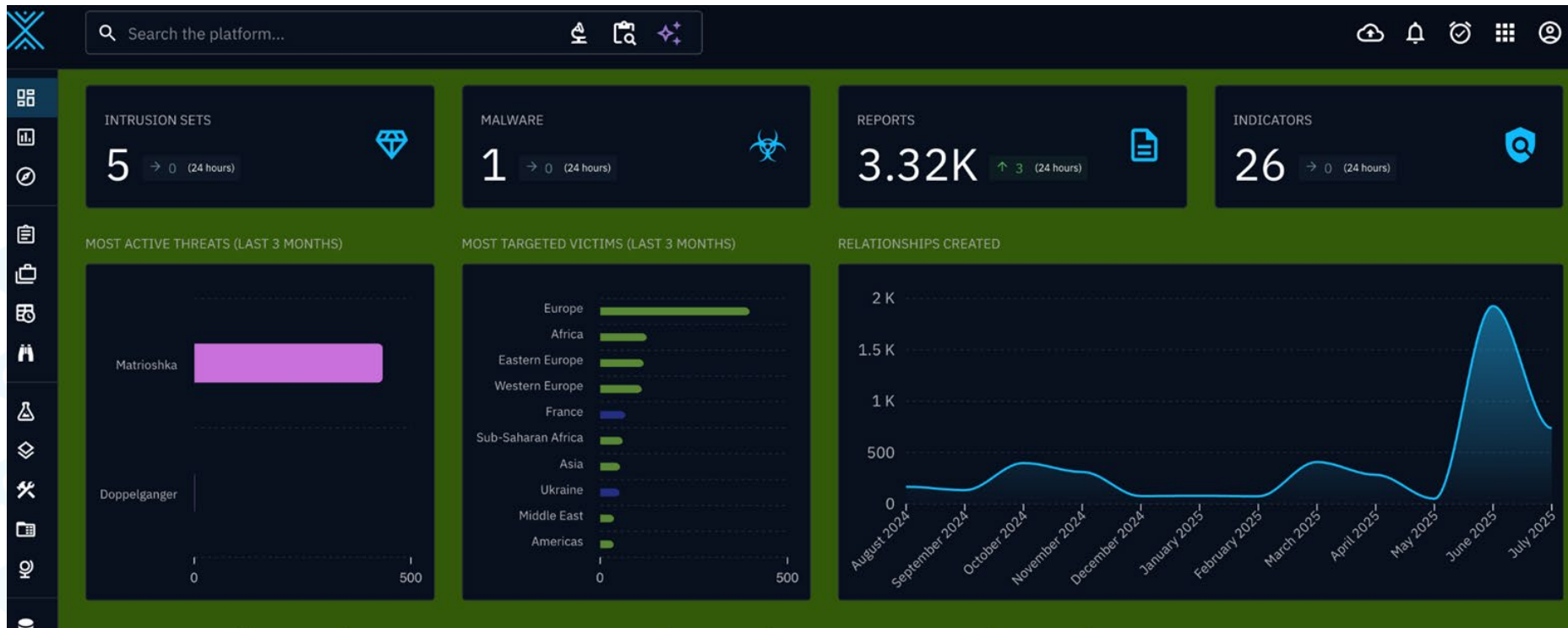
*Typosquatted website of the French Ministry for Europe and Foreign Affairs (source: diplomatie[.]gouv[.]fm)*



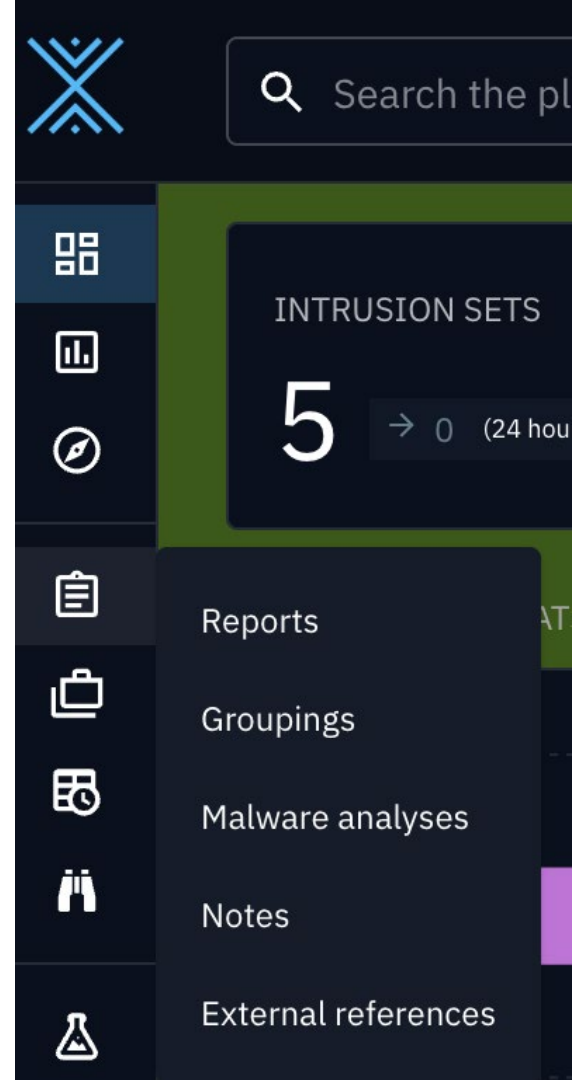
United Kingdom

*Sponsored content redirecting to a fake Ministry for Europe and Foreign Affairs website (source: facebook.com)*

# Now in Open CTI



# Find “Reports”





# Look for RRN

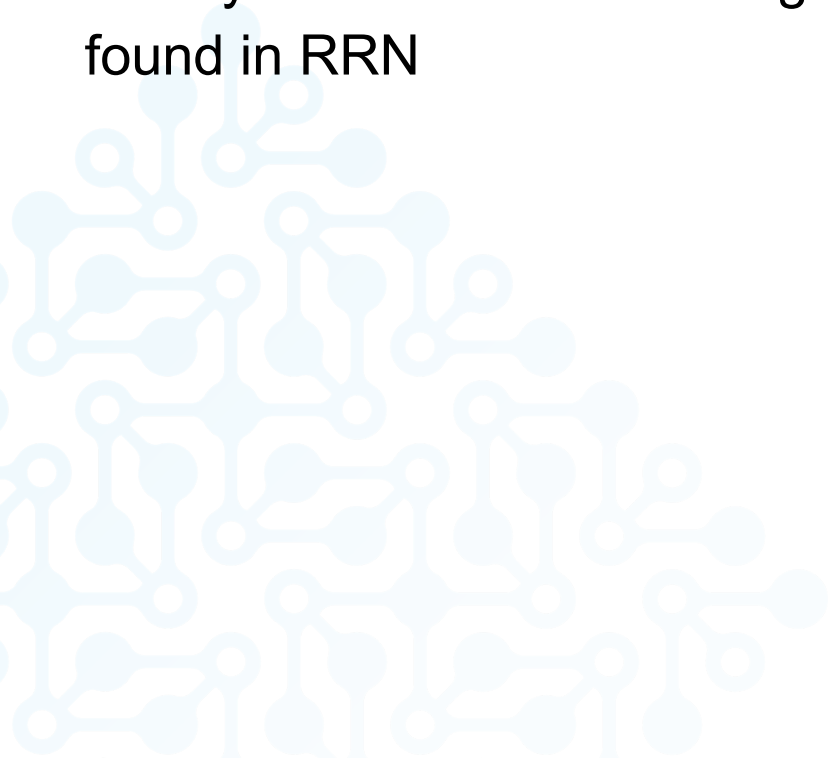


REPORT

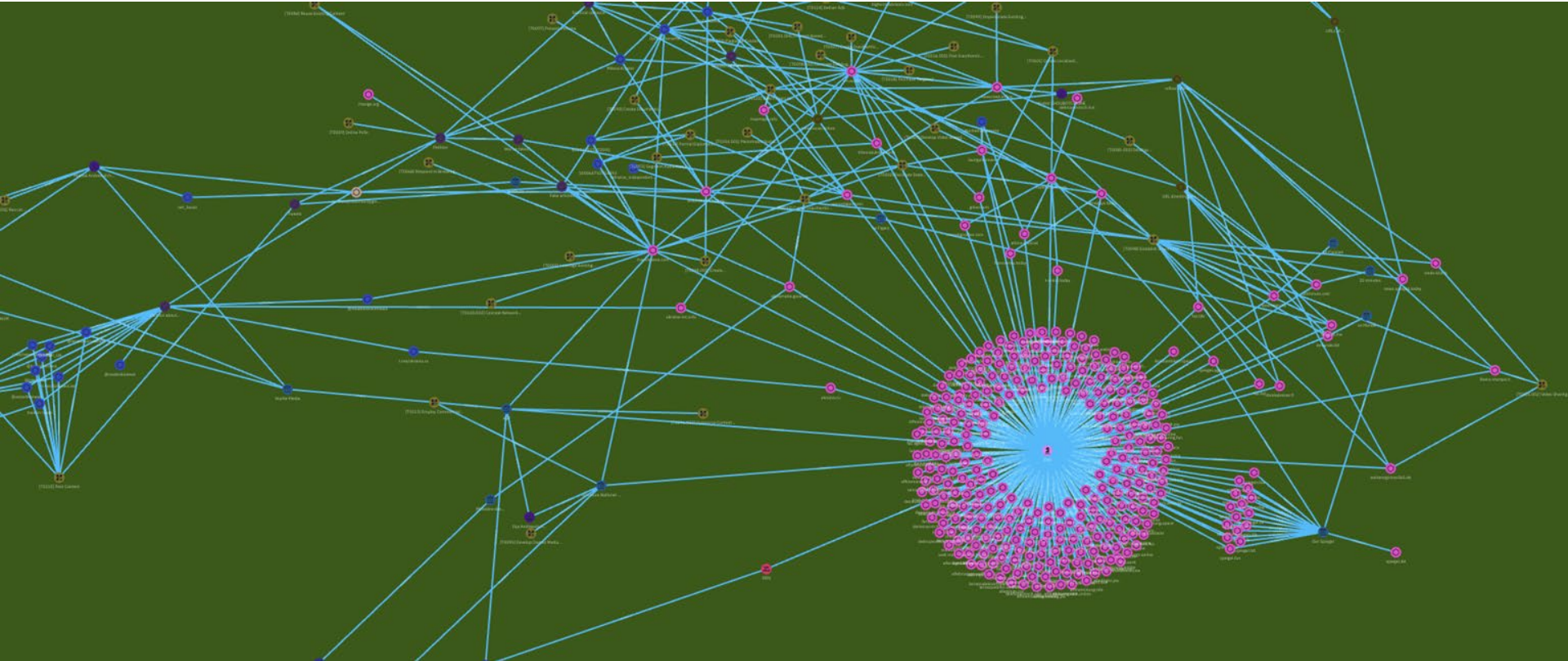
RRN: A complex and persistent informati...

# Click “knowledge”

Here you will find a knowledge graph of the attack patterns and assets found in RRN



It should look like this

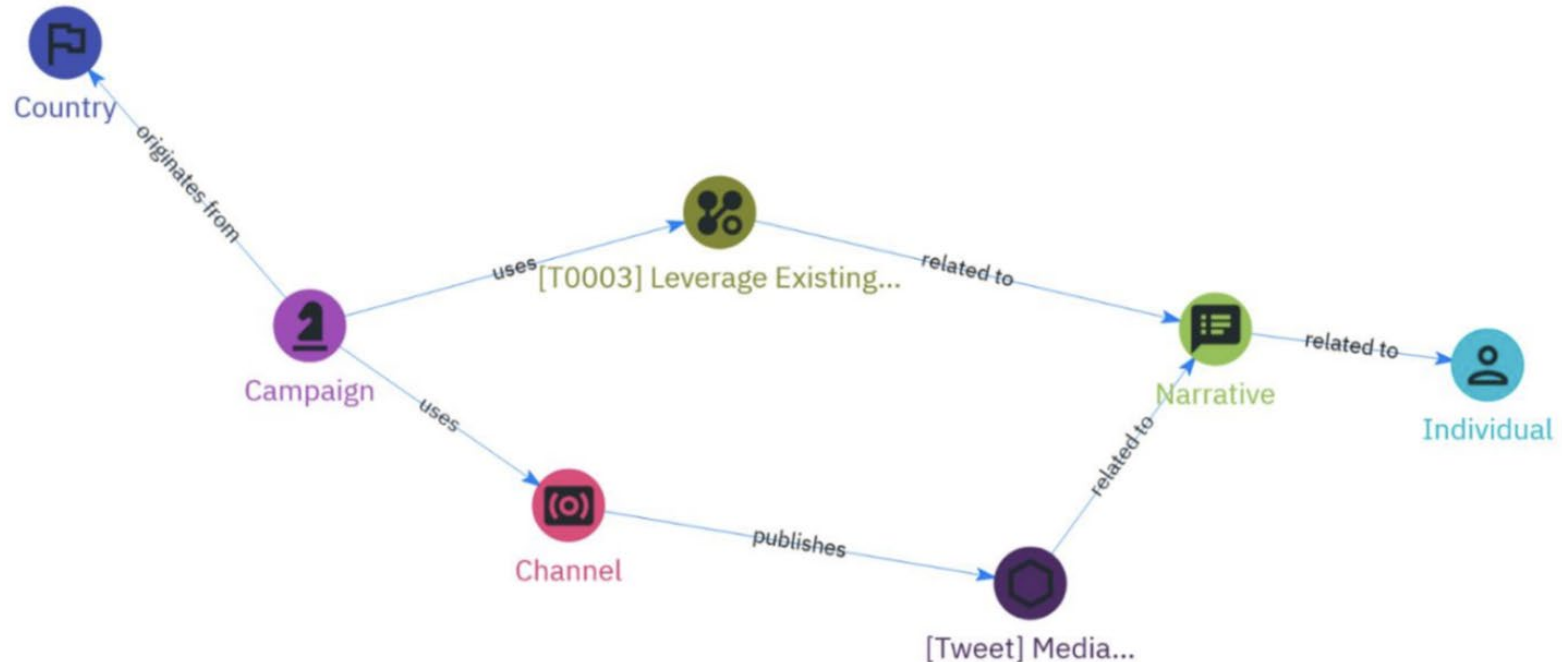


# STIX components

- STIX Domain Objects- macro elements of a report:  
Campaign, Threat Actor, Individual, etc.
- STIX Cyber-observable Objects- observable data (Media Content, URL, IP Address, etc.). It can also be the victim or the event (an election)
- STIX Relationship Objects- how the different elements are related

# We'll be looking at knowledge graphs in the reports

## MODEL FOR A CAMPAIGN



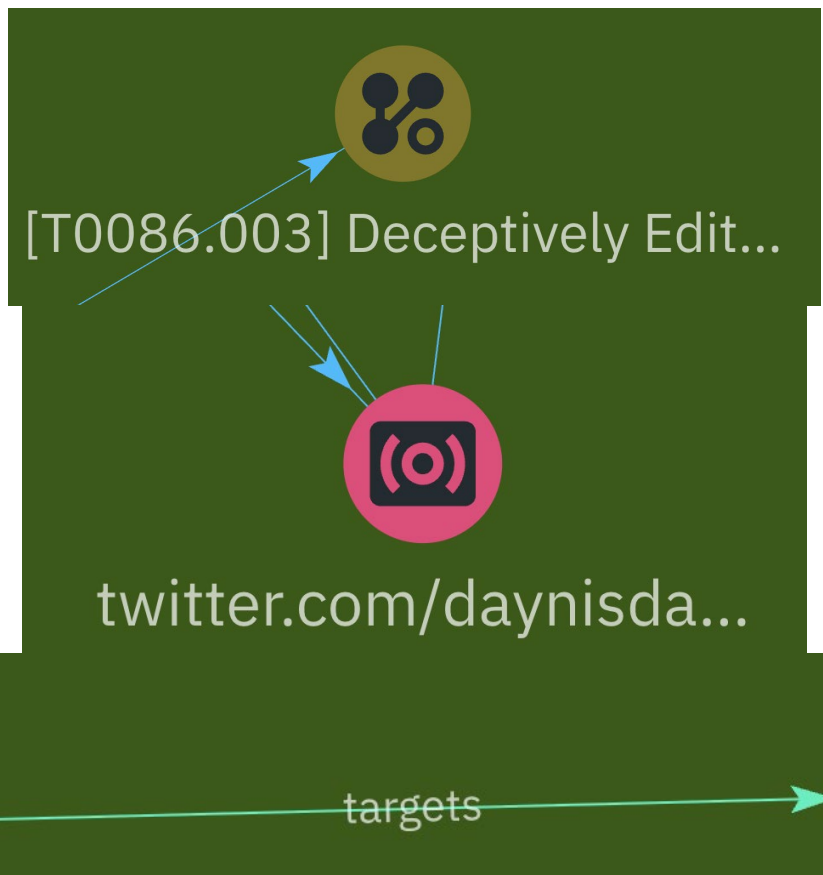


# What type of objects do you see?

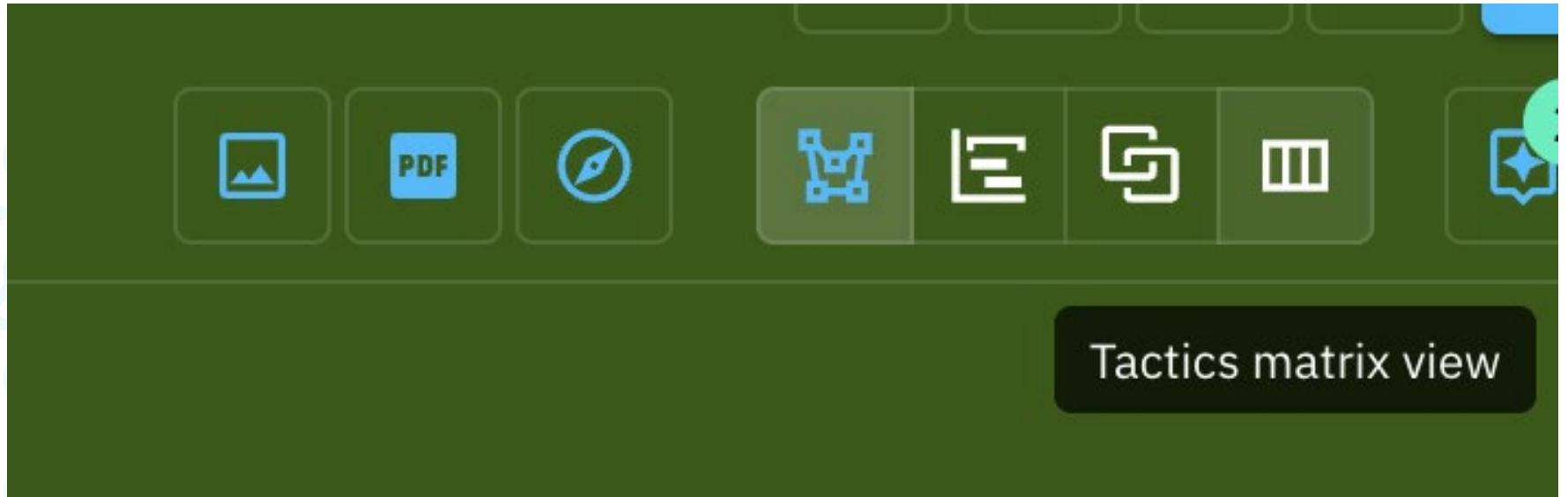
Attack Patterns

Assets

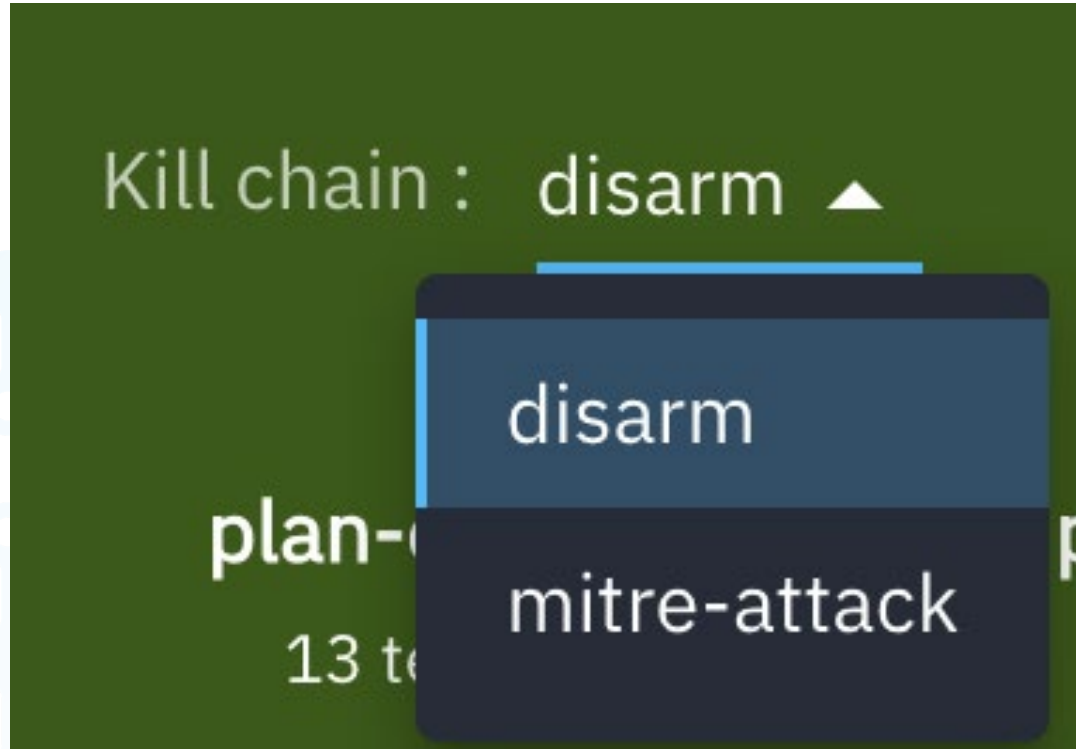
Relationships



## Matrix view



Here you can view TTPs from both Mitre and DISARM



# Here you can view TTPs

develop-narratives 6 techniques	conduct-pump-primi... 7 techniques	select-channels-an... 17 techniques	plan-objectives 13 techniques	persist-in-the-inf... 6 techniques	deliver-content 4 techniques	drive-online-harms 5 techniques	establish-social-a... 12 techniques	max
Demand Insurmountable Proof	Bait Influencer	Blogging and Publishing Networks	> Cause Harm	> Conceal Information Assets	Attract Traditional Media	Censor Social Media as a Political Force	> Acquire/Recruit Network	Ampl
> Develop Competing Narratives	Employ Commercial Analytic Firms	Bookmarking and Content Curation	> Cultivate Support	> Conceal Infrastructure	> Comment or Reply on Content	> Control Information Environment through Offensive Cyberspace Operations	> Build Network	Bait I
Develop New Narratives	Seed Distortions	> Chat Apps	Degrade Adversary	> Conceal Operational Activity	> Deliver Ads	> Harass	> Create Inauthentic Accounts	> (
Integrate Target Audience Vulnerabilities into Narrative	Seed Kernel of Truth	Consumer Review Networks	Dismay	Continue to Amplify	> Post Content	Platform Filtering	Create Inauthentic Social Media Pages and Groups	Direct Platf
Leverage Existing Narratives	Use Fake Experts	> Digital Community Hosting Asset	> Dismiss	> Exploit TOS/Content Moderation		> Suppress Opposition	Create Inauthentic Websites	> f
Respond to Breaking News Event or Active Crisis	Use Search Engine Optimisation	> Digital Content Creation Asset	> Dissuade from Acting	Play the Long Game			Cultivate Ignorant Agents	> J
		> Digital Content Delivery Asset	Distort				Develop Owned Media Assets	> f
		> Digital Content Hosting	Distract				> Infiltrate Existing Networks	/
			Divide					
			Facilitate State Propaganda					



Finally a very powerful tool



Investigations



# Feel free to type in any of the observables from RRN

Add entities

rrn.world

Add filter

3

	TYPE	VALUE	AUTHOR	LABELS	MARKING
<div><div></div><div></div></div>	DOMAIN NAME	rrn.world		<div>ru</div> <div>rrn</div>	TLP:CLEAR
<div><div></div><div></div></div>	INCIDENT RES...	Russia-based Facebook operation targeted Europ...	DFRLab	<div>russian invasion of...</div> <div>ru</div>	NONE
<div><div></div><div></div></div>	REPORT	Russia-based Facebook operation targeted Europ...		<div>russian invasion of...</div> <div>ru</div>	TLP:AMB...

## Expand elements

All types of target

ALL

NONE

- ☒ Attack Pattern (8)
- ☒ Campaign (1)
- ☒ Domain name (9)
- ☒ Label (2)
- ☒ Marking definition (1)
- ☒ Report (1)
- ☒ User account (2)

☒ Reset filters

All types of relationship

ALL

NONE

- ☒ related to (16)
- ☒ resolves to (4)
- ☒ has label (2)
- ☒ contains (1)
- ☒ has marking (1)

CANCEL

EXPAND