Hands on Threat Modeling with Open CTI

Stephen Campbell and Julian Neylan DISARM Foundation

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

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

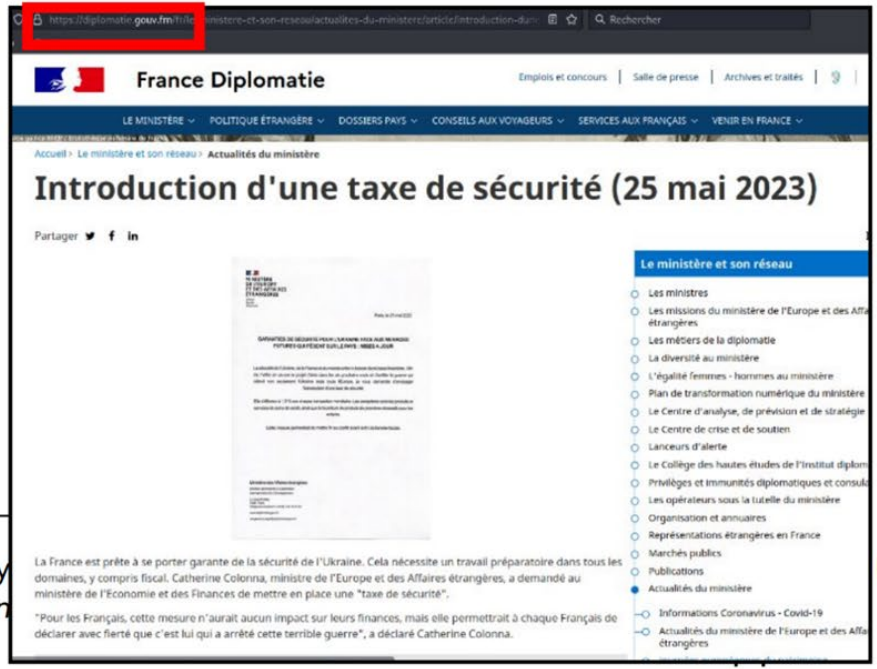
3. Satirical Cartoons

Example fake website

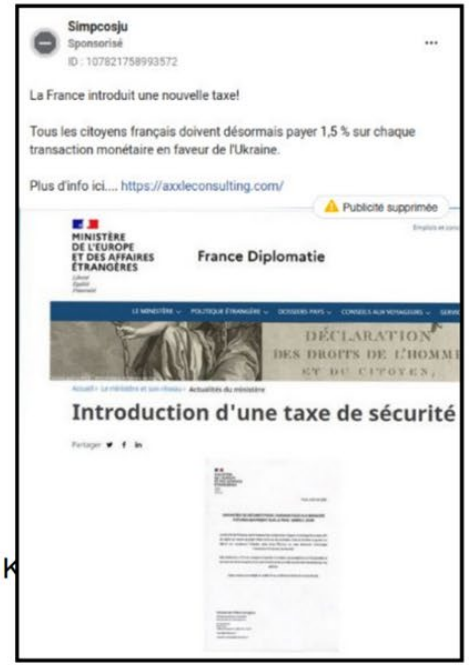
Article published on the typosquatted version of 20 Minutes *(source:* 20minuts[.]com*)*

Article published on the RRN *website (source:* rrn[.]world*)*

French Government impersonated



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



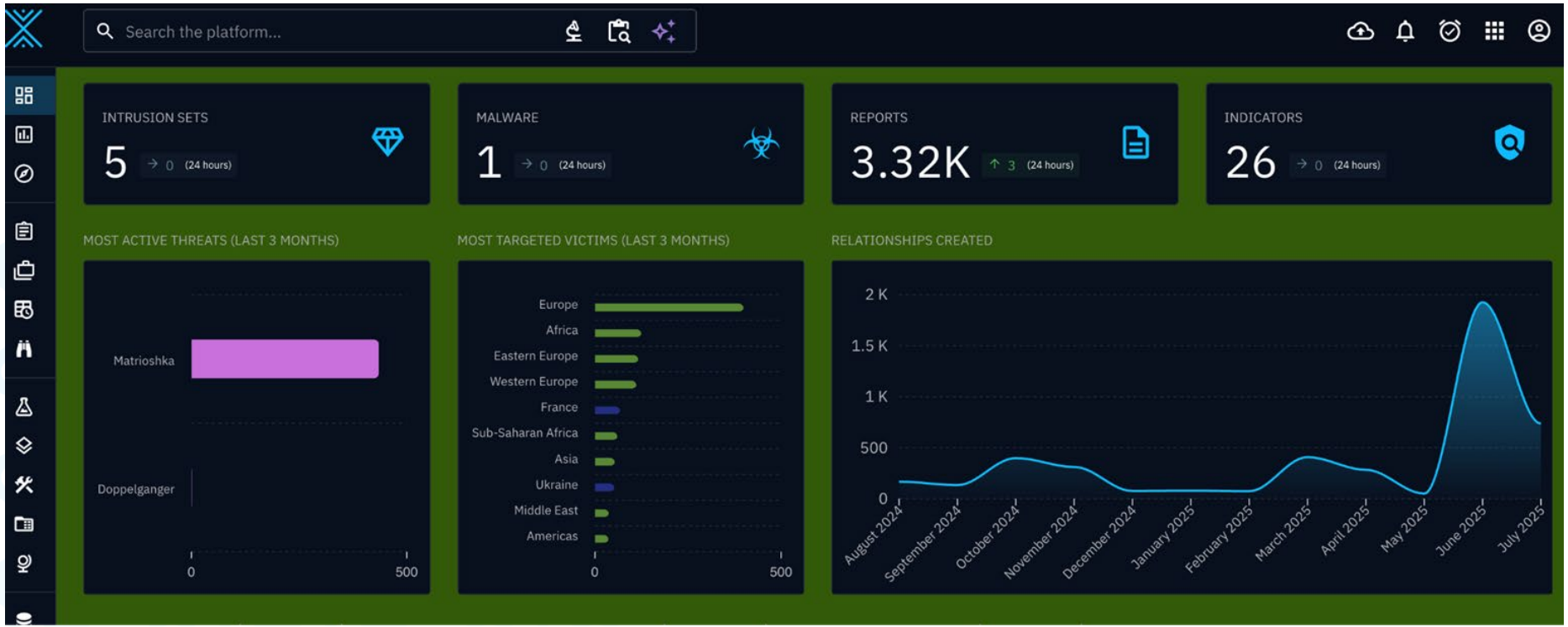
Sponsored content redirecting to a fake Ministry for Europe and Foreign Affairs website (source: facebook.com)

[32] Germany

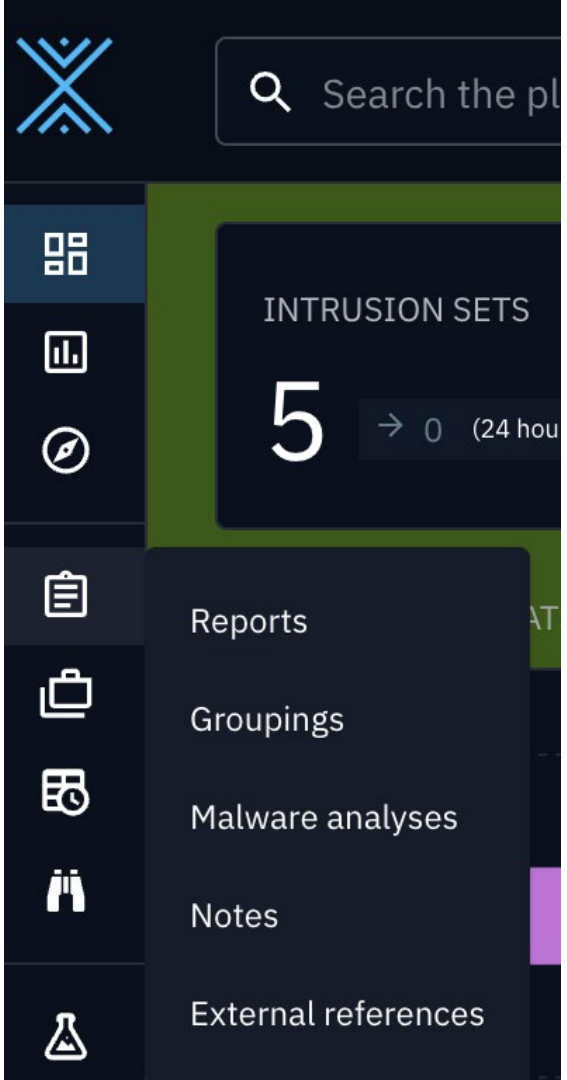
[33] *leparisien*

United K

Now in Open CTI



Find “Reports”

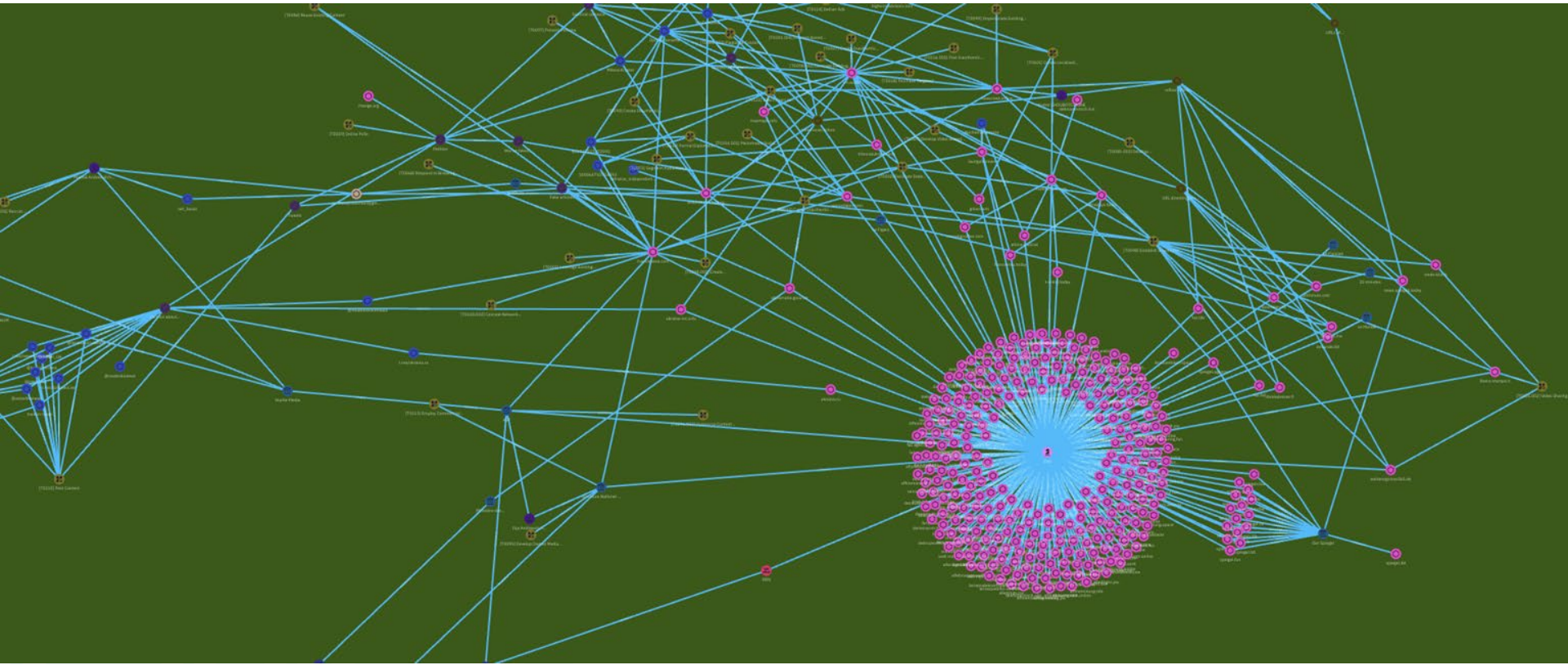


Look for RRN

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

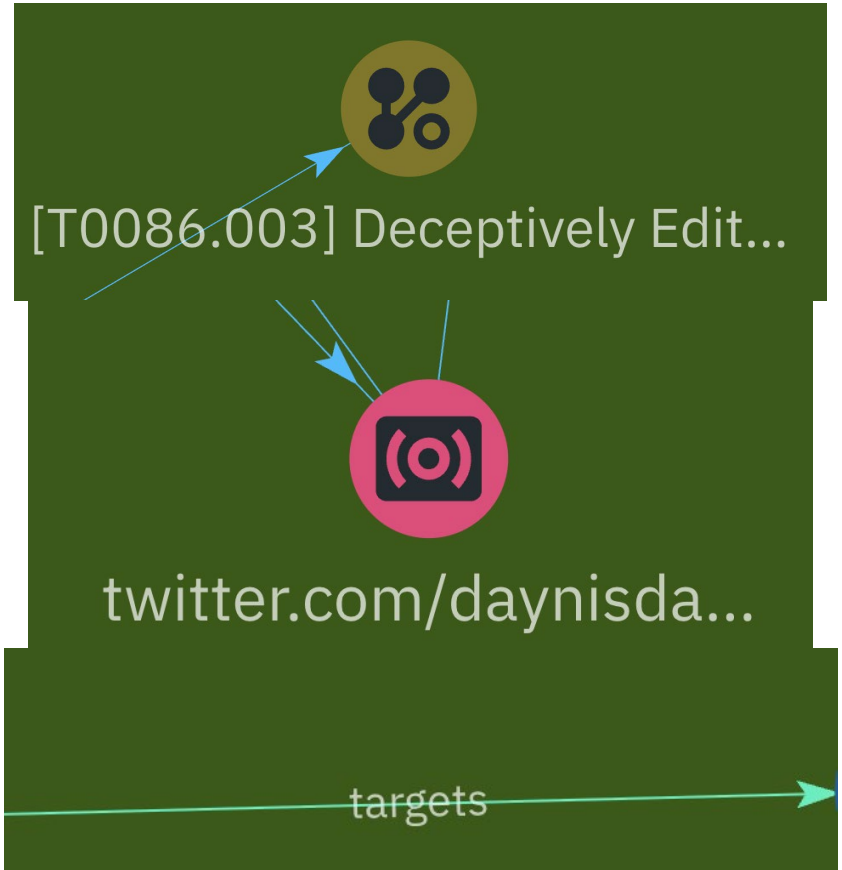
We'll be looking at knowledge graphs in the reports

What type of objects do you see?

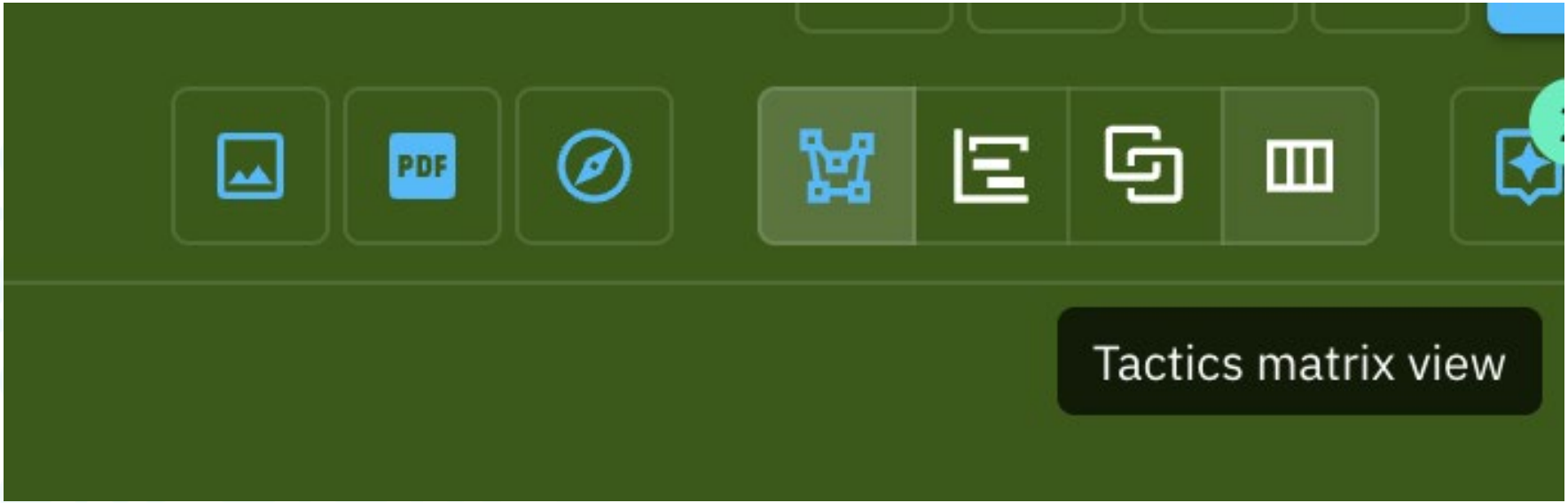
Attack Patterns

Assets

Relationships

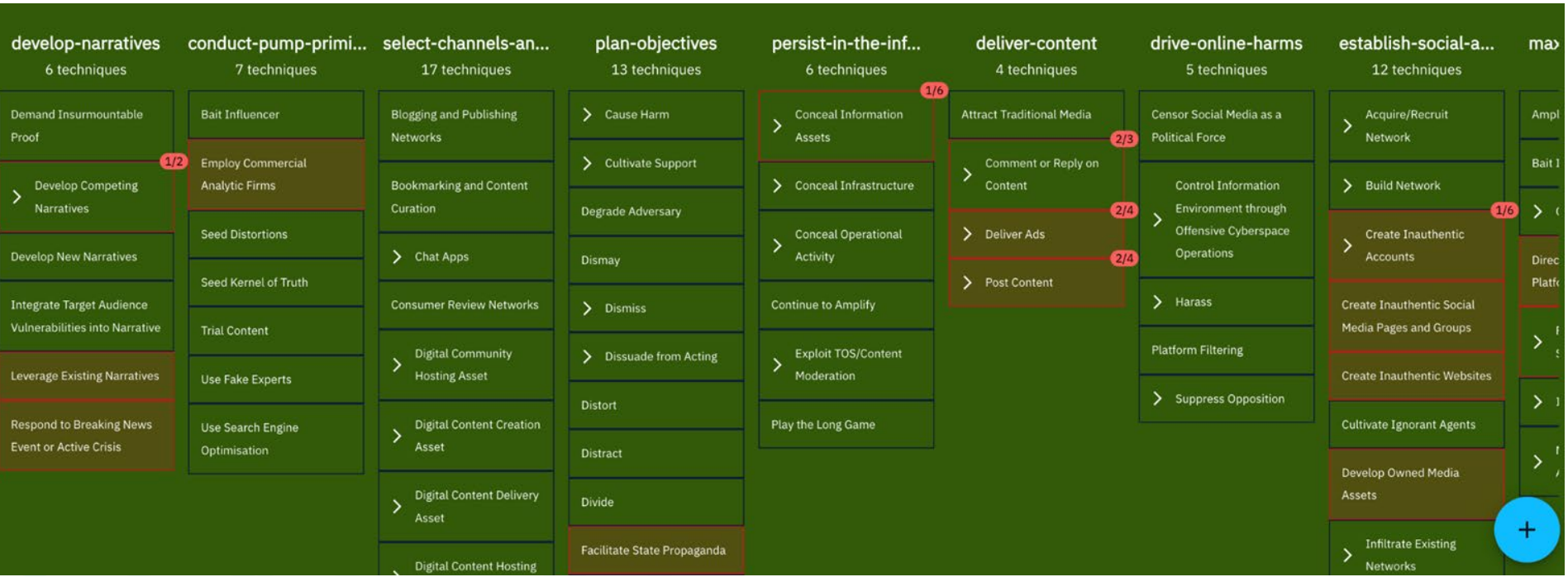


Matrix view



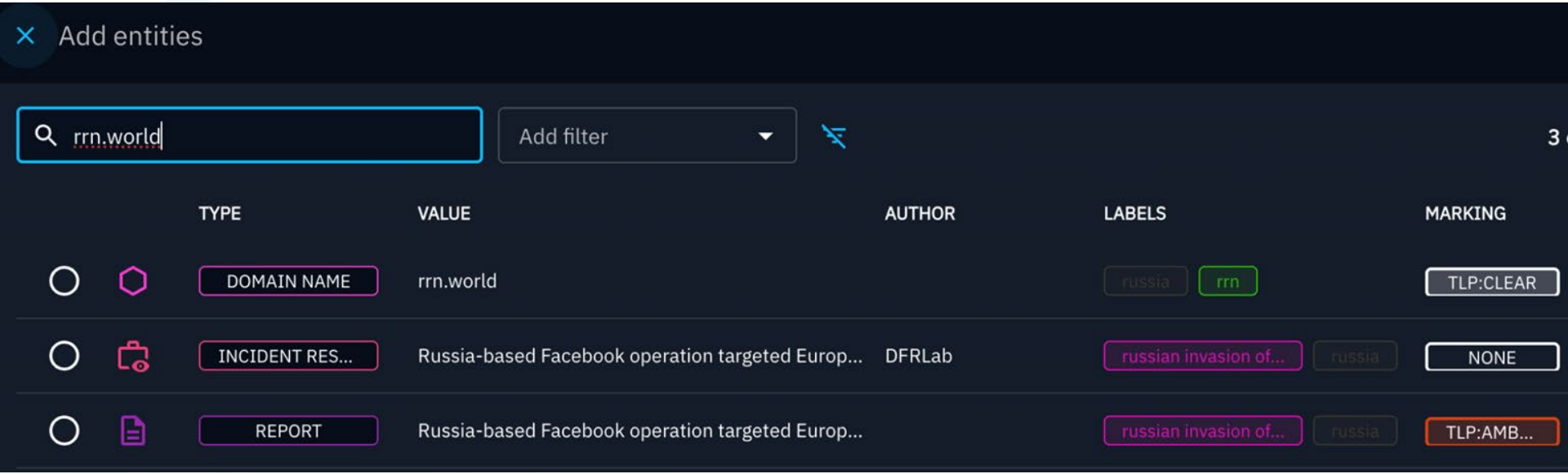
Here you can view TTPs from both Mitre and DISARM

Here you can view TTPs



Finally a very powerful tool

Feel free to type in any of the observables from RRN



Expand elements

All types of target

ALL NONE

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

All types of relationship

ALL NONE

- [x] related to (16)
- [x] resolves to (4)
- [x] has label (2)
- [x] contains (1)
- [x] has marking (1)

Reset filters

CANCEL EXPAND