**BALTHOR FOR PRESIDENT** (ANNOTATED VERSION)

It began as many awful things do these days—with a horrific minor news item (Report: “Feeding Frenzy in Eustis”, “Eustis Chronicle”, <date1>) from some previously uncharted geography. Kevin Campbell (Identity: “Kevin Campbell”, Individual) of Eustis, Ohio (Location: “Eustis”, Town, “Ohio”), stood accused of systematically depopulating the canine population of his hometown over a three-week long “feeding frenzy.”

Until recently, Campbell had been a stand-up member of his community. Just another lifelong Eustonian with a close-knit family and season tickets to the local AA baseball club.

Family and friends noticed a change in Campbell after an accident at the local superfund site (Event: “Accident at Superfund”, Local, <date2>) where he had been employed as an excavator operator for the past six years rendered him temporarily unconscious. Kevin Campbell was a different man when he awoke in the hospital.

Speaking exclusively in the third person, Campbell demanded to be referred to henceforth as “BALTHOR the GREAT.” (Identity: “BALTHOR the GREAT”, Pseudonym, “Kevin Campbell”) Upon his return to work, colleagues noticed a distinct lack of empathy in BALTHOR. He seemed to relish in the pain of others and began exhibiting a healthy appetite for raw meat that made him an instant lunchtime pariah.

Tipped off about his unceasing lust for flesh, the Eustis Police (Identity: “Eustis Police”, Government, Municipal) arrested Campbell (Event: “Arrest of Kevin Campbell”, Local, <date3>) after a weeks-long period in which the local populace was terrorized by nocturnal visions of a stooped man in tattered work clothes depopulating a town of its canine companions.  
  
The saga of BALTHOR would have died on the vine had Eustis PD not blundered twice in the span of a day’s time.

First, after BALTHOR made bail and was released on his own dubious recognizance, the police chief gathered the local media for a perp walk (Event: “Perp Walk Kevin Campbell”, Local, <date4>). Unintimidated, BALTHOR offered a sneering forty-minute diatribe (Respond to Breaking News Event or Active Crisis [T0068], Cultivate Support: Increase Prestige [T0136.008]) steeped in a brazen eschatological world view (Determine Strategic Ends: Ideological Advantage [T0074.004]). BALTHOR, as it turned out, espoused a belief in a natural obligation to consume any life which he could subdue in order to elevate his powers to heights great enough to enable BALTHOR to subjugate the entire world and bring about the end of life as we knew it (Content: 96:s4Ud1Lj96tHHlZDrwciQmA+, Fuzzy Hash, “BALTHOR’s Beliefs”).

The accusations facing the former Kevin Campbell would have made a juicy evening news story in and of their own, but the addition of this deeply unsavory bit of oratory ensured that BALTHOR’s ideas would receive national attention.

Formal news coverage transformed into secondary and tertiary social media content (Bait Legitimate Influencers [T0039], Traditional Media [T0111], Social Networks [T0104]) in which aghast content-creators amplified the idea of a local lunatic turned mad prophet into a positive feedback loop of algorithmic superpower (Content: 384:EWo4X1WaPW9ZWhWzLo+lWpct/, Fuzzy Hash, “Social media content about local lunatic turned mad prophet”).

Eventually the BALTHOR saga caught the attention of users at sepsis.zone (Community: “sepsis.zone”, Discussion Forum), a cut-rate forum (Discussion Forums [T0106]) leveraging Namibian- (Location: “Namibia”, Country) operated servers to host crowd-sourced content for misanthropes who delighted in the offensive. After an anonymous user replied to the initial news item thread with the words “#FreeBALTHOR,” (Narrative: “#FreeBALTHOR”, Hashtag) a shadow movement supporting the Ohio-based demiurge began to spread across the less-traveled corners of the internet.

Around the time that “#FreeBALTHOR” infiltrated content on more mainstream social media platforms (Social Networks: Mainstream Social Networks [T0104.001]), the second critical error committed by the Eustis Police Department became apparent. Though BALTHOR had readily confessed to his crimes, he had done so without having first been mirandized. BALTHOR was cleared on a technicality (Event: “BALTHOR freed”, <date5>).

Freshly divorced, unemployed, and shunned in his community, BALTHOR had only two priorities—the consumption of flesh and aimless destruction. Others, however, singled out BALTHOR for a loftier role in local history.

Declan Bumpus (Identity: “Declan Bumpus”, Individual, State-affiliated), a political consultant for fringe movements, professional provocateur, and frequent sepsis.zone commenter (User Account: “@dbumpus”, Discussion Forum), interpreted the sensation surrounding BALTHOR as both a sign of a mightier populism waiting to be harnessed and an opportunity to marshal power for himself.

If anyone at the Days Inn off the highway in Eustis, Ohio, had been a forensic accountant of any particular renown, they could have traced the credit card (Acquire/Recruit Network: Fund Proxies [T0093.001]) Declan Bumpus used for his week’s stay on its long, curving path of money laundering white water back to the state actors half a world away who were intent on destabilizing American democracy (Determine Strategic Ends: Geopolitical Advantage [T0074.001], Undermine: Subvert [T0135.003]).

Whoever they were, they had invested wisely.

“What if I told you that I could make your wildest dreams come true if you just do exactly as I say,” Bumpus offered.

“Sure,” BALTHOR croaked, burping up some of the roadkill breakfast that had made him fifteen minutes late to the meeting.

Bumpus elucidated a grand plan: play on the logical inconsistencies between the cherished myths of the United States and the practical reality of life in the Land of the Free (Undermine: Smear [T0135.001], Seed Kernel of Truth [T0042], Leverage Existing Narratives [T0003]),(Narrative: N00023, Geopolitical, “US not living up to its ideals”). Feed on the discontinuities and offer seemingly appealing alternatives that whitewashed moral repugnancy as patriotic duty. Start small and build big. Make an entire town question its foundations (Dissuade from Acting: Discourage [T0139.001]) and refashion reality howsoever they pleased. Consolidate power and curry influence.

Together they settled on a mayoral bid.

“Small potatoes,” Declan Bumpus said. “It’s not about holding office. It’s about having influence.”

Table Observables Found in Report "BALTHOR FOR PRESIDENT" (Gray)

|  |  |  |
| --- | --- | --- |
| **ID or Name** | **Type** | **Additional Info** |
| **Community** | | |
| sepsis.zone | Discussion Forum |  |
| **Content** | | |
| 96:s4Ud1Lj96tHHlZDrwciQmA+ | Fuzzy Hash | BALFOR’s Beliefs |
| 384:EWo4X1WaPW9ZWhWzLo+lWpct/ | Fuzzy Hash | Social media content about local lunatic turned mad prophet |
| **Event** | | |
| Accident at Superfund | Local | <date2> |
| Arrest of Kevin Campbell | Local | <date3> |
| Perp Walk Kevin Campbell | Local | <date4> |
| BALTHOR freed | Local | <date5> |
| **Identity** | | |
| Kevin Campbell | Individual |  |
| BALTHOR THE GREAT | Pseudonym | Kevin Campbell |
| Eustis Police | Government | Municipal |
| Declan Bumpus | Individual | State-affiliated |
| **Location** | | |
| Eustis | Town | Ohio |
| Namibia | Country |  |
| **Narrative** | | |
| #FreeBALTHOR | Hashtag |  |
| N00023 | Geopolitical | US not Living up to its Ideals |
| **Report** | | |
| Feeding Frenzy in Eustis | Eustis Chronicle | <date1> |
| **User Account** | | |
| @dbumpus | Discussion Forum |  |

Table ”Mad Prophet” BALTHOR's Personal Campaign (Yellow)

|  |  |  |
| --- | --- | --- |
| **Technique Title** | **ID** | **Use** |
| **Plan Strategy [TA01]** | | |
| Determine Strategic Ends: Ideological Advantage | T0074.004 | Unintimidated, BALTHOR offered a sneering forty-minute diatribe steeped in a brazen eschatological world view |
| **Plan Objectives [TA02]** | | |
| Cultivate Support: Increase Prestige | T0136.008 | Unintimidated, BALTHOR offered a sneering forty-minute diatribe steeped in a brazen eschatological world view |
| **Develop Narratives [TA14]** | | |
| Respond to Breaking News Event or Active Crisis | T0068 | Unintimidated, BALTHOR offered a sneering forty-minute diatribe steeped in a brazen eschatological world view |
| **Select Channels and Affordances [TA07]** | | |
| Social Networks | T0104 | Formal news coverage transformed into secondary and tertiary social media content |
| Social Networks: Mainstream Social Networks | T0104.001 | Around the time that “#FreeBALTHOR” infiltrated content on more mainstream social media platforms |
| Discussion Forums | T0106 | Eventually the BALTHOR saga caught the attention of users at sepsis.zone, a cut-rate forum leveraging Namibian-operated servers |
| Traditional Media | T0111 | Formal news coverage transformed into secondary and tertiary social media content |
| **Conduct Pump Priming [TA08]** | | |
| Bait Legitimate Influencers | T0039 | Formal news coverage transformed into secondary and tertiary social media content in which aghast content-creators amplified the idea |

Table Campaign of State-affiliated Threat Actor "Declan Bumpus" (Orange)

|  |  |  |
| --- | --- | --- |
| **Technique Title** | **ID** | **Use** |
| **Plan Strategy [TA01]** | | |
| Determine Strategic Ends: Geopolitical Advantage | T0074.001 | state actors half a world away who were intent on destabilizing American democracy |
| **Plan Objectives [TA02]** | | |
| Undermine: Smear | T0135.001 | Bumpus elucidated a grand plan: play on the logical inconsistencies between the cherished myths of the United States and the practical reality of life in the Land of the Free |
| Undermine: Subvert | T0135.003 | state actors half a world away who were intent on destabilizing American democracy |
| Dissuade from Acting: Discourage | T0139.001 | Make an entire town question its foundations and refashion reality howsoever they pleased |
| **Develop Narratives [TA14]** | | |
| Leverage Existing Narratives | T0003 | play on the logical inconsistencies between the cherished myths of the United States and the practical reality of life in the Land of the Free |
| **Establish Social Assets [TA15]** | | |
| Acquire/Recruit Network: Fund Proxies | T0093.001 | If anyone at the Days Inn off the highway in Eustis, Ohio, had been a forensic accountant of any particular renown, they could have traced the credit card Declan Bumpus used for his week’s stay on its long, curving path of money laundering white water back to the state actors |
| **Conduct Pump Priming [TA08]** | | |
| Seed Kernel of Truth | T0042 | the cherished myths of the United States |



Figure Profiles of BALTHOR (Yellow) and Bumpus (Orange) Campaigns

# DISCUSSION

Introduction  
Duncan’s is a great use case for showcasing the potential use of existing STIX objects[[1]](#footnote-1) to model disinformation, harm, or adversarial influence threats and to identify some of the objects and properties that may be missing. It does not cover any defender actions so it will not inform that side of the equation, but it will give us a start on the threat modeling. If we can forgive him for the grossness of the example 😉. But it is funny.   
  
Annotations  
In general, when I discuss disinformation, I talk about two categories of entities when modeling threats: behaviors and observables. Behaviors are actions. Observables are things. The annotated version of “BALTHOR FOR PRESIDENT” includes behaviors that have been modeled using the DISARM Framework using DISARM Red TTPs. These are highlighted in yellow when the behaviors relate to Kevin Campbell and in orange when they relate to Declan Bumpus. The annotated version also includes observables highlighted in gray.   
  
Think of observables as “things” that pertain to the information operations being conducted by threat actors[[2]](#footnote-2). They can be modeled using simple entity relationship diagrams or semantic ontologies. A subset of observables in disinformation, influence, or harm campaigns can be thought of as Indicators of Manipulation (IOMs), akin to Indicators of Compromise (IOCs) in cybersecurity. IOCs began to be codified in 2011 when Mandiant created the OpenIOC format to share IOCs across teams and organizations and Mitre created a standard format for representing cyber observables called CybOX[[3]](#footnote-3). As I understand it, in 2012 these two formats were integrated into STIX as the STIX Indicator SDO and STIX Cyber Observables. Then Mitre brought out ATT&CK for adversarial behaviors in 2013. The journey of disinformation intelligence followed the reverse trajectory, starting first with the codification of behaviors with AMITT in 2019. We now need to codify Indicators of Manipulation and other observables.

STIX Objects  
See Figure 4 for a simplified STIX entity relationship model of disinformation and the response to it. For simplicity relationships are not named. This is meant as a rough model to get the discussion going. See Figure 5 for the real-world Filigran model of disinformation (mostly showing the threat side of the equation) that is currently in use within the OpenCTI threat intelligence platform. Much more rigor has gone into this richer and more comprehensive model than the author’s rough model and so we will want to leverage as much of Filigran’s design as possible. I have not tried to align Duncan’s use case here with the Filigran model, although I believe that would be a much more productive exercise. I just don’t feel qualified to do so.

Note that in Figure 4 the existing Attack Pattern SDO is used to capture behaviors. A STIX Attack Pattern can involve one or more TTPs identified via external reference to non-STIX information such as DISARM technique IDs. Also, in Figure 4 the Information Attack, Channel, Community, Narrative, Event, Target Audience, and Defender objects are all potentially new STIX Domain Objects (SDOs) that do not exist today in STIX 2.1[[4]](#footnote-4). Content is a potential new STIX Cyber Observable (SCO). The Incident object is currently being prototyped as a STIX 2.1 Extension Object and is available in the [CTI STIX Common Object repo](https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/incident-core). The prototype version 2.0 of this Extension Object includes new Event, Impact, and Task SDOs, which may all be relevant to defending against disinformation. Note that the Incident-related Event SDO refers specifically to a “security event”, whereas the Event objects in Figure 4 and, I believe, in Figure 5 refer to real-world events of any nature. Real-world events form a critical component of a disinformation threat model since information operations often revolve around them, whether they are elections, rallies, invasions, or terrorist attacks. We will have to deal with this naming conflict so that we adhere to the STIX best practices for extension objects[[5]](#footnote-5).

I believe the Channel, Narrative, and Event objects were introduced by Filigran into OpenCTI in 2022, but Jean-Philippe will be able to give us specifics. I know that they are being actively used by the EEAS and by debunk. Perhaps the Infrastructure SDO, with types such as “command-and-control, “hosting-malware”, “phishing”, is too cyber-oriented to capture the types of technology platforms used in influence campaigns such as social media, video sharing, microblogging etc., so a dedicated SDO is desired? Perhaps Jean-Philippe or Dan Fritz can explain the origins of the Channel object. In my mind we may also need an object that captures the concept of a collection of user accounts organized around a specific topic, interest, or organization. *Hence my proposal for the SDO “Community”.* This would allow us to model online communities such as Facebook Groups and Pages, WhatsApp groups, Subreddits, 4chan Bulletin Boards, YouTube Channels, Telegram Channels etc. In the case of the BALTHOR use case, sepsis.zone is a discussion forum with its own website, but we also need to accommodate forums hosted on platforms such as Reddit, Quora, Digg e.g. the “Channel” might be “Reddit” but the “Community” would be “r/The\_Donald”.

There is no SDO in STIX 2.1 that would adequately capture narratives used in influence campaigns, hence the Narrative object. When SJ Terp used STIX to model disinformation, she repurposed the STIX Malware SDO for narratives. From a cognitive security perspective, narratives are the closest thing to malware since they can be perceived as cognitively infecting the target. They need their own SDO with their own identifier and properties. There is also no SDO in STIX 2.1 to capture content posted on websites, blogs, social media etc., hence the Content object. The closest equivalent in the Filigran model appears to be the Media-Content SCO, but it is not clear whether this would accommodate content on offline bill boards.

In disinformation speak we talk a lot about a “Target Audience” or “TA”, and so I propose creating a new SDO to capture this. The target audience may be defined by the attacker in terms of a set of demographic and/or psychographic variables and may consist of user account(s) from one or more Communities. Note that there are sometimes direct and indirect targets in an influence campaign: a common strategy in attacking democracies is to influence public opinion so that policymakers are forced into changing their behavior in response. Perhaps we tease out these nuances with different types of targets. There may also be unintended victims to a disinformation, influence, or harm campaign. So perhaps we need separate objects for targets and victims.

Anyway, this all needs some scrutiny. I am aware that a static model such as STIX may not be adequate for modeling information diffusion or epidemiology, so we may need to complement STIX with other models borrowed from the physics of gases or the study of infectious diseases. Regarding how to model Victims, OpenCTI includes “victimology” features, so Filigran may be able to advise here.   
  
I also added a Defender object on the defense side since we want to enable a whole-of-society approach and identify who the “good guys” are. In this case I imagine defenders to include NGOs and private sector actors involved with identifying and tracking adversaries in the public sphere, as well as national and international government agencies. Targeted individuals and communities, of course, can also take actions to defend themselves. I have not looked at CACAO yet, but in good time we will want to add a Playbook and maybe other CACAO objects to our model to complement the Course of Action object.

In terms of the high-level SDOs in Figure 4 such as Threat Actor, Campaign, and Intrusion Set, we will need to analyze the specification of these objects for their suitability to model disinformation and influence. I recommend we study the work of the TAC-TC. At the very least we will want to extend the open vocabulary for Threat Actor type (see below for discussion on vocabularies). With respect to this specific use case, whether Kevin Campbell’s rhetoric rises to the status of constituting a “campaign” that merits scrutiny by the counter-disinformation community is debatable. There may have been little instrumentality or design to his speech. And there does not appear to be any intent to deceive. So perhaps this is to be categorized as legitimate activity in which he is enjoying his right of freedom of expression, even if he does not have the right in our society to consume canines belonging to others 😊.

On the other hand, given the way the news around Kevin Campbell’s arrest spread, the unsavory characters this attracted, the potential for further harm to the canine population, and the likelihood that animal welfare organizations are likely to speak out and demand action, there is an argument to be made here that an organic harm campaign has emerged, and so we are justified in codifying and tracking the behaviors and observables associated with Campbell’s arrest and the attention it received. Using the DAD-CDM standard to identify and track information campaigns of domestic origin of any sort is likely to attract criticism from advocates of free speech and those who manipulate the countering of disinformation, misinformation, or online harm for political ends, but even Jim Jordan and Steven Miller would have a hard time reframing civil society tracking of the BALTHOR case as an attempt by liberals to censor conservative voices[[6]](#footnote-6).

Duncan’s use case invites us to consider the creation of guidelines for the use of the DAD-CDM standard in different geographies, especially those with very strong support for freedom of speech, even if we legally absolve ourselves of any responsibility for how the standard might be used by others. The rubber really meets the road on this debate when we start to model the defender side of the equation, especially when discussing any courses of action that involve removing, downranking, or labeling content.

In contrast to the ambiguity concerning the intentionality behind Kevin Campbell’s actions, Declan Bumpus appears to be an agent of a foreign power that is “intent on destabilizing democracy”, so intentionality is much more clearly behind his involvement and so we can classify this campaign as a subversive influence campaign.

A campaign, of course, typically refers to a concerted long-term effort by a threat actor. SJ Terp breaks campaigns into incidents and talks about threat actors as “incident creators”. Personally, I have always had trouble with this, as I believe it conflates offense and defense. The terms “incident” and “incident response” are widely used in the defender community to refer to “cybersecurity incident” and “cybersecurity incident response”. I doubt very much that threat actors talk about “creating incidents”, even if those that are affected might say that “an incident occurred”, where “incident” here is used in the common sense of the word. I much prefer Clint Watts’ term “[information attack](https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/)” for a short-term influence or harm effort initiated by an attacker, and so that is the term I propose for a new SDO for this.

James Pamment breaks down an “influence campaign” into one or more “influence operations” and/or “influence activities”[[7]](#footnote-7), but we are concerned in DAD-CDM with not just influence operations but also operations designed to cause harm. Perhaps the term “information operation” could be used, but in my mind this term is too broad or too benign to capture the concept of an “information attack”. *What is clear is that we need some kind of term for a short-term influence or harm effort*. Whatever term we choose I strongly advise against using “Incident” for this purpose, since we want to be able to leverage the new Incident extension object in our work, and which is clearly focused on the defense side of the equation. We also need to adhere to best practices when we name objects to ensure no conflict with existing STIX extensions or common objects5.

A pyramid of colorful triangles

Description automatically generated with medium confidence

I believe we can leverage the Intrusion Set SDO to model disinformation, given the difficulty in attributing a set of behaviors and resources to a specific threat actor. As in the case of cyber criminals, disinformers and manipulators may use or repurpose a set of TTPs and information assets across multiple campaigns. I believe the OpenCTI object “Arsenal” captures the information assets or social media assets component of this, but not an intrusion set in its entirety, but I’m not sure. Perhaps Jean-Philippe can explain. Intrusion sets would allow us to relate channels, infrastructure, tools, and attack patterns to threat actors, their motivations, their targets, and the vulnerabilities they exploit.

Figure SJ Terp's Pyramid

Object Properties

Every object in STIX has a set of properties. These include required and optional common properties as well as object-specific properties[[8]](#footnote-8). Among the common properties is a unique STIX object ID. Beyond that, most STIX objects can also be identified using an alternative identifying object-specific property such as a name. In our BALTHOR use case I have listed two or three properties per object only, for simplicity, because I am highlighting these objects and their properties in-line with the text, and listing all the properties would get unwieldy. I list these two or three properties per object in tabular format in tables 1-3.

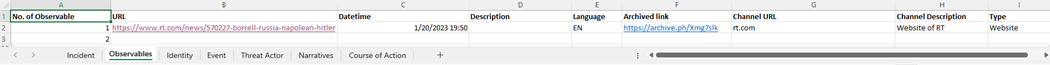
In practice the codification of objects and their properties is more elaborate and is done out-of-band rather than in-line. For example, the European External Action Service currently writes a report on each FIMI “incident” (they use the SJ Terp terminology) in a standard manner and then codifies objects and their properties pertaining to this report using an Excel workbook with one worksheet per object type. Properties for each object are captured in Excel columns. A screenshot is shown here to illustrate. Use of Excel is an intermediate step before the creation of STIX objects in OpenCTI.

Figure Sample Excel Workbook Used to Codify a FIMI Report

The full documentation for how the EEAS codifies FIMI objects and their properties is available in the EEAS’ FIMI STIX Codebook[[9]](#footnote-9). For example, for the STIX Object “Incident” the EEAS lists eleven properties: Name, Description, Label, Incident Type, First Seen, Last Seen, Severity, Presumed Objective, Confidence Level, Marking, and External References. Examples of these properties can be seen in the [First FIMI Report](https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en) from the EEAS published February 7th, 2023.

The properties for the Filigran objects in Figure 5 are termed “attributes” and are listed in the Filigran documentation on their [Notion page](https://www.notion.so/filigran/OpenCTI-FIMI-DAD-STIX-2-1-Model-8b2cca33ec1b473f933892a7b59d610d#0465dc202aa84601b75f6529630452bc). Note that the Filigran documentation also includes the relationships between the objects.

The power of structured threat information is most visible in properties which identify objects. See the “ID or Name” column in Table 1 for examples. These identifying properties allow our machines to “join the dots”. By so doing, the machines can perform link analysis and build out a more comprehensive graphical picture of the threat environment. Take the “ID or Name” property of the object “Community” in my simplified data model. If we codify all of our research in STIX format and store all related objects into a database such as OpenCTI, then when we load up a new disinformation report such as “BALTHOR FOR PRESIDENT”, we may find that “sepsis.zone” already exists in the database from a previously codified campaign, and, for example, that its leaders have a criminal history. Or we may find that User Account “@dbumpus” has already been reported by another organization in our information sharing community or ISAC and through this connection we might establish that he is an agent of the Russian government.

Presently the identification of connections to existing objects in an OpenCTI database and the creation of relationships to these objects needs to be done manually. With the recent $5M injection of funds into Filigran, however, the roadmap includes automation of these connections. That is the power of machine-readable structured threat intelligence[[10]](#footnote-10). Of course, to get these benefits, we all need to decide as a community what these identifiers are going to be and which datatype we are going to use, whether string, integer, long etc. That’s where the DAD-CDM STIX extensions come in.

Identifying Objects and Defining Vocabularies

We need to agree on how we are going to identify objects so that we can join the dots properly. If some researchers codify the User Account as “@dbumpus” and others as “dbumpus” then we may end up with a lot of false negatives in our research. We need to agree as a community on whether to include the “@” or not. Beyond that, for objects that have some permanence to them, we need to agree on their names. Thus, if we cannot agree whether to use the country code “GB” or “UK” for the United Kingdom of Great Britain then we are going to make it harder for our machines to join the dots.   
  
This is where taxonomies come in. Taxonomies are used to classify and identify objects. For example, the DISARM Frameworks use a taxonomy for well-known disinformation incidents and campaigns: these have a “disarm\_id” and a “name”[[11]](#footnote-11). For example, the incident with the disarm\_id “I00005” has a name of “Brexit vote”, a “year\_started” of “2016”, an “attributions\_seen” of “Russia”, a “found\_in\_country” of “UK”, and a “urls” of <https://www.forbes.com/sites/emmawoollacott/2018/11/01/russian-trolls-used-islamophobia-to-whip-up-support-for-brexit/#1369afb665f2>. In STIX, taxonomies are implemented using vocabularies. Where you must choose from a predefined list, these are fixed vocabularies called “enumerations”. Where it is recommended but not obligatory to choose from a predefined list these lists are called “open vocabularies”. Here is the STIX documentation:  
  
“Enumerations and open vocabularies are defined in STIX in order to enhance interoperability by increasing the likelihood that different entities use the same exact string to represent the same concept. If used consistently open vocabularies make it less likely that one entity refers to the energy sector as "Energy" and another as "Energy Sector", thereby making comparison and correlation easier. While using predefined values from STIX vocabularies is strongly encouraged, in some cases this may not be feasible. To address this, producers are permitted to use values outside of the open vocabulary. In the case of enumerations, producers are required to use only the values defined within the STIX specification.”[[12]](#footnote-12)

Depending on which objects we decide to define in DAD-CDM we may need an open vocabulary for the Channel, Community, and or User Account objects which allows us to capture legitimate values for the “Type” property, such as “Discussion Forum”, “Telegram Channel”, “Facebook Page” etc. As you see from Table 1 we might also want open vocabularies for long-standing geopolitical narratives. For example, the long-standing master narrative of Iran revolves around the martyrdom of Imam Hussein in 680 CE, in Karbala, in modern-day Iraq. The grandson of the Prophet Muhammad, Hussain was betrayed and killed in a battle with his Sunni rivals over who succeeded his grandfather. This battle fueled the schism between Sunni and Shia Islam[[13]](#footnote-13).   
  
We could provide such master narratives with a short catchy name and an identification such as “N00023”. When working with the World Health Organization during the COVID pandemic, SJ Terp codified 163 narratives related to COVID-19 misinformation. For example, “N0001” is “Gargling with bleach will prevent or cure COVID-19”11. Most likely, DAD-CDM would not maintain such narratives but rather use a property with a data type of “external-reference”, described in the STIX documentation as “A non-STIX identifier or reference to other related external content”[[14]](#footnote-14). In the case of geopolitical master narratives, a DAD-CDM user in the US might point, for example, to a taxonomy maintained by the Council on Foreign Relations, while in the case of COVID-19 narratives, a DAD-CDM user in Asia Pacific might point to a taxonomy maintained by the World Health Organization. We might take the same approach with DISARM TTPs, in the same way that STIX uses external references to point to externally defined taxonomies of cyber-attacks such as CAPEC[[15]](#footnote-15).

Where DAD-CDM could potentially provide a contribution is in getting the counter-disinformation community to agree on a taxonomy of disinformation themes. Jake Shapiro’s Foreign Influence Efforts database, for example, uses the “Key” property of its “Topic” object with examples such as the following: “Economic Issues”, “Gun Control”, “Immigration”, “Military Operations”, “Political Party”, “Climate Change”[[16]](#footnote-16). New York University Abu Dhabi classifies the following “Domains of Interest” in its threat model: “National Security”, “Democracy”, “Economy”, “Public Safety”, and “Public Health”[[17]](#footnote-17). The European External Action Service uses the property “Label” of its “Incident” object and lists several examples in its first FIMI report, including “Russian invasion of Ukraine”, “Russian influence”, “Attacks against public officials”, “Chinese influence”, “Energy crisis”, “Bioweapons”, “Nuclear weapons”, “War crimes”, “Gender disinformation”[[18]](#footnote-18). The Atlantic Council’s codebook “Dichotomies of Disinformation” lists the following “Topics” in its “Content” object: “Government”, Military”, “Political Party”, “Elections”, “Non-State Political Party”, “Business”, “Influential Individuals”, “Racial, Ethnic, Religious, or “Sexual Identity Group”, “Terrorism”, “Immigration”, “Economic Issue”, “Other”[[19]](#footnote-19).

The FIMI-ISAC in Europe is planning on standardizing certain taxonomies for use by its members. Perhaps we can leverage these.   
  
For some objects, however, vocabularies will not be possible, especially those of an ephemeral nature, or those that are simply too numerous. This includes Content. In our use case, I have used a fuzzy hash to identify a piece of content. [Fuzzy](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-168.pdf) or [piecewise](https://www.sciencedirect.com/science/article/pii/S1742287606000764) hashing is used when we want to correlate or compare objects that are similar but not identical. This is the case, for example, with cloned websites identified using the SSDeep algorithm. We can potentially use this approach to correlate or compare content that morphs over time across social media from its original source instance to the intermediate forms of the content modified by “useful idiots” along the way to the final instance that reaches its target. This approach might enable us to get a handle on the flow of misinformation.

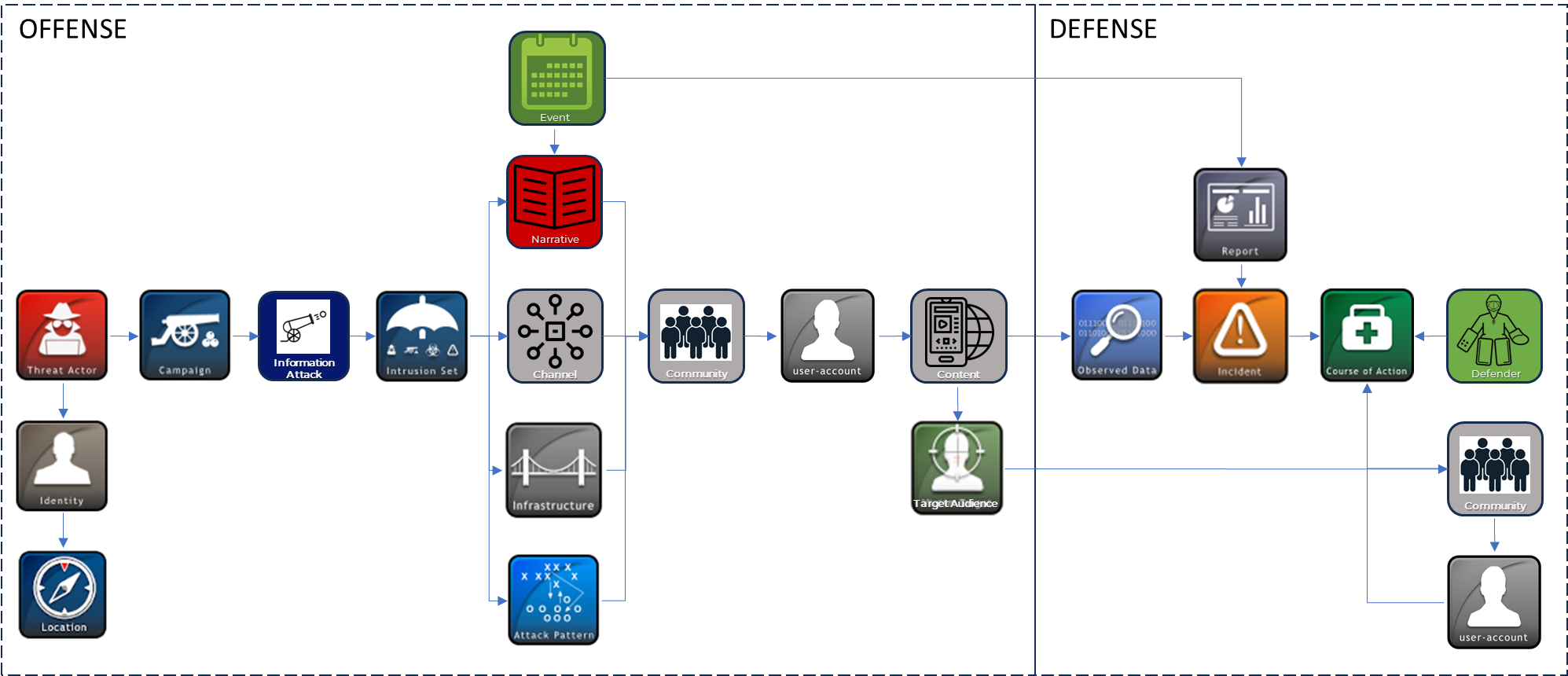


Figure Hypothetical Simple STIX Model of Disinformation Threat and Response

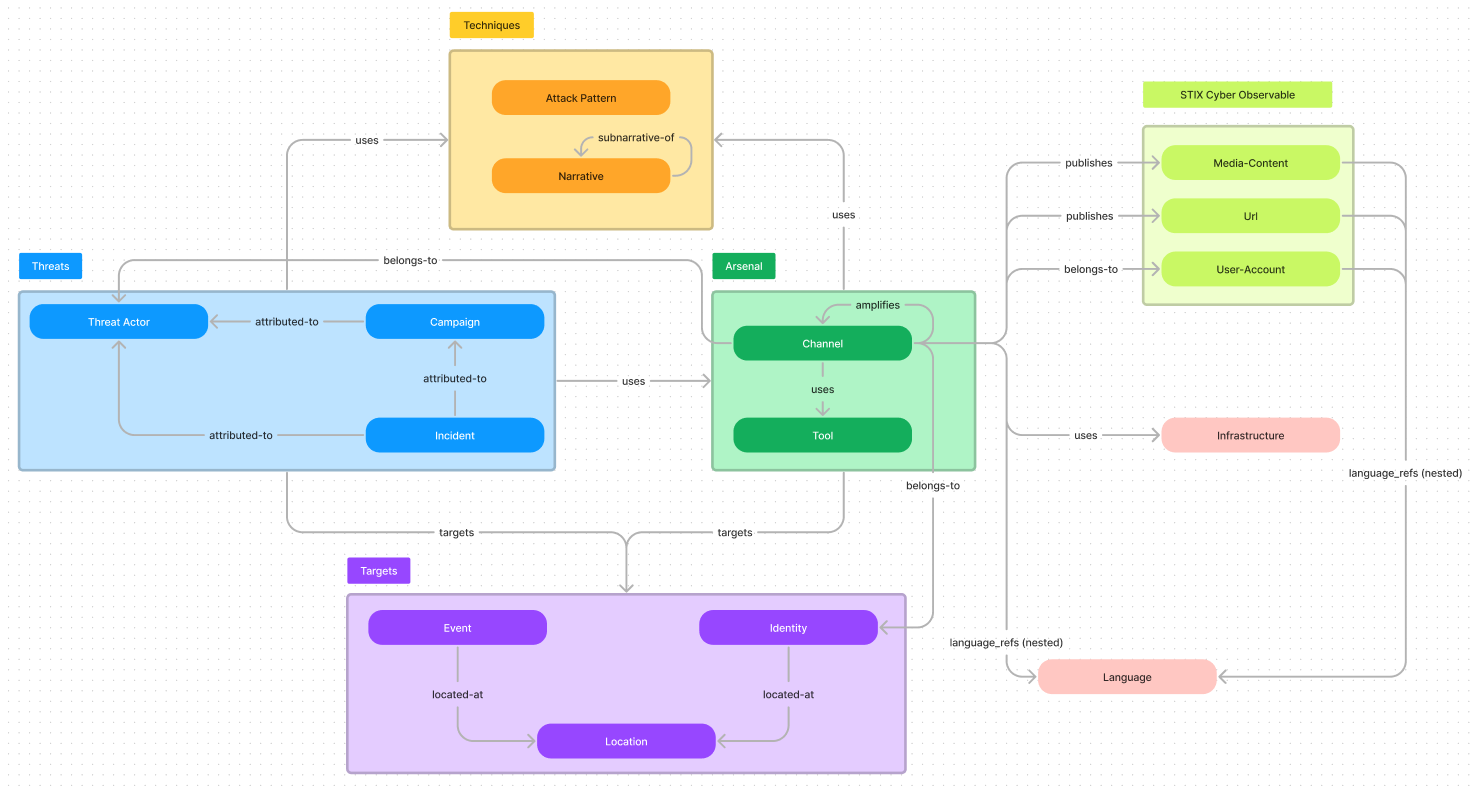


Figure Filigran Disinformation Model

1. For an overview see <https://www.cyberresilienceinstitute.org/training/stix-2-1-programmers-guide/>. For details see the full specification at <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>. For best practice guidance see <https://docs.oasis-open.org/cti/stix-bp/v1.0.0/stix-bp-v1.0.0.html>. [↑](#footnote-ref-1)
2. This is the way I use the term. Steven Bradley too. It is a catchall term for everything in the disinformation threat model other than behaviors. Is that too broad or confusing, given that STIX defines STIX Cyber observables quite specifically? [↑](#footnote-ref-2)
3. [Microsoft PowerPoint - Cyber Observable eXpression (CybOX) Use Cases - (ITSAC 2011) - Sean Barnum.pptx (mitre.org)](https://cybox.mitre.org/documents/Cyber%20Observable%20eXpression%20(CybOX)%20Use%20Cases%20-%20(ITSAC%202011)%20-%20Sean%20Barnum.pdf) [↑](#footnote-ref-3)
4. The policy for STIX Extensions is available at [STIX TC Extension Definition Policy - version 1.1 - Google Docs](https://docs.google.com/document/d/1cGAQy93KuYZAgYUbzSomU_WIeDSUP4H7OVwbaBX5Szc/edit). What is not clear to me is how to categorize an object as an SCO versus an SDO. SCOs are defined “for characterizing host-based and network-based information” of a granular nature. They include ephemeral data such as network traffic, emails, and processes, and potentially more stable data such as user accounts and software. Where would online communities or target audiences fit? They are more stable and less ephemeral than network traffic or emails, but they are also numerous. [↑](#footnote-ref-4)
5. <https://docs.oasis-open.org/cti/stix-bp/v1.0.0/cn01/stix-bp-v1.0.0-cn01.html#_Toc111555349> [↑](#footnote-ref-5)
6. For a conservative take on this debate see <https://www.nas.org/blogs/article/curtailing-the-censorship-industrial-complex>. For a more liberal take see [Digital Bridge: GDPR turns 5 — Censorship vs accountability — TTC4’s China paradox – POLITICO](https://www.politico.eu/newsletter/digital-bridge/gdpr-turns-5-censorship-vs-accountability-ttc4s-china-paradox/). [↑](#footnote-ref-6)
7. [2020-How\_do\_you\_define\_a\_problem\_like\_influence.pdf (carnegieendowment.org)](https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf) [↑](#footnote-ref-7)
8. For properties of SDOs see [here](https://www.cyberresilienceinstitute.org/wp-content/uploads/articulate_uploads/an-introduction-to-the-stix-2-1-data-model-scorm12-kKIpV39s/scormcontent/index.html#/lessons/WmOeiBLT7-VfV-eIv1w2lh9CFawimV14). For SCOs see [here](https://www.cyberresilienceinstitute.org/wp-content/uploads/articulate_uploads/an-introduction-to-the-stix-2-1-data-model-scorm12-kKIpV39s/scormcontent/index.html#/lessons/O90tQtn9a0_z8lE0G6NB80efVU3eTc2O). [↑](#footnote-ref-8)
9. Not publicly available. We could request that DAD-CDM PGB members get access to this. [↑](#footnote-ref-9)
10. For an explanation of the power of structured treat intelligence I recommend the chapter “Structured Intelligence – What Does It Even Mean?” in Aaron Roberts’ *Cyber Threat intelligence. The Non-Nonsense Guide for CISOs and Security Managers*. 2021. <https://www.amazon.com/Cyber-Threat-Intelligence-No-Nonsense-Security/dp/1484272196>. [↑](#footnote-ref-10)
11. <https://github.com/DISARMFoundation/DISARMframeworks/blob/main/DISARM_MASTER_DATA/DISARM_DATA_MASTER.xlsx>. [↑](#footnote-ref-11)
12. <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_vbsdt43uxrv0> [↑](#footnote-ref-12)
13. <https://cis.mit.edu/publications/analysis-opinion/2022/clashing-narratives-keep-us-and-iran-odds> [↑](#footnote-ref-13)
14. <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_72bcfr3t79jx> [↑](#footnote-ref-14)
15. <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_axjijf603msy> [↑](#footnote-ref-15)
16. [Introducing the Online Political Influence Efforts dataset - Diego A Martin, Jacob N Shapiro, Julia G Ilhardt, 2023 (sagepub.com)](https://journals.sagepub.com/doi/10.1177/00223433221092815) [↑](#footnote-ref-16)
17. <https://www.ndss-symposium.org/wp-content/uploads/2023-657-paper.pdf> [↑](#footnote-ref-17)
18. <https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en> [↑](#footnote-ref-18)
19. <https://github.com/DFRLab/Dichotomies-of-Disinformation> [↑](#footnote-ref-19)