

EDMO BELUX 2.0

OpenCTI-coded case studies of FIMI campaigns targeting Belgium and Luxembourg

Maria Giovanna Sessa (EU DisinfoLab)

June 2025

Co-funded by the European Union. Views and opinions expressed are however those of the author(s)



Co-funded by
the European Union

only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

We are witnessing Foreign Information Manipulation and Interference (FIMI) campaigns becoming increasingly complex, coordinated, and transnational in nature. According to the definition provided by the [European External Action Service](#), FIMI consists of state or non-state actors conducting manipulative, intentional, and coordinated activities, although “mostly non-illegal”, that target a country’s values, procedures, and processes. Therefore, not all disinformation is FIMI, and not all FIMI employs disinformation.

Yet, much of the analysis across the defender community remains fragmented, due in part to the lack of a shared language and structured data model to map and analyse FIMI incidents. This disconnect makes it difficult to link insights across cases – leading to missed patterns, attribution gaps, and an overall weakened response. In this report, we explore how the use of STIX 2.1 and OpenCTI can help address this challenge. We present five disinformation campaigns targeting Belgium and Luxembourg as case studies, demonstrating how complex narratives can be transformed into structured threat intelligence.

By encoding FIMI incidents into STIX objects and feeding them into OpenCTI, we are not only standardising data but also surfacing relationships that are often missed in traditional narrative analysis. This enables a comparative approach across campaigns – for example, allowing us to spot recurring TTPs, shared infrastructure, or clusters of actors operating across language and platforms. These insights enable new layers of interpretation, turning raw data into actionable intelligence, and laying the groundwork for a more coordinated and resilient defense against foreign information interference.

AN INTRODUCTION TO STIX, OPENCTI, AND THE CODING OF THE EVIDENCE-BASED CASE STUDIES

What is STIX language?

The defender community produces a wealth of valuable reports, investigations, and analyses, but the lack of a common language and harmonised data collection standards risks fragmenting this knowledge. Without consistent terminology and structured data, we may fail to track recurrent offenders, recognise common patterns, or identify relationships between elements. Moreover, establishing shared frameworks for data collection and sharing allows researchers to connect emerging findings to broader disinformation and foreign interference campaigns. Therefore, it is essential to ensure that insights contribute to a more comprehensive, interconnected understanding of disinformation campaigns.

[Structured Threat Information Expression](#) (STIX) helps achieve such standardisation.

Developed by the MITRE corporation and now maintained under the governance of OASIS (Organisation to the Advancement of Structured Information Standards, STIX was originally created to enable cyber threat intelligence sharing in a consistent, machine-readable format. Since its inception, STIX has evolved through multiple versions – with STIX 2.1 being the current standard.

Therefore, incidents and campaigns are broken down into their key components – known as STIX Core Objects – based on the information available. These consist of:

- [STIX Domain Objects \(SDO\)](#): These objects represent behaviours and analytical constructs that threat analysts use to assess and interpret the threat landscape. They help provide context, structure, and deeper insights into potential threats.

- STIX Cyber-observable Objects (SCO): These objects represent observed facts about a network or host. They help provide a more detailed view of potential threats by linking lower-level observations to higher-level intelligence.
- STIX Relationship Objects (SRO): These objects establish connections between different STIX components, including SDO and SCO. By linking these elements, they contribute to a more comprehensive understanding of the threat landscape.

For example, one can imagine an interference campaign that spreads a forged press release on social media. On the one hand, the campaign itself would be represented as a STIX Domain Object (SDO). On the other hand, the fake URL or email used to spread would be captured as a STIX Cyber-observable Object (SCO). Finally, a STIX Relationship Object (SRO) would link these two, indicating that the fake email or URL was used as part of the campaign. The difference between these components will become clearer as we delve into OpenCTI and its coding.

What is OpenCTI?

[OpenCTI](#) is an open-source platform designed to help the collection, analysis, and sharing of cyber threat intelligence. It enables users to structure threat information using STIX 2.1 format, correlate different intelligence sources, and visualise threats. This sort of repository is currently used by a large part of the counter-disinformation community to encode complex disinformation and FIMI incidents and campaigns, dissected into their key components (e.g., actors, tactics, distribution channels, etc.)

By integrating OSINT, fact-checking reports, and investigative journalism data, OpenCTI helps establish connections between state and non-state actors engaged in disinformation, facilitating attribution of coordinated campaigns. The platform's collaborative nature supports cross-sector intelligence sharing among governments, fact-checkers, researchers, and civil society organisations, reinforcing a more resilient response to disinformation threats.

While OpenCTI offers many advantages, it also has some limitations. As a platform designed for advanced threat intelligence workflows, it presents two key challenges. First, it requires a solid understanding of threat intelligence analysis, including STIX 2.1. Second, it lacks disinformation-specific features, such as dedicated taxonomies for encoding Foreign Information Manipulation and Interference (FIMI). Additionally, since encoding disinformation involves qualitative elements like narratives, there is a risk of inconsistencies that hinder standardisation.

How does OpenCTI work?

Before delving into the case studies, some [terminological clarifications](#). (Note: These terms are not only technical definitions but also function as analytical tools within the structured threat intelligence process.) For a more comprehensive explanation of how to operate OpenCTI, we recommend Viginum's dedicated [guidebook](#).

- **Reports:** They are collections of threat intelligence on specific topics (e.g., threat actors, malware, or attack techniques), with relevant context and details. They are used to group related intelligence into a comprehensive cyber threat story using STIX 2.1. This deliverable turns five case studies of disinformation campaigns targeting Belgium and Luxembourg into structured OpenCTI reports. In simpler terms, what we refer to as “case study” (i.e., the coding of a single FIMI campaign, OpenCTI calls “report”).

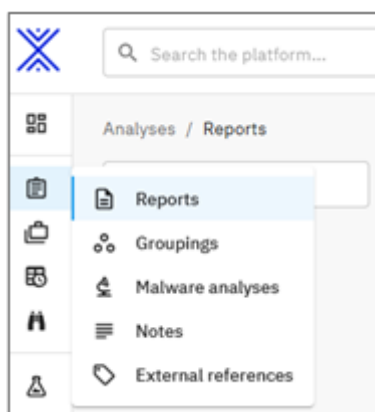


Figure 1. Screenshot of the “Analyses” section in OpenCTI, where “Reports” are collected

- Overview: This tab contains all properties of the report and recent activities.

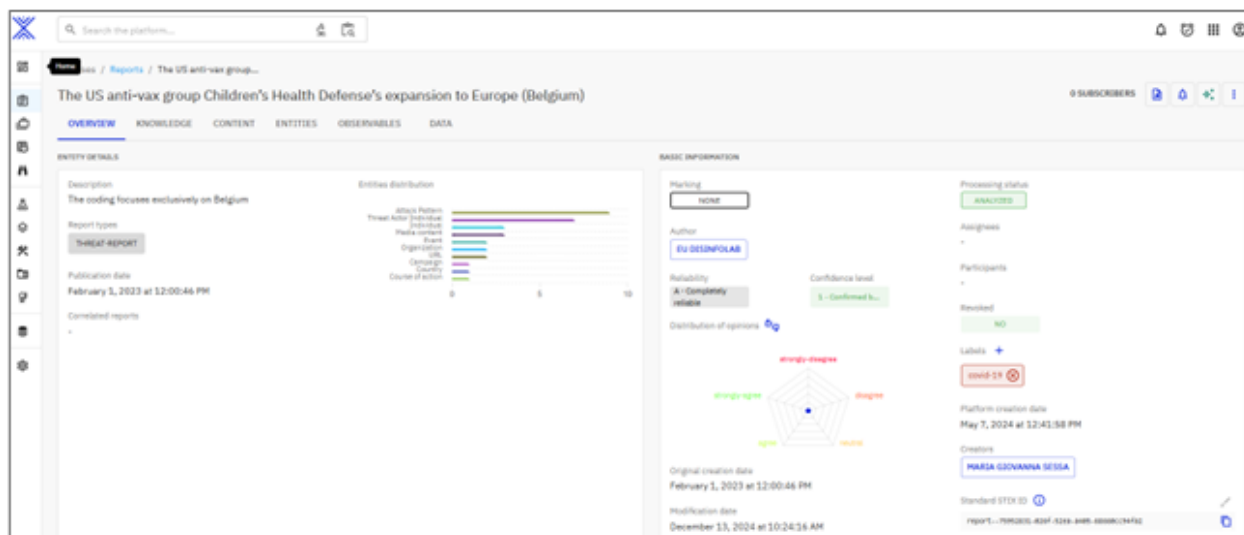


Figure 2. Screenshot of a Report's "Overview" section in OpenCTI

- Knowledge: This tab groups all the structured knowledge contained in the report, visually represented in the so-called diamond model. The Knowledge tab visualisation is the reference for our analysis of the five case studies that populate this deliverable. It is also where the STIX Relationship Objects (SRO) become visible. SROs link together different STIX components – such as connecting a campaign (SDO) to the fake accounts used to spread it (SCO). These links allow to map relationships and thus form the backbone of the analytical graph (shown as segments connecting SDOs and SCOs).

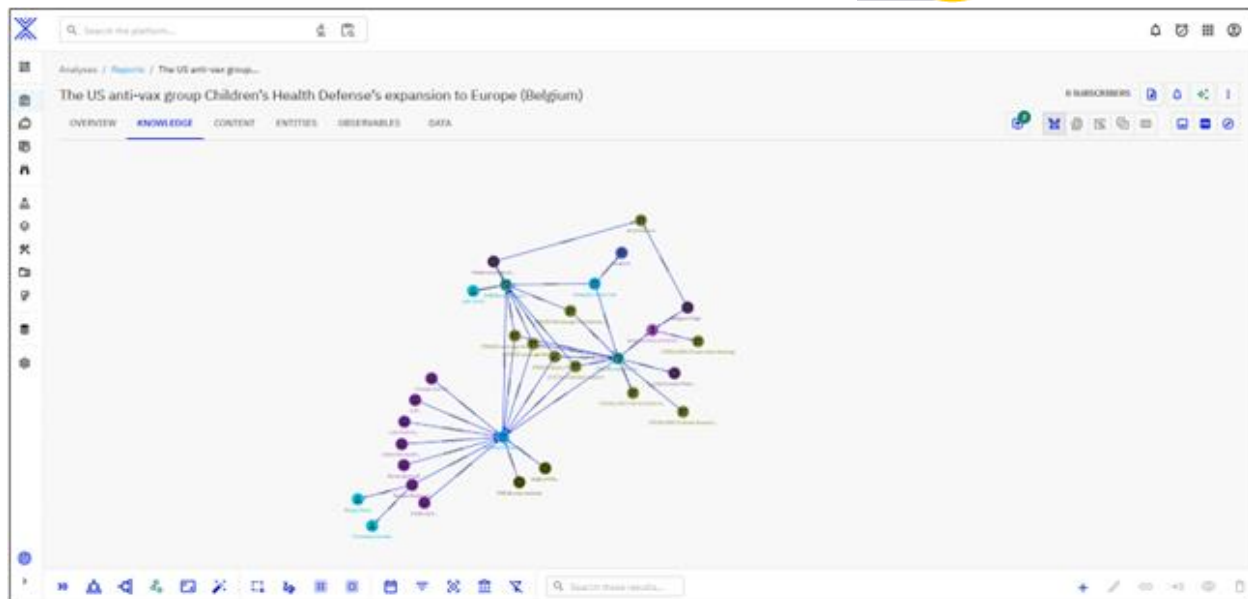


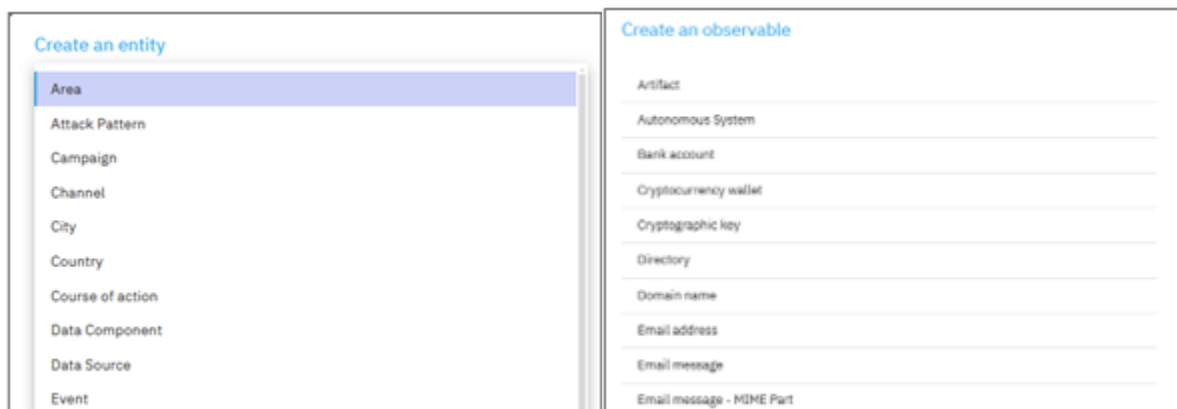
Figure 3. Screenshot of the Report's "Knowledge" section in OpenCTI

- **Content:** This tab allows for the uploading of content-related documents (e.g., the PDF of the encoded investigation or a written deliverable).
- **Entities:** This tab lists all Stix Domain Objects (SDO) contained in the Report, with search and filters available. When creating an entity, coders can choose from a list of SDOs including, among other things, the country where the incident took place, the Attack Pattern (i.e., the TTPs), or the Course of Action (i.e., incident response).

Two specifications:

- **Attack Pattern:** In OpenCTI, attack patterns help categorise threat actor behaviours and provide insight into the Tactics, Techniques, and Procedures (TTPs) used.

- MITRE ATT&CK: OpenCTI natively supports [MITRE ATT&CK](#), which is a globally recognised framework that categorises TTPs used by cyber adversaries (e.g. phishing, impersonation, data obfuscation, etc.). MITRE developed and maintains the STIX standard. and represent how attackers operate.
 - DISARM: OpenCTI can also leverage the [DISARM Framework](#), specifically designed for modelling and analysing disinformation tactics (e.g. distorting facts, segmenting the audience, establishing inauthentic news sites, etc.).
 - *Course of Action*: The CoA represents defensive measures, mitigation strategies, or response actions that organisations can take to prevent, detect, or respond to a cyber threat. In OpenCTI, CoAs are used to link attack patterns with recommended countermeasures.
-
- **Observables**: This tab contains all Stix Cyber Observables (SCO) in the report, with search and filters available. When creating an entity, coders can choose from a list of SCOs including, among other things, domain names, bank account, or email addresses connected to the FIMI campaign.



The screenshot displays two side-by-side panels from the OpenCTI interface. The left panel, titled 'Create an entity', features a list of entity types: Area, Attack Pattern, Campaign, Channel, City, Country, Course of action, Data Component, Data Source, and Event. The 'Area' option is currently selected and highlighted in blue. The right panel, titled 'Create an observable', shows a list of observable types: Artifact, Autonomous System, Bank account, Cryptocurrency wallet, Cryptographic key, Directory, Domain name, Email address, Email message, and Email message - MIME Part. Each type is followed by a horizontal line indicating a text input field.

Figure 4. Screenshot of list of entities and observables in OpenCTI

- Data: This tab contains documents that are associated to the report, either uploaded to or generated from the platform.

What are we coding?

The rest of this document elaborated on the coding of five case studies as OpenCTI Reports. These are disinformation and foreign influence campaigns that EDMO BELUX partners and other researchers have previously covered. For each one, we will provide a short summary, focusing exclusively on the parts that concern Belgium and Luxembourg. Then, we will comment on the Knowledge graph view to describe our OpenCTI coding, focusing on Entities/SDO, Objects/SCO (displayed as graph nodes and coloured depending on their type) and their Relationships/SRO (displayed as graph links). Key insights are highlighted within each individual case study, and summarised comparatively in the concluding remarks. Moreover, the findings are linked to Tactics, Techniques, and Procedures (TTPs) drawn from the [DISARM Red Framework](#), which is a methodological framework specifically developed to identify, categorise, and analyse disinformation behaviours.

The chosen case studies focus on FIMI campaigns targeting Belgium and Luxembourg. A few of these cases (the first, second and fourth in the list below) were previously documented by EDMO BELUX, allowing us to build on existing findings and ensure analytical continuity within the project. This selection supports a form of secondary analysis, drawing on prior investigations to re-express known campaigns through structured threat intelligence. By doing so, we aim not only to validate and enrich earlier insights, but also to surface new patterns through the use of STIX and OpenCTI.

1. Pro-Russian disinformation on Telegram, based on: Maria Giovanna Sessa, Tom Willaert and Jeroen Van Soest, “The disinformative ecosystem. Link sharing practices on Telegram as evidence of cross-platform amplification,” *EDMO Belux*, 9 November 2022. Available at: <https://belux-edmo.s3-accelerate.amazonaws.com/wp->

[content/uploads/2023/03/EDMOBELUX_The-disinformative-ecosystem-FINAL-updated.pdf](#).

2. Children's Health Defense, based on: Roman Adamczyk and Alexandre Alaphilippe, "The US anti-vax group Children's Health Defense's expansion to Europe," *EDMO Belux*, January 2023. Available at: <https://belux-edmo.s3-accelerate.amazonaws.com/wp-content/uploads/2023/02/20230131-Childrens-Health-Defense-Europe.pdf>.
 3. #Qatargate, based on: Louis Colart and Joël Matriche, "La grotesque campagne de désinformation en ligne autour du Qatargate," *Le Soir*, 14 August 2023. Available at: <https://www.lesoir.be/531047/article/2023-08-14/la-grotesque-campagne-de-desinformation-en-ligne-autour-du-qatargate>.
 4. Facebook Hustles, based on: Maria Giovanna Sessa, "Facebook Hustles: The Belgian spin-off," *EU DisinfoLab*, 26 July 2023. Available at: <https://www.disinfo.eu/publications/facebook-hustles-the-belgian-spin-off/>.
 5. Paperwall, based on: Alexandre Alaphilippe, "PAPERWALL: Chinese information operation targets Belgium and Luxembourg," *EU DisinfoLab*, 14 March 2024. Available at: <https://www.disinfo.eu/paperwall-chinese-information-operation-targets-belgium-and-luxembourg>.
1. **The disinformative ecosystem. Link sharing practices on Telegram as evidence of cross-platform amplification**
 - This case study (Sessa et al., 2022) examines pro-Russian disinformation across 30 Dutch-speaking Telegram channels. Initially focused on pandemic-related falsehoods, these communities later shifted to spreading anti-Ukraine narratives, a transition enabled by the lack of content moderation on the encrypted messaging app.

- The study extracted the 30 most frequently shared domains between August 2018 and September 2022. The study highlights the complexity of the disinformation ecosystem, which includes mainstream and fringe social media platforms, mainstream and fringe news outlets, authoritative sources, as well as publishing and crowdfunding platforms.

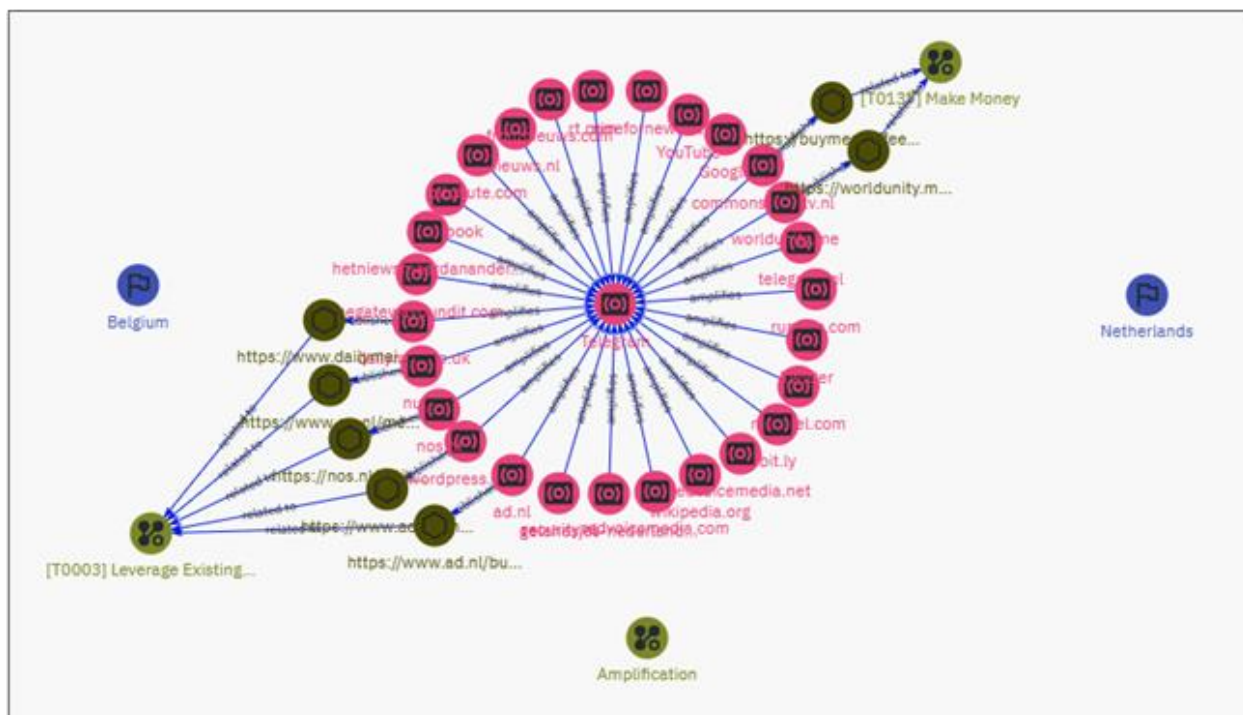


Figure 5. Screenshot of the “Knowledge” graph view in OpenCTI for the report on Pro-Russian disinformation on Telegram (visualisation elaborated by the author of this report)

ENTITIES (SDO)	
Channels	Relationship (SRO):
<ul style="list-style-type: none"> Telegram: main platform for this study. BitChute: alt-tech social media platform. Het Nieuws Maar Dan Anders: Dutch-speaking disinformative website. RT.com: Russian state-media. YouTube: mainstream video-streaming social media platform. Etc. (for the other channels see Figure 5) 	<ul style="list-style-type: none"> The various channels include a multitude of mainstream and fringe outlets, which are all related to Telegram in the sense that they get amplified by the encrypted messaging app.
Country:	Relationship (SRO):
<ul style="list-style-type: none"> Belgium 	<ul style="list-style-type: none"> We did not include relationships with the two countries to avoid visual overload. However, all the media

<ul style="list-style-type: none"> Netherlands 	mentioned are targeted in Dutch-speaking communities in Belgium and the Netherlands.
Attack pattern:	Relationship (SRO):
<ul style="list-style-type: none"> [T0003] Leverage Existing Narratives [T0137] Make money Amplification 	<ul style="list-style-type: none"> The study reports some content from the channels amplified on Telegram, which either leverage pandemic-related conspiracies or fundraise to continue their activities. We did not include relationships for the amplification attack pattern to avoid visual overload, which involves all the channels identified.
OBSERVABLES (CDO)	
URL (i.e., some links shared within the Telegram channels):	Relationship (SRO):
<ul style="list-style-type: none"> “Buy me a coffee” (source: CommonSenseTV). “Donate with cryptocurrency” (source: World Unity). 	<ul style="list-style-type: none"> Each URL is connected to the channel that “publishes” the content and is “related to” an attack pattern, either leveraging existing narratives or monetising.

<ul style="list-style-type: none"> • “Cause of death of actor Rik Mayall remains a mystery to wife” (source: AD). • “Children victims of abuse and violence at aid organisation SOS Children’s Villages” (source: AD). • “Deadly outbreak at Flemish care center puts Colombian variant in spotlight” (source: NOS). • “KRO-NCRV director wants Ongehoord Nederland removed from broadcasting system immediately” (source: Nu). • “Veteran NASA engineer says she’ll RETIRE if her application for a religious exemption from COVID vaccine is rejected and insists it’s her First Amendment right NOT to get the shot” (source: Mail Online). 	
---	--

This case study highlights a dense and layered disinformation ecosystem that cuts across platform boundaries [T0119.002: Post Across Platform]¹ [T0080: Map Target Audience Information Environment], linguistic communities, and content formats. The link-sharing behaviour observed in Dutch-speaking Telegram channels [T0043: Chat apps] illustrates how Telegram functions as a central amplification hub for both fringe and mainstream content. Disinformation narratives – particularly those tied to the COVID-19 pandemic and, later, anti-

Ukraine sentiments [T0003: Leverage Existing Narratives] [T0022: Leverage Conspiracy Theory Narratives] [T0118: Amplify Existing Narratives] – were circulated through a web of domains that include Russian state media [T0002: Facilitate State Propaganda], alt-tech platforms, disinformative domestic sites, and even reputable mainstream outlets [T0114.001: Social Media] [T00114.002: Traditional Media]. The use of Telegram as a permissive, unmoderated infrastructure enabled the sustained circulation of polarised content [T0124.003: Exploit Platform TOS/Content Moderation].

The visual coding (Figure 5) exposes how economic incentives and narrative strategies intersect. Multiple observables – such as URLs linking to donation platforms [T0017.001: Conduct Crowdfunding Campaigns] – show that these Telegram channels actively try to monetise, suggesting that the spreading of conspiracy content is both ideologically and financially opportunistic. The relationships visualised in the graph suggest a coordinated ecosystem that tackles Dutch-speaking communities in Belgium and the Netherlands [T0072.001: Geographic Segmentation] [T0102: Leverage Echo Chambers/Filter Bubbles].

2. The US anti-vax group Children’s Health Defense’s expansion to Europe

- This case study (Adamczyk & Alaphilippe, 2023) explores the spread of health-related disinformation, highlighting how foreign actors promoting anti-vaccine narratives have infiltrated Belgium and EU institutions through the establishment of a non-profit organisation, high-profile events that garnered media attention, and lobbying efforts.
- Children’s Health Defense Europe (CHD), constituted as a non-profit in Belgium on 27 August 2020, is the European version of Robert Kennedy Jr’s anti-vax movement Children’s Health Defense.
- The investigation was conducted in the framework of EDMO BELUX 1.0. As this deliverable has a clear geographic interest, the coding of the report into OpenCTI only focuses on the parts that clearly concern Belgium, although the organisation has ties to

the United States, organised events in Germany and Switzerland, and received support from German personalities and Italian fringe media.

- The investigation identified a series of individuals working for CHD Europe who contacted Members of the European Parliament.
- Two press conferences on 23 January 2022 and 14 November 2022 were held at the Brussels Press Club and received media coverage by Belgian fringe media. One counted on the participation of a MEP, and another launched a lobbying campaign called #HandsOffOurChildren against the COVID-19 vaccination of children.

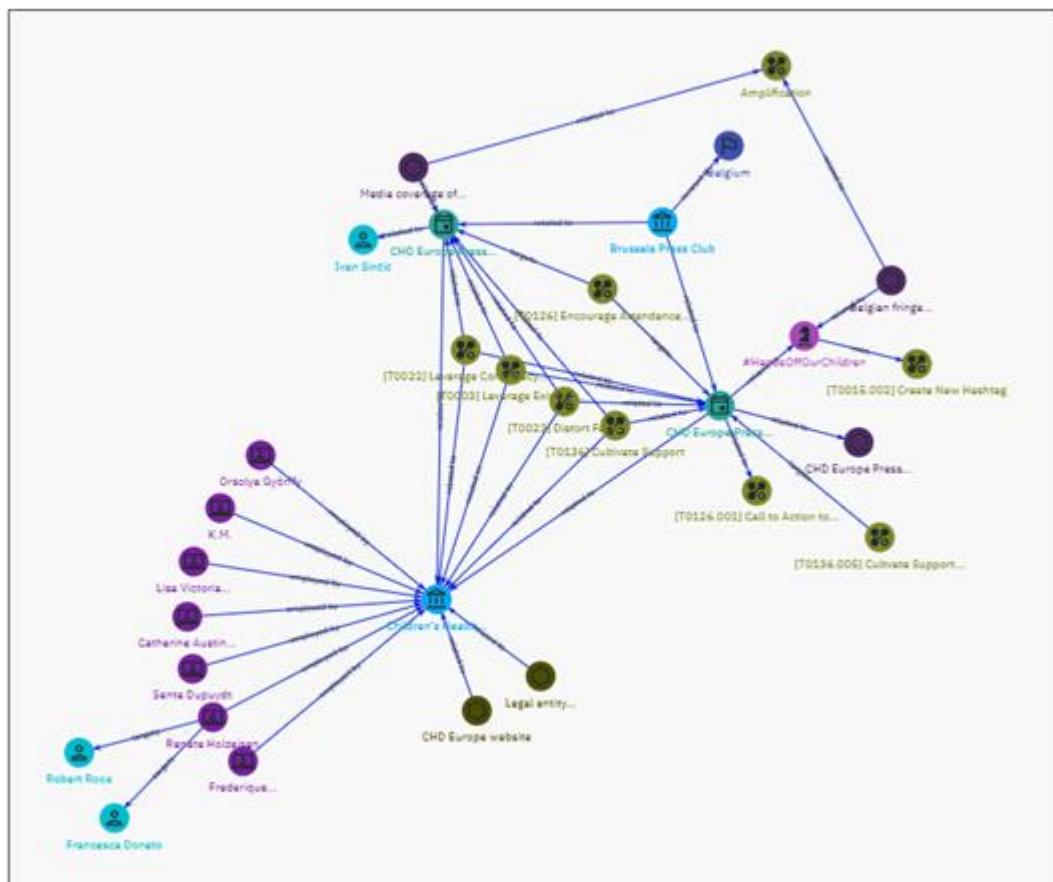


Figure 6. Screenshot of the “Knowledge” graph view in OpenCTI for the report on Children’s Health Defense (visualisation elaborated by the author of this report)

ENTITIES (SDO)	
Organisation:	Relationship (SRO):
<ul style="list-style-type: none"> Children Health's Defense Europe is the central hub of the investigation. The Brussels Press Club provided a platform for the press conference of CHD Europe, including media and politicians. 	<ul style="list-style-type: none"> Threat actors identified in the investigation are "employed by" and press conferences "related to" the organisations.
Threat actors:	Relationship (SRO):
<ul style="list-style-type: none"> Orsolya Györfy: CHD Europe's Executive Director. K.M.: CHD Europe's Operations Specialist. Lisa Victoria Renberg: CHD Europe's Community Coordinator. Etc. (for the other threat actors see Figure 6) 	<ul style="list-style-type: none"> All these threat actors are "employed by" CHD Europe.

Individuals:	Relationship (SRO):
<ul style="list-style-type: none"> • Francesca Donato: MEP who interacted with CHD Europe. • Robert Roos: MEP who interacted with CHD Europe. • Ivan Sinčić: MEP who interacted with CHD Europe. 	<ul style="list-style-type: none"> • Threat actor Renate Holzeisen, lawyer and CHD Europe board member, “targets” these MEPs. • In the lack of a better option allowed by the platform, the CHD Europe Press Conference (23/01/2022) is encoded as “related to” Ivan Sinčić, who attended it.
Event:	Relationship (SRO):
<ul style="list-style-type: none"> • CHD Europe Press Conference on 23 January 2022). • CHD Europe Press Conference (14 November 2022). 	<ul style="list-style-type: none"> • The press conferences are “related to” the CHD Europe organisation that organised them and the Brussels Press Club that hosted them, the media coverage they received, the individuals they invited (Ivan Sinčić) or the campaign (#HandsOffOurChildren) they advertised.
Campaign:	Relationship (SRO):
<ul style="list-style-type: none"> • #HandsOffOurChildren: an online campaign supported by CHD Europe as it amplifies its agenda. 	<ul style="list-style-type: none"> • The campaign is “related to” the press conference that amplified it, as well as the Belgian fringe media that amplified the event.

Country:	Relationship (SRO):
<ul style="list-style-type: none"> • Belgium 	<ul style="list-style-type: none"> • The Brussels Press Club is “located at” (in) Belgium.
Attack pattern:	Relationship (SRO):
<ul style="list-style-type: none"> • [T0022] Leverage Conspiracy Theory Narratives • [T0003] Leverage Existing Narratives • [T0023] Distort Facts • [T0136] Cultivate Support • [T0126] Encourage Attendance at Events • [T0126.001] Call to Action to Attend • [T0015.002] Create New Hashtag • Amplification 	<ul style="list-style-type: none"> • CHD Europe is “related to” these attack patterns, which are themselves “related to” the two press conferences. • The attack pattern of encouraging attendance to events “targets” both press conferences. • The CHD Europe Press Conference (14 November 2022) is “related to” a call to action to reach out to MEPs regarding the Green Pass. • The #HandsOffOurChildren campaign “uses” the namesake hashtag. • The media coverage given to the press conference is “related to” the practice of amplification.

OBSERVABLES (CDO)	
URL:	Relationship (SRO):
<ul style="list-style-type: none"> Evidence that CHD Europe was constituted as a non-profit legal entity. CHD Europe's website. 	<ul style="list-style-type: none"> The two URLs are "related to" the CHD Europe organisation.
Media content:	Relationship (SRO):
<ul style="list-style-type: none"> Article from a Belgian fringe media amplifying the CHD Europe Press Conference. Article about CHD Europe Press Event. Article announcing the CHD Europe Press Conference. 	<ul style="list-style-type: none"> The media content is "related to" the event or campaign they provide coverage to as well as the Amplification Course of Action.

This case reveals how the CHD Europe [T0092.001: Create Organisations] serves as a central node in a coordinated foreign information manipulation effort targeting Belgium and European institutions [T0072.001: Geographic Segmentation]. The organisation's ability to infiltrate legitimate political and media spaces [T0093: Acquire/Recruit Network] [T0100.001: Co-opt Trusted Individuals] – such as the Brussels Press Club and direct interactions with members of the European Parliament – demonstrates a sophisticated blending of online and offline tactics. The use of press conferences, campaigns like #HandsOffOurChildren [T0015.002: Create New

Hashtag], and strategic media coverage points to a clear intent to manufacture credibility and drive political influence [T0136: Cultivate Support] [T0126: Encourage Attendance at Events] [T0057: Organise Events] [T0126.001: Call to Action to Attend] .

By linking CHD Europe to various actors and mapping their interactions through press conferences and campaign messaging, the visual representation in OpenCTI (Figure 6) demonstrates how the leveraging of existing narratives [T0003] and distortion of facts [T0023] [T0076: Distort] are repeatedly employed to reinforce anti-vaccine sentiments [T0068: Respond to Breaking News Event or Active Crisis]. The media coverage by fringe media outlets further amplifies these narratives [T0022: Leverage Conspiracy Theory Narratives] [T0081.005: Identify Existing Conspiracy Narratives/Suspicions] into EU discourse, signalling a coordinated effort to erode trust in public health and authoritative sources [T0075.001: Discredit Credible Sources].

3. The online disinformation campaign surrounding Qatargate

- The case study (Colart & Matriche, 2023) covers foreign interference in EU politics, which inevitably fuelled Euroscepticism.
- Uncovered at the end of 2022, #QatarGate was a large-scale corruption scheme designed to buy political influence in the European Parliament, benefiting Qatar's geopolitical interests while undermining EU integrity.
- While Qatar was initially the primary focus, Morocco played a significant role as well. The scandal was also referred to as #BrusselsGate, given the central role of the European capital.
- Several MEPs acted as paid proxies of foreign state actors, who conducted a coordinated disinformation campaign online to discredit individuals involved in the investigation and geopolitical adversaries such as the United Arab Emirates (UAE).

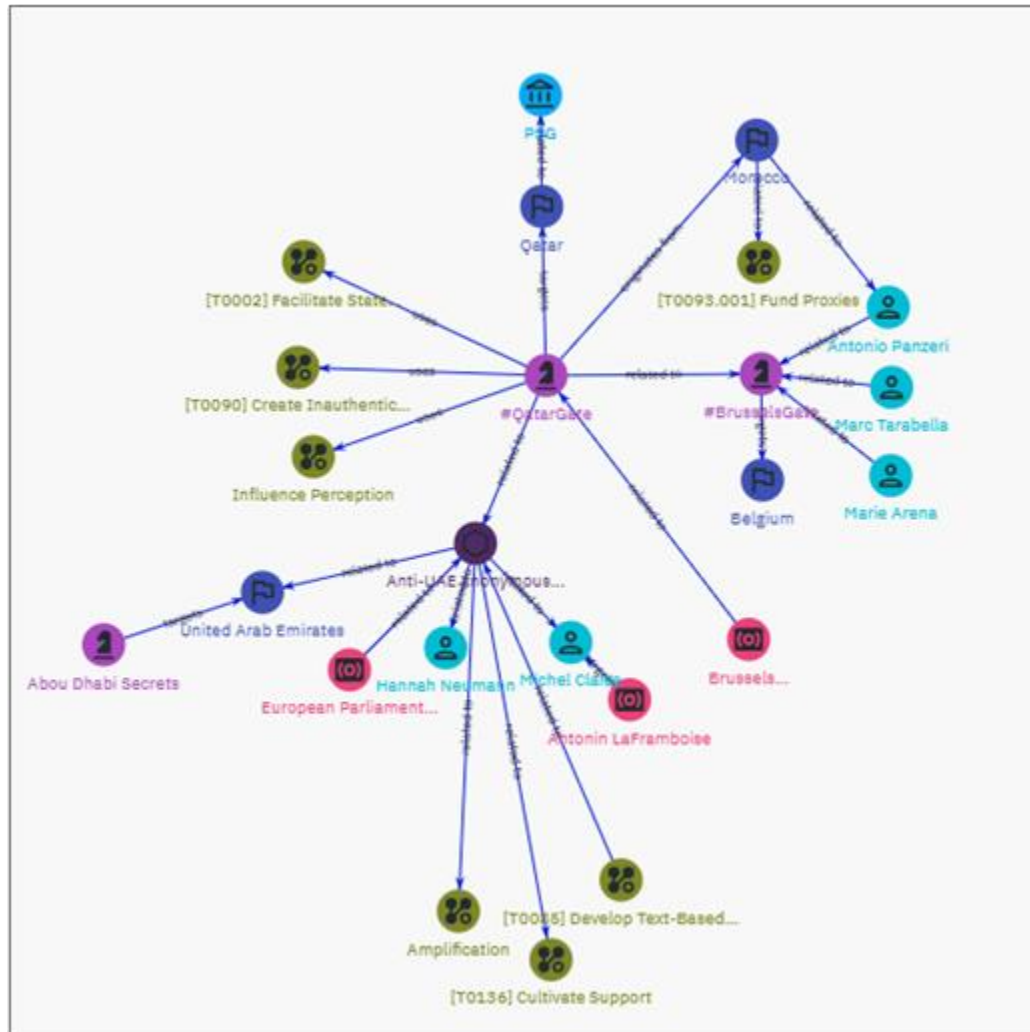


Figure 7. Screenshot of the “Knowledge” graph view in OpenCTI for the report on #Qatargate (visualisation elaborated by the author of this report)

ENTITIES (SDO)	
Organisation:	Relationship (SRO):
<ul style="list-style-type: none"> PSG is the football club owned by Qatar Sports Investments and it has previously employed fake X accounts against adversaries, similarly to those used to target individuals calling out Qatargate. 	<ul style="list-style-type: none"> Qatar is “related to” PSG as it owns it.
Individuals:	Relationship (SRO):
<ul style="list-style-type: none"> Antonio Panzeri: MEP involved in #QatarGate and #BrusselsGate. Marc Tarabella: MEP involved in #QatarGate and #BrusselsGate. Marie Arena: MEP involved in #QatarGate and #BrusselsGate. Hannah Neumann: MEP who denounced #QatarGate. Michel Claise: investigating judge who triggered #QatarGate. 	<ul style="list-style-type: none"> Marie Arena, Marc Tarabella, and Antonio Panzeri are “related to” #BrusselsGate. Maroc paid Antonio Panzeri, and so it “is “related to” paid him. The anti-UAE anonymous articles target Hannah Neumann and Michel Claise, and thus, they are “related to” them.

Channel:	Relationship (SRO):
<ul style="list-style-type: none"> • Antonin LaFramboise: fake X account targeting those calling out #QatarGate. • European Parliament Files: Medium blog that denounced #QatarGate with a series of anonymous articles attacking the United Arab Emirates. • Brussels Whistleblower: fake X account involved in #QatarGate. 	<ul style="list-style-type: none"> • Antonin LaFramboise “targets” Michel Claise. The European Parliament Files and the Brussels Whistleblower are “related to” the anti-UAE anonymous articles and #QatarGate, respectively.
Campaign:	Relationship (SRO):
<ul style="list-style-type: none"> • Abou Dhabi Secrets: Le Soir investigation related to #QatarGate. • #BrusselsGate: scandal related to #QatarGate. • #QatarGate: scandal at the centre of the investigation. 	<ul style="list-style-type: none"> • #QatarGate is “related to” #BrusselsGate. Despite its name, #QatarGate actually “originates from” Morocco. The individuals identified are “related to” these scandals.
Country:	Relationship (SRO):

<ul style="list-style-type: none"> • Belgium: targeted country and scenario of the #BrusselsGate and #QatarGate scandals. • Morocco: main country responsible for the #BrusselsGate and #QatarGate scandals. • Qatar: country involved in the #BrusselsGate and #QatarGate scandals. • United Arab Emirates: country connected to the #BrusselsGate and #QatarGate scandals. 	<ul style="list-style-type: none"> • #BrusselsGate “targets” Belgium. #QatarGate “originates from” Morocco. #QatarGate “targets” Qatar by favouring the country. The anti-UAE anonymous articles used in the scandal are “related to” the United Arab Emirates.
Attack pattern:	Relationship (SRO):
<ul style="list-style-type: none"> • Amplification • [T0136] Cultivate Support. • [T0085] Develop Text-Based Content • Influence Perception • [T0002] Facilitate State Propaganda 	<ul style="list-style-type: none"> • The anti-UAE anonymous articles are “related to” amplification, support cultivation, and the development of text-based content. • The #QatarGate scandal “uses” perception influence, state propaganda and inauthentic accounts to pursue its goals.

<ul style="list-style-type: none"> [T0090] Create Inauthentic Accounts [T0093.001] Fund Proxies 	<ul style="list-style-type: none"> Morocco “is related to” payments to MEPs, acting as proxies.
OBSERVABLES (CDO)	
Media content:	Relationship (SRO):
<ul style="list-style-type: none"> Anti-UAE anonymous articles: published by the European Parliament Files blog. 	<ul style="list-style-type: none"> The #QatarGate scandal as the European Parliament Files are “related to” these articles, which are in turn related to the individuals they target and the abovementioned attack patterns.

The #QatarGate case reveals a sophisticated, multilayered foreign influence operation targeting EU political institutions. State actors – particularly Morocco and Qatar – carried out covert efforts to manipulate the political environment [T0129: Conceal Operational Activity], while simultaneously working to cultivate political support and undermine democratic integrity.

The operations involved direct financial transactions with MEPs acting as proxies [T0093.001: Fund Proxies] who helped advance the malign actors’ agenda. In parallel, the campaign deployed inauthentic social media accounts [T0090: Create Inauthentic Accounts] [T0104: Social Networks] [T0114.001: Social Media] and anonymous blogs [T0090.001: Create Anonymous Accounts] [T0082: Develop New Narratives] to attack key investigative figures and discredit ideological opponents [T0002: Facilitate State Propaganda] [T0066: Degrade Adversary]. Overall, the investigation illustrates a coordinated attempt to distort the information environment at the heart of Europe, undermining trust in democratic institutions and decision-making processes.

4. Facebook Hustles: The Belgian spin-off

- The case study (Sessa, 2023) uncovered a large-scale scam, which involved 1,500+ Facebook ads leading to 160+ fake media websites. These sites impersonated legitimate news outlets to trick users into providing personal information for a fraudulent investment platform. The scam relied on social engineering and hijacked Facebook pages with millions of followers.
- Belgium was a major focus of the operation, with six major news outlets impersonated, including Le Soir and RTBF. Prominent Belgian politicians, such as Prime Minister Alexander De Croo and Elio Di Rupo were falsely portrayed as endorsing the investment scheme to create credibility.
- The scammers exploited Facebook's ad system and produced content in French and Dutch, targeting Belgian users.

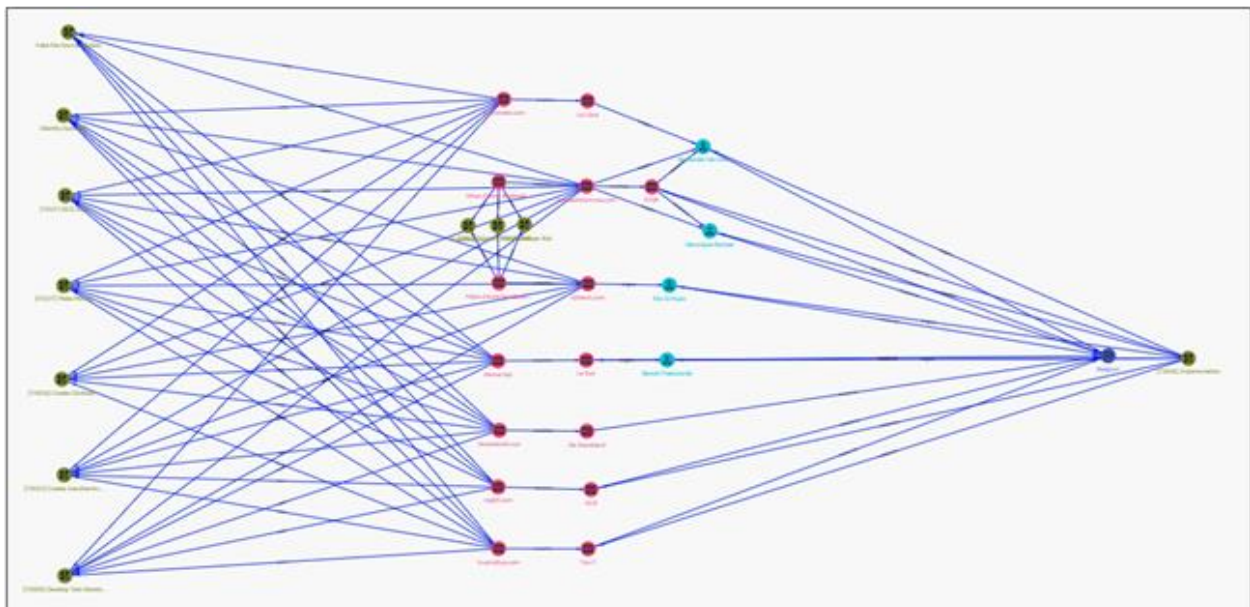


Figure 8. Screenshot of the “Knowledge” graph view in OpenCTI for the report on Facebook Hustles (visualisation elaborated by the author of this report)

ENTITIES (SDO)	
Individuals:	Relationship (SRO):
<ul style="list-style-type: none"> Alexander de Croo: Prime Minister of Belgium at the time of the investigation. Véronique Barbier: journalist for RTBF. Elio Di Rupo is a Belgian politician and former Prime Minister. Benoit Poelvoorde is a Belgian actor. 	<ul style="list-style-type: none"> The impersonated media target these public figures by including them in their fake content: e.g., the impersonated La Libre “targets” Alexander De Croo and the Impersonation attack pattern “targets” him. In turn, these individuals are “related to” Belgium.
Channel:	Relationship (SRO):
<ul style="list-style-type: none"> La Libre: impersonated French-speaking Belgian media. ezwealthformula.com kjhtech.com 	<ul style="list-style-type: none"> The impersonation attack pattern “targets” these fake media, which in turn “target(s)” Belgian public figures. ezwealthformula.com “amplifies” the impersonated version of RTBF, which is

<ul style="list-style-type: none"> • Le Soir: impersonated French-speaking Belgian media • De Standaard: impersonated Dutch-speaking Belgian media. • HLN: impersonated Dutch-speaking Belgian media. • 7sur7: impersonated French-speaking Belgian media. • RTBF: impersonated French-speaking Belgian public service broadcaster. • fedromate.com • facebook.com/BetagbySunflag. • facebook.com/ZonaGallos. • itacow.com. • bluesatoshi.xyz. • mjghf.com. 	<p>“related to” some Belgian public figures.</p> <ul style="list-style-type: none"> • Deceptive websites (e.g., fedromate.com, itacow.com, bluesatoshi.xyz, etc.) and Facebook pages (e.g., “Betag by Sunflag” and “Zona Gallos”) “amplify the content of the impersonated media; for instance, fedromate.com “amplifies” La Libre.
--	--

<ul style="list-style-type: none"> • trustrollup.com. 	
Country:	Relationship (SRO):
<ul style="list-style-type: none"> • Belgium: targeted country. 	<ul style="list-style-type: none"> • All the impersonated individuals are “related to” Belgium, and all the impersonated media “target(s)” Belgium.
Attack pattern:	Relationship (SRO):
<ul style="list-style-type: none"> • Impersonation • Amplification • [T0007] Create Inauthentic Social Media Pages and Groups • [T0114] Deliver Ads 	<ul style="list-style-type: none"> • Impersonation is “related to” the fake websites and “targets” Belgian public figures. • The two Facebook pages “use(s)” impersonation, inauthentic social media pages, and ads.
<ul style="list-style-type: none"> • Fake the Source of Data • Identity Spoofing • [T0137.002] Scam 	<ul style="list-style-type: none"> • Each deceptive website and Facebook page in the campaign “uses” these attack patterns to deceive and monetise.

<ul style="list-style-type: none"> • [T0137] Make Money • [T0016] Create Clickbait • [T0013] Create Inauthentic Websites • [T0085] Develop Text-Based Content 	
---	--

The case exemplifies how impersonation, ad exploitation, and fraudulent amplification were combined in a large-scale scam operation targeting Belgian users [T0072.002: Demographic Segmentation]. Thousands of Facebook ads [T0114: Deliver Ads] [T0018: Purchase Targeted Advertisement] [T0104: Social Networks] and over a hundred deceptive websites were deployed, many following identical templates [T0013: Create Inauthentic Websites] [T0084.001: Use Copy pasta] [T0085: Develop Text-Based Content] [T0086: Develop Image-Based Content]. These sites impersonated trusted media outlets and featured fabricated endorsement from well-known public figures to boost credibility and deceive victims [T0023: Distort Facts] [T0016: Create Clickbait].

OpenCTI's graph structure (Figure 8) shows how each component of the scam contributes to a broader architecture of monetisation and deception. Scam websites were repeatedly reused and then amplified through hijacked Facebook pages and the platform's advertising infrastructure, managing to evade detection while maximising reach [T0129.001: Conceal Network Identity] [T0129.008: Redirect URLs]. The campaign's targeting based on language and geography, combined with persuasive impersonation techniques, emphasises a calculated strategy to exploit trust and extract financial gain from Belgian users.

5. PAPERWALL: Chinese information operation targets Belgium and Luxembourg

- The case study (Alaphilippe, 2024) delves into a Chinese-originated influence campaign that established a network of 123 dummy media outlets worldwide, with a significant presence in Europe, including Belgium and Luxembourg.
- Websites like 'Boic Post' in Belgium and 'Gaul Journal' in Luxembourg mimic legitimate local news sites by publishing plagiarised content in local languages. They also feature English-language sections promoting Chinese interests, such as content from Chinese state-media CGTN, indicating a strategy to enhance the visibility of pro-China narratives.
- These sites lack transparency, providing no information about their ownership or journalistic staff. The rapid and frequent updates of plagiarised content suggest the use of automated systems to maintain the appearance of active news outlets, aiming to influence public perception and search engine ranking.

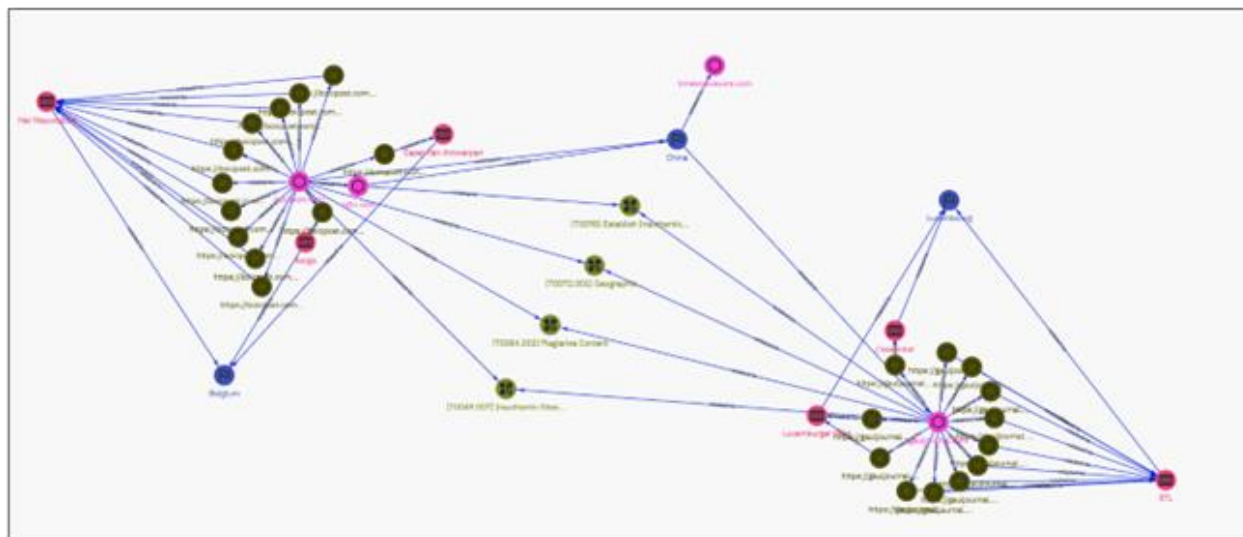


Figure 9. Screenshot of the “Knowledge” graph view in OpenCTI for the report on Paperwall (visualisation elaborated by the author of this report)

ENTITIES (SDO)	
Channel: ²	Relationship (SRO):
<ul style="list-style-type: none"> Het Nieuwsblad: daily newspaper circulating in Flanders. Belga: Belgian press agency. Gazet Van Antwerpen: daily newspaper circulating in Flanders. RTL: Luxembourgish national public broadcaster. Luxemburger Wort: German-language Luxembourgish daily newspaper; L'Essentiel: daily French-speaking Luxembourgish newspaper. 	<ul style="list-style-type: none"> Boic Post is “related to” the production of false articles, which mimic (and therefore are “related to”) the first three legacy media listed. Gaul Journal is “related to” the production of false articles, which mimic (and therefore are “related to”) the last three legacy media listed.
Country:	Relationship (SRO):
<ul style="list-style-type: none"> Belgium: targeted country. 	<ul style="list-style-type: none"> Belgium and Luxembourg are the targeted countries as the various impersonated media are “related to”

<ul style="list-style-type: none"> • Luxembourg: targeted country. • China: interfering foreign actor. 	<p>their information ecosystem, which China is attacking.</p>
Attack pattern:	Relationship (SRO):
<ul style="list-style-type: none"> • [T0098] Establish Inauthentic News Sites • [T0072.001] Geographic Segmentation • [T0084.002] Plagiarise Content • [T0049.007] Inauthentic Sites Amplify News and Narratives 	<ul style="list-style-type: none"> • The Chinese websites “related to” the various attack patterns: creating false websites, plagiarising content from legitimate sources, and targeting Belgium and Luxembourg.
OBSERVABLES (CDO)	
Domain names	Relationship (SRO):
<ul style="list-style-type: none"> • Boic Post (boicpost.com) is a deceptive website pretending to be a Belgian information outlet. 	<ul style="list-style-type: none"> • Boic Post and Gaul Journal are “related to” China and the many deceptive URLs mimicking authentic media. Moreover, Boic Post is also “related to” CGTN, as it amplifies its content

<ul style="list-style-type: none"> • Gaul Journal (gauljournal.com) is a deceptive website pretending to be a Luxembourgish information outlet. • CGTN (cgtn.com) is an English-speaking media outlet owned by the Chinese Communist Party. • TimesNewswire (timesnewswire.com) is a website belonging to the Paperwall network. 	
URL:	Relationship (SRO):
<ul style="list-style-type: none"> • For the first time proven with Belgian figures, the richer you are, the greater the risk of these cancers (Boic Post impersonating Het Nieuwsblad). • Crazy scumbag Biden lashes out at Putin during donor reception (Boic Post impersonating Belga). • Everyday life in a Ukrainian school while there is war outside (Gaul Journal impersonating RTL). 	<ul style="list-style-type: none"> • Boic Post and Gaul Journal are “related to” the various URLs, which are in turn “related to” the legitimate media they are impersonating.

<ul style="list-style-type: none"> • Concert: win your tickets for the Whitney Shay concert (Gaul Journal impersonating L'Essentiel) • Etc. (for the other URLs see Figure 9) 	
---	--

The investigation's graphic representation in OpenCTI (Figure 9) focuses on two websites that masquerade as legitimate local news sources but belong to a worldwide Chinese covert influence campaign, targeting Belgium and Luxembourg. Boic Post and Gaul Journal publish plagiarised content in local languages drawn from established French- and Flemish-speaking media, as well as English-language articles aligned with Chinese state interests. This dual-language strategy suggests a deliberate attempt to manipulate both domestic perception and international narratives, [T0098: Establish Inauthentic News Sites] [T0084.002: Plagiarise Content] [T0072.001: Geographic Segmentation].

The graph produced reveals how these deceptive outlets are structurally linked to both their local targets and broader strategic objectives. URLs impersonating headlines from legitimate Belgian and Luxembourgish media serve as vehicles for falsehoods and subtle influence, amplified through a network of low-transparency, rapidly updated domains. The replication of content and format – often without author attribution – points to automation and scripted production routines, [T0049.007: Inauthentic Sites Amplifying News and Narratives]. Additionally, the connection to CGTN and platforms like TimesNewswire reveals a wider ecosystem that blends state media amplification with locally disguised fronts. By mapping these links, OpenCTI uncovers how the campaign operationalises visibility and credibility to infiltrate Western information environments – underscoring how digital infrastructure and content manipulation are weaponised in FIMI efforts targeting the EU.

DISCUSSION AND CONCLUDING REMARKS

These five case studies examined reveal a diverse yet increasingly recognisable architecture of Foreign Information Manipulation and Interference (FIMI) targeting Belgium and Luxembourg. While the nature of the campaigns – ranging from anti-vaccine lobbying to Chinese state-linked proxies – differs significantly in origin and intent, OpenCTI's structuring modelling exposes underlying commonalities. For instance, common goals are to deceive the audience, degrade adversaries, and cultivate support. Moreover, recurrent TTPs include the geographic segmentation of the audience, the frequent use of inauthentic media infrastructures and impersonation of trusted figures or outlets. Cross-platform amplification strategies are designed to maximise reach, evade detection, and in several cases monetise.

OpenCTI enabled the visualisation and documentation of these campaigns through STIX 2.1 encoding, allowing each incident to be mapped not only in isolation but as part of a broader, transnational threat ecosystem that menaces information integrity. The graph-based representations allow analysts to connect all the moving parts in ways that static narrative reporting would not. Taken together, these cases demonstrate the power of structured threat intelligence to bring clarity to these incidents, transforming fragmented reports into an interoperable knowledge base. This shift enables more timely and coordinated responses, helps close attribution gaps, and supports the development of anticipatory rather than reactive defense mechanisms.

Yet, the effort to encode interference, manipulation, and disinformation operations remains an inherently complex and evolving challenge. The nuances of intent, cultural context, and narrative framing often resist neat categorisation. Furthermore, ongoing refinement of analytical frameworks is essential – both to adapt to shifts in our understanding of the field and to mitigate subjective interpretations in data labelling. This also calls for the development of interoperable standards that bridge the methodological gaps between governments, civil society, and the private sector. Maintaining and updating platforms that support this work is crucial – ensuring, for example, that OpenCTI integrates the most recent version of the DISARM Red Framework.

We take the opportunity to acknowledge that potential inaccuracies in the case study coding should be attributed to our own interpretative error. Finally, the analytical potential of OpenCTI is somewhat constrained, e.g., the limited expressiveness of STIX Relationship Objects (SROs), which often require coders to default to generic associations such as “related to”, reducing the granularity of the links that can be represented.

Ultimately, despite its drawbacks, the adoption of structured threat intelligence methodologies does more than help track harmful narratives – it shows how malign actors operate, build entire alternative information ecosystems, and strategically target specific groups. By encoding previously documented disinformation cases into OpenCTI, we were able to revisit and deepen our understanding of these incidents, uncovering previously overlooked relationships, tactics, and patterns of coordination. This tool empowers a broad coalition of stakeholders – governments, researchers, media organisations, and civil society – to detect and respond to information threats more swiftly and cohesively. By converting anecdotal findings into actionable intelligence, we lay the foundation for a more democratic, transparent, and resilient information environment.