



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Guide d'utilisation d'OpenCTI pour la lutte contre les manipulations de l'information d'origine étrangère

Partie 1 : Capitaliser la connaissance

Guide d'utilisation de VIGINUM

Version 2.0 | Avril 2025

Table des matières

1. Capitalisation de la connaissance relative aux ingérences numériques étrangères	3
1.1 La standardisation des pratiques, préalable à l'interopérabilité	3
1.2 Capitaliser : faire de la connaissance une ressource à long terme	3
2. Principes généraux	5
2.1 Le format de données STIX	5
2.2 Le principe des inférences	6
3. Modélisation de la connaissance	7
3.1 Fenêtre « Aperçu » des rapports	7
3.2 Fenêtre « Connaissance »	8
3.2.1 Modéliser l'imputation et l'attribution	9
3.2.2 Modéliser les moyens & méthodes d'attaque	10
3.2.3 Modéliser les éléments techniques (observables)	11
3.2.4 Modéliser l'activité sur les réseaux sociaux	11
3.2.5 Modéliser la victimologie	12
4. Annexes	13
4.1 Comment créer une campagne	13
4.2 Comment choisir un label	13
4.3 Comment choisir l'état de traitement d'un rapport	13
4.4 Comment tracer les liens	14
4.5 Comment étayer les liens	14
4.6 Comment dater les liens	15
4.6.1 Datation concernant la victimologie et les outils et méthodes d'attaques	15
4.6.2 Datation concernant l'attribution	15
4.7 Description des principales entités utilisées	16
4.7.1 Entités (STIX Domain object)	16
4.7.2 Observables	18

1. CAPITALISATION DE LA CONNAISSANCE RELATIVE AUX INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

1.1 LA STANDARDISATION DES PRATIQUES, PREALABLE A L'INTEROPERABILITE

Ces dernières années, le paysage international de la lutte contre les manipulations de l'information a connu de profondes mutations, marqué par la multiplication du nombre d'initiatives au sein de la société civile, du secteur privé et des gouvernements. Aussi, à mesure que ces initiatives se multiplient, l'enjeu est désormais celui de l'adoption d'une grammaire commune permettant à la fois de décrire la menace informationnelle de manière identique et de faciliter le partage d'informations.

En tant que service technique et opérationnel, VIGINUM œuvre depuis plusieurs années à la promotion et au développement de standards communs permettant de répondre à cet objectif. Au cours de l'année de 2024, VIGINUM a publié une traduction en français de la matrice DISARM¹, permettant de décrire les campagnes de manipulation de l'information de manière structurée, et contribue aux travaux du *Defending Against Deception Common Data Model* (DAD-CDM)², un projet piloté par l'organisation à but non lucratif américaine OASIS qui vise à adapter le langage STIX à la lutte contre les manipulations de l'information.

Ainsi, dans la continuité du premier [guide d'utilisation](#) d'OpenCTI publié par VIGINUM en janvier 2024, ce nouveau guide a pour vocation de proposer un cadre de référence sur la manière de capitaliser la connaissance de la menace informationnelle sur la plateforme OpenCTI³. Ce référentiel vise à faciliter l'uniformisation de bonnes pratiques de capitalisation dans l'outil afin de garantir l'exploitation des connaissances capitalisées dans la durée, leur compréhension par tous, ainsi que leur interopérabilité dans le cas d'éventuels partages.

N.B. : VIGINUM distingue le processus d'imputation, qui consiste à relier techniquement des observables à un mode opératoire informationnel (MOI), du processus d'attribution, qui relève de choix politiques. Dans le présent document, les termes « attribution » et « imputation » sont employés de manière interchangeable pour désigner la relation STIX « attribué à ». Il convient également de noter que les exemples présentés ci-dessous sont fictifs ou ont fait l'objet d'ajustements pour faciliter la description des étapes de capitalisation sur OpenCTI. Ils ne doivent donc pas être considérés comme le fruit de la capitalisation officielle de VIGINUM.

1.2 CAPITALISER : FAIRE DE LA CONNAISSANCE UNE RESSOURCE A LONG TERME

Appliquée à la lutte contre les ingérences numériques étrangères, la capitalisation est entendue comme l'action d'identifier, de modéliser et de conserver la connaissance dans un format structuré, pérenne et partageable.

Cette capitalisation peut se faire sous différentes formes, qu'il s'agisse de notes textuelles, de graphiques ou de plateformes dédiées à l'analyse de la menace, à l'image d'OpenCTI.

¹ https://fr.linkedin.com/posts/viginum_disarm-traduction-fran%C3%A7aise-activity-7159231318042550273-l5eO

² <https://www.oasis-open.org/2023/11/16/oasis-defending-against-disinformation-dad-cdm/>

³ OpenCTI est une plateforme *open source* codéveloppée initialement par l'ANSSI, le CERT-EU et l'association *Luatix*. L'entreprise française *Filigran* contribue aujourd'hui à son développement.

Capitaliser la connaissance sur la menace informationnelle dans *OpenCTI* permet notamment :

- de minimiser les risques de perte de connaissances critiques ;
- de standardiser la modélisation de la menace entre analystes ;
- de faciliter la recherche et l'analyse de données contextuelles et techniques ;
- d'améliorer le partage d'informations entre les acteurs impliqués dans la lutte contre les manipulations de l'information (entités gouvernementales, monde académique, médias, ONG, entreprises, etc.).

La connaissance capitalisable sur *OpenCTI* peut inclure tout à la fois des sources internes, telles que des rapports d'analyse, et des sources externes, telles que des rapports techniques d'éditeurs de sécurité informatique, des articles de presse, ou encore des déclarations ou des documents officiels relatifs à la menace informationnelle.

2. PRINCIPES GÉNÉRAUX

2.1 LE FORMAT DE DONNEES STIX

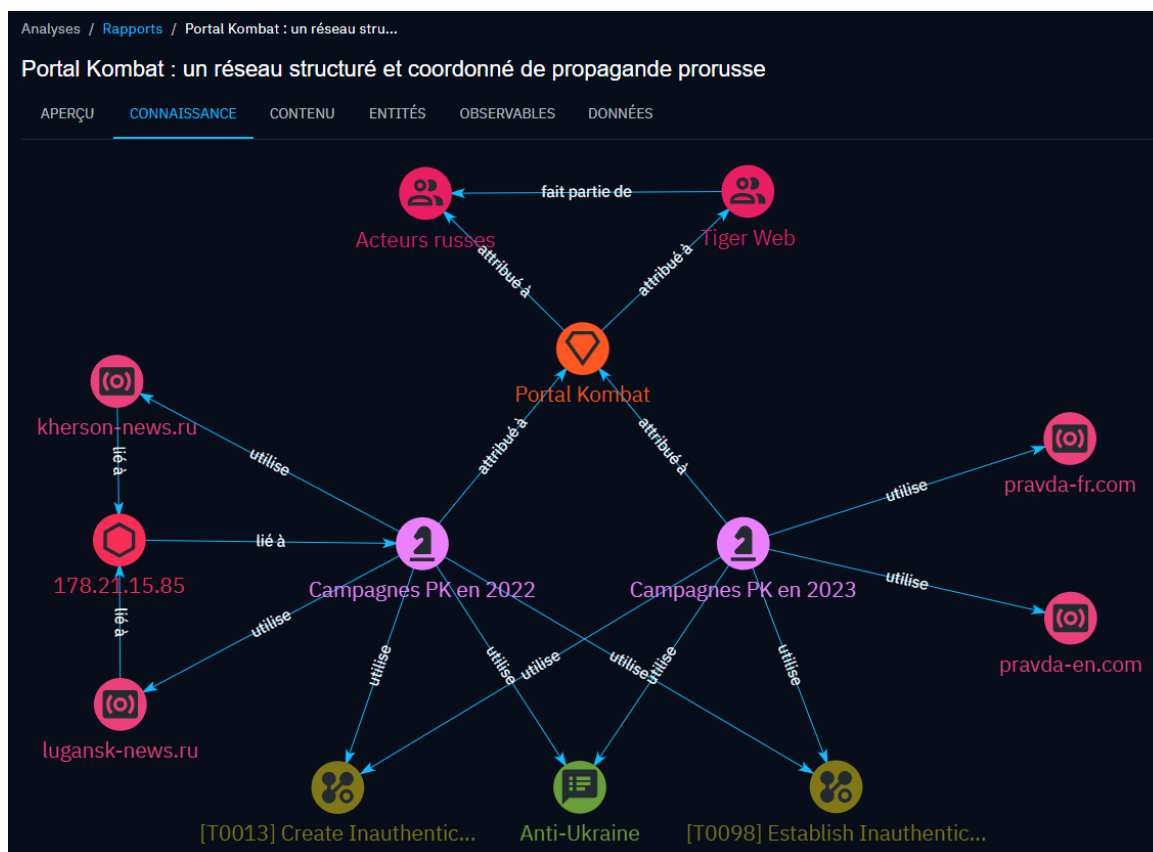
STIX (*Structured Threat Information eXpression*) est un format structuré développé par l'ONG américaine OASIS. Il permet de décrire des informations relatives à la menace informatique grâce à des **objets** (observables ou entités) liés entre eux par des **relations** (liens). Le modèle a été initialement construit pour la *Cyber Threat Intelligence* (CTI), mais est progressivement adapté à la lutte contre la manipulation de l'information (LMI).

Dans *OpenCTI*, le format STIX est utilisé pour construire des graphes de connaissance. Les objets représentent des entités telles que des modes opératoires, des pays, des organisations ou des individus. Les liens permettent quant à eux de créer du sens : « un mode opératoire **est attribué** à un acteur », « une organisation **est localisée** dans un pays », « une campagne **utilise** un narratif », etc.

Pour ce faire, les liens sont :

- **nommés** : avec un nombre de choix limité : « utilise », « attribué à », « localisé dans », « cible », « fait partie de », etc. ;
- **directionnels** : un mode opératoire est attribué à un acteur, et non l'inverse. Il faudra donc choisir la direction adaptée.

En lien avec OASIS, la société française *Filigran* a proposé des adaptations du format STIX pour répondre aux besoins spécifiques de la LMI. La liste des entités natives et des entités ajoutées par *Filigran* est disponible en annexe [4.8](#).



Exemple de graphe de connaissance

2.2 LE PRINCIPE DES INFÉRENCES

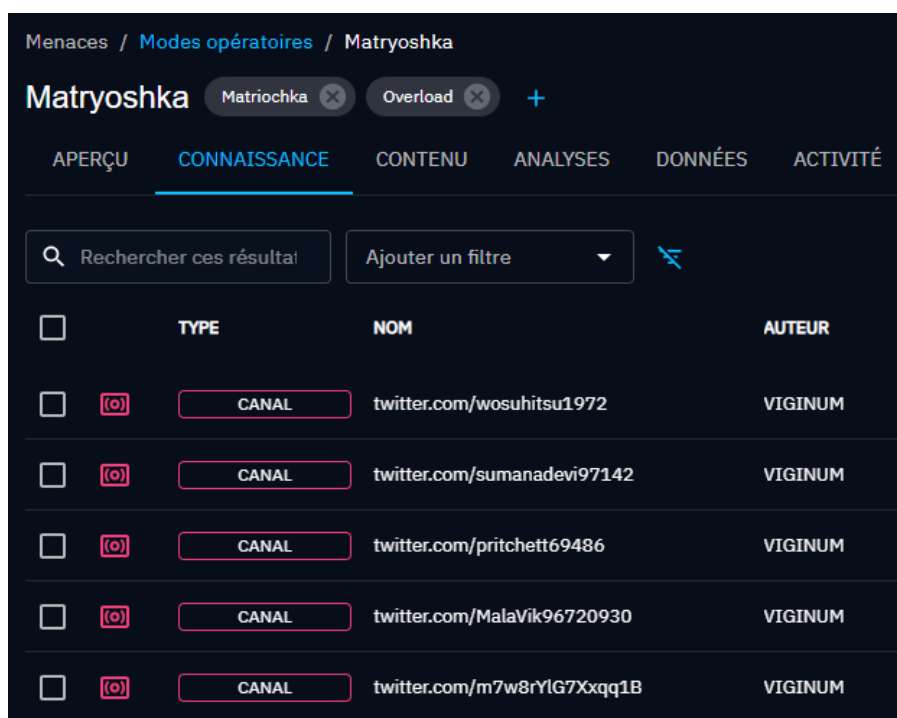
OpenCTI propose une série de règles prédéfinies (appelées inférences) qui structurent la manière dont les nouvelles relations sont inférées dans la base de données.

À titre d'exemple, un utilisateur peut activer la règle d'inférence suivante : si une entité A est attribuée à une entité B et que cette entité B est elle-même attribuée à une entité C, alors l'entité A est attribuée par défaut à l'entité C.

Concrètement, si le Mode opératoire « RRN » utilise le narratif « France en Afrique », et que le Mode opératoire « RRN » est attribué à l'entité « Acteurs russes », l'entité « Acteurs russes » utilisera par inférence le narratif « France en Afrique ».

Les inférences sont donc capitales pour retrouver facilement :

- l'ensemble des Modes opératoires qui ont ciblé une même organisation, un même secteur ou un même individu ;
- l'ensemble des Modes opératoires qui utilisent un outil, un narratif ou une tactique, technique et procédure (TTP) ;
- l'ensemble des Modes opératoires liés à un Acteur ;
- l'ensemble des éléments techniques (IP, mails, numéros de téléphone, etc.) associés à une Campagne, à un Mode opératoire ou à un Acteur.



Menaces / Modes opératoires / Matryoshka		
Matryoshka Matriochka Overload +		
APERÇU CONNAISSANCE CONTENU ANALYSES DONNÉES ACTIVITÉ		
Rechercher ces résultats Ajouter un filtre		
<input type="checkbox"/>	TYPE	NOM
<input type="checkbox"/>	<input type="checkbox"/> CANAL	twitter.com/wosuhitsu1972
<input type="checkbox"/>	<input type="checkbox"/> CANAL	twitter.com/sumanadevi97142
<input type="checkbox"/>	<input type="checkbox"/> CANAL	twitter.com/pritchett69486
<input type="checkbox"/>	<input type="checkbox"/> CANAL	twitter.com/MalaVik96720930
<input type="checkbox"/>	<input type="checkbox"/> CANAL	twitter.com/m7w8rYlG7Xxqq1B
		VIGINUM

Exemple de Canaux utilisés par un Mode opératoire

3. MODÉLISATION DE LA CONNAISSANCE

La connaissance est capitalisée, manuellement ou automatiquement, dans *OpenCTI* à l'aide de la fonctionnalité « Rapports ».

3.1 FENETRE « APERÇU » DES RAPPORTS

Figurent ci-dessous les éléments à compléter impérativement dans cette fenêtre :

1. un **nom** : qui correspond au titre exact du document capitalisé ;
2. une **description** : qui correspond à un résumé textuel du contenu du document capitalisé ;
3. le **type de rapport** : productions internes ou rapports externes ;
4. une **date** : qui correspond à la date de publication du document capitalisé ;
5. une **référence externe**, qui correspond au lien vers le document original (en source ouverte ou vers une base de données interne) ;
6. un **marquage** : qui correspond au marquage du document capitalisé (par exemple, TLP:CLEAR ou TLP:RED⁴) ;
7. un **état de traitement** à jour ;
8. un **auteur** : qui correspond à l'auteur ou aux auteurs du document capitalisé.

Analyses / Rapports / Portal Kombat : un réseau stru...

Portal Kombat : un réseau structuré et coordonné de propagande prorusse 1

APERÇU CONNAISSANCE CONTENU ENTITÉS OBSERVABLES DONNÉES

DÉTAILS DE L'ENTITÉ 2

Description
Entre les mois de septembre et décembre 2023, VIGINUM a analysé l'activité d'un réseau de « portails d'information » numériques aux caractéristiques similaires, qui diffuse des contenus pro-russes à destination d'audiences internationales. Si ce réseau, constitué d'au moins 193 sites, couvrirait à sa création les informations de localités russes et ukrainiennes, il a, dès le lendemain de l'invasion...

Types de rapport 3
EXTERNE

Date de publication 4
12 mars 2024 à 13:01:14

Rapports connexes

ENTITIES DISTRIBUTION

Canal
Motif d'attaque
Campagne
Acteur (groupe)
Mode opératoire
Adresse IPv4
Narratif

INFORMATIONS DE BASE

Marquage 6
TLP:CLEAR

Auteur 8
VIGINUM

Fiabilité (de l'auteur)
inconnu

Niveau de confiance
1 - Confirmed b...

Etat du traitement 7
ANALYZED

Référénts
Participants
Révoqué
NON

Labels +

Date de création de l'entité
27 février 2025 à 13:19:51

Créateurs

Date de création originale
12 mars 2024 à 13:01:14

Date de modification
27 février 2025 à 13:19:51

STIX ID standard
report--cd5e343e-53

RÉFÉRENCES EXTERNES 5
VIGINUM
https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_RAPPOR...

HISTORIQUE RÉCENT
adds Unknown in Contains

Exemple de la fenêtre « aperçu »

⁴ Pour plus d'informations sur la politique de partage et d'utilisation des informations à caractère opérationnel, voir : <https://www.cert.ssi.gouv.fr/csirt/politique-partage/>.

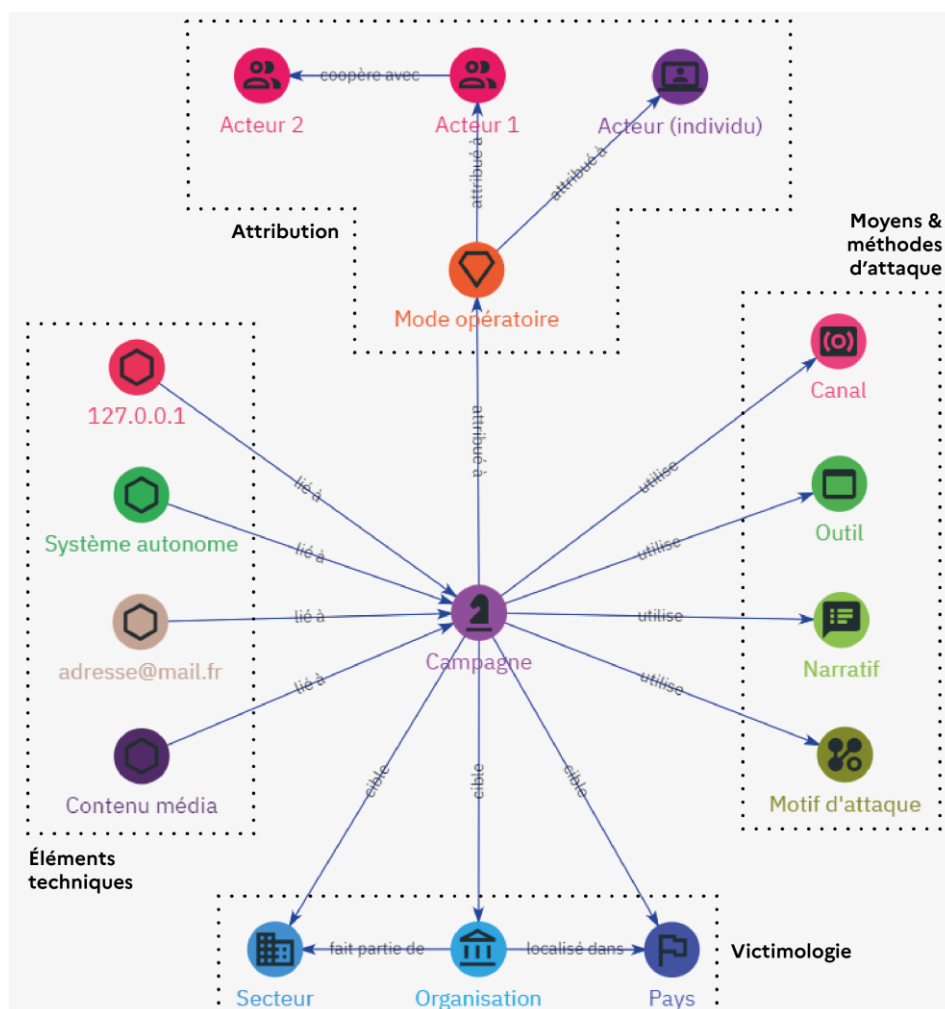
Si l'analyste les considère pertinents pour la capitalisation, d'autres éléments peuvent être renseignés :

- un indice de confiance ;
- un ou plusieurs **labels**⁵ ;
- des **référénts**.

3.2 FENETRE « CONNAISSANCE »

La fenêtre « Connaissance » est l'endroit où est construit le graphe de connaissance. Ce sont les entités et les liens renseignés dans le graphe qui produiront des inférences. Pour assurer la traçabilité de la connaissance, **l'analyste capitalise**, ou « fiche », **les informations qui figurent dans le document** en cours de capitalisation, sans préjuger de leur véracité ou non.

Les éléments à capitaliser dans le graphe concernent les imputations ou déclarations officielles d'attribution, la victimologie, les moyens et méthodes d'attaque employés par le mode opératoire, ainsi que les éléments techniques associés à la campagne.



⁵ Cf. annexe 4.2.

Les différentes entités (IP, Narratif, Pays ciblé, etc.) **doivent être liées à une campagne annuelle**⁶, ce qui permet de conserver un indicateur temporel sur les actions des modes opératoires et facilite l'analyse de l'évolution de leurs techniques au fil du temps.

Ci-après, des schémas montrent les différents liens possibles (et leur sens) entre les entités utiles à la capitalisation LMI. D'autres liens sont possibles entre les entités, mais il est toujours **préférable d'indiquer un lien « qualifié »** (*attribué à, coopère avec, localisé dans, cible, etc.*) plutôt que d'appliquer le lien de base (*lié à*), qui ne produit pas d'inférence.

3.2.1 Modéliser l'imputation et l'attribution

La Campagne est l'entité centrale des graphes de connaissance. Elle est attribuée, selon les données disponibles, à un Mode opératoire ou directement à un Acteur.

Par exemple, un Mode opératoire sera attribué à un ou plusieurs Acteurs (« Acteur organisation » ou « Acteur individu ») qui peuvent faire partie d'autres acteurs ou coopérer entre eux. Cette structure est notamment pratique pour reconstituer des organigrammes, par exemple pour rattacher un mode opératoire à un individu connu et une unité précise d'un service de renseignement étranger.

Points d'attention pour la modélisation de l'attribution et l'imputation :

1) Faire apparaître impérativement la menace d'origine

La capitalisation concernant des activités présumées étatiques doit toujours faire apparaître une entité Acteur qui correspond à l'origine de la menace.

Exemple : pour capitaliser un rapport de *Meta* sur des activités du Mode opératoire RRN, imputé en source ouverte au gouvernement russe, il faut impérativement faire apparaître l'entité « Acteurs Russes » dans le graphe de connaissance. La mention de ces deux entités dans le graphe permet de retrouver le document depuis la fenêtre de l'entité « Acteurs Russes ».

2) Lier ou non le mode opératoire à la menace pays

Les Modes opératoires ne sont pas forcément attribués, dans le graphe, à une entité « Acteurs pays ». En effet, ce lien n'est pertinent que si le document capitalisé fournit des éléments tangibles relatifs à l'imputation du mode opératoire à un acteur spécifique.

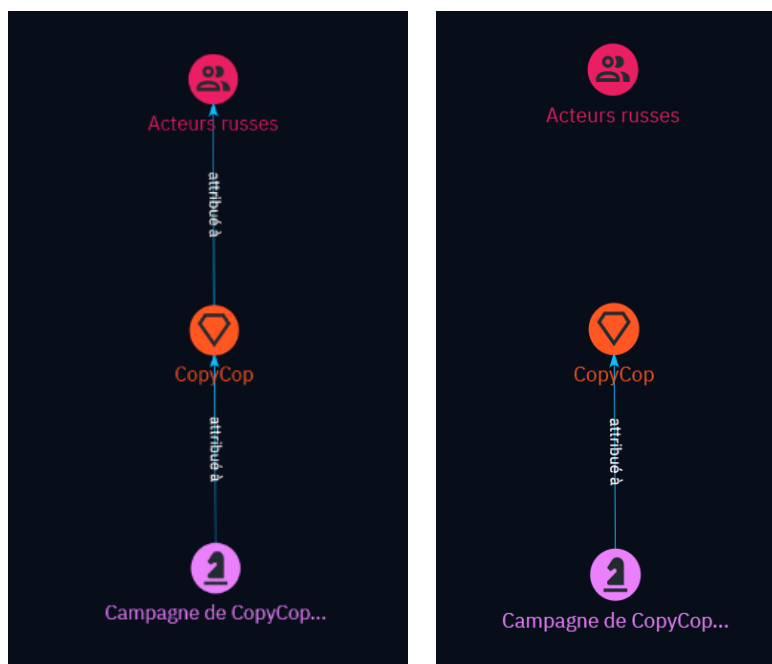
Cette subtilité permet de garder la traçabilité des imputations techniques et des déclarations publiques d'attribution **jugées d'intérêt**, et donc de retrouver facilement quels gouvernements, éditeurs de sécurité ou chercheurs ont attribué la parenté du Mode opératoire RRN au gouvernement russe, à quelle date, avec quel niveau de marquage, et pourquoi.

Exemples :

- si le document offre des éléments techniques liant RRN à des Acteurs russes, une relation entre le Mode opératoire RRN et l'entité « Acteurs Russes » doit être créée ;
- si le document est relatif à une déclaration publique d'attribution, qu'elle soit étayée ou non, il est important d'en garder la trace : une relation entre le mode opératoire Mode opératoire RRN et l'entité « Acteurs Russes » doit alors être créée ;

⁶ Cf. annexe [4.1](#).

- si le document se contente de rappeler en introduction que « *RRN is likely conducted by the Russian government* » mais n'étaye pas cette imputation, aucune relation entre le mode opératoire Mode opératoire RRN et l'entité « Acteurs Russes » ne doit être créée.



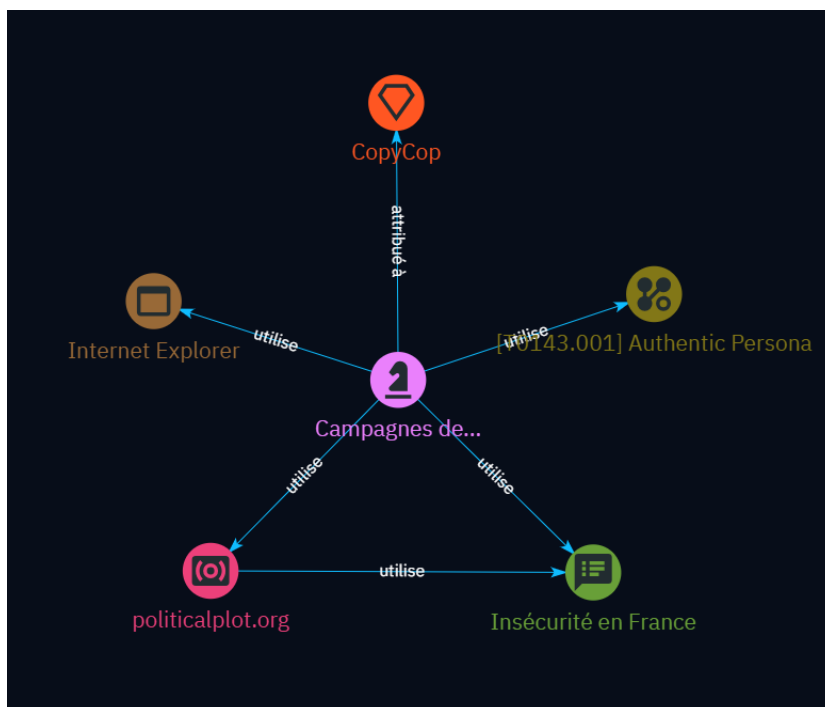
Modélisation de l'attribution

3.2.2 Modéliser les moyens & méthodes d'attaque

La Campagne **utilise** :

- des TTPs ;
- des Canaux ;
- des Outils ;
- des Narratifs ;

Des liens peuvent également être créés en plus entre les différents moyens ou outils utilisés, par exemple un Canal **utilise** un Narratif.



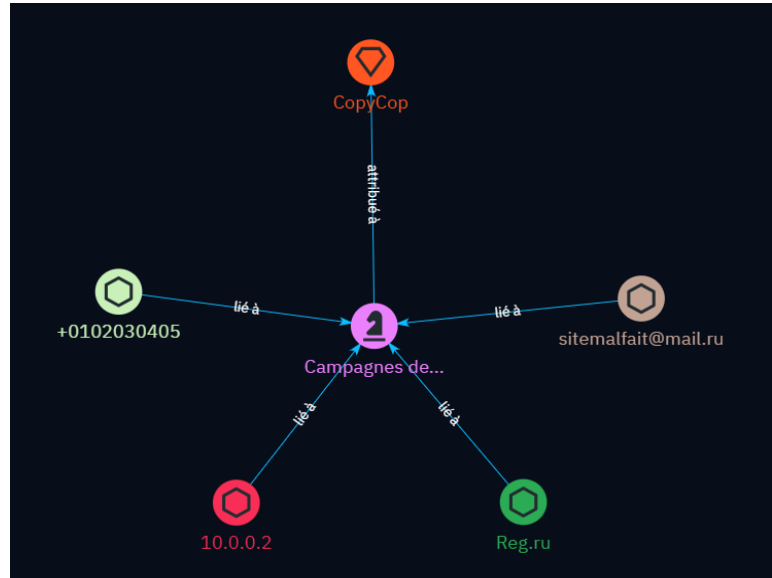
Modélisation des moyens et méthodes d'attaque

3.2.3 Modéliser les éléments techniques (observables)

Les observables sont **liés** à la Campagne :

- adresse mail ;
- adresse IPv4 ;
- nom de domaine ;
- numéro de téléphone ;
- URL ;
- etc.

Les éléments techniques peuvent également être liés entre eux, notamment pour préciser qu'un Nom de domaine **résout** une Adresse IPv4.



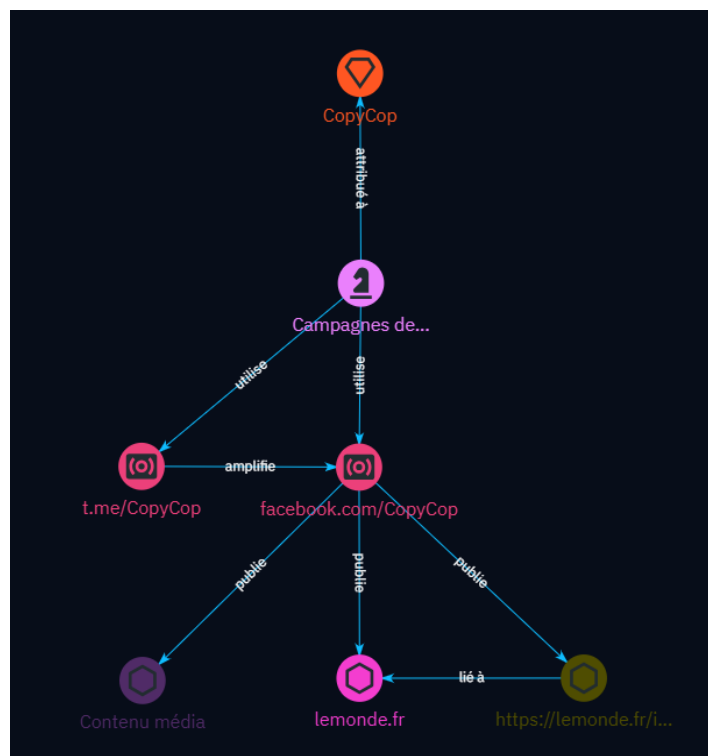
Modélisation des éléments techniques

3.2.4 Modéliser l'activité sur les réseaux sociaux

Une Campagne :

- **utilise** un ou plusieurs Canaux ;
- ces Canaux **amplifient** d'autres Canaux.

Ces éléments peuvent également être liés entre eux, notamment pour préciser que tels Canaux **publient** un Contenu média, une URL, un Nom de domaine, etc.



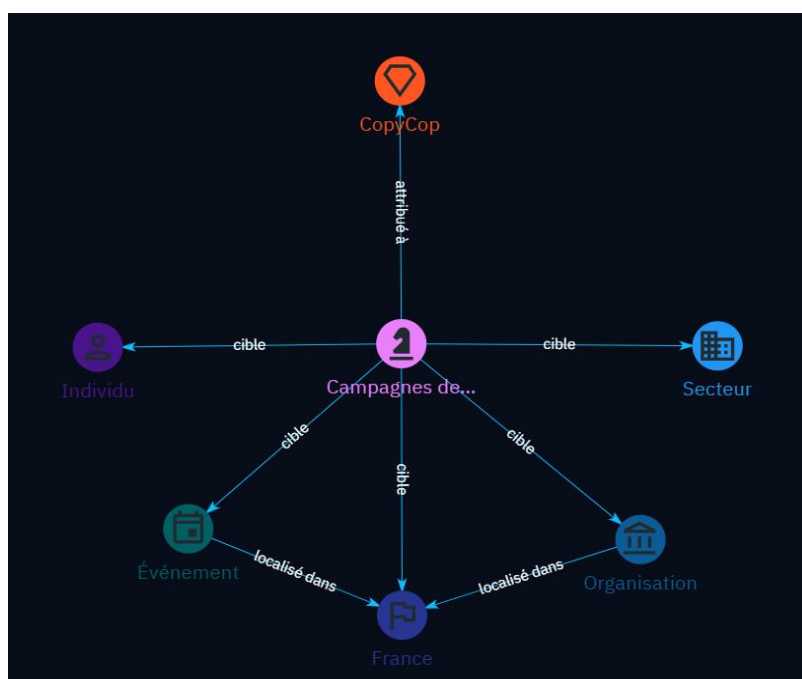
Modélisation de l'activité sur les réseaux sociaux

3.2.5 Modéliser la victimologie

La Campagne **cible** :

- des Secteurs ;
- des Pays ;
- des Événements ;
- des Individus ;
- des Organisations.

Les éléments sur la victimologie peuvent également être liés entre eux, notamment pour préciser qu'un Événement **est localisé** dans un Pays.



Modélisation de la victimologie

4. ANNEXES

4.1 COMMENT CREER UNE CAMPAGNE

Afin d'harmoniser les intitulés des Campagnes, élément central de la capitalisation dans les graphes de connaissance, une convention de nommage a été mise en place. **Les activités des acteurs et des modes opératoires doivent être liées à des campagnes annuelles** qui permettent de suivre chronologiquement l'évolution de leur victimologie, de leur TTP et des attributions.

Exemples :

- « Campagnes de RRN en 2023 » ;
- « Campagnes de Storm-1516 en 2019 » ;
- « Campagnes de Portal Kombat en 2036 ».

Si une campagne de manipulation de l'information n'a pas encore été attribuée, il est **possible de créer une campagne non-attribuée**, en précisant sa nature et la date de détection.

Exemples :

- « Campagne non-attribuée de *deepfakes* de célébrités sur *Bluesky* en décembre 2023 » ;
- « Campagne non-attribuée ciblant la page *Wikipedia* d'Emmanuel MACRON en juillet 2019 ».

Si la campagne est ensuite attribuée, elle peut être **fusionnée avec la campagne annuelle** de l'Acteur ou du Mode opératoire correspondant. À titre d'exemple, si la première campagne ci-dessus est attribuée *a posteriori* au Mode opératoire RRN, il sera possible de la fusionner avec la campagne « Campagnes de RRN en 2023 ».

4.2 COMMENT CHOISIR UN LABEL

Des labels peuvent être ajoutés à quasiment n'importe quel type d'entité : mode opératoire, rapport, organisation, etc. Ils sont principalement employés pour **faciliter les recherches transverses** sur les connaissances capitalisées dans *OpenCTI*.

Pour l'heure, les labels correspondent à des **thématiques transverses** (« élections », « intelligence artificielle », « Jeux Olympiques », et la langue dans laquelle l'opération informationnelle a été conduite, etc.).

4.3 COMMENT CHOISIR L'ETAT DE TRAITEMENT D'UN RAPPORT

L'état de traitement (également appelé statut) permet de savoir rapidement si un rapport a été capitalisé ou non.

Il existe aujourd'hui quatre états de traitement :

- *NEW* ;
- *IN_PROGRESS* ;
- *ANALYZED* ;

- **CLOSED.**

NEW est le statut indiqué par défaut sur un rapport. Il doit être conservé en l'état tant que le rapport n'est pas capitalisé.

IN_PROGRESS indique que le rapport est en cours de capitalisation. Ce statut permet à l'analyste d'indiquer que les informations d'un rapport ne sont pas encore parfaitement complétées.

ANALYZED indique que le rapport est parfaitement complété. L'analyste doit indiquer ce statut à chaque fois qu'il a terminé de capitaliser un rapport.

CLOSED est un statut réservé aux erreurs et doublons. L'analyste peut indiquer ce statut pour signaler que le rapport ne doit pas être pris en compte, et devra être supprimé de la plateforme.

4.4 COMMENT TRACER LES LIENS

Pour que les inférences se fassent correctement, les liens entre les entités d'un graphe de connaissance doivent :

1. être tracés dans la « bonne » direction ;
2. être nommés de façon adaptée.

Hormis pour les observables, les liens sont **tracés en étoile à partir de l'entité centrale, la Campagne**.

Vous trouverez des exemples de capitalisation de graphe tout au long de ce guide. Les directions et types de nommage principaux sont listés ci-dessous :

- une Campagne *est attribuée* à un Mode opératoire ou à un Acteur ;
- une Campagne *cible* une Organisation, un Secteur, un Individu, un Pays ;
- une Campagne *utilise* un Motif d'attaque, un Outil, un Narratif, un Canal ;
- un Acteur *est situé* dans un Pays ;
- un Acteur *coopère avec* un autre Acteur ;
- un Acteur *fait partie* d'un autre Acteur ;
- un Mode opératoire *est attribué* à un Acteur ;
- une Adresse IPv4, une Adresse email, un Numéro de téléphone, un Nom de domaine ou une URL sont *liés* à une Campagne ;
- une Organisation *fait partie* d'un Secteur ;
- une Organisation *est située* dans un Pays.

4.5 COMMENT ETAYER LES LIENS

Les liens doivent être correctement créés pour produire des inférences pertinentes. La plupart des relations ont besoin d'être étayées, c'est-à-dire justifiées par les éléments du document capitalisé.

L'analyste doit remplir correctement les champs suivants à partir des éléments contenus dans le document en cours de capitalisation :

- les bonnes dates de début et/ou de fin d'observation ;

- l'auteur du document ;
- le marquage du document.

4.6 COMMENT DATER LES LIENS

Chaque relation peut être datée. Les **dates doivent être systématiquement modifiées** lors de la création d'une relation, puisqu'elles indiqueront sinon par défaut, dans les champs « Date de début d'observation » et « Date de fin d'observation », la date de publication du document capitalisé.

La datation est très importante, car elle permet de visualiser sur *OpenCTI* la chronologie de Campagnes, d'attributions, ou de l'utilisation d'outils par les Modes opératoires.

4.6.1 Datation concernant la victimologie et les outils et méthodes d'attaques

La datation des relations concernant la victimologie et les outils et méthodes d'attaques est identique. Elle se concentre sur les informations fournies dans le document. Il existe quatre cas de figure :

Cas 1 : l'auteur a observé le début d'une activité (ciblage d'une Organisation, d'un Pays, d'un Secteur, utilisation d'un outil ou d'un motif d'attaque, etc.) et la fin de cette activité.

→ *Les dates de début d'observation et de fin d'observation doivent être renseignées.*

Cas 2 : l'auteur a observé le début d'une activité, mais celle-ci est en cours.

→ *Seule la date de début d'observation doit être renseignée.*

Cas 3 : l'auteur a observé la fin d'une activité en cours depuis une date inconnue.

→ *Seule la date de fin d'observation doit être renseignée.*

Cas 4 : l'auteur a observé une activité, mais ne mentionne aucune date précise.

→ *Aucune date ne doit être renseignée.*

4.6.2 Datation concernant l'attribution

La datation des relations concernant l'attribution diffère quelque peu de la datation concernant la victimologie et les outils et méthodes. Elle se concentre en effet sur **la date à laquelle l'auteur énonce l'attribution**.

Quelle que soit l'entité à laquelle un Mode opératoire ou une Campagne est attribué (Acteur, Organisation, Individu), cela implique :

- que la « Date de début d'observation » correspond toujours à la date de publication du document capitalisé, cette date étant normalement indiquée par défaut lors de la création de la relation ;
- que l'attribution n'a jamais de « Date de fin d'observation », qu'il convient donc de supprimer.

4.7 DESCRIPTION DES PRINCIPALES ENTITES UTILISEES

4.7.1 Entités (STIX Domain object)

Campagne

(Objet STIX natif)

L'entité Campagne est l'élément central des graphes de connaissance dans *OpenCTI*. L'ensemble des éléments techniques, d'attribution et des actions attaquantes sont rattachés « en étoile » autour d'une Campagne annuelle attribuée à un Mode opératoire, un Acteur, ou non-attribuée.

Acteur (groupe)

(Objet STIX natif)

Dans *OpenCTI*, un Acteur (groupe) correspond à une organisation (administration, entreprise, groupe informel, etc.) qui est à l'origine des activités malveillantes, les supervise, les finance, les commande ou les soutient.

L'entité est utilisée pour :

- représenter les organisations en elle-même : service de renseignement étranger, entreprise participant à des manœuvres, groupe d'hacktivistes, etc.
- représenter des « méta-Acteurs » ou des catégories d'acteurs. Exemples : toutes les organisations qui prennent part à des manœuvres informationnelles attribuées publiquement au gouvernement russe font partie d'un méta-Acteur « Acteurs russes », afin de pouvoir les retrouver depuis une page dédiée sur *OpenCTI*.

Acteur (individu)

(Objet STIX natif)

Dans *OpenCTI*, un Acteur (individu) correspond à une personne physique qui est à l'origine des activités malveillantes, les supervise, les finance, les commande ou les soutient. Exemples : un membre connu d'un service de renseignement étranger, l'employé d'une entreprise participant à des manœuvres informationnelles, un propagandiste pro-Russe, etc.

Mode opératoire

(Objet STIX natif)

Lorsque l'acteur précis derrière les activités malveillantes n'est pas connu (cf. section [3.2.1](#)), ou que le suivi des opérations est assuré en utilisant le concept de mode opératoire informationnel (MOI), la Campagne est attribuée à un Mode opératoire.

VIGINUM définit un MOI comme un ensemble de comportements, d'outils, de tactiques, techniques et procédures et de ressources adverses mis en œuvre par un acteur ou un groupe d'acteurs malveillants dans le cadre d'une ou de plusieurs opérations informationnelles numériques. Il n'est pas à confondre avec un groupe d'attaquants (Acteurs), composé d'organisations ou d'individus (cf. *supra*).

Canal

(Ajout Filigran)

Un Channel (Canal) est un **compte de réseau social ou un nom de domaine** utilisé par un Acteur ou un

Mode opératoire dans le cadre d'une manœuvre informationnelle. L'observable « Nom de domaine » n'est utilisée que pour capitaliser les sites légitimes.

Pour retrouver plus facilement les Canaux et éviter de créer des doublons (par exemple parce qu'un acteur exploiterait un compte X et un compte *Telegram* avec un nom composé de la même chaîne de caractères), il est également important de renseigner le type de Canaux lors de la création d'un Canal. Exemples de nommage :

- *Facebook* : *facebook.com/username* (*UserID*, *groupID* ou *pageID* en alias de l'entité) ;
- *X* : *twitter.com/username* (*handle* en alias de l'entité) ;
- *Telegram* : *t.me/channelorgroupname* (nom du groupe en alias de l'entité) ;
- Nom de domaine : *mechantemanoevre.ru*.

Si l'analyste n'a pas identifié les comptes impliqués dans une manœuvre informationnelle mais souhaite néanmoins représenter l'utilisation, par exemple, de la plateforme en ligne *Bluesky* ou *X*, un nom de chaîne générique peut être utilisé (« *bluesky.com* » ou « *x.com* »).

Événement

(Ajout Filigran)

L'Event (Évènement) décrit un événement physique exploité lors d'une campagne. Ces événements doivent être assez larges pour qu'ils soient susceptibles d'être la cible de plusieurs manœuvres.

Par exemple, privilégier « Jeux olympiques de Paris 2024 », plutôt que « Épreuve de kayak homme en individuel le 13 août 2024 pendant les Jeux olympiques de Paris ».

Outre un événement sportif, il peut par exemple s'agir d'une rencontre internationale, d'une élection, d'une visite diplomatique, d'une catastrophe naturelle, etc.

Individu

(Objet STIX natif)

Personne physique qui n'est pas considérée comme un Acteur de la menace : cible de Campagnes, individu dont l'identité a été usurpée, etc.

Organisation

(Objet STIX natif)

Personne morale qui n'est pas considérée comme un Acteur de la menace : entreprise, ONG ou association cible de Campagnes, média dont l'identité a été usurpée, etc.

Secteur

(Objet STIX natif)

L'entité Secteur est utilisée pour représenter le ciblage de certains intérêts. Les secteurs retenus sont « haut niveau » à dessein. Voici des exemples de secteurs susceptibles d'être ciblés par une Campagne :

- Institutions de l'État ;
- Intérêts économiques, industriels et scientifiques ;

- Patrimoine culturel ;
- Personnalités de l'État ;
- Politique étrangère ;
- Sécurité et défense nationale.

L'entité sert également à représenter des secteurs d'activités, tels que médias, ONG, etc.

Infrastructure

(Objet STIX natif)

Cet objet STIX modélise les ressources physiques ou virtuelles exploitées par les attaquants, notamment les hébergeurs des sites (*GoDaddy*, *NameSilo*, etc.) utilisés dans le cadre d'une manœuvre informationnelle.

Narratif

(Ajout Filigran)

Cette entité décrit les narratifs exploités par un mode opératoire ou un acteur lors d'une campagne. Ces narratifs doivent être assez larges pour qu'ils soient susceptibles d'être exploités par plusieurs acteurs ou durant une période de temps relativement longue.

Par exemple, privilégier « Néocolonialisme », plutôt que « Accusations contre la France concernant le prétendu envoi de migrants pour combattre en Ukraine en juin 2024 ».

Motif d'attaque

(Objet STIX natif)

Entité permettant de décrire, à partir de la matrice DISARM⁷, les actions des attaquants : amplification par des trolls [T0049.001], création d'avatars [T0097], faciliter la propagande étatique [T0002], etc.

Outil

(Objet STIX natif)

Cette entité décrit des logiciels légitimes exploités par un Mode opératoire ou un Acteur dans le cadre de ses Campagnes, par exemple une solution commerciale pour la mise en place de redirections ou de gestion de bots sur les réseaux sociaux.

4.7.2 Observables

Les observables permettent de modéliser les éléments techniques observés lors d'une Campagne. Ils sont particulièrement utiles pour représenter l'infrastructure numérique exploitée pour conduire une manœuvre. Voici une liste (non exhaustive) des observables les plus pertinents pour documenter les manœuvres informationnelles :

- adresse email ;
- adresse IPv4 ;
- contenu média ;

⁷ Cf. <https://www.disarm.foundation/>.

- nom de domaine (attention, **les sites attaquants ne sont pas renseignés en tant que Nom de domaine, mais comme Canaux**, cf. [4.8.1](#)) ;
- numéro de téléphone ;
- système autonome ;
- URL.

Type d'entité	Malveillant	Légitime
	Acteur (Organisation)	Organisation
	Acteur (Individu)	Individu
	Canal	Nom de domaine

Tableau récapitulatif de l'utilisation des entités.

Contenu média

(Ajout Filigran)

Cet observable modélise un contenu média de type publication, vidéo, audio, image, etc. Son nommage est déterminé selon une convention :

- [Vidéo] Titre de la vidéo ;
- [Article] Titre de l'article ;
- [Podcast] Titre du podcast ;
- [Tweet] Titre du tweet ;
- [Facebook] Titre du post ;
- [Contenu sponsorisé] Titre du post sponsorisé.

Pour créer un observable Contenu média, il est nécessaire de renseigner une URL.

À PROPOS DE VIGINUM



Créé le 13 juillet 2021 et rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation.

Ce service technique et opérationnel de l'État a pour mission de détecter et caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

[Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN](#)

--

Crédits photos : Cai Fang sur *Unsplash*