



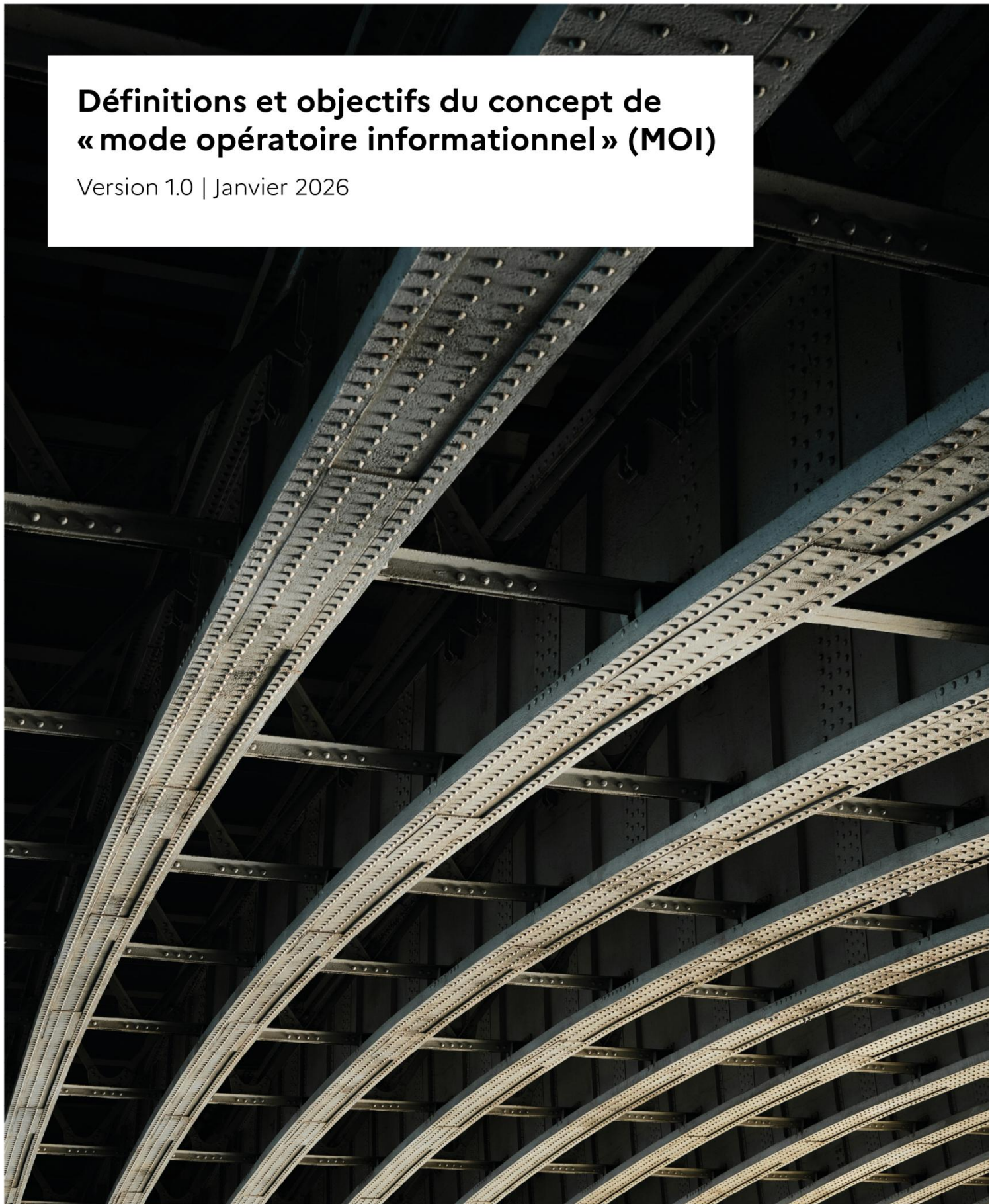
RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Définitions et objectifs du concept de « mode opératoire informationnel » (MOI)

Version 1.0 | Janvier 2026



Sommaire

1. Introduction	3
2. Définitions	5
2.1 Les dimensions de la manipulation de l'information	5
2.2 Définition d'un « mode opératoire informationnel ».....	5
2.3 Principales caractéristiques d'un MOI	6
3. Exemples	9
3.1 <i>Spamouflage</i>	9
3.2 Activités clandestines liées au <i>Baku Initiative Group</i>	9
3.3 <i>Storm-1516, CopyCop et Lakhta</i>	10
3.4 « <i>Team Jorge</i> ».....	12

1. INTRODUCTION

Depuis une dizaine d'années, la communauté dédiée à la lutte contre la manipulation de l'information (LMI) se structure, et ses membres (entités gouvernementales, médias, ONG, etc.) multiplient les initiatives pour adopter des concepts communs permettant de mieux comprendre, analyser, et décrire la menace informationnelle numérique. Si certains de ces concepts sont déjà bien appréhendés et exploités par l'écosystème, comme ceux d'« opération informationnelle » ou de « tactiques, techniques & procédures » (TTP), les experts décrivent néanmoins de manière différente les ensembles d'éléments techniques¹, comportementaux² et contextuels³ qu'ils observent – alors même qu'ils disposent de capteurs et de méthodologies d'analyse similaires.

Cette absence de grammaire opérationnelle commune est susceptible de nuire à la bonne compréhension de la menace informationnelle. À titre d'exemple, les activités numériques malveillantes attribuées à l'entreprise russe « *Social Design Agency* »⁴ (SDA) sont généralement rassemblées sous le nom de *Doppelgänger*, mais ce dernier a tour à tour été présenté comme une « opération », une « campagne », un « réseau », ou même un « acteur malveillant » (« *Threat Actor* »)⁵. Dans certains cas, le nom le plus usité par la communauté pour décrire ces ensembles est, par ailleurs, le même que celui de l'acteur malveillant (comme *Lakhta*⁶), ou ne recouvre qu'une petite partie de l'ensemble des éléments liés à un acteur malveillant (comme *Pravda*⁷), augmentant encore la confusion.

Le besoin de nommer ces ensembles est pourtant bien compris par la communauté de LMI, qui a déjà popularisé des noms tels que *Spamouflage*⁸ ou *Matriochka*⁹. Certaines organisations proposent même désormais, à partir de concepts issus du domaine de la *Cyber Threat Intelligence* (CTI), des conventions de nommage intégrant les acteurs de la menace informationnelle numérique¹⁰. Afin de résoudre ces difficultés et éventuelles confusions, VIGINUM a défini et propose d'employer le concept de « **mode opératoire informationnel** » (MOI), et son équivalent en langue anglaise, « **Information Manipulation Set** » (IMS). Ce concept a pour principaux avantages :

- d'offrir une dénomination simple, adaptée et centrée sur les éléments techniques, comportementaux et contextuels identifiés et suivis par la communauté ;
- de fonctionner même si les attaquants ne sont pas connus, ni présager de leur origine, de leurs intentions ou de leur niveau de ressources (humaines, financières et techniques) ;
- d'être interopérable avec des concepts éprouvés issus de la CTI, ainsi que les standards et les

¹ Adresses IP, enregistrements Whois, certificats SSL, empreintes de navigateur, etc.

² Partages, contenus identiques, dates de création d'un compte de réseau social, etc.

³ Victimologie, motivations des activités malveillantes, opportunités, effets finaux recherchés, etc.

⁴ Entreprise conduisant des opérations informationnelles numériques au profit de l'Administration présidentielle russe. Cf.

<https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency>.

⁵ VIGINUM s'appuie sur la définition d'acteur malveillant, ou acteur de la menace, proposée dans la documentation du modèle STIX : « *Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent* ». Source :

https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_k017w16zutw.

⁶ *Lakhta* étant à la fois le nom d'un ensemble d'éléments techniques, comportementaux et contextuels, et le nom de l'organisation clandestine à l'origine de ces activités. Cf. <https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes>.

⁷ *Pravda* étant le nom d'un réseau de sites liés à *Portal Kombat*, qui constitue un ensemble plus large et préexistant à ce réseau.

Cf. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.

⁸ Cf. <https://graphika.com/reports/spamouflage>.

⁹ Cf. https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf.

¹⁰ Comme *Microsoft* : <https://learn.microsoft.com/en-us/unified-secops/microsoft-threat-actor-naming>.

outils déjà exploités au sein de la communauté de la LMI, comme le modèle STIX¹¹ et *OpenCTI*.

Utilisé dans trois rapports techniques publiés par VIGINUM en 2025, le concept de MOI a depuis été réemployé dans les travaux d'autres acteurs de la communauté de LMI, à l'image du Service européen d'action extérieur (SEAE), de l'Agence de l'Union européenne pour la cybersécurité (ENISA)¹² et des membres du *Doppelgänger Working Group* (DGWG)¹³.

La présente note propose une définition précise de « mode opératoire informationnel », qui s'articule avec d'autres concepts utilisés par VIGINUM pour représenter la manipulation de l'information (cf. section [2.1](#)). Elle vise également à aider la communauté à identifier des MOI parmi les ensembles suivis, en détaillant leurs principales caractéristiques (section [2.3](#)) et en proposant des exemples concrets à partir d'activités malveillantes connues en source ouverte, attribuées ou non, issues de différents types d'acteurs, et observées dans différentes régions du monde (section [3](#)).

¹¹ Cf. <https://oasis-open.github.io/cti-documentation/stix/intro.html>.

¹² Cf. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

¹³ Cf. https://www.disinfo.eu/wp-content/uploads/2026/01/20260115_building-a-common-operational-picture-of-FIMI_01.pdf.

2. DEFINITIONS

2.1 Les dimensions de la manipulation de l'information

Pour bien comprendre l'intérêt du concept de MOI, il convient de clarifier dans un premier temps la façon dont sont schématisées les activités informationnelles numériques malveillantes. Le concept s'articule en effet avec d'autres dénominations existantes, permettant ainsi de représenter de manière holistique les « échelles » de la manipulation de l'information : depuis les activités visibles en ligne (un compte de réseau social diffusant un contenu) jusqu'aux personnes physiques qui en sont à l'origine (opérateurs, voire commanditaires). Cette représentation s'appuie sur des concepts issus de la doctrine militaire, qui sépare traditionnellement la guerre en cinq « niveaux » ou « dimensions » : politique, stratégique, opérative, tactique et technique.

Transposés à la manipulation de l'information, ces cinq niveaux correspondent :

- **politique** : aux acteurs ou « commanditaires » qui décident d'exploiter le levier des activités informationnelles numériques parmi une gamme d'actions possibles, qu'il s'agisse d'un État ou de tout autre type d'acteur (entreprise privée, ONG, influenceur, etc.) ;
- **stratégique** : aux acteurs ou « opérateurs » missionnés, recrutés ou financés pour traduire les objectifs politiques en actions, quel que soit leur type (État, organisation, individu), les commanditaires ne possédant pas systématiquement ces moyens en propre ;
- **opératif** : aux campagnes informationnelles conduites par les opérateurs pour atteindre les objectifs stratégiques, traduits en objectifs informationnels (promouvoir, dénigrer, polariser, inciter à l'action dans le champ physique, etc.) ;
- **tactique** : aux opérations informationnelles conduites par les opérateurs pour remplir les objectifs opératifs et décliner en actions les campagnes, par exemple la publication de contenus polarisants, et qui exploitent une ou plusieurs infrastructures numériques ;
- **technique** : aux infrastructures numériques (« *digital assets* ») contrôlées et exploitées par les opérateurs pour remplir les objectifs tactiques, qu'il s'agisse de comptes de réseaux sociaux, de sites Internet, d'adresses courriels, etc.

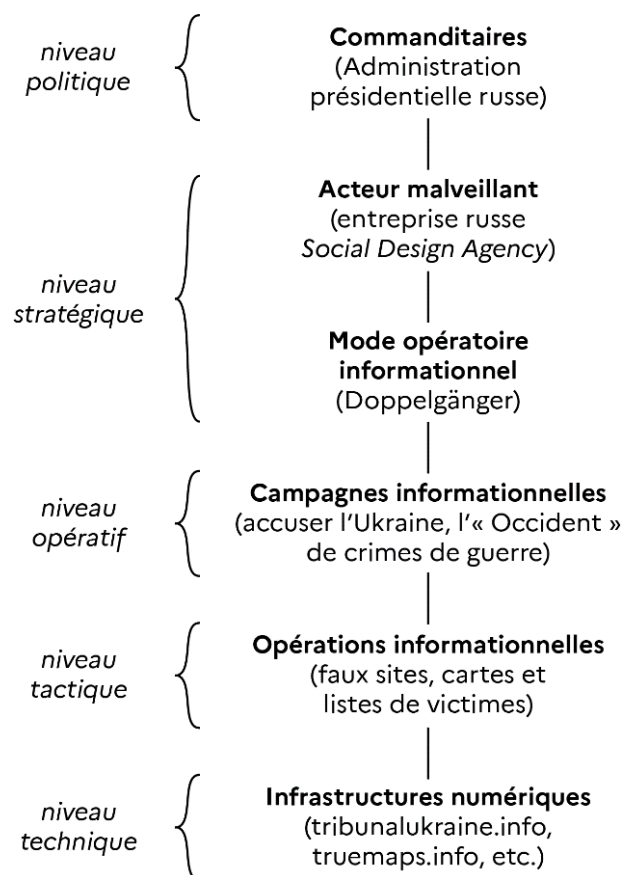
Néanmoins, comme c'est également le cas pour les attaques informatiques, les opérateurs des activités informationnelles numériques malveillantes ne sont pas toujours connus, et les défenseurs doivent alors créer des ensembles fictifs (« *Matriochka* », « *Spamouflage* », « *Doppelgänger* ») regroupant les éléments techniques, comportementaux et contextuels identifiés qui sont estimés imputables à un seul acteur malveillant. Indispensable pour analyser les activités numériques malveillantes dans le brouillard des opérations informationnelles et suivre la menace sur le long terme, VIGINUM propose de définir ce niveau d'abstraction avec la notion de « mode opératoire informationnel ».

2.2 Définition d'un « mode opératoire informationnel »

VIGINUM définit un mode opératoire informationnel (MOI) comme un ensemble de comportements, d'outils et de tactiques, techniques et procédures (TTP) adverses présumés liés au même acteur malveillant ou groupe d'acteurs malveillants, qui peut être inconnu. Un ou plusieurs MOI peuvent être attribués techniquement à un acteur malveillant, et une ou plusieurs campagnes peuvent être imputées à un MOI. Un MOI ne doit pas être confondu avec un acteur malveillant (« *Threat Actor* »), qui peut être un État, une organisation ou un individu. Enfin, un MOI peut être exploité pour conduire des campagnes informationnelles, qui peuvent être constituées de plusieurs opérations informationnelles (ou incidents).

Le concept de MOI permet ainsi de faire le lien entre les activités numériques observées et les opérateurs de ces activités, qu'ils soient identifiés ou non. Il se place donc au niveau stratégique en tant qu'émanation de l'acteur malveillant, et ensemble de moyens utilisés pour conduire les campagnes informationnelles. D'après cette définition, un même acteur malveillant peut conduire ou avoir opéré plusieurs modes opératoires informationnels.

Le concept de « mode opératoire informationnel » a été pensé comme le pendant dans le champ informationnel du concept de « mode opératoire d'attaque » (MOA) utilisé en CTI¹⁴, qui représente des ensembles à l'origine d'intrusions informatiques. Sa traduction, à savoir « *Information Manipulation Set* » (IMS), est également construite sur l'équivalent anglais de MOA, « *Intrusion Set* ». Ci-dessous figure un premier exemple intégrant le concept de mode opératoire informationnel, illustré par des activités numériques malveillantes imputées publiquement à *Doppelgänger*¹⁵ :



2.3 Principales caractéristiques d'un MOI

Le concept de MOI répond avant tout à un besoin de clarification. Afin de faciliter l'identification des MOI parmi les ensembles suivis par la communauté de la LMI, VIGINUM propose de les confronter à **deux conditions cumulatives** qui constituent l'épine dorsale du concept : **la clandestinité et la coordination**. L'explication de ces deux conditions, illustrées par de courts exemples, sera suivie par des

¹⁴ Cf. <https://www.cert.ssi.gov.fr/uploads/CERTFR-2021-CTI-004.pdf>.

¹⁵ Cf. https://www.sgdsn.gov.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf et <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>.

cas d'étude plus approfondis (cf. section 3) permettant de mieux appréhender l'intérêt et les subtilités du concept.

La première condition, dite de « clandestinité », insiste sur les intentions malveillantes des opérateurs : un ensemble peut être considéré comme un MOI si et seulement si **les opérateurs engagent des efforts manifestes pour éviter l'imputation, c'est-à-dire le rattachement des infrastructures numériques entre elles¹⁶, et leur attribution à un acteur malveillant¹⁷**. La clandestinité s'opère donc entre l'acteur malveillant et les infrastructures numériques sous leur contrôle, et permet d'exclure du concept tous les ensembles liés à des acteurs malveillants agissant en leur nom propre, ainsi que les ensembles non attribués disposant de différentes infrastructures numériques avec la même bannière.

- **Exemple 1** : les opérateurs de *Doppelgänger* ont déployé des efforts évidents pour que le public – et la communauté de la LMI – ne puisse pas lier techniquement leurs faux sites entre eux ni les imputer à l'entreprise russe *Social Design Agency* et leur commanditaire, à savoir l'Administration présidentielle russe. *Doppelgänger* peut donc être considéré comme un MOI dès lors qu'il répond également à la seconde condition.
- **Exemple 2** : les activités numériques d'une entité gouvernementale s'appuyant sur des canaux officiels, par exemple les comptes X de la diplomatie russe, ou les contenus liés à la « Fondation pour combattre l'injustice » (FCI)¹⁸, affichent tous clairement leur affiliation avec ces mêmes structures. Elles ne peuvent donc pas constituer des MOI à part entière.
- **Exemple 3** : le média pro-Russe anglophone *The Islander*, qui n'est pas clairement imputé à un acteur, coordonne un ensemble d'infrastructures numériques (comptes X et *Substack*), et remplit à cet égard la seconde condition, mais ces infrastructures sont cependant clairement rattachables entre elles¹⁹. Les activités numériques liées à *The Islander* ne peuvent donc pas constituer un MOI à part entière.

La seconde condition, dite de « coordination », insiste quant à elle sur le degré d'interaction entre les infrastructures numériques employées : un ensemble peut être considéré comme un MOI si et seulement si **les infrastructures numériques sont employées de manière coordonnée, et présumées opérées par le même acteur ou groupe d'acteurs travaillant pour le même commanditaire**. Cette condition permet d'assurer la cohérence des éléments techniques, qui doivent posséder des liens techniques ou comportementaux forts.

- **Exemple 1** : les infrastructures numériques liées à *Doppelgänger* forment un ensemble homogène, car rattachables entre elles par un faisceau de liens techniques et comportementaux forts et convergents²⁰. *Doppelgänger* peut donc être considéré comme un MOI s'il répond également à la première condition.
- **Exemple 2** : des comptes *TikTok* publiant les mêmes contenus que d'autres comptes *TikTok* ou chaînes *YouTube*, ou des sites hébergés sur la même adresse IP, ne sont pas forcément opérés

¹⁶ Par exemple en créant des comptes de réseaux sociaux et des sites avec des noms, des chartes graphiques et des dates de création différentes, en évitant les interactions entre eux, en déposant et en hébergeant des sites *via* des services différents, etc.

¹⁷ Par exemple en omettant d'afficher l'affiliation de sites ou de comptes de réseaux sociaux à l'acteur qui les contrôle, en indiquant de fausses informations de contact, en hébergeant des sites sur des serveurs partagés, dans un pays tiers, ou en les protégeant *via* des services d'anonymisation comme *Cloudflare*, etc.

¹⁸ Fausse ONG créée par Evgueny PRIGOJINE en 2021 pour documenter les « violations des droits humains » dans les pays occidentaux. Cf. https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports.

¹⁹ Elles disposent en effet du même nom, de la même charte graphique, redirigent directement les unes vers les autres, etc.

²⁰ Tels que la chaîne de diffusion, des éléments de code source, l'hébergement numérique, etc.

par le même acteur malveillant. Ils ne peuvent donc pas constituer un MOI.

- **Exemple 3** : les infrastructures numériques de *Storm-1679*²¹ et de *Matriochka* constituent deux ensembles cohérents, parfois rassemblés sous le nom d'*Overload*, mais VIGINUM n'est pas en mesure de les lier techniquement entre eux, et continue donc pour l'heure de les considérer comme deux MOI distincts²². Les deux MOI pourraient être fusionnés si des éléments techniques soutiennent cette hypothèse dans le futur.

²¹ Les activités documentées par le *Microsoft Threat Analysis Center* (MTAC) sous cette appellation ne recouvrent que la publication de faux contenus par un groupe de chaînes *Telegram* présumées opérées, ou au moins coordonnées, par les mêmes acteurs malveillants. Cf. <https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/>.

²² Cf. <https://checkfirst.network/operation-overload-an-ai-fuelled-escalation-of-the-kremlin-linked-propaganda-effort> et <https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes>.

3. EXEMPLES

3.1 Spamouflage

Largement documenté par la communauté de la LMI depuis 2019²³, *Spamouflage* désigne un ensemble d'éléments techniques, comportementaux et contextuels actif depuis au moins 2018, et également connu sous le nom de *Dragonbridge*, *Storm-1376* et *Taizi Flood*. Les infrastructures numériques liées à *Spamouflage* serviraient principalement à diffuser des narratifs favorables aux intérêts du Parti communiste chinois (PCC) auprès d'une audience internationale et à discréditer des opposants au PCC, notamment en amont de périodes électorales, sur des plateformes telles que X, Facebook, YouTube, Reddit ou encore TikTok.



Exemples de publications liées publiquement au MOI Spamouflage. Source : Institute for Strategic Dialogue

Sur la base des éléments publiés, VIGINUM peut décrire *Spamouflage* comme un mode opératoire informationnel à part entière, encore non formellement imputé à un acteur malveillant, car il est constitué :

- de comptes de réseaux sociaux masquant ostensiblement leurs liens entre eux et avec leurs opérateurs, dans le but probable d'éviter leur modération par les plateformes et leur rattachement à une entité gouvernementale chinoise ;
- de comptes de réseaux sociaux utilisés de manière coordonnée, rattachés entre eux par des liens techniques et comportementaux forts (date de création, pseudonymes, éléments biographiques, nombre d'abonnés, etc.), et présumés opérés par le même acteur malveillant.

3.2 Activités clandestines liées au *Baku Initiative Group*

Documenté par VIGINUM²⁴, le *Baku Initiative Group* (BIG) est une ONG fondée en juillet 2023 en Azerbaïdjan. L'organisation diffuse depuis sa création des contenus hostiles à la France sous l'angle de la « lutte contre le néocolonialisme », en exploitant notamment la situation économique et politique dans les territoires ultramarins, ainsi que les mouvements et idées indépendantistes. La majeure partie des activités numériques du BIG (sites Internet et comptes de réseaux sociaux) sont conduites au nom

²³ Cf. <https://graphika.com/reports/spamouflage>, <https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections>, https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us/ et <https://edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html>.

²⁴ Cf. https://www.sgdsn.gouv.fr/files/files/Publications/20241202_NP_SGDSN_VIGINUM_RAPPORT-BIG.pdf.

de l'organisation, qui est donc considérée comme un acteur malveillant. VIGINUM estime toutefois qu'en parallèle de ses activités publiques, le BIG opère un mode opératoire informationnel, puisqu'à plusieurs reprises, il s'est appuyé pour amplifier ses narratifs sur un ensemble de comptes :

- masquant ostensiblement, malgré un succès limité, leurs liens entre eux et avec le pouvoir azerbaïdjanais, dans le but évident de maintenir un déni plausible et de donner l'impression d'une contestation organique ;
- opérés de manière coordonnée, possédant des liens techniques et comportementaux forts (*hashtags*, messages et période d'activité, etc.), et très probablement opérés par le même groupe d'acteurs malveillants²⁵.



Exemples de publications de comptes clandestins amplifiant les narratifs du Baku Initiative Group.
Source : VIGINUM

Depuis au moins 2022, VIGINUM a noté à plusieurs reprises l'apparition de MOI liés à des acteurs malveillants préexistants, le premier permettant d'appuyer de manière clandestine les activités d'acteurs souhaitant renforcer le déni plausible, atteindre de nouvelles audiences, ou contourner des sanctions et restrictions techniques. Des médias russes liés ou proches de l'État, tels que *RT*²⁶ ou *Rybar*²⁷, auraient notamment commencé à conduire des MOI dans cette optique.

3.3 Storm-1516, CopyCop et Lakhta

Storm-1516, aussi connu publiquement sous le nom de *Neva Flood*, est un ensemble d'éléments techniques, comportementaux et contextuels actif depuis *a minima* août 2023. Cet ensemble est responsable de plus de 150 opérations informationnelles ciblant principalement les intérêts de l'Ukraine, de pays occidentaux et de pays post-soviétiques, notamment durant des processus électoraux. *Storm-1516* se caractérise par une chaîne de diffusion complexe exploitant à la fois des infrastructures numériques en propre, mais également celle de relais financés ou liées à d'autres ensembles. À ce jour, VIGINUM estime que les opérations informationnelles imputées à *Storm-1516* ont impliqué au moins trois ensembles clandestins et coordonnés, qui constituent chacun un mode

²⁵ Cf. <https://www.sgdsn.gov.fr/publications/nouvelle-caledonie-manoeuvres-informationnelles-impliquant-des-acteurs-0> et https://www.sgdsn.gov.fr/files/files/Publications/20241202_NP_SGDSN_VIGINUM_RAPPORT-BIG.pdf.

²⁶ Cf. <https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners>.

²⁷ Cf. <https://dfrlab.org/2025/09/23/sanctioned-russian-actor-linked-to-new-media-outlet-targeting-moldova/>.

opérateur informationnel à part entière :

- *Storm-1516*, imputé par le gouvernement américain au renseignement militaire russe et à un *think tank* moscovite, le Centre d'expertise géopolitique (CGE), responsable de la coordination des opérations, de la création des contenus, des narratifs, et du dépôt et du maintien d'un nombre limité d'infrastructures numériques (chaînes *YouTube* et comptes *X*) ;
- *CopyCop*, imputé à un ancien policier américain exilé en Russie depuis 2016, John Mark DOUGAN, qui serait responsable de l'enregistrement et du maintien de faux sites Internet exploités par *Storm-1516*, mais également par d'autres acteurs malveillants russes et pro-Russes ;
- *Lakhta*, non formellement imputé mais lié historiquement à la galaxie PRIGOJINE, qui a participé aux opérations de *Storm-1516* en primo-diffusant des contenus du MOI via ses infrastructures numériques (comptes *X*), et s'est appuyé sur celles de *Storm-1516* pour ses propres opérations²⁸.

Le concept de MOI se révèle donc essentiel pour analyser l'imbrication de plusieurs modes opératoires, puisqu'il permet de délimiter strictement des ensembles non liés par des éléments techniques, comportementaux ou contextuels, de mieux appréhender les aires de responsabilité et la structure des différents acteurs malveillants qui en sont responsables, et de suivre plus finement l'évolution de chacun des MOI impliqués dans le temps.

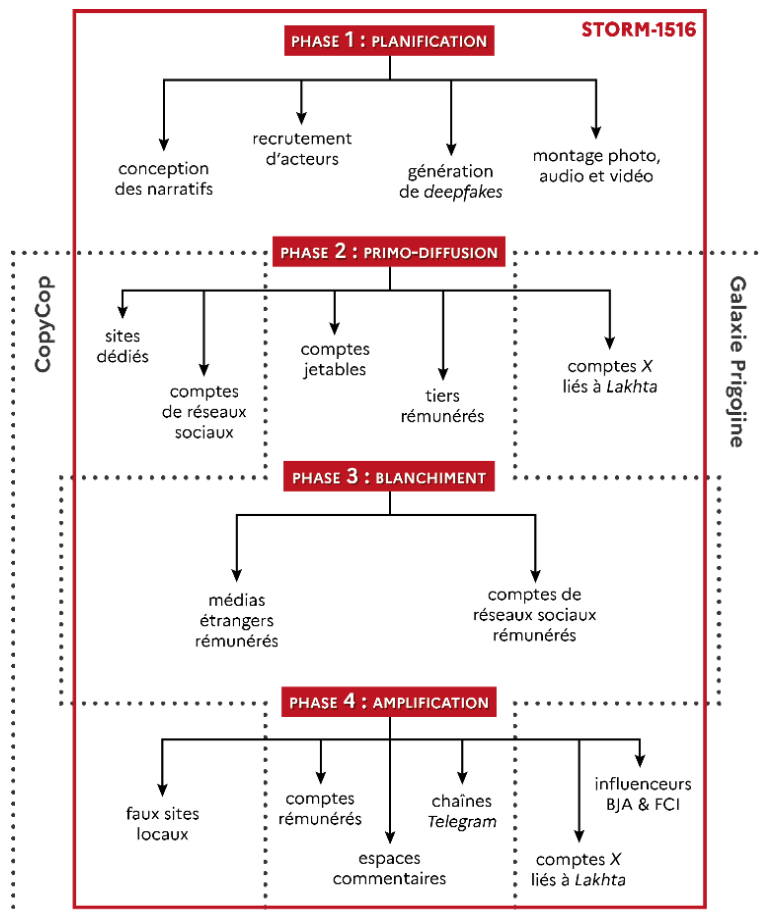


Schéma de diffusion des contenus de Storm-1516, s'appuyant notamment sur des éléments d'infrastructures numériques liés aux MOI CopyCop et Lakhta. Source : VIGINUM

²⁸ Cf. <https://www.sgdsn.gouv.fr/publications/analyse-du-mode-operatoire-informationnel-russe-storm-1516>.

3.4 « Team Jorge »

« *Team Jorge* » est le nom donné par le consortium de journalistes *Story Killers*²⁹ à une officine israélienne ayant conduit des campagnes de manipulation de l'information au profit de divers clients publics et privés depuis au moins 2015, notamment durant des processus électoraux. Pour ce faire, *Team Jorge* s'appuyait notamment sur un outil, appelé *Advanced Impact Media Solutions (AIMS)*, permettant de gérer la création de faux articles de presse et de dizaines de milliers de profils inauthentiques sur les réseaux sociaux, dont *Facebook*, *Twitter*, *Instagram*, *YouTube* ou encore *Reddit*.

Les campagnes attribuées à *Team Jorge* ont notamment servi à promouvoir des projets pour divers clients privés, mais également à dénoncer des initiatives et des personnalités, comme les sanctions contre des oligarques russes, la coupe du monde de football 2022 au Qatar, ou des hommes d'affaires asiatiques. Certaines opérations informationnelles numériques étaient par ailleurs combinées avec des intrusions informatiques.



Captures d'écran de l'outil AIMS employé par l'officine. Source : *Forbidden Stories*

VIGINUM estime que l'acteur malveillant « *Team Jorge* » a conduit un mode opératoire informationnel au profit de ses clients, car :

- l'acteur malveillant a manifestement cherché à cacher les liens entre ses différentes infrastructures numériques et l'officine, dans le but probable de garantir l'anonymat de ses clients et d'éviter des poursuites légales ;
- les infrastructures numériques étaient utilisées de manière coordonnée, puisqu'elles participaient à des campagnes précises, présentaient des liens techniques et comportementaux

²⁹ Cf. <https://forbiddenstories.org/fr/story-killers>.

forts (date de création, suivi, abonnements, etc.), et étaient directement opérées par l'officine.

Le concept de MOI est donc applicable à tout type d'acteurs (entités gouvernementales, structures privées, officines agissant au travers de sociétés-écrans), même s'il implique un groupe d'acteurs malveillants opérant différentes parties du MOI (définition des narratifs, dépôt d'infrastructures numériques, création des contenus, etc.), même s'il est mis à disposition de divers « clients » ou commanditaires, et quelles que soient leurs intentions.

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](#)

Crédit photo couverture : Photo de [Piermanuele Sberni](#) sur [Unsplash](#).