



Livre blanc sur la modélisation de la manipulation de l'information

Bertrand Boyer
Anaïs Meunier
M82_Project

Novembre 2025

Livre blanc sur la modélisation de la manipulation de l'information

Bertrand Boyer, Anaïs Meunier,

M82_Project

Livre blanc sur la modélisation de la manipulation de l'information,
Bertrand Boyer, Anaïs Meunier
Novembre 2025

M82_project. Association à but non lucratif, le M82_project vise à constituer, animer et développer un réseau d'acteurs et d'experts du domaine de la cyber sécurité, de la cyberdéfense et de la lutte contre la manipulation de l'information. Par ses actions, M82_project cherche en particulier à sensibiliser le public, les décideurs et les responsables publics ou privés en s'appuyant sur des expertises variées.

Bertrand Boyer. Saint-cyrien, breveté de l'École de guerre, auditeur de l'IHEDN, et diplômé de Telecom ParisTech. Disposant d'une double culture opérationnelle et technique, il est parmi les premiers officiers à penser la conflictualité dans le cyberspace. Il publie plusieurs ouvrages et articles sur cette question dont *Cybertactique : conduire la guerre numérique* (2014), un *Dictionnaire de la Cybersécurité et des réseaux* (2016), et *Guérilla 2.0* qui a reçu le Prix du Festival international de la cybersécurité en 2020.

Anaïs Meunier. Ancienne analyste de Viginum, le service de lutte contre les ingérences numériques étrangères, elle a développé une expertise dans la modélisation de ces phénomènes à travers les standards de la CTI. Son passage dans le domaine de la cyber sécurité a également permis d'acquérir des compétences en analyses et en OSINT, notamment autour de la cybercriminalité et de la menace APT, qui lui ont servi à tester et à confirmer ses hypothèses de modélisation.

Document publié sous licence Creative Commons : CC-BY

TL:DR

La lutte contre la manipulation de l'information (LMI) est une discipline récente dont le cadre conceptuel en construction est très largement hérité de la cybersécurité et de la terminologie militaire. Pourtant, face aux spécificités des menaces informationnelles contemporaines, les limites d'une telle transposition apparaissent clairement et militent pour une adaptation et une clarification de certains concepts. Ce livre blanc propose ainsi un cadre d'analyse articulé autour de trois axes principaux.

Le premier repose sur la distinction claire entre deux types d'opérations informationnelles : **les opérations stratégiques**, qui visent à transformer durablement les croyances, notamment en déplaçant la fenêtre d'Overton ou en exacerbant les fractures sociales ; et **les opérations tactiques**, qui cherchent à modifier ponctuellement les comportements sans altérer en profondeur les convictions. Cette typologie permet alors de concevoir des modèles d'analyse différenciés.

Le deuxième axe identifie **trois modalités d'action** qui sont communes aux deux typologies proposées : **les actions planifiées**, qui sont des opérations délibérées avec des objectifs et des moyens clairement définis ; **les actions d'opportunités ou dynamiques** qui consistent à exploiter des événements non anticipés pour imposer un récit ; et **le drumbeat, ou martèlement** répétitif de récits simplistes sur le long terme, visant à structurer les perceptions dans la durée.

Enfin, **le troisième axe** propose un **modèle d'analyse défensive centré sur l'incident**. Face à l'asymétrie entre un attaquant disposant d'une vision globale et un défenseur qui ne perçoit que des fragments, ce modèle s'appuie sur **six dimensions clés** : l'incident, l'infrastructure, les effets, les cibles, l'adversaire et la temporalité. **Il permet une capitalisation rigoureuse des incidents** afin de révéler les capacités adverses de manière factuelle plutôt que spéculative.

Les implications opérationnelles de cette approche sont multiples :

- **évacuation du terme campagne** pour décrire les éléments observés car la campagne correspond à une vision spécifiquement attaquant, pratiquement inexploitable dans le cadre de la LMI.
- **Détection, caractérisation et capitalisation centrée sur le niveau incident.**
- **Distinction claire entre mesures d'impact côté défenseur, et mesures d'effet (MOE) ou de performance (MOP) côté attaquant.**
- **Accumulation méthodique d'observables** qui ouvrant la voie à un **véritable renseignement sur la menace** informationnelle (*Informational Threat Intelligence, ITI*)

En structurant l'analyse de la menace informationnelle comme un processus de renseignement, cette méthode permet d'éviter les pièges de la surinterprétation, tout en produisant une connaissance actionnable, adaptée aux exigences d'une réponse efficace et ciblée.

Table des matières

Livre blanc sur la modélisation de la manipulation de l'information	1
TL:DR	3
L'enjeu d'une grammaire commune	5
Partie 1 : de quoi les menaces informationnelles sont-elles le nom ? ...	6
Les deux danseurs	8
Les opérations stratégiques d'influence : l'art de faire douter et de convaincre	9
Les opérations tactiques (psyops classiques) : l'art de faire agir	11
Les trois temps de la valse	12
Le ciblage planifié	12
Les actions d'opportunité ou le dynamic targeting.....	13
Le bruit de fond - drumbeat	14
Partie 2 : de la campagne à l'incident, vers une approche défensive réaliste.....	16
Les six dimensions de l'attaque informationnelle.....	17
L'incident.....	18
L'infrastructure.....	19
Les effets	19
Cibles	19
Adversaire	20
La temporalité	21
La capitalisation progressive : de l'incident à l'infrastructure	21
Conclusion.....	22
Bibliographie	23

L'enjeu d'une grammaire commune

La cybersécurité et la cyberdéfense bénéficient aujourd'hui d'un recul qui, bien que limité, permet de faire émerger des méthodologies formelles d'analyse ainsi que des modélisations de la menace. A contrario, la lutte contre la manipulation de l'information, dans son volet numérique comme dans son incarnation plus physique, ne bénéficie pas de la même profondeur. Aussi la LMI s'est-elle rapidement inspiré des exemples existants et a fait largement appel à la cybersécurité pour se structurer. En cherchant l'analogie partout où cela était possible, la jeune matière se lance dans des *framework*¹, cherche à implémenter une *kill chain*, explore la *pyramid of pain*². Le vocabulaire importe alors les notions que nous connaissons en cybersécurité comme, les modes opératoires adverses (MOA), les tactiques, techniques et procédures (TTPs), les infrastructures etc.

Cet ensemble de notion permet de donner corps à la menace. Mais comme le souligne VIGINUM dans son *Guide d'utilisation d'OpenCTI pour la lutte contre les manipulations de l'information d'origine étrangère*³, 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.

Que l'on parle de *Cyber Threat Intelligence*⁴ (CTI) ou de LMI, le recours à la terminologie militaire est d'usage courant pour décrire les actions et les menaces. On parle alors d'attaque, d'incident, d'actions, d'opérations, de campagnes, de tactiques, etc. La cybersécurité a même industrialisé cette pratique pour permettre aux outils de capitalisation et de visualisation de traiter les incidents dans un cadre plus vaste de

¹ <https://www.disarm.foundation/>

² Sara-Jayne Terp, « Cognitive Security: Pyramid of Pain », *Disarming Disinformation*, 29 avril 2021, <https://medium.com/disarming-disinformation/cognitive-security-pyramid-of-pain-3f0f860e86cd>.

³ Viginum, *Guide d'utilisation d'OpenCTI pour la lutte contre les manipulations de l'information d'origine étrangère* (SGDSN, 2025), <http://www.sgdsn.gouv.fr/publications/guide-dutilisation-dopencti-pour-la-lutte-contre-les-manipulations-de-linformation>.

⁴ La Cyber Threat Intelligence « consiste en la collecte, l'analyse et la diffusion systématiques d'informations relatives aux activités d'une entreprise dans le cyberspace et, dans une certaine mesure, dans l'espace physique. Elle vise à informer les décideurs à tous les niveaux. »

campagnes d'attaque. Cette démarche vise essentiellement à donner matière à l'analyse afin d'aboutir au Graal de la CTI : l'attribution.

Cependant, l'importation directe de ces concepts révèle rapidement ses limites. Modéliser la menace suppose de disposer d'une grille partagée d'analyse, d'une compréhension commune des phénomènes observés afin de mieux y répondre. Or, les spécificités de la lutte informationnelle nécessitent un cadre conceptuel adapté, qui dépasse les analogies parfois trompeuses avec la cybersécurité.

Partie 1 : de quoi les menaces informationnelles sont-elles le nom ?

En cybersécurité, la description de la menace repose pour partie sur une définition claire de son périmètre d'application. Pour l'ANSSI, « une cybermenace a pour objectif la compromission de la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.⁵ » Les notions ici de disponibilité, d'intégrité et de confidentialité d'un système ou de l'information sont moins propices à l'"interprétation et sont des propriétés mesurables. La caractérisation d'une atteinte semble donc reposer sur un socle technique et juridique relativement solide.

En matière de menace informationnelle l'approche apparaît d'emblée plus complexe et met en œuvre une série de notions intriquées dont certaines relèvent de la terminologie militaire. Ainsi pour VIGINUM, « la menace informationnelle en ligne impliquant des acteurs étrangers, se traduit par des manœuvres d'ingérence ou des campagnes numériques de manipulation de l'information, avec pour objectifs de porter atteinte aux intérêts de l'entité ciblée et/ou promouvoir les revendications d'un acteur. Prenant la forme d'opérations planifiées ou d'actions opportunistes, ces manœuvres informationnelles cherchent à diffuser de fausses informations ou à amplifier des contenus malveillants déjà présents dans le débat public⁶. » Cette définition, bien qu'opération-

⁵ ANSSI, Panorama de la cybermenace 2024 (SGDSN, 2025), 52,
<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>.

⁶ Viginum, Guide de sensibilisation à la menace informationnelle pendant les Jeux Olympiques et Paralympiques à destination des médias et journalistes fact-checkeurs (SGDSN, 2024), 8,
https://www.sgdsn.gouv.fr/files/files/Publications/Guide_sensibilisation_factcheckeurs_vf.pdf.

nelle, soulève la question de la distinction entre « manœuvre d'ingénierie », « campagne numériques » ou encore « action informationnelle ».

Ce recours au champ lexical de l'affrontement nous impose de revenir sur les fondements de la terminologie militaire qui lui a donné naissance. Ainsi, **dans le cadre de la planification d'un engagement armé, une action produit un effet sur une cible, l'objectif étant de modifier l'état de cette cible** : on parle alors d'état final recherché (EFR). L'EFR traduit donc ce à quoi l'on espère aboutir comme situation.

Dans la plupart des cas, une action isolée ne suffit pas à modifier durablement l'état de la cible, il faut alors **combiner les effets** et donc **synchroneiser les actions**. C'est alors tout l'objet du « plan d'opération ». Ce plan fixe le « qui fait quoi » dans le temps afin de réaliser les actions identifiées.

Dans ce contexte, **une opération est une série d'actions élémentaires planifiées, coordonnées, afin de remplir des objectifs (militaires) qui concourent à l'atteinte de l'état final recherché**. Elle est donc **limitée dans le temps et vise une cible particulière**.

Au niveau stratégique et opératif on a recours à **une approche graphique** pour représenter cette série d'action que l'on répartit sur des lignes d'opération (ou lignes d'effort). On appelle cela l'**« OPS Design »**.

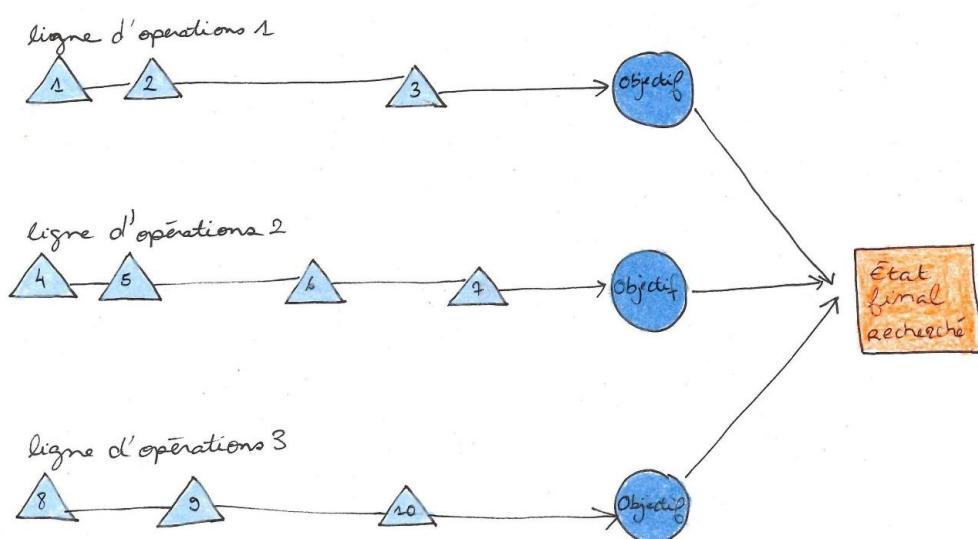


Figure 1. Schéma simplifié du design des opérations

Une campagne désigne alors **plusieurs opérations conduites par une force ou un attaquant dans un cadre espace/temps limité**. Ce découpage permet de concevoir et de conduire les actions militaires. Comprendre ce mécanisme chez un adversaire permet, d'une certaine façon, de le modéliser et donc de lui donner un caractère prévisible. Les mémentos de tactique rassemblent ainsi les techniques qui permettent la mise en œuvre de ces actions. Dès lors, à chaque niveau de commandement d'une structure militaire, depuis la section jusqu'au corps d'armée, du chasseur à l'escadre, de la frégate au groupe aéronaval, chacun peut-il s'appuyer sur des recueils de procédures pour conduire ses actions élémentaires. Comprendre et connaître les procédures de l'adversaire permet d'anticiper ses mouvements, de les contrer et constitue donc un avantage significatif.

Les tactiques, techniques et procédures d'un adversaire constituent donc une forme de signature permettant de le caractériser, de l'identifier et donc d'adopter des contres mesures efficaces. C'est une des raisons qui ont poussé les analystes de la menace cyber à adopter la terminologie militaire.

Mais **cette approche est-elle transposable lorsqu'on parle d'opération d'influence ou de manipulation de l'information ?** En France le cadre doctrinal rapproche deux concepts pourtant totalement distincts : l'influence et la lutte informationnelle. Ainsi regroupé sous un chapeau commun, ces deux notions laissent à penser que la lutte contre ces phénomènes (la LMI) répondrait à la même approche unificatrice.

Les deux danseurs

Pour proposer un cadre d'analyse adapté à la LMI ou plus largement pour conduire une analyse de la menace informationnelle nous distingueront deux types d'opérations informationnelles qui divergent tant par leurs objectifs que par leurs temporalités de mise en œuvre et de production d'effets.

L'action sur les perceptions et l'utilisation de l'information peut chercher à modifier les croyances ou simplement à faire agir les audiences cibles. Ainsi, susciter le doute, rependre une rumeur, fragiliser la confiance (dans les institutions) mobilise des moyens et des techniques qui ne sont pas strictement identiques à ceux nécessaires pour entraîner une action (acte d'achat, mobilisation, vote, etc.).

Les effets produits ne s'inscrivent pas non plus dans la même temporalité. Là où, pour façonner des opinions, pour persuader, il faudra plusieurs mois ou années, pour « faire agir » le seul ressort de l'émotion peut suffire. Cette approche qui distingue les actions d'influence en fonction de leurs finalités et de la temporalité permet dans un premier temps, de mieux comprendre la menace et dans un second temps, de clarifier les périmètres d'action potentiels des acteurs de la réponse à celle-ci.

Ainsi, répondre à une tentative de diffusion d'une fausse information (comme l'armée française en a été capable lors de l'affaire du faux charnier de Gossi⁷) ne fait pas appel aux mêmes mécanismes que ceux nécessaires à la lutte contre le mode opératoire d'attaque (MOA) Doppelgänger⁸. Les deux actions sont pourtant regroupées sous la bannière unique de « manipulation de l'information ». Dans notre approche, ce sont les finalités et les temporalités qui définiront le cadre d'analyse et qui, *in fine*, orienteront sur les modalités de réponse à ces menaces. Ainsi nous distingueront les opérations d'influence stratégiques ou profondes de celles dont l'objectif demeure tactique pour l'obtention d'un gain immédiat (occupation de l'espace informationnel, bruit médiatique...).

Les opérations stratégiques d'influence : l'art de faire douter et de convaincre

Les opérations stratégiques d'influence visent à persuader un auditoire, elles cherchent à transformer durablement les convictions et les croyances des populations cibles. Ces actions s'appuient notamment sur l'exploitation de biais cognitifs qui favorisent l'ancrage de certains récits. On pourra par exemple évoquer l'illusion de fréquence qui, en répétant un discours, tant à le faire accepter plus facilement ou encore

⁷ https://www.lemonde.fr/afrique/article/2022/04/23/sahel-dans-la-guerre-de-l-information-l-armee-francaise-replique-et-accuse-le-groupe-wagner_6123340_3212.html Après son retrait de la base de Gossi au Mali, l'armée française a diffusé une vidéo accusant le groupe Wagner d'avoir mis en scène un charnier pour discréditer l'opération Barkhane. Selon l'état-major français, cette manipulation visait à accuser faussement la France de crimes de guerre via une campagne de désinformation sur les réseaux sociaux. L'incident s'inscrit dans un contexte plus large d'exactions présumées commises par les forces maliennes et leurs alliés russes, notamment à Hombori et à Moura.

⁸ Doppelgänger est mode opératoire d'attaque exploité par la Russie depuis 2022, visant à saper le soutien à l'Ukraine et à semer la division dans les pays occidentaux. Elle utilise notamment de faux sites clonés de médias ou d'institutions officielles pour diffuser des récits pro-Kremlin. Cette opération est menée par des entreprises russes comme Struktura et ASP, et comprend plusieurs volets comme RRN, Matriochka ou Storm-1099.

le biais de confirmation qui fait que l'on a tendance à retenir des informations qui confirment des croyances préétablies⁹. Ces actions s'inscrivent dans une logique de minage informationnel, de pollution du terrain, de « sédimentation »¹⁰. Elles saturent progressivement un espace cognitif et en interdisent l'accès à d'autres récits. Leur objectif supposé est la fracturation sociale durable, la fragilisation des fondements des sociétés démocratiques. Ces opérations s'inscrivent dans le temps long et leurs effets ne sont mesurables qu'à travers des indicateurs indirects, souvent sur plusieurs années.

Le récit du « déclin de l'Occident » porté par la Russie constitue un cas d'école d'opération stratégique. Né en réaction à la perception post-Soviétique d'un déclassement, ce récit est structuré par une réécriture de l'histoire opérée par Vladimir Poutine depuis son accession au pouvoir. À partir 2014, des médias d'État de propagande russe comme *Russia Today* ou *Sputnik* développent systématiquement une grille de lecture présentant les démocraties occidentales comme corrompues, décadentes et vouées à l'effondrement¹¹. Cette approche ne se contente pas de critiquer des politiques spécifiques mais questionne la légitimité même du modèle démocratique. Chaque crise (gilets jaunes, Brexit, polarisation américaine) est présentée comme une preuve supplémentaire de cette décadence structurelle. L'objectif n'est pas de convaincre immédiatement les audiences de rejeter la démocratie, mais de normaliser l'idée que d'autres modèles politiques (autoritaires) pourraient être plus efficaces.

L'efficacité de ces opérations ne se mesure pas en termes de réaction immédiate, mais par leur capacité à élargir la fenêtre d'Overton¹², à ancrer durablement des récits dans l'inconscient collectif et le débat public, pour ultimement provoquer une dislocation du tissu social par le

⁹ Pour une présentation détaillée des biais cognitifs utilisés dans le cadre des opérations d'influence voir la présentation de la matrice DIMA élaborée par M82_project : <https://m82-project.org/articles/dima/dima/>

¹⁰ Arild Bergh, « Understanding Influence Operations in Social Media: a cyber kill chain approach », *Journal of Information Warfare* 19, no 4 (2020): 110-31. P. 117

¹¹ Affaires mondiales Canada, « Le recours de la Russie à la désinformation et à la manipulation de l'information », AMC, 4 février 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=fra.

¹² La fenêtre d'Overton, est un concept développé par Joseph P. Overton pour qui la viabilité d'une idée politique dépend du fait qu'elle se situe dans une fenêtre d'acceptabilité publique.

clivage durable. Dans ce contexte, les modalités de défense ne peuvent se concevoir que sur le long terme. L'éducation et des politiques publiques seront les outils les plus adaptés. Ici, le « contre-récit » aura peu d'impact et pourra même renforcer le discours initial. Comme l'a démontré l'échec des mesures de contre radicalisation¹³. C'est d'abord la mise en place d'une offre alternative positive qui permettra de minimiser l'impact de ces actions. On ne luttera donc pas contre mais différemment.

Les opérations tactiques (psyops classiques) : l'art de faire agir

Les opérations d'information ou *Psyops* suivant la terminologie anglo-saxonne, sont conduites traditionnellement dans le cadre des conflits armés. Elles visent la modification comportementale ponctuelle d'audiences limitées dans un périmètre espace-temps contraint.

Elles cherchent à infléchir des actions sans nécessairement transformer les convictions profondes. L'exemple classique de ces actions est incarné par les appels et incitations à la reddition. Elles peuvent être efficaces, à l'image des opérations conduites par la coalition lors de la première guerre du Golfe, en 1991, où une vaste campagne de déception avait contribué à alimenter la crainte d'un débarquement chez les irakiens alors que l'offensive terrestre se préparait depuis le Nord-ouest de l'Arabie Saoudite¹⁴. Pour autant, ces actions ne changent pas durablement la conviction des audiences. Si les soldats irakiens ont massivement déserté, ou ce sont rendus (plus de 85 000 prisonniers), ils n'ont pas toutefois abandonné leur socle de croyance ni embrassé la cause de la coalition.

L'exploitation des manifestations du « Convoi de la liberté », au Canada en 2022¹⁵ et son rebond en France, illustre également cette exploitation tactique. Des comptes russes ont amplifié massivement les contenus liés aux manifestations de camionneurs contre les restrictions sanitaires, non pas pour soutenir durablement leur cause, mais pour exacerber les ten-

¹³ Dumoulin, M. (2018). Déconstruire la radicalisation : implications et limites de la notion. *Confluences Méditerranée*, 105(2), 171-181. <https://doi.org/10.3917/come.105.0171>.

¹⁴ Mazzucchi, N. (2021). La guerre du Golfe, première guerre info-centrée. *Revue Défense Nationale*, 843(8), 32-38. <https://doi.org/10.3917/rdna.843.0032>.

¹⁵ <https://www.tf1info.fr/societe/convoi-de-la-liberte-comment-le-hashtag-convoideلالiberte-devenu-viral-est-il-ne-en-france-2210702.html>

sions sociales au moment précis où le Canada soutenait l'Ukraine. L'objectif supposé était de détourner l'attention politique et de créer une crise interne qui affaiblirait temporairement la position canadienne. Une fois les manifestations terminées, ces mêmes comptes ont cessé de s'intéresser au sujet, révélant le caractère purement tactique de l'opération. En amplifiant artificiellement les revendications, le mouvement s'est densifié et le nombre de manifestants a augmenté.

Il y a donc une différence fondamentale entre les actions et les convictions ou les croyances. Ces opérations tactiques agissent sur le premier niveau, laissant le second intact.

La première étape d'une politique de lutte contre la manipulation de l'information consistera donc à déterminer à quel type de menace on fait face. Les opérations tactiques ne requièrent pas les mêmes aptitudes que celles qui cherchent à agir en profondeur sur un contexte. Ce qui rend l'exercice complexe c'est que ces deux typologies d'opération possèdent des modalités communes. Or l'analyste, le défenseur observe ces modalités, sans toujours distinguer la famille à laquelle elle se raccorde.

Les trois temps de la valse

Ces deux types d'opérations, influence stratégique ou tactique peuvent mobiliser trois modalités d'action distinctes, qui constituent autant de modes opératoires observables.

Le ciblage planifié

En matière d'opération militaire, **le ciblage est la méthode qui traduit en action les effets recherchés**. Cette méthode se divise en deux phases dont la première consiste à comprendre l'adversaire en étudiant son fonctionnement à l'image d'un système. Puis, dans une deuxième phase, il s'agit d'identifier les vulnérabilités critiques puis les cibles qui seront visées par l'opération. Cette démarche est tout à fait transposable aux opérations d'influence conduites par des acteurs étatiques en conflit.

Si l'on considère ces techniques, on distingue, dans leur mise en œuvre, le ciblage planifié du ciblage dynamique. Dans le premier cas, on planifie très en amont les objectifs qui seront traités ainsi que les moyens de les atteindre. Ce processus nécessite de fixer des effets à produire, ainsi

qu'un cadre espace-temps contraint. En matière de lutte informationnelle, on peut distinguer la même typologie d'action.

L'opération du charnier de Gossi illustre cette modalité : action planifiée très en amont, convergence de moyens, construction de relais pour diffuser l'information et validation du récit. L'action visait à alimenter le récit : « la France commet des crimes de guerre ». Cette action planifiée a été déjouée par le renseignement qui a permis de détecter les préparatifs de l'opération en amont et donc de documenter la manipulation.

Les tentatives de manipulation informationnelle contre les Jeux olympiques de Paris 2024 sont, à l'inverse un exemple de l'échec d'opérations planifiées face à une détection précoce. VIGINUM a identifié 43 manœuvres informationnelles hostiles entre avril 2023 et septembre 2024, dont une opération particulièrement révélatrice menée par des acteurs liés à l'Azerbaïdjan¹⁶. Le 26 juillet 2024, des « visuels appelant à boycotter les JOP-24 » ont été massivement diffusés sur X avec les hashtags #PARIS2024 et #BOYCOTTPARIS2024. L'analyse a révélé que 91 comptes étaient à l'origine de plus de 1 600 publications en 48 h, dont 40 comptes créés spécifiquement en juillet 2023, soit un an avant, uniquement pour publier des contenus de boycott. Cette planification très en amont, caractéristique des opérations délibérées, a échoué car « les manœuvres identifiées ont, pour la plupart, peiné à obtenir une visibilité suffisante dans le débat public numérique francophone pour produire des effets réels sur le bon déroulement des événements¹⁷. »

La mesure d'efficacité, dans ce cadre, a lieu directement après l'événement considéré. La série d'actions est close, soit par la diminution des ressources allouées soit sur ordre.

Les actions d'opportunité ou le dynamic targeting

À côté de ces actions planifiées, nous observons régulièrement ce que l'on peut qualifier d'actions dynamiques. Dans ce cadre, **chaque événement (parfois anodin) peut être exploité pour soutenir un récit et contribuer à sa diffusion plus large.**

¹⁶ Viginum, Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024 (SGDSN, 2024), <https://www.sgdsn.gouv.fr/publications/synthese-de-la-menace-informationnelle-ayant-vise-les-jeux-olympiques-et-paralympiques>.

¹⁷ Viginum, Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024. P.4

L'affaire du Rafale indien en est une illustration significative. Lors de l'opération *Sindoor*, en mai 2025, au moins un appareil de l'*Indian Air Force* a été perdu dans un affrontement avec le Pakistan. Cet incident a immédiatement été exploité par des réseaux de désinformation, qui ont alimenté plusieurs récits convergents visant à discréditer non seulement l'efficacité de l'avion, mais aussi la qualité de la coopération militaire française. Selon le ministère des Armées français, « des contenus ont été rapidement repris et amplifiés par des comptes à forte audience, souvent associés à des écosystèmes pro-pakistanais ou proches de certaines puissances étrangères. L'objectif n'était donc pas de rapporter un fait, mais de construire un récit : celui d'un échec opérationnel de l'Inde, et d'une remise en cause du Rafale¹⁸ ».

Cette exploitation s'est manifestée à trois niveaux : d'abord, une amplification disproportionnée des pertes, ensuite diffusion d'images détournées de leur contexte, et enfin instrumentalisation commerciale par des compétiteurs industriels, notamment chinois, pour promouvoir leurs propres équipements¹⁹. Cette saisie d'opportunité visait à exploiter un événement militaire réel pour porter atteinte à l'image du matériel français sur le marché international, particulièrement en Asie-Pacifique.

Par nature non prévisibles car s'appuyant sur des événements non planifiés, ces opérations ne peuvent être anticipées. Dans ce cadre, la mesure de leur efficacité peut être : le récit est-il devenu organique, a-t-il pris ? A-t'on réussi à détourner l'intérêt initial sur l'événement vers le récit imposé ? Une mesure peut être effectuée sur une temporalité moyenne après l'événement avec des rebonds qui peuvent avoir lieu plusieurs mois plus tard.

Le bruit de fond - *drumbeat*

Cette modalité consiste à marteler un récit (en général simpliste) durant des mois voire des années. L'objectif ici n'est pas de produire un effet rapidement mais d'élargir la fenêtre d'Overton et, dans la durée, d'ancre une vision du monde. Ces méthodes fragilisent le tissu social et viennent à sa dislocation et au clivage durable.

¹⁸ Ministère des Armées, Le Rafale face à la désinformation : lecture stratégique d'un ciblage informationnel, 26 juin 2025, <http://www.defense.gouv.fr/desinformation/nos-analyses-froid/rafale-face-desinformation-lecture-strategique-dun-ciblage-informationnel>.

¹⁹ Pierre Sauveton, « La Chine s'en prend au Rafale pour freiner son succès à l'export », OpexNews, 6 juillet 2025, <https://opexnews.fr/rafale-chine-desinformation/>.

Les campagnes russes contre les vaccins occidentaux illustrent parfaitement cette modalité. Depuis 2015, des comptes liés à l'IRA (*Internet Research Agency*²⁰) diffusent de manière constante des contenus anti-vaccination sur les réseaux sociaux américains et européens. Plutôt que de nier frontalement l'efficacité des vaccins, ces campagnes amplifient les doutes existants, relaient des témoignages d'effets secondaires (réels ou supposés) et questionnent systématiquement les motivations des autorités sanitaires. Cette approche ne vise pas à convaincre immédiatement, mais à normaliser le scepticisme vaccinal dans le débat public, créant ainsi un terrain favorable lors de crises sanitaires comme la COVID-19.

Le récit selon lequel « la France arme les terroristes » au Sahel constitue également un cas d'école de *drumbeat* déployé par les réseaux d'influence russes depuis 2021. Selon le département d'État américain, ce récit a été systématiquement martelé à travers « un réseau coordonné de pages Facebook au Mali présentant la Russie comme un 'partenaire viable' et 'une alternative à l'Occident'²¹ ». Ce *drumbeat* répète inlassablement que la France, sous couvert de lutte anti-terroriste, alimente en réalité les groupes djihadistes pour justifier sa présence militaire et économique. Le récit est relayé par des médias locaux, des influenceurs payés, et est amplifié sur les réseaux sociaux. Cette manipulation s'appuie sur l'exploitation déformée d'événements réels (bloquages de convois français, incidents avec des civils) pour ancrer progressivement l'idée d'une duplicité française structurelle²². L'objectif n'est pas de prouver cette accusation, mais de la rendre évidente dans l'inconscient collectif local, préparant ainsi l'acceptation des "conseillers" russes comme alternative crédible.

Dans le cadre du *drumbeat*, il est illusoire de vouloir conduire une mesure des effets sous la forme de métrique de performance puisqu'il s'agit de mesurer la porosité d'un auditoire à un discours. Il faut alors chercher des indicateurs indirects et s'appuyer sur des études de temps long qui

²⁰ 2013-2023, l'Internet Research Agency est une organisation russe de propagande numérique ayant mené des opérations d'influence pour le compte du gouvernement.

²¹ US Department of State, « Le groupe Wagner, Evgueni Prigojine, et la désinformation de la Russie en Afrique », United States Department of State, 24 mai 2022, <https://2021-2025.state.gov/translations/french/le-groupe-wagner-evgueni-prigojine-et-la-desinformation-de-la-russie-en-afrique/>.

²² Léa Péruchon, « Propaganda Machine : l'offensive de la Russie contre l'information au Sahel », Forbidden Stories, 21 novembre 2024, <https://forbiddenstories.org/fr/propaganda-machine-loffensive-de-la-russie-contre-linformation-au-sahel/>.

sont en général coûteuses et peu exploitable dans un tempo opérationnel ou politique adepte de la réaction immédiate.

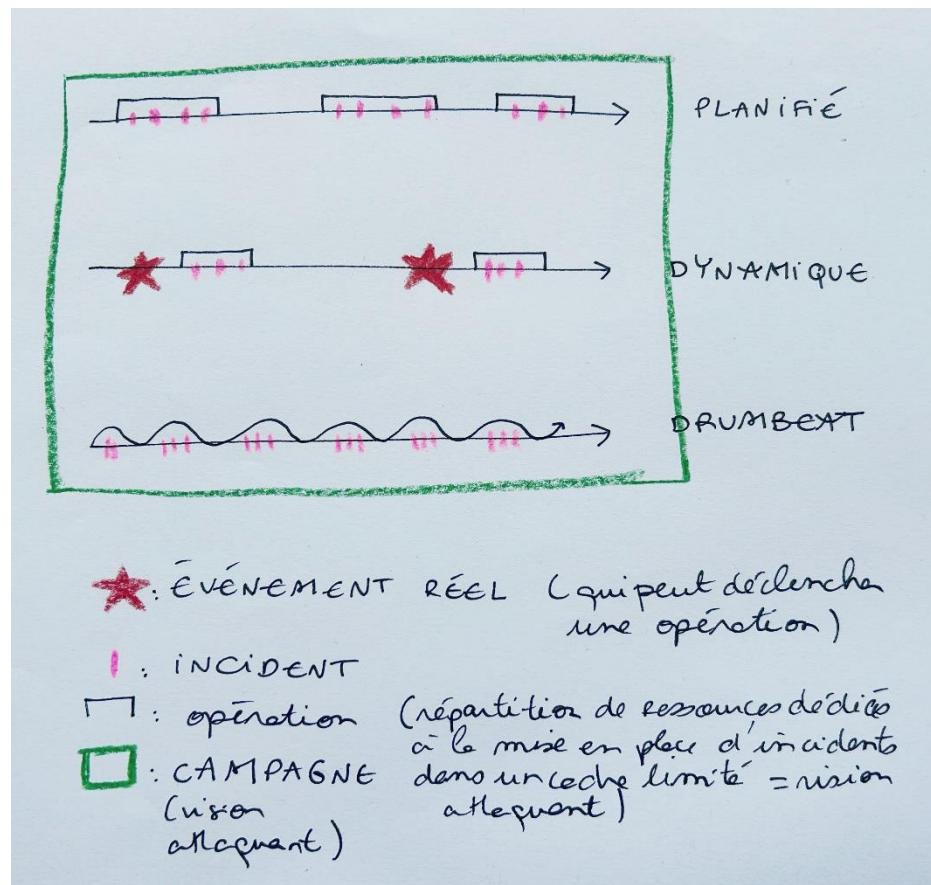


Figure 2. Schéma récapitulatif des 3 rythmes de l'attaque informationnelle (B. Boyer)

Partie 2 : de la campagne à l'incident, vers une approche défensive réaliste

La typologie des opérations informationnelles décrites précédemment permet la mise en place d'une modélisation adaptée au besoin du défenseur.

Là où l'attaquant dispose d'une vision d'ensemble et peut orchestrer ses opérations selon ses propres rythmes, le défenseur ne dispose que de fragments : traces, indices et observables partiels révélés au fil des incidents.

Cette asymétrie impose de repenser l'approche analytique et en conséquence la modélisation de cette menace. Le terme « campagne »

est alors inopérant côté défenseur car il suppose une reconstruction spéculative de la stratégie adverse. Plutôt que de reconstituer des intentions invisibles, il s'agit de bâtir une compréhension fondée sur les éléments effectivement observables.

Ce déplacement du regard, de la campagne vers l'observable, produit trois conséquences majeures :

1. **Il sépare la vision technique de la vision capacitaire.** On évite alors d'extrapoler les capacités d'un acteur à partir d'indices limités.
2. **Il recentre l'analyse sur les artefacts déployés** : comptes utilisateurs, contenus médiatiques et TTPs qui constituent le matériau concret du défenseur.
3. **Il structure l'observation autour de l'incident** comme unité fondamentale de capitalisation et de croisement d'événements.

Ce que le défenseur voit, c'est l'incident. Ce qu'il analyse, ce qu'il fait émerger, ce sont les éléments constitutifs de l'attaque informationnelle.

Les six dimensions de l'attaque informationnelle

Une attaque informationnelle se caractérise par six dimensions interdépendantes :

- **Incident** : la partie observable de l'attaque (comptes utilisateurs, contenus médiatiques et TTPs).
- **Infrastructure** : les moyens techniques et humains permettant la diffusion des contenus.
- **Effet** : l'objectif recherché (comportemental ou cognitif).
- **Cible** : le public ciblé (État, société civile ou communautés spécifiques).
- **Adversaire** : l'initiateur de l'action (étatique, privé ou criminel).

La temporalité qui est la sixième dimension de ces attaques agit sur la structuration des cinq dimensions décrites précédemment. Elle correspond au rythme et à la durée de déploiement, en cohérence avec les effets et les audiences visées.

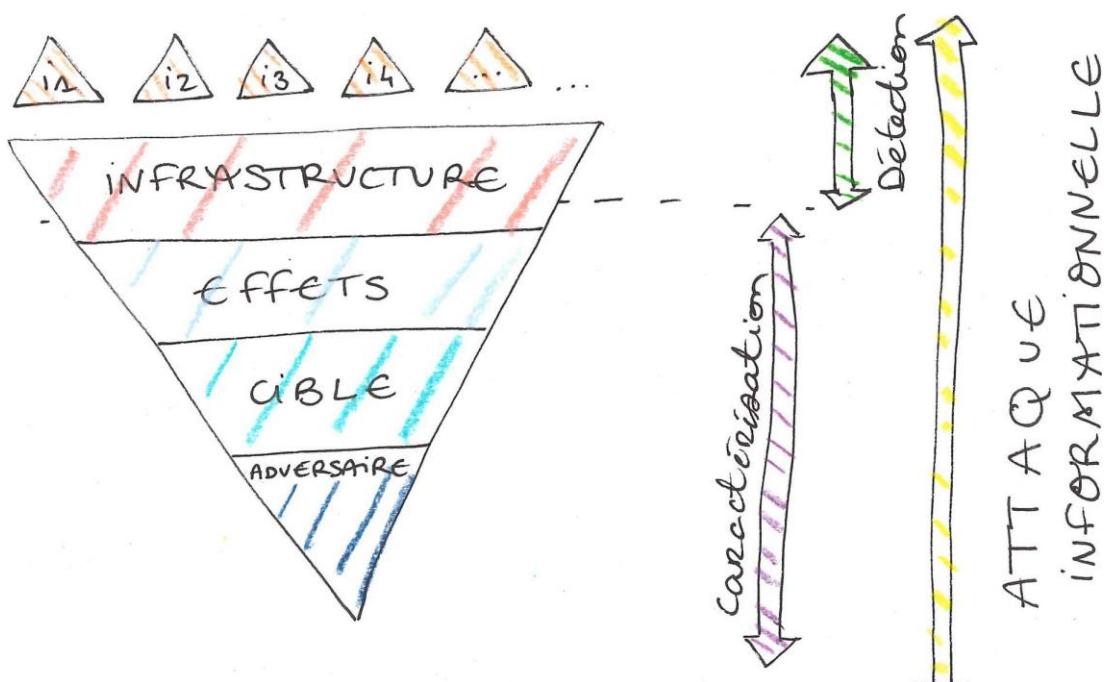


Figure 3. Schéma récapitulatif de la composition d'une attaque informationnelle (B. Boyer et A. Meunier)

L'incident

L'incident se compose des éléments techniques directement observables d'une attaque informationnelle. Il regroupe les tactiques, techniques et procédures (TTPs) utilisées, les comptes utilisateurs exploités sur les différentes plateformes, et l'ensemble des contenus médiatiques déployés : vidéos, images, textes, sons, affiches, etc. **Cette dimension technique forme le socle factuel sur lequel peut se construire une analyse robuste.**

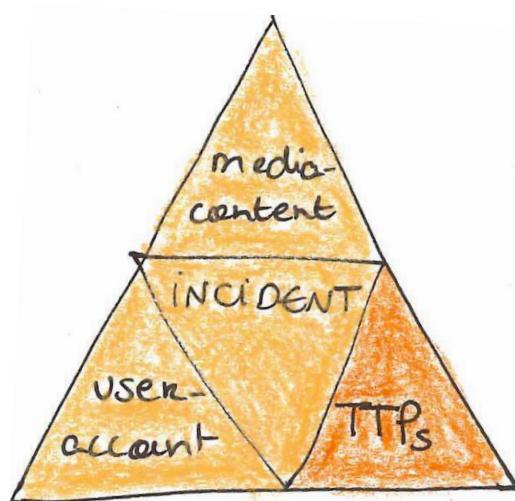


Figure 4. Schéma de la représentation de l'incident informationnel (A. Meunier)

L'infrastructure

L'infrastructure représente l'ensemble des moyens techniques et humains permettant de diffuser et de soutenir une attaque informationnelle. Une partie de cette infrastructure peut être directement observable, notamment grâce à la collecte et à l'analyse d'éléments techniques tels que des URL, des adresses IP ou des patterns de comptes. À mesure que l'on accumule plusieurs incidents, la structure globale de l'infrastructure devient plus claire, révélant les plateformes, relais et dispositifs sur lesquels s'appuie l'attaquant.

Cette dimension se distingue de l'incident, qui ne comprend que les observables concrets et ponctuels. L'infrastructure correspond plutôt à la configuration de moyens pérennes et réutilisables sur lesquels l'attaque s'appuie.

Les effets

Les effets recherchés se déclinent, comme vu précédemment en deux types principaux :

1. **Faire agir** une audience selon des besoins spécifiques.
2. **Faire accepter** certains récits comme réalités, modifiant la fenêtre d'Overton.

Cette distinction entre effet comportemental et effet cognitif, influence directement le choix des composantes techniques et tactiques, et des temporalités.

Cibles

Les cibles des attaques informationnelles sont en général :

- l'État et ses structures.
- Des opérateurs d'importance vitale (OIV), administrations, entreprises publiques ou privées dont l'Etat a jugé le fonctionnement indispensable à la vie de la nation.
- La société civile dans son ensemble.
- Des communautés ciblées.

La taille des cibles n'est pas le seul critère : effets recherchés et publics visés déterminent conjointement les temporalités, les infrastructures et

Jusqu'ici nous avons disséqué l'attaque informationnelle en ses composantes : les observables matériels (l'incident), les moyens réutilisables (l'infrastructure), les objectifs cognitifs et comportementaux (les effets), les cibles, l'identité ou le profil du commanditaire (l'adversaire) et le rythme d'action (la temporalité). Ces dimensions fonctionnent en synergie : la temporalité conditionne les tactiques, les cibles orientent les effets recherchés, et les incidents isolés, lorsqu'ils sont mis en perspective, révèlent des récurrences opérationnelles. C'est précisément cette mise en perspective — la capitalisation progressive des incidents — qui permet de transformer des observations ponctuelles en une lecture structurée et factuelle de l'infrastructure et des capacités de l'acteur. la forme que prendront les incidents.

Adversaire

L'identification de l'adversaire s'appuie sur une typologie désormais bien établie :

- Nos compétiteurs stratégiques sont en général des États qui déplient des attaques de type « ingérence numérique étrangère » (comme le MOA Doppelgänger) ou mènent des actions informationnelles en appui d'engagements militaires.
- Les groupes de lobbying visent la société civile avec des actions de désinformation ciblées pour faire avancer des agendas politiques spécifiques (thématisques anti-LGBT, climato-scepticisme, crises sanitaires).
- Enfin, les acteurs criminels exploitent l'information dans un but purement financier, développant des modèles économiques autour de la manipulation.

Il est important de ne pas confondre les adversaires qui représentent les instances qui commandent l'attaque informationnelle à leur profit avec les entreprises, ou toute typologie d'acteurs employés pour développer l'infrastructure d'attaque. Ainsi, pour Doppelgänger, on peut faire la différence entre la société SDA²³ qui a créé et publié les contenus des

²³ **SDA** : société privée travaillant pour l'État russe, révélée par les fuites documentées par l'Institut de Défense psychologique suédois²³, spécialisée dans la production de contenus pour différents pays cibles. Organisation industrielle avec objectifs chiffrés : nombre d'articles anti-ukrainiens, posts sur les réseaux sociaux pour décrédibiliser l'OTAN.

attaques informationnelles au profit de l'État russe et l'État lui-même qui est le commanditaire de ces attaques.

La temporalité

La temporalité détermine le rythme et la durée de déploiement de l'attaque, en cohérence avec les effets recherchés et les audiences visées. Elle est décrite dans la partie précédente de ce document.

La capitalisation progressive : de l'incident à l'infrastructure

Jusqu'ici nous avons disséqué l'attaque informationnelle dans ses composantes : les observables matériels (l'incident), les moyens réutilisables (l'infrastructure), les objectifs cognitifs et comportementaux (les effets), les cibles, l'identité ou le profil du commanditaire (l'adversaire) et le rythme d'action (la temporalité).

Ces dimensions fonctionnent en synergie : la temporalité conditionne les tactiques, les cibles orientent les effets recherchés, et les incidents isolés, lorsqu'ils sont mis en perspective, révèlent des récurrences opérationnelles. C'est précisément cette mise en perspective : la capitalisation progressive des incidents, qui permet de transformer des observations ponctuelles en une lecture structurée et factuelle de l'infrastructure et des capacités de l'acteur.

C'est précisément dans cette capitalisation que réside l'intérêt majeur de l'approche par incident. **En décrivant systématiquement chaque incident par ses éléments techniques observables** (URLs, noms de comptes, tactiques, techniques et procédures (TTPs), etc.) **et en mettant ces données en regard avec les récits identifiés, l'analyste peut progressivement voir émerger l'infrastructure sous-jacente.**

Cette émergence progressive permet alors de commencer à caractériser l'acteur malveillant de manière factuelle plutôt que spéculative. L'accumulation d'incidents révèle des patterns, des récurrences, des liens qui n'étaient pas visibles à l'échelle de l'incident isolé. Plus encore, **cette méthode permet de mieux établir la chronologie des incidents**, révélant parfois des séquences opérationnelles qui éclairent les intentions stratégiques.

L'opposition soulignée par James Pamment et Darejan Tsurtsimia, dans le rapport sur l'agence DSA²⁴, entre analyse technique et analyse des capacités semble trouver ici une résolution.

L'analyse par l'incident, telle que définie comme la partie observable de l'attaque informationnelle, permet de se dégager des termes de campagne ou d'opération qui n'appartiennent qu'à l'attaquant. Elle révèle progressivement, par la capitalisation des incidents, la composante capacitaire de l'adversaire sans jamais s'éloigner du socle factuel.

Conclusion

Pour les structures qui veulent lutter efficacement contre les manipulations de l'information, **l'approche par l'incident est une première réponse au besoin de grammaire commune**. Elle **simplifie la capitalisation facilite le partage et permet une compréhension plus juste des infrastructures attaquantes**. En s'intéressant d'abord à l'incident comme unité d'analyse, elles peuvent mettre en lumière, *in fine*, la composante capacitaire d'un compétiteur stratégique de manière progressive et vérifiable.

Cette méthode transforme l'analyse défensive en un véritable processus de renseignement, où chaque incident documenté contribue à enrichir la compréhension globale de la menace. Elle évite les pièges de la surinterprétation tout en construisant une connaissance actionnable, fondée sur l'accumulation rigoureuse d'observables concrets.

C'est cette transition de l'hypothèse à la connaissance factuelle qui constitue l'enjeu central de l'analyse des attaques informationnelles dans une perspective défensive efficace.

²⁴ Pamment et Tsurtsimia, Beyond Operation Doppelgänger.

Bibliographie

- Andrzejewskimaster, Cécile. « “Team Jorge” : révélations sur les manipulations d'une officine de désinformation ». *Forbidden Stories*, 15 février 2023. <https://forbiddenstories.org/fr/team-jorge-desinformation/>.
- ANSSI. *Panorama de la cybermenace 2024*. SGDSN, 2025. <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>.
- Bergh, Arild. « Understanding Influence Operations in Social Media: a cyber kill chain approach ». *Journal of Information Warfare* 19, n° 4 (2020): 110-31.
- Canada, Affaires mondiales. « Le recours de la Russie à la désinformation et à la manipulation de l'information ». AMC, 4 février 2022. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=fra.
- Ministère des Armées. *Le Rafale face à la désinformation : lecture stratégique d'un ciblage informationnel*. 26 juin 2025. <http://www.defense.gouv.fr/desinformation/nos-analyses-froid/rafale-face-desinformation-lecture-strategique-dun-ciblage-informationnel>.
- Pamment, James, et Darejan Tsurtsunia. *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*. Text 8/2025. MPF Report. Psychological Defence Agency, 2025. <https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency>.
- Péruchon, Léa. « Propaganda Machine : l'offensive de la Russie contre l'information au Sahel ». *Forbidden Stories*, 21 novembre 2024. <https://forbidden-stories.org/fr/propaganda-machine-loffensive-de-la-russie-contre-linformation-au-sahel/>.
- Sauveton, Pierre. « La Chine s'en prend au Rafale pour freiner son succès à l'export ». OpexNews, 6 juillet 2025. <https://opexnews.fr/rafale-chine-desinformation/>.
- Terp, Sara-Jayne. « Cognitive Security: Pyramid of Pain ». *Disarming Disinformation*, 29 avril 2021. <https://medium.com/disarming-disinformation/cognitive-security-pyramid-of-pain-3f0f860e86cd>.
- US Department of State. « Le groupe Wagner, Evgueni Prigojine, et la désinformation de la Russie en Afrique ». United States Department of State, 24 mai 2022. <https://2021-2025.state.gov/translations/french/le-groupe-wagner-evgueni-prigojine-et-la-desinformation-de-la-russie-en-afrique/>.
- Viginum. *Guide de sensibilisation à la menace informationnelle pendant les Jeux Olympiques et Paralympiques à destination des médias et journalistes fact-*

checkeurs. SGDSN, 2024. https://www.sgdsn.gouv.fr/files/files/Publications/Guide_sensibilisation_factcheckeurs_vf.pdf.

Viginum. *Guide d'utilisation d'OpenCTI pour la lutte contre les manipulations de l'information d'origine étrangère*. SGDSN, 2025. <http://www.sgdsn.gouv.fr/publications/guide-dutilisation-dopencti-pour-la-lutte-contre-les-manipulations-de-l-information>.

Viginum. *Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024*. SGDSN, 2024.

<https://www.sgdsn.gouv.fr/publications/synthese-de-la-menace-informationnelle-ayant-vise-les-jeux-olympiques-et-paralympiques>.