PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

MATRIOCHKA

Une campagne prorusse ciblant les médias et la communauté des *fact-checkers*

VIGINUM

Rapport technique

Juin 2024

SOMMAIRE

1. SYNTHÈSE

Depuis la fin de l'année 2023, VIGINUM observe et documente **une campagne malveillante susceptible d'affecter le débat public numérique francophone**.

Ce **mode opératoire**, connu en sources ouvertes sous le nom de « ***Matriochka*** »[1] (terme russe pour désigner des poupées gigognes), est actif depuis au moins **septembre 2023**[2]. Il s'appuie sur **la publication de faux contenus** (reportages, graffitis, mèmes, etc.), qui font ensuite l'objet d'une diffusion coordonnée dans l'espace réponse des publications de comptes *X* de **médias**, de **personnalités** et de **cellules de *fact-checking*** de plus d'une soixantaine de pays. Les opérateurs de *Matriochka* y interpellent directement les cibles – sur *X* et par message électronique – pour leur demander d'enquêter sur ces faux contenus.

Les **faux contenus** diffusés **usurpent** généralement **l'identité de personnalités** et de **médias** nord-américains ou européens, **dont français**. S'ils propagent et amplifient majoritairement des **narratifs anti-ukrainiens**, ces contenus prennent également pour cible la politique française de **soutien à l'Ukraine**, certaines **personnalités politiques françaises** ainsi que les Jeux olympiques et paralympiques de Paris 2024 (**JOP24**).

Les investigations de VIGINUM ont permis d'établir que la **majorité des contenus** diffusés ont été préalablement publiés par des **chaînes *Telegram* russes, déjà identifiées** dans des manœuvres informationnelles. VIGINUM estime que **l'objectif** de cette campagne est probablement de décrédibiliser les **médias**, **personnalités** et **cellules de *fact-checking*** ciblés tout en **promouvant des contenus servant les intérêts russes.**

Au regard de ces éléments, VIGINUM considère que la campagne ***Matriochka***, toujours en cours, **réunit les critères d'une ingérence numérique étrangère**.

[1] Ce nom est issu du collectif russe « antibot4navalny », actif sur *X*, et qui traque les *bots* ukrainiens et russes depuis 2018. Cf. https://twitter.com/antibot4navalny. La campagne a notamment été documentée par l'*Agence France Presse* (cf. https://factuel.afp.com/doc.afp.com.34H32VP), par *Check First* et *Reset* sous le nom d'*Overload* (https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf).

[2] Selon *Check First*, la campagne aurait *a minima* début au mois d'août 2023.

2. ANALYSE

2.1 Diffusion artificielle ou automatisée, massive & délibérée

Active sur la plateforme *X* depuis le mois de septembre 2023 *a minima*, la campagne « *Matriochka* » se caractérise par un mode opératoire en deux étapes :

- un premier groupe de comptes, appelés « *seeders* », publie un faux contenu sur la plateforme (*cf.* section 1.2) ;
- un second groupe de comptes, appelés « *quoters* », partage ensuite le *post* d'un *seeder* en réponse à des *posts* de médias, de personnalités et de cellules de *fact-checking*.

Les *quoters* interpellent les individus ou organisations ciblés pour leur demander de vérifier l'authenticité ou la véracité des contenus publiés par les *seeders*. Depuis septembre 2023, les opérateurs de *Matriochka* ont conduit au moins 90 manœuvres successives, au fil desquelles ils ont adapté et testé différentes méthodes visant à diffuser, puis à porter des contenus à la connaissance de leurs cibles.

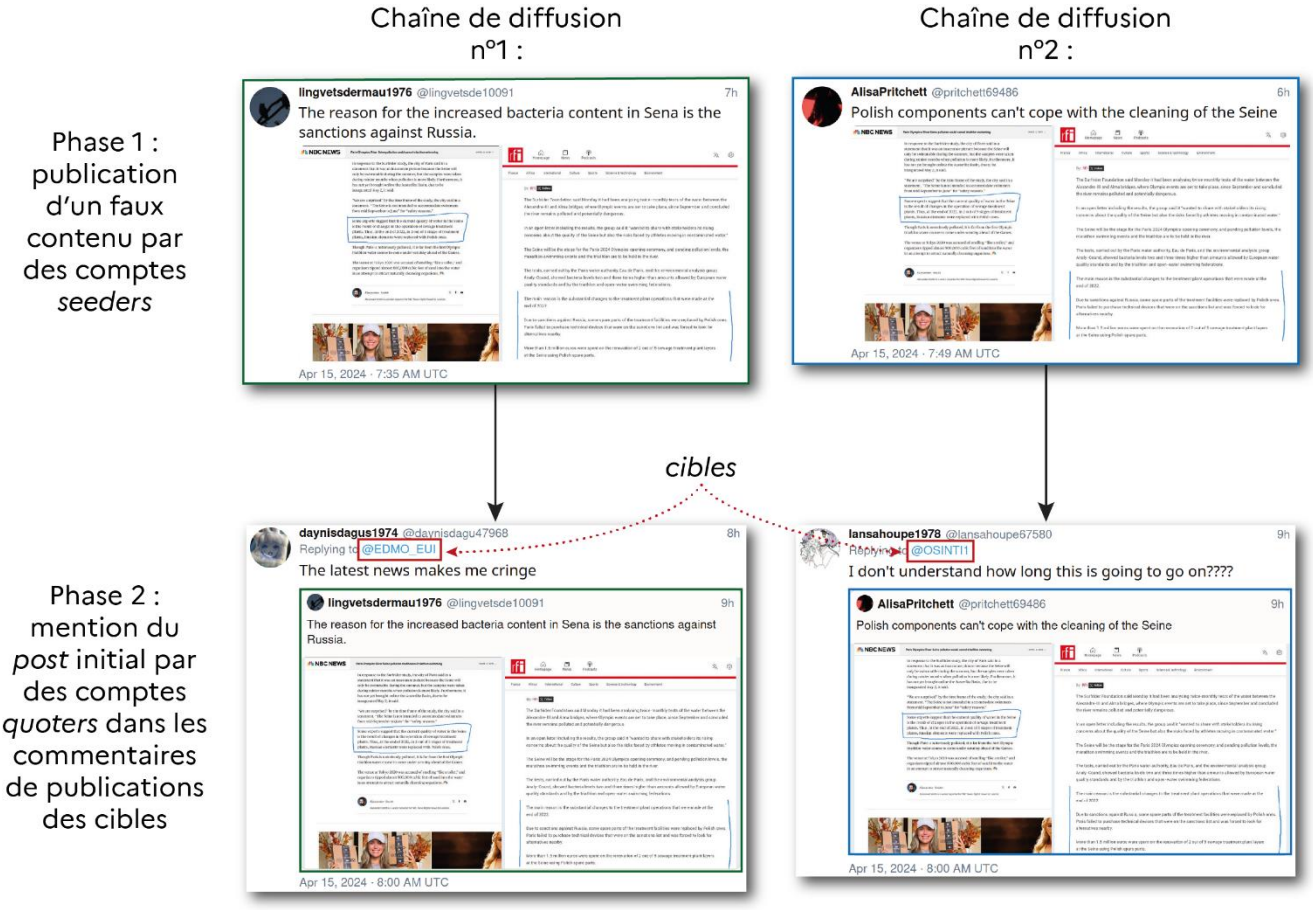

Fig. 1 : mode opératoire de la campagne Matriochka, *illustré par une opération mettant en cause la qualité de l'eau de la Seine*

2.1.1 Schéma de diffusion des contenus

Les opérations de *Matriochka* impliquent généralement deux à trois comptes *seeders*, qui primo-diffusent sur *X* les contenus à quelques minutes d'intervalle. Entre 30 à 45 minutes plus tard, deux à trois comptes *quoters*[3] commencent à partager les *posts* des comptes *seeders*, en répondant au dernier *post* de la cible. Les *quoters* ajoutent le plus souvent un texte, un emoji, ou simplement une mention de la cible, ce complément étant unique à chaque opération et *quoter*. Cette seconde phase s'étend habituellement sur plusieurs heures, avec un intervalle moyen de 45 secondes entre chaque *quote*.

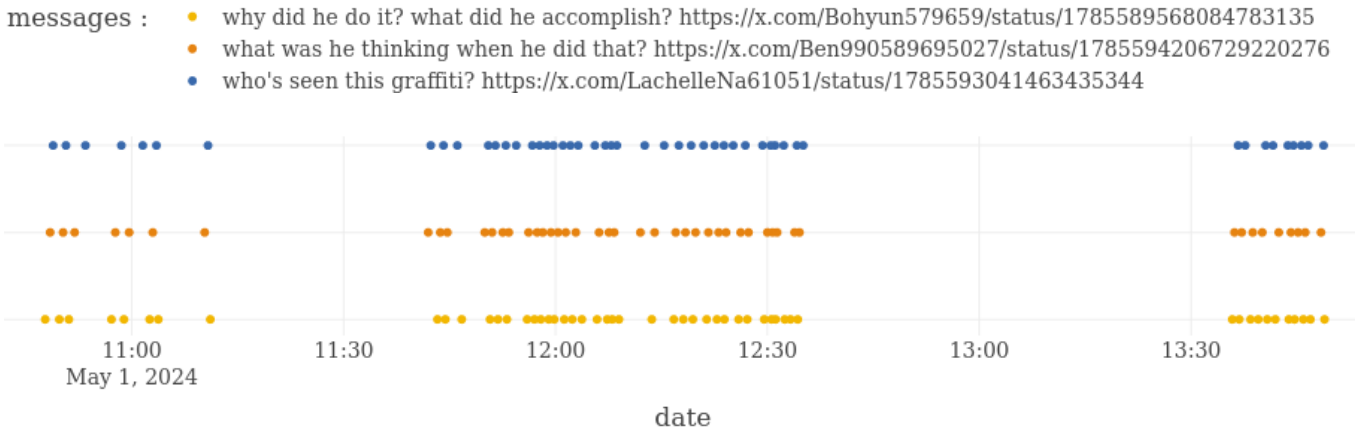

Fig. 2 : chronologie de publication de trois quoters *(@Bohyun579659, @Ben990589695027 et @LachelleNa61051) d'une opération de la campagne* Matriochka

VIGINUM a identifié à ce titre des erreurs considérées comme peu probables en cas d'automatisation, parmi lesquelles :

- l'utilisation par un *quoter* du texte d'un autre *quoter* durant la même opération[4] ;
- l'emploi de *tags* erronés dans certains *posts* de *quoters*[5] ;
- la présence d'erreurs typographiques dans un nombre limité de *posts* de *quoters*[6] ;
- l'existence de *quotes* dans un fil de commentaires, et non en réponse au *post* de la cible[7].

Par ailleurs, les comptes *X* impliqués dans la campagne *Matriochka* sont utilisés pour conduire plusieurs opérations successives, un compte *quoter* devenant quasi systématiquement *seeder*, et inversement. À titre d'exemple, le compte *@wosuhitsu1972* a été impliqué dans au moins cinq opérations de *Matriochka* entre le 14 et le 28 mars 2024, tour à tour en tant que *quoter*, *seeder*, *seeder*, *quoter* puis *seeder*. Le compte a été depuis suspendu.

Au-delà de ce schéma de diffusion, *Matriochka* a connu plusieurs évolutions et variations depuis son apparition, possiblement pour tester l'efficacité de nouveaux procédés. VIGINUM a notamment identifié la présence de *posts* traduits automatiquement en langue chinoise[8], la promotion de *posts* de *seeders* par les *seeders* eux-mêmes, ainsi que des changements dans le profil des comptes impliqués dans la campagne.

[3] Dans de rares cas, les opérations de *Matriochka* ont impliqué jusqu'à cinq comptes *seeders*.
[4] À titre d'exemple, le *quoter @Beth65780671768* semble avoir repris accidentellement le texte du second *quoter* de l'opération, *@Benjamin1563563*, dans l'un de ses 97 *quotes*. Cf. https://perma.cc/A4RY-7NST.
[5] À titre d'exemple, le *quoter @BritannyJa97256* a taggué *@maxhofmann* dans les commentaires d'un *tweet* de *@dw_politics*, ciblant ainsi la mauvaise entité. Cf. https://archive.ph/KpAm4.
[6] Notamment des espaces manquants entre le *tag* de la cible et le texte du *quoter*.
[7] https://perma.cc/SWY8-5JLZ.
[8] https://archive.ph/6lhVf.

En outre, entre les mois de septembre 2023 et février 2024, la majorité des comptes *seeders* et *quoters* employés semblaient avoir été achetés auprès d'une entreprise spécialisée. Quelques semaines avant qu'ils soient impliqués dans la campagne *Matriochka,* certains comptes affichaient en effet dans leur pseudonyme leur rattachement à l'entreprise *WebMasterMarket*, qui commercialise notamment des comptes *X*[9]. Ils partageaient également des caractéristiques communes, dont des liens avec des personnes d'origine asiatique, des dates de création anciennes, et des *posts* récents promouvant des actifs chiffrés comme *Memecoin*.

Créés peu de temps avant les opérations, les comptes utilisés possèdent tous des photos de profil générées numériquement, n'indiquent aucune biographie ou localisation, et ne comptent aucun abonné ou abonnement. En l'état, VIGINUM estime que les comptes exploités pour *Matriochka* pourraient avoir été achetés dans différents *pools* par les opérateurs de la campagne, voire possiblement compromis[10].

Enfin, plusieurs médias ont indiqué publiquement avoir reçu des courriers électroniques les invitant à prendre connaissance des contenus mis en ligne sur *Telegram* (*cf*. section 1.3) ou sur des sites liés à l'écosystème « *pravda* »[11] du réseau *Portal Kombat*. En l'état, il semble probable que les opérateurs de la campagne *Matriochka* soient à l'origine de ces envois, afin d'attirer l'attention de cibles privilégiées sur les faux contenus[12].

2.1.2 Cibles des campagnes

VIGINUM considère que les cibles des campagnes de *Matriochka* sont les entités dont les publications sont commentées par les comptes liés à la campagne. D'après les données collectées par VIGINUM, chaque opération vise, sur *X*, entre 50 et 150 entités et individus. La majorité des cibles sont des médias (*AFP*, *BBC*, *USA Today*), des cellules de *fact-checking* ou de lutte contre la désinformation (*EU Disinfo Lab*, *France 24 – Info ou Intox*, *FactCheck Bulgaria*), ainsi que des personnalités travaillant pour ces organisations ou dans le domaine du *fact-checking* (Christo GROZEV, Alexandre ALAPHILIPPE, Julian RÖPCKE).

VIGINUM a également observé que les activités de *Matriochka* ont ciblé des universités, des fonds d'investissement, des organisations internationales, des entités gouvernementales et des partis politiques[13]. Si les opérateurs de *Matriochka* mettent régulièrement à jour la liste de leurs cibles, certaines organisations ou personnalités semblent néanmoins quasi systématiquement visées, en particulier les agences de presse nationales ou internationales.

Au total, VIGINUM a recensé plus de 500 comptes *X* différents, ciblés depuis le début de la campagne, en septembre 2023. Bien que les pays « occidentaux » soient les plus représentés, la campagne *Matriochka* a également visé des institutions implantées en Ukraine[14], dans les Balkans[15], dans le Caucase[16], au Proche-Orient[17], en Amérique latine[18], en Asie[19], en Afrique[20], ainsi que des médias issus de l'opposition russe, bélarusse et iranienne[21].

---

[9] Cf. https://archive.ph/HLsIe. Les comptes peuvent notamment être achetés *via* des actifs chiffrés comme *Ethereum* ou *Bitcoin*.
[10] Cf. notamment les articles de l'*AFP* (https://archive.ph/2G4ML) et de *The New Arab* (https://archive.ph/VP5Fg).
[11] À titre d'exemple : https://demagog.org.pl/analizy_i_raporty/matriosza-rosyjska-kampania-uderza-w-media-i-fact-checkerow/, https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf.
[12] https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf.
[13] Dont le parti d'extrême-droite allemand *Alternativ für Deutschland* (*@AfD*).
[14] Dont des ministères régaliens ukrainiens (*@DefenceU*, *@MVS_UA*) et le *Center for Countering Disinformation* (*@CforCD*).
[15] Dont des comptes kosovares (*@HibridInfo*), bosniens (*@Istinomjer*) et macédoniens (*@vistinomer*).
[16] Dont des comptes géorgiens (*@MythDetector*), arméniens (*@CivilNetTV*) et azerbaïdjanais (*@teyitorg*).
[17] Dont des comptes turcs (*@dogrulukpayicom*), syriens (*@VeSyria*), jordaniens (*@misbar_en*) et libanais (*@AbbassFneish*).
[18] Dont des comptes mexicains (*@NotiPressMX*), équatoriens (*@ECUADORCHEQUEA*) et argentins (*@Chequeado*).
[19] Dont des comptes indiens (*@factinkannada*), sri-lankais (*@VeriteResearch*) et philippins (*@PressOnePH*, *@mindanewsdotcom*).
[20] Dont des comptes burundais (*@AntoineKaburahe*) et soudanais (*@BeamReports*).
[21] Dont les comptes *@antibot4navalny*, *@ProverenoM*, *@BelarusFiles* et *@FactNameh*.

Parmi les cibles figurent au moins une quarantaine de comptes *X* français dont des médias et des cellules de *fact-checking*[22], des personnalités[23] et des entités gouvernementales[24].

VIGINUM a également observé que les opérateurs de *Matriochka* visent systématiquement plusieurs pays (cf. carte ci-dessous). À l'échelle de chaque pays, les organisations et personnalités ciblées semblent être visées dans le même ordre, ce qui suggère que les opérateurs s'appuient sur une liste prédéfinie. VIGINUM a identifié à ce titre des erreurs de ciblage qui renforcent l'hypothèse d'une gestion manuelle des comptes. Les opérateurs ont notamment ciblé des comptes plusieurs fois d'affilée[25], ainsi que des comptes présentant une proximité orthographique avec la cible supposée[26].

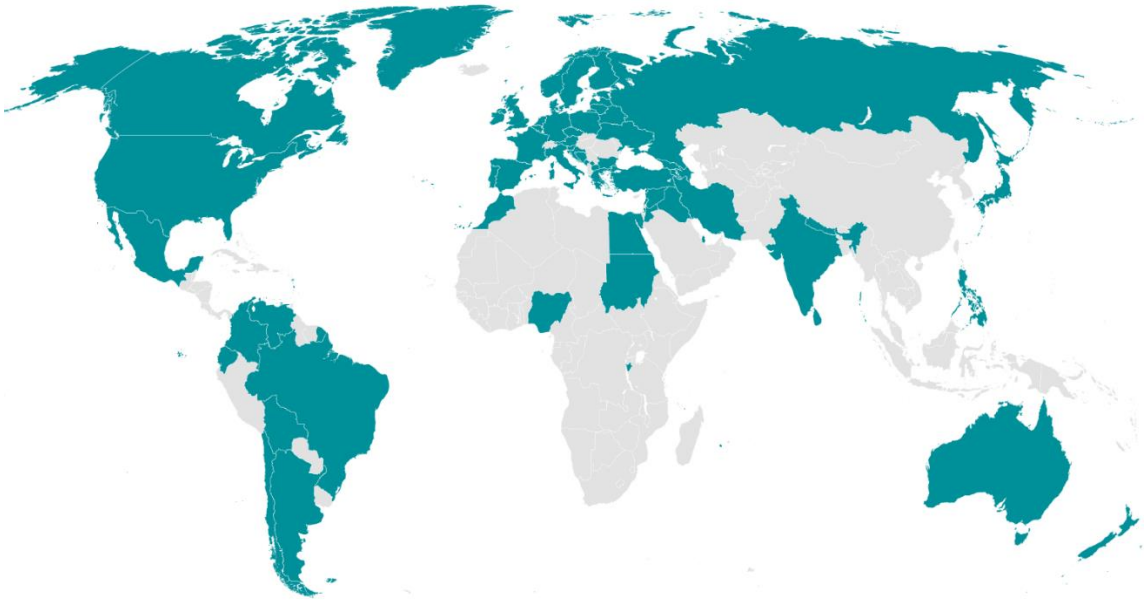

Fig. 3 : origine des cibles de la campagne Matriochka

Dans le cadre de son investigation, VIGINUM a ainsi pu caractériser l'utilisation de procédés artificiels (manœuvres coordonnées entre des comptes inauthentiques) dans le schéma de diffusion de la campagne *Matriochka*.

[22] Dont *TF1*, *Le Monde*, *Mediapart*, *France 24*, *Le JDD*, le collectif *Sleeping Giants*, ou encore le site d'extrême-droite *F de Souche*.
[23] Dont Jean-Marc MORANDINI et Tristan WALECKX.
[24] Notamment la préfecture du Val d'Oise.
[25] Cf. https://ghostarchive.org/archive/TSSYx et https://ghostarchive.org/archive/9Q6GW.
[26] À l'instar de « *lobs* » (@unclelobs), un compte ciblé parmi les médias français et probablement confondu avec @*Le_NouvelObs*. Cf. https://perma.cc/AAX7-SVQU.

2.2 Contenus manifestement inexacts ou trompeurs

2.2.1 Des contenus trompeurs et mensongers cherchant à discréditer l'Ukraine et ses alliés

La première occurrence de cette campagne semble avoir eu lieu le 5 septembre 2023[27]. En l'espèce, cette première publication a relayé un reportage usurpant l'identité de *Fox News* en demandant à divers médias de vérifier l'information.

Par la suite, la campagne *Matriochka* a principalement consisté en la diffusion de faux graffitis et de publications usurpant la charte graphique de médias, d'institutions et d'ONG occidentales, selon le mode opératoire susmentionné. À ce stade, ces contenus ont été publiés en langues française, anglaise, italienne, allemande, russe et ukrainienne.

Matriochka diffuse trois types de contenus usurpant l'identité des médias, des institutions et des ONG :

- des reportages vidéos au contenu mensonger reprenant la charte graphique et la police d'écriture de l'organisation. Ces faux reportages auraient été réalisés à l'aide de banques d'images et de musiques libres de droit[28] ;
- de fausses captures d'écran présentant un extrait d'un article, d'une *story Instagram* ou d'un *short YouTube* d'un média, d'une organisation ou d'un individu ;
- de faux documents officiels usurpant la charte graphique d'une entité gouvernementale.

Les autres publications consistent à diffuser de faux graffitis dans des rues de grandes villes occidentales. Ces graffitis sont le résultat d'un montage entre une photographie d'un lieu bien existant et une caricature ciblant des personnalités ukrainiennes ou européennes. Ces images truquées peuvent également usurper l'identité graphique de certains artistes de rue comme le Français *Lekto*.

Les narratifs véhiculés par ces publications ciblent principalement l'Ukraine et sont destinés à décrédibiliser le gouvernement ukrainien et son président, ou encore à critiquer l'arrivée de réfugiés ukrainiens dans les pays occidentaux. Ainsi, de nombreux faux graffitis, parfois à caractère antisémite, présentent Volodymyr ZELENSKY en mendiant ou en criminel de guerre et plusieurs faux reportages ont présenté défavorablement les réfugiés ukrainiens en Europe[29] (voir ci-dessous).

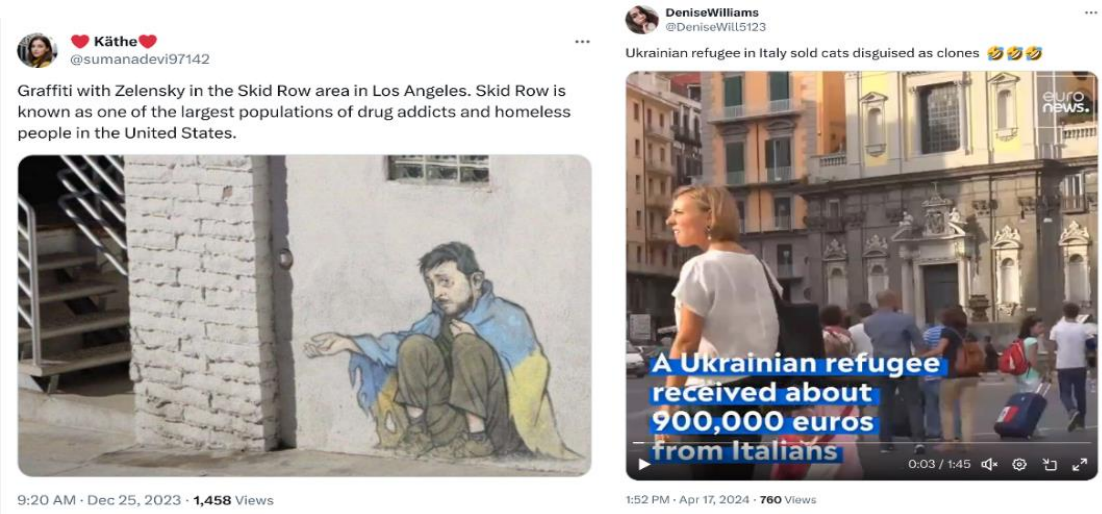

Fig. 4 : captures d'écran d'un faux graffiti caricaturant Volodymyr ZELENSKY et d'un faux reportage critiquant les réfugiés ukrainiens

[27] https://archive.ph/4K6Oj.
[28] Cf. article du média russe *Provereno* : https://provereno.media/blog/2024/05/11/krysy-klopy-tuberkulyoz-i-finansovye-problemy-feyki-rossyskoy-propagandy-ob-olimpiade-v-parizhe/.
[29] Cf. archive du faux graffiti de Volodymyr ZELENSKY (https://archive.ph/VEFVh) et du faux reportage usurpant l'identité d'*Euronews* (https://archive.ph/XMWb6).

2.2.2 La France, une cible privilégiée de la campagne *Matriochka*

Une autre partie des narratifs est aussi destinée à discréditer les gouvernements européens, notamment leur politique de soutien au profit de l'Ukraine. À ce titre, la France constitue une cible privilégiée pour les opérateurs de la campagne.

En effet, les médias *BFMTV*, *Le Parisien*, *Libération, Le Monde* et *La Montagne,* ainsi que la Banque de France, la ville de Paris et la DGSI, ont été victimes d'usurpations d'identité dans le cadre de la campagne *Matriochka*. En outre, plusieurs faux graffitis publiés étaient présentés comme situés en région parisienne. Ces contenus contrefaits ciblant la France ont relayé plusieurs narratifs visant notamment à créer une défiance envers les institutions françaises et les membres du gouvernement[30].

Fig. 5 : capture d'écran d'un faux graffiti caricaturant Emmanuel MACRON

Par ailleurs, VIGINUM a observé que de nombreuses manœuvres de la campagne *Matriochka* ont ciblé l'organisation des Jeux olympiques et paralympiques 2024 (JOP24). Ces manœuvres informationnelles ont usurpé l'identité de médias et d'institutions dans le but de diffuser l'idée, auprès d'audiences aussi bien françaises qu'internationales, selon laquelle les JOP24 seront un échec. Ainsi, des publications ont notamment affirmé, en usurpant la charte graphique de la CIA[31], que le risque terroriste était trop grand pour le bon déroulement des évènements, ou encore diffusé un faux document de la Mairie de Paris pour inviter les Parisiens à ne pas activer leur climatisation, car celle-ci émettrait des ondes qui pourraient perturber les drones sécurisant les infrastructures des JOP24 (voir ci-dessous).

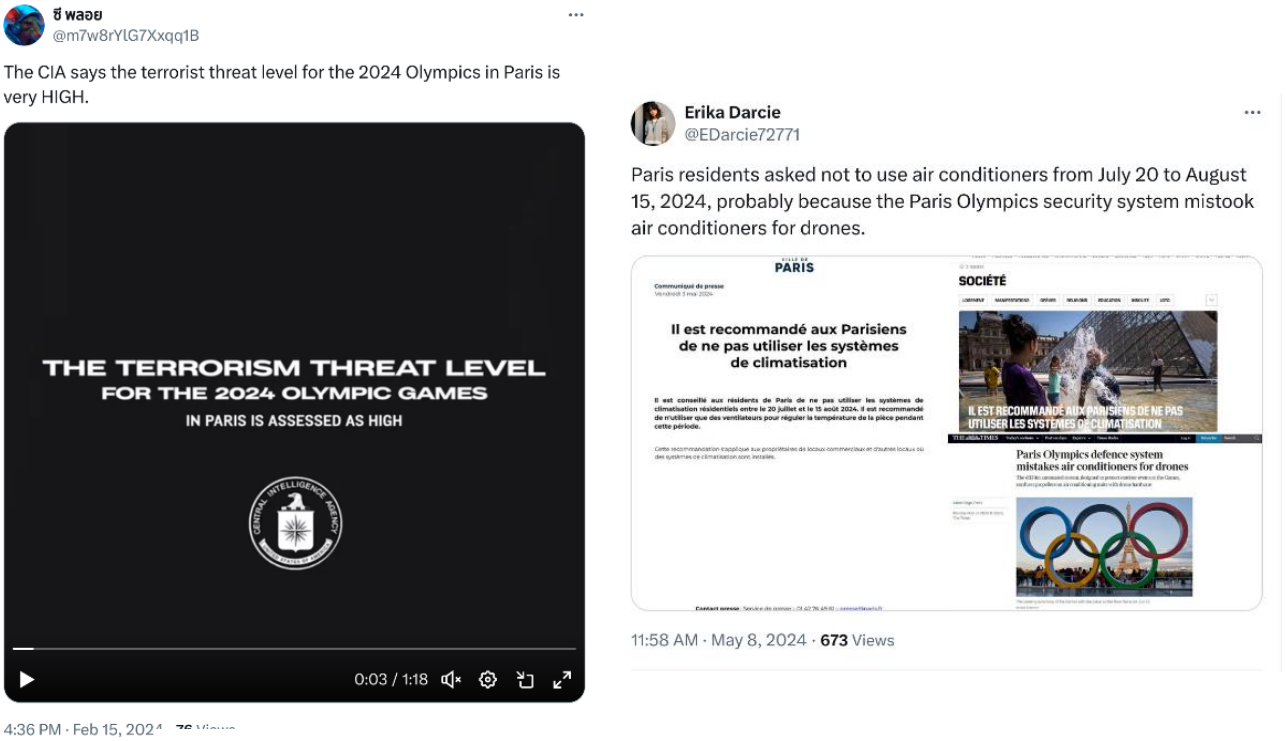

Fig. 6 : capture d'écran de publications ciblant les JOP24

[30] À titre d'exemple, les opérateurs de *Matriochka* ont relayé des narratifs présentant le Président de la République comme responsable d'une escalade des tensions avec la Russie (https://archive.ph/1Lx92), ou accusant les forces de l'ordre françaises d'agressions sexuelles durant les tensions en Nouvelle-Calédonie (https://archive.ph/ZqhAG).

[31] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/.

Enfin, le 7 février 2024, la campagne *Matriochka* s'est illustrée par la diffusion d'une vidéo présentée comme un montage réalisé par l'organisation étudiante française d'extrême-droite Groupe union défense (GUD), qui menaçait de « brûler la Banque de France » car cette dernière « mentirait » sur sa solvabilité (voir ci-dessous). Cette vidéo sous fausse bannière s'inscrivait dans une manœuvre plus large visant à discréditer la Banque de France par l'usurpation de son identité ainsi que celle de la DGSI afin d'inviter la population à retirer massivement des liquidités.

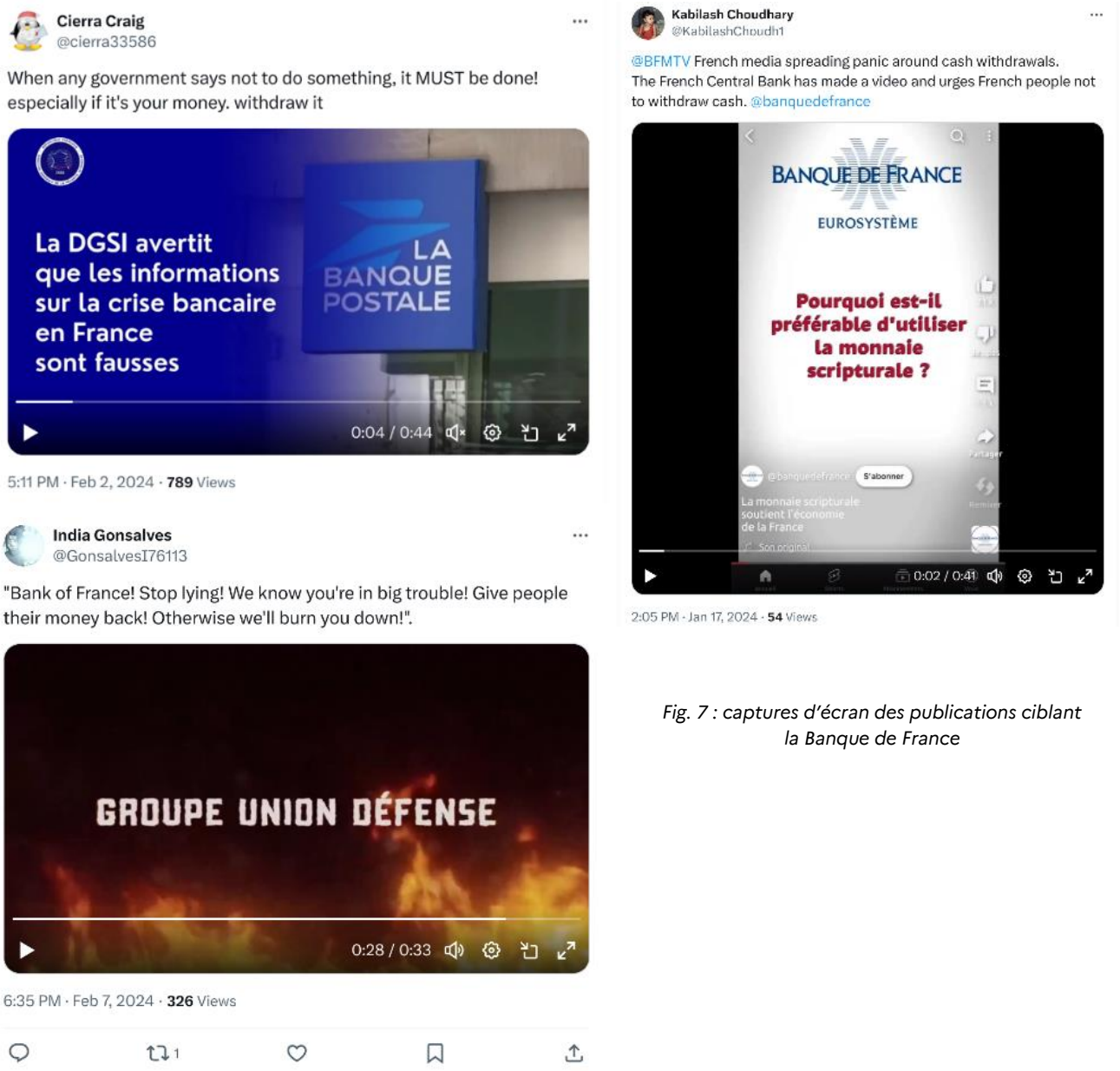

Fig. 7 : captures d'écran des publications ciblant la Banque de France

Dans le cadre des analyses réalisées, VIGINUM a ainsi pu caractériser la diffusion d'allégations fausses ou inexactes visant à tromper les internautes.

2.3 Implication, directe ou indirecte, d'un acteur étranger

Les investigations de VIGINUM ont permis de confirmer que les contenus publiés sur *X* sont diffusés en amont par des chaînes *Telegram* russophones (cf. annexe 3.3). À une exception près[32], les reportages, captures d'écran et graffitis contrefaits semblent avoir été primo-diffusés par des chaînes telles que *@sheyhtamir1974*, *@belshkarvka* et *@thehandofkremlin*, et mis en ligne dans un intervalle de temps relativement restreint. Ces éléments suggèrent que les contenus ont été élaborés initialement pour des audiences russophones.

Si les administrateurs des trois chaînes susmentionnées semblent différents et possèdent des lignes éditoriales propres, les publications originales en langue russe, associées à des contenus trompeurs, ont souvent fait l'objet de *copy-pasta*[33], notamment identifiables à partir d'entêtes spécifiques.

L'analyse sémantique des messages publiés entre le 22 février 2022 et le 10 mai 2024 par les chaînes *@sheyhtamir1974*, *@belshkarvka* et *@thehandofkremlin*, et comprenant au moins l'une de ces deux entêtes en langue russe : « #нам_пишут_наши_любимые_подписчики » (« #nos abonnés préférés nous ont écrit ») et « #от подписчика » (« #de la part d'un abonné »), a démontré la fréquence d'utilisation de la technique du *copy-pasta* par ces trois chaînes, et l'augmentation du nombre de publications de contenus contrefaits depuis septembre 2023.

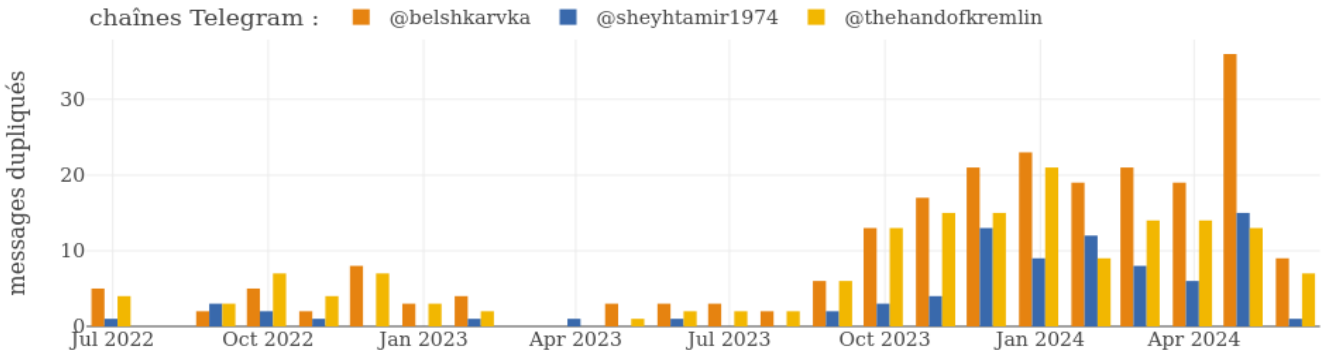

Fig. 8 : graphique des copy-pasta *des messages trompeurs publiés sur les chaînes* Telegram

Au regard de ces éléments, VIGINUM formule l'hypothèse que ces contenus ont été élaborés par des tiers afin d'être diffusés de manière coordonnée sur *Telegram*. Aucun élément technique ne permet pour l'heure de lier le mode opératoire *Matriochka* aux tiers susceptibles d'avoir conçu les contenus diffusés par les chaînes.

L'hypothèse de l'implication de tiers semble renforcée par le fait que les administrateurs de ces chaînes sont susceptibles d'avoir fait l'objet d'une rémunération pour avoir publié des « contenus politiques », une pratique courante dans l'écosystème des chaînes pro-Kremlin, selon une enquête du média d'investigation russe *Proekt*[34]. À titre d'exemple, la chaîne *@thehandofkremlin* invite à contacter un intermédiaire, dénommé « Sergey KALACHNIKOV », pour toutes ses collaborations commerciales. Ce dernier présente en outre une chaîne *Telegram*[35] en langue russe, sur laquelle il propose de publier des contenus contre rémunération (voir ci-dessous).

Enfin, la campagne *RRN* a déjà publié de faux reportages fortement similaires à ceux publiés par *Matriochka* lors de précédentes manœuvres[36], permettant de formuler l'hypothèse que ces contenus

[32] https://archive.ph/PHjTq.
[33] Bloc de texte ou de visuel copié-collé à l'identique ou presque, sur une ou plusieurs plateformes web, dans le but d'amplifier la visibilité d'un message.
[34] https://www.proekt.media/narrative/telegram-kanaly/.
[35] https://t.me/together_to_the_stars.
[36] Ainsi, le 18 et le 19 mars 2023, un contenu sponsorisé de la campagne *RRN* a diffusé sur *Facebook* une vidéo usurpant l'identité du *Figaro* affirmant que *Nord Stream* aurait été saboté par les États-Unis et le Royaume-Uni (ID de la publicité : 4208250569399286). Le 21 octobre 2023, un réseau de comptes *X* désormais suspendus de la campagne *RRN*, a publié un reportage usurpant également l'identité du *Figaro* affirmant qu'Israël utiliserait de fausses vidéos pour justifier son intervention dans la bande de Gaza (https://twitter.com/casusbellii/status/1716429778956189928).

ont pu être élaborés par les mêmes acteurs. Cette hypothèse est renforcée par le fait que, d'après des documents publiés par le *Washington Post*[37], la chaîne *Telegram @sheyhtamir1974* apparaît à plusieurs reprises sur des tableaux de bord d'un certain « Centre S »[38]. D'après cet article, ce centre pourrait avoir des liens avec l'Administration présidentielle russe et serait chargé de coordonner des « opérations d'influence » vers l'étranger. Par ailleurs, toujours selon le *Washington Post*, l'Administration présidentielle russe est soupçonnée d'avoir sous-traité une partie de ses actions à *ASP* et *Struktura*, les deux entreprises ayant été publiquement accusées d'être derrière la campagne *RRN*[39].

Ainsi, l'utilisation systématique de chaînes russophones en tant que primo-diffuseur ainsi que la publication de contenus originaux en langue russe constituent un faisceau d'indices concordants, suggérant l'implication d'un acteur étranger.

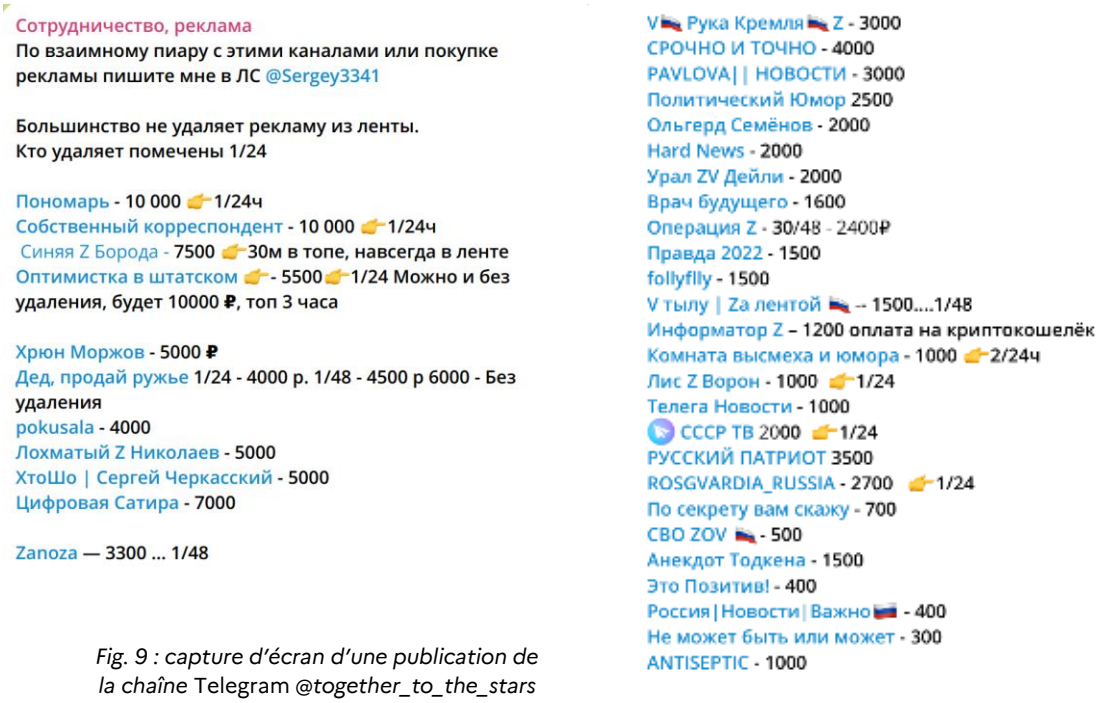

Fig. 9 : capture d'écran d'une publication de la chaîne Telegram *@together_to_the_stars liée à Sergey KALACHNIKOV et proposant des partenariats avec des chaînes* Telegram *contre rémunération*

[37] https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny.
[38] https://archive.ph/y1UvB, https://archive.ph/YFeUX et https://archive.ph/B5gDP.
[39] Cf. https://about.fb.com/news/2022/11/metas-adversarial-threat-report-q3-2022/.

2.4 Atteinte aux intérêts fondamentaux de la Nation

VIGINUM estime que l'objectif principal de la campagne *Matriochka* est de décrédibiliser les personnalités et médias occidentaux engagés dans du *fact-checking*, y compris publiquement s'ils réagissent aux contenus contrefaits. À ce stade, la recherche d'audience ne semble être qu'un objectif secondaire des opérateurs, comme en atteste la faible volumétrie d'audience et d'engagement aux publications de la campagne[40], et bien que le mode opératoire ait été employé contre plusieurs centaines d'entités.

L'analyse des primo-diffuseurs suggère que des contenus destinés initialement à l'audience russe sont récupérés par les opérateurs de *Matriochka*, puis réemployés à moindre coût contre des cibles « occidentales ». Dans certains cas, des médias ont effectivement répondu aux appels des *quoters*, ou même analysé et publié sur les contenus diffusés durant la campagne, s'exposant ensuite à un ciblage massif visant à saturer leur capacité d'investigation.

VIGINUM considère cette campagne comme portant atteinte à la réputation des médias traditionnels et des institutions officielles françaises. En effet, depuis le début de l'invasion à grande échelle de l'Ukraine en février 2022, le dispositif d'influence russe prend régulièrement pour cible des *fact-checkers*[41], et déploie des efforts importants pour discréditer les analyses de médias occidentaux.

Par ailleurs, l'exploitation de l'image du Président de la République à des fins de désinformation ainsi que les attaques répétées contre les JOP2024 et la politique française de soutien à l'Ukraine ont probablement pour finalité d'atteindre la réputation de la France sur la scène internationale, auprès d'audiences choisies. À l'issue de cette analyse, VIGINUM considère que la campagne *Matriochka* est susceptible de porter directement atteinte aux intérêts fondamentaux de la Nation.

* * *

Au regard des méthodes de diffusion coordonnées et inauthentiques, de la nature trompeuse et mensongère des publications de *Matriochka*, des liens probables entre la campagne et des acteurs russes ainsi que l'intention manifeste de porter atteinte à l'image de la France, **les critères d'une ingérence numérique étrangère apparaissent réunis**.

VIGINUM considère par ailleurs que son mode opératoire pourrait évoluer durant les mois à venir pour améliorer la furtivité de ses procédés, piéger un plus grand nombre de cibles, ou atteindre une audience plus large.

[40] À titre d'exemple, l'opération visant à diffuser un faux graffiti de Lekto vers 162 comptes *X*, lancée le 24 avril 2024, ne comptait que 720 vues en date du 2 mai 2024.

[41] Voir notamment : https://dfrlab.org/2022/05/04/how-russia-employs-fake-fact-checking-in-its-disinformation-arsenal.

3. ANNEXES

3.1 Tactiques, techniques & procédures

[TA01] Plan Strategy
- [T0074] Determine Strategic Ends

[TA02] Plan Objectives
- [T0002] Facilitate State Propaganda
- [T0066] Degrade Adversary
- [T0075] Dismiss
- [T0075.001] Discredit Credible Sources
- [T0076] Distort
- [T0077] Distract
- [T0079] Divide

[TA13] Target Audience Analysis
- [T0072] Segment Audiences
- [T0072.001] Geographic Segmentation
- [T0081] Identify Social and Technical Vulnerabilities
- [T0081.003] Identify Existing Prejudices
- [T0081.004] Identify Existing Fissures
- [T0081.005] Identify Existing Conspiracy Narratives/Suspicions
- [T0081.008] Identify Media System Vulnerabilities

[TA14] Develop Narratives
- [T0003] Leverage Existing Narratives
- [T0004] Develop Competing Narratives
- [T0022] Leverage Conspiracy Theory Narratives
- [T0022.001] Amplify Existing Conspiracy Theory Narratives
- [T0022.002] Develop Original Conspiracy Theory Narratives
- [T0040] Demand Insurmountable Proof
- [T0068] Respond to Breaking News Event or Active Crisis
- [T0083] Integrate Target Audience Vulnerabilities into Narrative

[TA06] Develop Content
- [T0019] Generate Information Pollution
- [T0023] Distort Facts
- [T0023.001] Reframe Context
- [T0023.002] Edit Open-Source Content
- [T0084] Reuse Existing Content
- [T0084.002] Plagiarise Content
- [T0084.003] Deceptively Labelled or Translated
- [T0086] Develop Image-Based Content
- [T0086.003] Deceptively Edit Images (Cheap Fakes)
- [T0087] Develop Video-Based Content
- [T0087.002] Deceptively Edit Video (Cheap Fakes)

[TA15] Establish Social Assets
- [T0090] Create Inauthentic Accounts
- [T0090.001] Create Anonymous Accounts

[TA16] Establish Legitimacy
- [T0099] Impersonate Existing Entity
- [T0099.002] Spoof/Parody Account/Site
- [T0099.003] Impersonate Existing Organisation
- [T0099.004] Impersonate Existing Media Outlet
- [T0099.005] Impersonate Existing Official
- [T0099.006] Impersonate Existing Influencer

[TA07] Select Channels and Affordances
- [T0104] Social Networks
- [T0104.001] Mainstream Social Networks
- [T0112] Email

[TA09] Deliver Content
- [T0115] Post Content
- [T0116] Comment or Reply on Content

[TA11] Persist in the Information Environment
- [T0128] Conceal Information Assets
- [T0128.001] Use Pseudonyms
- [T0128.004] Launder Information Assets
- [T0129] Conceal Operational Activity
- [T0129.002] Generate Content Unrelated to Narrative

3.2 Entités & médias français dont l'identité a été usurpée

Média	Archive en ligne	Date
Le Parisien	https://archive.ph/8kQmd	21/09/2023
La Montagne	https://archive.ph/oCZmb	09/10/2023
Le Monde	https://archive.ph/pefZ7	16/11/2023
RFI	https://archive.ph/9I6ZG	24/11/2023
DGSI	https://archive.ph/vFEsk	02/02/2024
Figaro	https://archive.ph/0d6l3	08/03/2024
France 24	https://archive.ph/PdIVl	28/03/2024
France 24	https://archive.ph/1SW5K	11/04/2024
Figaro	https://archive.ph/MndmD	12/04/2024
RFI	https://archive.ph/rta16	15/04/2024
RFI	https://archive.ph/sVNOk	18/04/2024
RFI	https://archive.ph/WvAl3	19/04/2024
BFMTV	https://archive.ph/kTtES	08/05/2024
BFMTV	https://archive.ph/Wb5VG	08/05/2024
Ville de Paris	https://archive.ph/N2OzX	08/05/2024
Libération	https://archive.ph/biAIN	11/05/2024
BFMTV	https://archive.ph/NGyE8	13/05/2024

3.3 Exemples de diffusion des contenus de la campagne

Contenu	Chaîne *Telegram* de primo-diffusion	Date de diffusion	Comptes *seeder Matriochka* sur X	Date de diffusion
Reportage du *Spiegel* sur un gardien de but	https://archive.is/a0R2H	28/04/2024 à 19h01	https://archive.is/dkk0k	30/04/2024 à 12h30
Reportage de *BFM TV* sur l'Eurovision	https://archive.is/w6ejq	11/05/2024 à 10h07	https://archive.is/1GmF8	13/05/2024 à 12h39
Graffitis antisémites à Paris	https://archive.is/P2nMD	10/05/2024 à 15h37	https://archive.is/hAH62	15/05/2024 à 13h34

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 : flickr | www.CGPGrey.com ; photo coupée et passage en noir et blanc