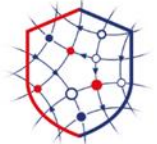




**RÉPUBLIQUE
FRANÇAISE**

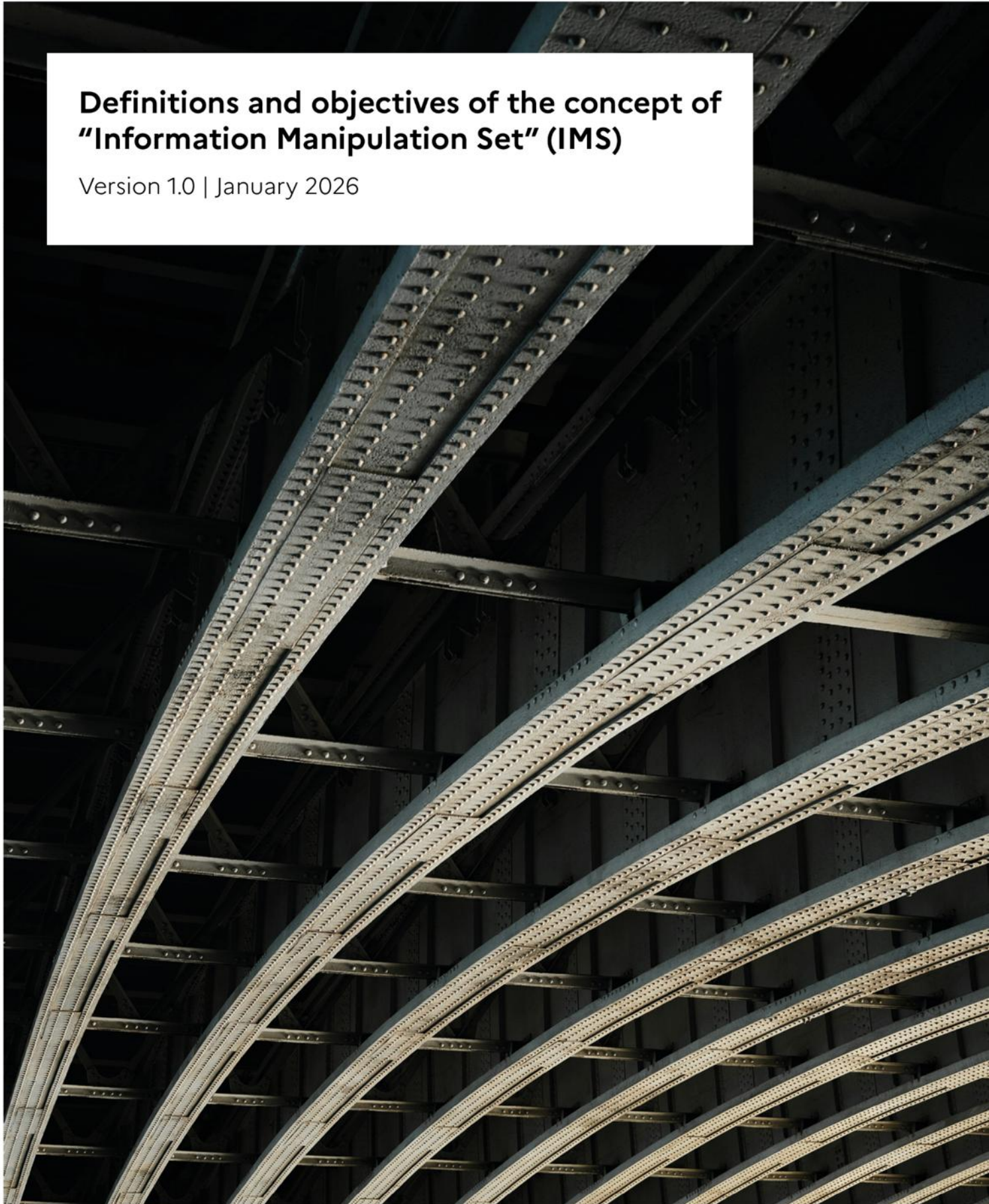
*Liberté
Égalité
Fraternité*



VIGINUM

Definitions and objectives of the concept of "Information Manipulation Set" (IMS)

Version 1.0 | January 2026



Summary

1. Introduction	3
2. Definitions	5
2.1 Levels of information manipulation	5
2.2 Definition of an "Information Manipulation Set"	5
2.3 Main features of the concept.....	6
3. Examples	8
3.1 <i>Spamouflage</i>	8
3.2 Covert activities linked to the <i>Baku Initiative Group</i>	8
3.3 <i>Storm-1516, CopyCop and Lakhta</i>	9
3.4 « <i>Team Jorge</i> »	11

1. INTRODUCTION

Over the past decade, the FIMI-Defender¹ community has become more organized, and its members (governmental entities, media, non-governmental organizations, etc.) have launched numerous initiatives to develop shared concepts for a better understanding, analysis, and description of digital information threat. While some of these concepts, such as "information operations" and "Tactics, Techniques & Procedures" (TTPs), are already well understood and exploited within the FIMI-Defender ecosystem, stakeholders continue to employ different terminology to describe the sets of technical,² behavioural,³ and contextual⁴ elements they monitor, even when similar sensors and analytical frameworks are in place.

The lack of a consistent terminology has complicated the understanding and description of information threats. For instance, malicious digital activities attributed to the Russian company "*Social Design Agency*"⁵ (SDA) are generally referred to under the name *Doppelgänger*. However, these activities have also been presented as an "operation," a "campaign," a "network," or a "Threat Actor."⁶ Sometimes, the name most commonly used by the community to describe these sets coincides with the name of the Threat Actor itself (e.g., *Lakhta*⁷), while other times, it only covers a small part of the entire set of elements related to a malicious actor (e.g., *Pravda*⁸), which tends to increase confusion.

Nevertheless, the community understands the need to name these sets, and has already popularized designations such as *Spamouflage*⁹ or *Matryoshka*.¹⁰ Based on concepts from the Cyber Threat Intelligence (CTI), some organizations are now proposing naming conventions that integrate the digital information threat.¹¹ To overcome these difficulties and potential confusion, VIGINUM proposes the concept of "**Information Manipulation Set**" (IMS). This concept offers the following key advantages:

- it provides a simple and appropriate designation focused on the technical, behavioural, and contextual elements identified and monitored by the community;
- it functions even if the attackers are unknown and it does not foreshadow their origin, intentions, or level of resources (human, financial, and technical);
- it is interoperable with established CTI concepts, standards, and tools already used within the FIMI-Defender community, such as the STIX format¹² and *OpenCTI*.

The concept of IMS was employed in three technical reports published by VIGINUM in 2025 and has

¹ Foreign Information Manipulation and Interference.

² IP addresses, Whois records, SSL certificates, browser fingerprints, etc.

³ Shares, identical content, social network account creation dates, etc.

⁴ Victimology, motivations of malicious activities, opportunities, etc.

⁵ Russian company conducting digital information operations on behalf of the Russian Presidential Administration. See <https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency>.

⁶ VIGINUM relies on the definition proposed in the STIX model documentation: "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.

⁷ *Lakhta* being both the name of a set of technical elements, and the name of the covert organisation behind these activities. See <https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes>.

⁸ *Pravda* being the name of a network of sites linked to *Portal Kombat*, which constitutes a larger and pre-existing set. See https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.

⁹ See <https://graphika.com/reports/spamouflage>.

¹⁰ See https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf.

¹¹ Such as *Microsoft*: <https://learn.microsoft.com/en-us/unified-secops/microsoft-threat-actor-naming>.

¹² See <https://oasis-open.github.io/cti-documentation/stix/intro.html>.

since been used by other organizations within the community, such as the European External Action Service (EEAS), the European Union Agency for Cybersecurity (ENISA)¹³ and the members of the Doppelgänger Working Group (DGWG).¹⁴

The present document precisely defines "Information Manipulation Set" and articulates its relationship with other concepts used by VIGINUM to describe FIMIs (see Section [2.1](#)). It aims to help the community identify IMSs among the monitored sets by detailing their main characteristics (Section [2.3](#)) and providing concrete examples of malicious activities. These examples encompass both attributed and unattributed activity, originating from a diverse range of actors across multiple regions of the world (Section [3](#)).

¹³ See https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

¹⁴ See https://www.disinfo.eu/wp-content/uploads/2026/01/20260115_building-a-common-operational-picture-of-FIMI_01.pdf.

2. DEFINITIONS

2.1 Levels of information manipulation

In order to understand the importance of the concept of IMS, it is essential to first clarify how malicious digital information activities are schematized. The concept of IMS draws on existing terms to provide a comprehensive view of the "levels" of digital information manipulation, ranging from visible online activities — such as a social network account disseminating a content — to the individuals behind them (e.g. operators and sponsors). This representation is based on military doctrine, which traditionally separates warfare into five levels or dimensions: political, strategic, operational, tactical, and technical.

In the context of digital information manipulation, these five levels correspond to:

- **Political:** actors or "sponsors" who decide to exploit digital information operations among a range of possible actions. This may refer to a State or any other type of actor, such as a private company, NGO, or influencer;
- **Strategic:** actors or "operators" who are commissioned, recruited, or funded to operationalise political objectives, where sponsors do not always possess the necessary in-house expertise;
- **Operational:** the information campaigns conducted by operators to fulfil strategic objectives translated into information objectives (e.g., promote, denigrate, polarize, or incite action in the physical realm);
- **Tactical:** the information operations conducted by the operators to fulfil operational objectives and implement campaigns into actions. For example, this could involve the publication of polarizing content by exploiting one or more digital assets;
- **Technical:** the digital assets controlled and exploited by the operators to fulfil tactical objectives. These infrastructures can be social network accounts, websites, email addresses, etc.

As is often characteristic of cyberattacks, the operators of malicious digital information activities are not always known. In such cases, defenders create dedicated sets ("*Matryoshka*," "*Spamouflage*," "*Doppelgänger*") that group the technical, behavioural, and contextual elements that are deemed attributable to a single malicious actor or group of actors. This level of abstraction is essential for analysing malicious digital activity within the fog of information operations and maintaining threat monitoring over time. VIGINUM defines this concept as "Information Manipulation Set."

2.2 Definition of an "Information Manipulation Set"

VIGINUM defines an Information Manipulation Set as a collection of adversarial behaviours, tools, and Tactics, Techniques, and Procedures (TTPs) presumed to be linked to the same Threat Actor or group of Threat Actors, which may be unknown. One or more IMSs can be technically attributed to a threat actor, and one or more campaigns can be attributed to an IMS. An IMS should not be confused with a Threat Actor, which may consist of a State, organization or individual. Finally, an IMS can be used to conduct information campaigns, which can be broken down into several information operations (or incidents).

Therefore, this concept bridges the gap between observed digital activities and their operators, whether they are identified or not. At the strategic level, it encompasses the set of means used to conduct information campaigns, serving as a tangible manifestation of the Threat Actor. According to this definition, a single Threat Actor can operate, or have operated, multiple IMSs.

The concept of IMS has been modelled after the concept of "Intrusion Set" used in Cyber Threat Intelligence (CTI¹⁵), which represents sets linked to cyberattacks. The following provides an initial example of integrating the concept of IMS, illustrated by malicious digital activities publicly attributed to *Doppelgänger*:¹⁶



2.3 Main features of the concept

The concept of IMS primarily serves to provide clarity. To help identify IMSs within the sets monitored by the FIMI-Defender community, VIGINUM proposes assessing them against **two core and cumulative criteria: clandestinity and coordination**. These two conditions are explained and illustrated with brief examples below. More in-depth case studies are provided in section 3 to better understand the nuances of the concept.

The first condition, "clandestinity," emphasizes the malicious intent of the operators. A set can only be considered an IMS if its **operators demonstrably make efforts to avoid attribution, i.e., the linking of digital assets to each other¹⁷ and to a Threat Actor.¹⁸** Clandestinity operates between the malicious actors and their digital assets, allowing for the exclusion of sets linked to actors operating under their own names and unattributed sets with different infrastructures sharing the same branding.

¹⁵ See <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-004.pdf>.

¹⁶ See https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf and <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>.

¹⁷ For example, by creating social media accounts and sites with different names, graphic charters, creation dates, avoiding interactions between them, registering and hosting sites via different services, etc.

¹⁸ For example, by omitting to display the affiliation of sites or social media accounts to the actor who actually controls them, by providing false contact information, by hosting sites on shared servers in a third country, by protecting them via anonymization services like *Cloudflare*, etc.

- **Example 1:** *Doppelgänger* operators made clear efforts to prevent the public — including the FIMI-Defender community — from linking their fake sites to each other or attributing them to the Russian company "Social Design Agency" and its sponsor, the Russian Presidential Administration. *Doppelgänger* therefore qualifies as an IMS, provided it also fulfils the second condition.
- **Example 2:** Digital activities of a government entity that rely on official channels — such as the X accounts of Russian diplomacy or content related to the "*Foundation to Battle Injustice*" (R-FBI)¹⁹ — clearly display their affiliation with these structures. Therefore, they cannot qualify as IMSs.
- **Example 3:** The pro-Russian English-language media outlet *The Islander* is not clearly attributed to a Threat Actor but coordinates a set of digital infrastructures, including X and *Substack* accounts. This fulfils the second condition. However, these infrastructures are clearly linked to each other.²⁰ Therefore, digital activities related to *The Islander* fail to qualify as an IMS.

The second condition emphasizes the degree of interaction between identified digital infrastructures: a set can be considered an IMS only **if the digital assets are employed in a coordinated manner and presumed to be operated by the same actor or group of actors working for the same sponsor**. This condition ensures the coherence of the technical elements, which must possess strong technical or behavioural links.

- **Example 1:** The digital assets linked to *Doppelgänger* form a homogeneous set because they are linked by strong, convergent technical and behavioural connections.²¹ *Doppelgänger* can therefore be considered an IMS provided it meets the first condition as well.
- **Example 2:** *TikTok* accounts that post the same content as other *TikTok* accounts, *YouTube* channels, or sites hosted on the same IP address are not necessarily operated by the same malicious actor. Therefore, they cannot qualify as an IMS.
- **Example 3:** *Storm-1679*²² and *Matryoshka*'s digital assets constitute two coherent sets that are sometimes grouped under the name *Overload*. However, as VIGINUM cannot establish a technical link between these activities at this time, it therefore maintains their classification as separate IMSs.²³ Nevertheless, these two IMSs may be merged should future technical evidence substantiate this hypothesis.

¹⁹ Fake NGO created by Yevgeny PRIGOZHIN in 2021 to document "human rights violations" in Western countries. See https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports.

²⁰ They have the same name, the same graphic charter, redirect directly to each other, etc.

²¹ Such as the dissemination chain, elements of source code, hosting, etc.

²² The activities documented by *Microsoft* under this designation only cover the publication of fake content by a group of *Telegram* channels presumed to be operated, or at least coordinated, by the same malicious actors. See <https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/>.

²³ See <https://checkfirst.network/operation-overload-an-ai-fuelled-escalation-of-the-kremlin-linked-propaganda-effort> and <https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes>.

3. EXAMPLES

3.1 Spamouflage

Widely documented by the FIMI-Defender community since 2019,²⁴ *Spamouflage* is a name that designates a set of technical, behavioural, and contextual elements that have been active since at least 2018. It is also known as *Dragonbridge*, *Storm-1376*, and *Taizi Flood*. *Spamouflage* is likely used to disseminate narratives favourable to the interests of the Chinese Communist Party (CCP) to an international audience and discredits CCP opponents, particularly during election periods, on platforms such as *X*, *Facebook*, *YouTube*, *Reddit*, and *TikTok*.



Examples of posts publicly associated to the IMS Spamouflage. Source: Institute for Strategic Dialogue

Based on publicly available information, VIGINUM classifies *Spamouflage* as an IMS characterised by the following elements:

- social media accounts that mask their links to each other and to their operators. This is probably to avoid moderation by the platforms and being associated with a Chinese government entity;
- social media accounts are used in a coordinated manner and are linked to each other by strong technical and behavioural connections, such as creation dates, pseudonyms, biographical elements, and number of followers. These accounts are presumed to be operated by the same malicious actor.

3.2 Covert activities linked to the Baku Initiative Group

Documented by VIGINUM, the *Baku Initiative Group* (BIG) is an NGO founded in Azerbaijan in July 2023.²⁵ Since its inception, the BIG has disseminated anti-French content under the guise of "fighting neocolonialism," exploiting economic and political situations in overseas territories, as well as independence movements and claims. The majority of BIG's digital activities, including its websites and social media accounts, are conducted in the organization's name. Therefore, BIG is considered as a Threat Actor. However, VIGINUM assesses that BIG operates a parallel Information Manipulation Set alongside its public-facing activities. To amplify its narratives, BIG has repeatedly relied on a set of social network accounts that:

²⁴ See <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/ and <https://edition.cnn.com/2023/11/13/us/china-online-disinformation-invs/index.html>.

²⁵ See https://www.sgdsn.gouv.fr/files/files/Publications/20241202_NP_SGDSN_VIGINUM_RAPPORT-BIG_ENG.pdf.

- attempted to hide — albeit with limited success — their connections to one another and to the Azerbaijani government. This is clearly done to maintain plausible deniability and simulate organic dissent;
- operated in a coordinated manner with strong technical and behavioural links (e.g., hashtags, messages, periods of activity, etc.), highly likely by the same group of Threat Actors.²⁶



Examples of posts designed to surreptitiously amplify BIG's narratives

Since at least 2022, VIGINUM has repeatedly observed IMSs associated with pre-existing Threat Actors. These IMSs enable actors to covertly support activities that strengthen plausible deniability, reach new audiences, or circumvent sanctions and technical restrictions. For example, Russian state-linked or state-affiliated media outlets, such as *RT*²⁷ and *Rybar*²⁸, have publicly been accused of conducting IMSs with this goal in mind.

3.3 Storm-1516, CopyCop and Lakhta

Storm-1516, also known as *Neva Flood*, is a set of technical, behavioural, and contextual elements that has been active since at least August 2023. It is responsible for over 150 information operations, primarily targeting Ukraine, Western countries, and post-Soviet countries, particularly during elections. *Storm-1516* is characterised by a complex dissemination chain that exploits its own digital infrastructures as well as those of relays financed by or linked to other IMSs. To date, VIGINUM estimates that the information operations attributed to *Storm-1516* have involved at least three clandestine and coordinated sets, each of which constitutes a distinct Information Manipulation Set.

- *Storm-1516* is attributed by the U.S. government to Russian military intelligence and to the *Centre of Geopolitical Expertise* (CGE), a Moscow-based think tank. It is likely employed to coordinate operations, create content and narratives, and register and maintain a limited number of digital infrastructures, such as *YouTube* channels and *X* accounts.

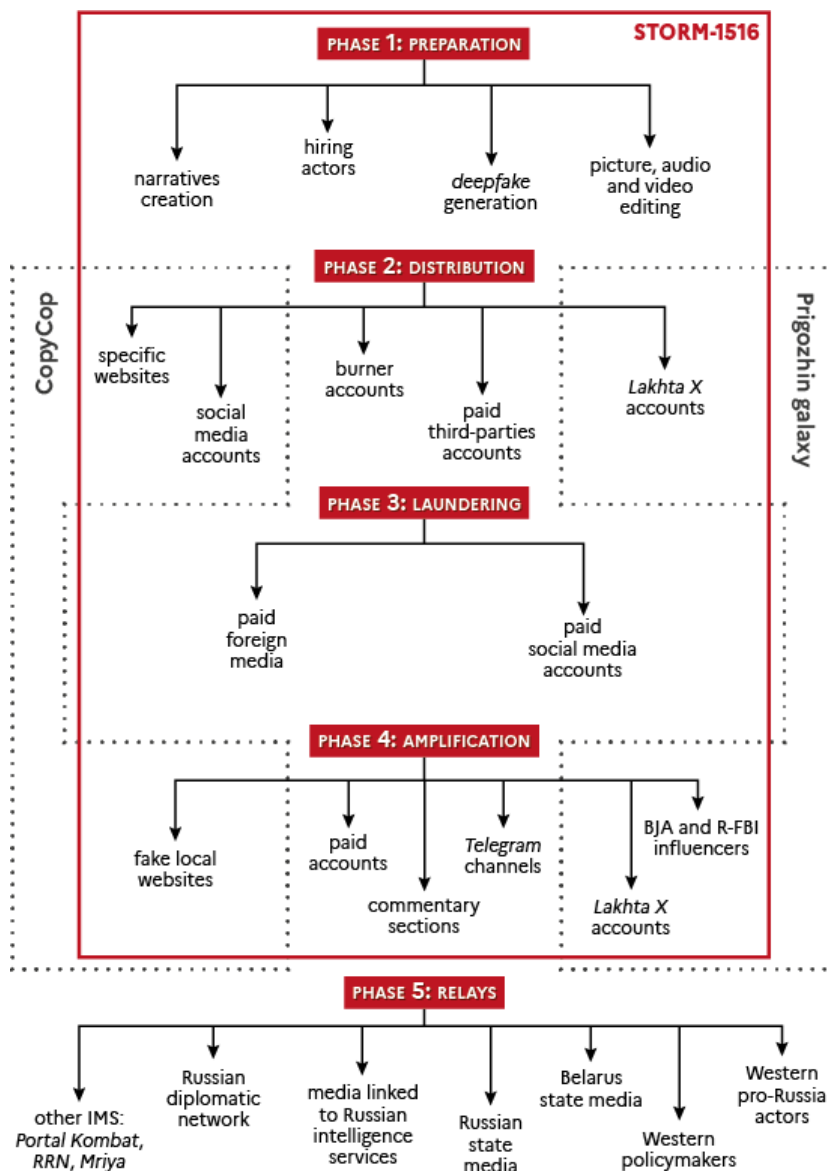
²⁶ See <https://www.sgdsn.gouv.fr/publications/nouvelle-caledonie-manoeuvres-informationnelles-impliquant-des-acteurs-0> and https://www.sgdsn.gouv.fr/files/files/Publications/20241202_NP_SGDSN_VIGINUM_RAPPORT-BIG.pdf.

²⁷ See <https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners>.

²⁸ See <https://dfrlab.org/2025/09/23/sanctioned-russian-actor-linked-to-new-media-outlet-targeting-moldova/>.

- CopyCop is attributed to John Mark DOUGAN, a former American police officer exiled in Russia since 2016. He is likely responsible for registering and maintaining fake websites exploited by Storm-1516 and other Russian and pro-Russian actors;
- Lakhta has not been formally attributed, but it is historically linked to the PRIGOZHIN galaxy. Lakhta participated in Storm-1516's operations by disseminating content via its digital assets (X accounts). Lakhta also relied on Storm-1516's digital assets for few of its own operations.²⁹

The concept of IMS is therefore essential for analysing interconnected sets, because it allows us to clearly define sets that are not linked by technical, behavioural, or contextual elements. This improves our understanding of the areas of responsibility and the structure of the various malicious actors involved, and enable us to monitor the evolution of each IMS more closely over time.



Sources: Clemson University, Gnida Project, Microsoft, U.S. Dept. of the Treasury, VIGINUM, Washington Post

Storm-1516 content dissemination chain, which partly relies on digital assets linked to CopyCop and Lakhta IMSs. Source: VIGINUM

²⁹ See <https://www.sgdsn.gov.fr/publications/analyse-du-mode-operatoire-informationnel-russe-storm-1516>.

3.4 « Team Jorge »

The *Story Killers* consortium of journalists³⁰ named "Team Jorge" an Israeli agency that has conducted information manipulation campaigns on behalf of various public and private clients since at least 2015, particularly during election processes. The agency has relied on a tool called "Advanced Impact Media Solutions" (AIMS) to create fake news articles and manage tens of thousands of inauthentic accounts on social networks, including on *Facebook*, *Twitter*, *Instagram*, *YouTube*, and *Reddit*.

Campaigns attributed to *Team Jorge* have likely promoted projects for various private clients, and have denounced initiatives and individuals, including sanctions against Russian oligarchs, the 2022 FIFA World Cup in Qatar, and Asian businessmen. Some digital information operations have also been combined with cyberattacks. VIGINUM considers that the Threat Actor "Team Jorge" has conducted an IMS on behalf of its clients because:

- the Threat Actor manifestly sought to conceal the links between its digital infrastructures and the agency to guarantee its clients' anonymity and avoid legal proceedings;
- digital assets directly controlled by the agency were used in a coordinated manner as they participated in specific campaigns, and presented strong technical and behavioural links (creation dates, following, subscriptions, etc.).



Screenshots of the tool AIMS employed by the agency. Source: Forbidden Stories

The concept of IMS is therefore applicable to any type of actor, including governmental entities, private structures, and agencies operating through shell companies. It can involve a group of malicious actors operating different parts of the IMS (defining narratives, deploying digital infrastructures, producing content) and can be made available to various clients or sponsors, regardless of their intentions.

³⁰ See <https://forbiddenstories.org/fr/story-killers>.

ABOUT VIGINUM



Created on 13 July 2021 and attached to the SGDSN (General Secretariat for Defence and National Security), VIGINUM is tasked with protecting France and its interests against foreign digital interference.

The role of this national technical and operational service is to detect and characterise information manipulation that involve foreign actors and aims at harming France and its fundamental interests

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

Cover photo credit: [Piermanuele Sberni](#) on [Unsplash](#).